

Lecture Notes on Network Information Theory

Abbas El Gamal
Department of Electrical Engineering
Stanford University

Young-Han Kim
Department of Electrical and Computer Engineering
University of California, San Diego

Table of Contents

Preface

1. Introduction

Part I. Background

- 2. Entropy, Mutual Information, and Typicality
- 3. Point-to-Point Communication

Part II. Single-hop Networks

- 4. Multiple Access Channels
- 5. Degraded Broadcast Channels
- 6. Interference Channels
- 7. Channels with State
- 8. Fading Channels
- 9. General Broadcast Channels
- 10. Gaussian Vector Channels
- 11. Distributed Lossless Source Coding
- 12. Source Coding with Side Information
- 13. Distributed Lossy Source Coding
- 14. Multiple Descriptions
- 15. Joint Source–Channel Coding

Part III. Multi-hop Networks

- 16. Noiseless Networks
- 17. Relay Channels
- 18. Interactive Communication
- 19. Discrete Memoryless Networks
- 20. Gaussian Networks
- 21. Source Coding over Noiseless Networks

Part IV. Extensions

- 22. Communication for Computing
- 23. Information Theoretic Secrecy
- 24. Information Theory and Networking

Appendices

- A. Convex Sets and Functions
- B. Probability and Estimation
- C. Cardinality Bounding Techniques
- D. Fourier–Motzkin Elimination
- E. Convex Optimization

Preface

This set of lecture notes is a much expanded version of lecture notes developed and used by the first author in courses at Stanford University from 1981 to 1984 and more recently beginning in 2002. The joint development of this set of lecture notes began in 2006 when the second author started teaching a course on network information theory at UCSD. Earlier versions of the lecture notes have also been used in courses at EPFL and UC Berkeley by the first author, at Seoul National University by the second author, and at the Chinese University of Hong Kong by Chandra Nair.

The development of the lectures notes involved contributions from many people, including Ekine Akuiyibo, Ehsan Ardestanizadeh, François Baccelli, Bernd Bandemer, Chiao-Yi Chen, Yeow-Khiang Chia, Sae-Young Chung, Paul Cuff, Michael Gastpar, John Gill, Amin Gohari, Robert Gray, Chan-Soo Hwang, Shirin Jalali, Tara Javidi, Yashodhan Kanoria, Gowtham Kumar, Amos Lapidoth, Olivier Lévêque, Sung Hoon Lim, Moshe Malkin, Mehdi Mohseni, James Mammen, Paolo Minero, Chandra Nair, Alon Orlitsky, Balaji Prabhakar, Haim Permuter, Anant Sahai, Anand Sarwate, Devavrat Shah, Shlomo Shamai (Shitz), Ofer Shayevitz, Yossi Steinberg, Han-I Su, Emre Telatar, David Tse, Alex Vardy, Lele Wang, Tsachy Weissman, Michele Wigger, Yu Xiang, Sina Zahedi, Ken Zeger, Lei Zhao, and Hao Zou. We would also like to acknowledge the feedback we received from the students who have taken our courses.

The authors are indebted to Tom Cover for his continual support and inspiration.

They also acknowledge partial support from the DARPA ITMANET and NSF.

Lecture Notes 1

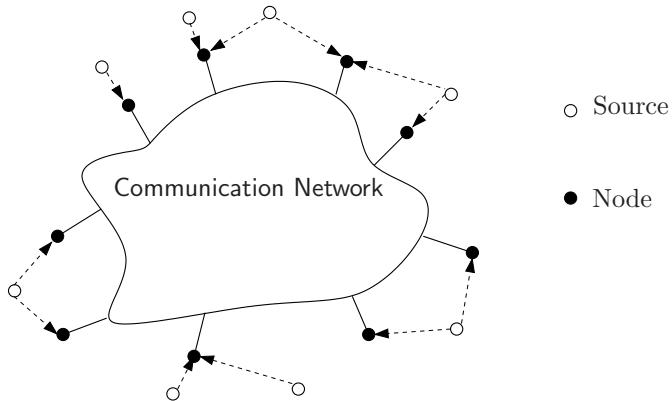
Introduction

- Network Information Flow
- Max-Flow Min-Cut Theorem
- Point-to-Point Information Theory
- Network Information Theory
- Outline of the Lecture Notes
- Dependency Graph
- Notation

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Network Information Flow

- Consider a general networked information processing system:

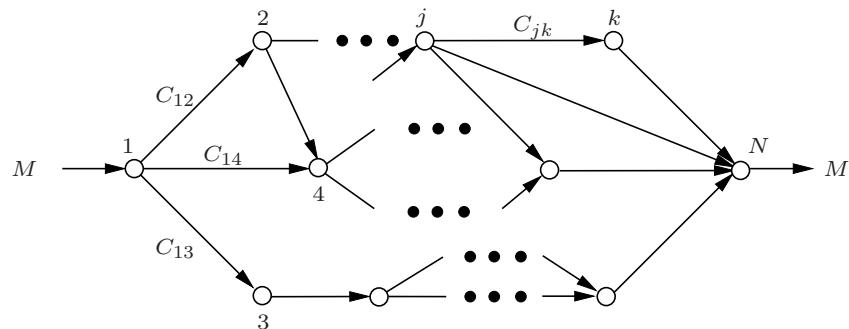


- The system may be the Internet, multiprocessor, data center, peer-to-peer network, sensor network, networked agents
- Sources may be data, speech, music, images, video, sensor data
- Nodes may be handsets, base stations, processors, servers, routers, sensor nodes
- The network may be wired, wireless, or a hybrid of the two

- Each node observes a subset of the sources and wishes to obtain descriptions of some or all the sources in the network, or to compute a function, make a decision, or perform an action based on these sources
- To achieve these goals, the nodes communicate over the network and perform local processing
- Information flow questions:
 - What are the *necessary and sufficient* conditions on information flow in the network under which the desired information processing goals can be achieved?
 - What are the optimal communication/computing techniques/protocols needed?
- Shannon answered these questions for point-point-communication
- Ford–Fulkerson [1] and Elias–Feinstein–Shannon [2] answered them for noiseless unicast networks

Max-Flow Min-Cut Theorem

- Consider a noiseless unicast network modeled by directed graph $(\mathcal{N}, \mathcal{E})$ with link capacities C_{jk} bits/transmission:



- Source node 1 wishes to send message M to destination node N
- What is the highest transmission rate from node 1 to node N (network capacity)?

- Max-flow min-cut theorem (Ford–Fulkerson, Elias–Feinstein–Shannon, 1956): Network capacity is

$$C = \min_{\mathcal{S} \subset \mathcal{N}, 1 \in \mathcal{S}, N \in \mathcal{S}^c} C(\mathcal{S}) \text{ bits/transmission,}$$

where

$$C(\mathcal{S}) = \sum_{j \in \mathcal{S}, k \in \mathcal{S}^c} C_{jk}$$

is capacity of the *cut* \mathcal{S}

- Capacity is achieved error free and using simple forwarding (routing)

Point-to-Point Information Theory

- Shannon provided a complete theory for point-to-point communication [3, 4].
- He put forth a model for a communication system
- He introduced a probabilistic approach to defining information sources and communication channels
- He established four fundamental theorems:
 - Channel coding theorem: The *capacity* $C = \max_{p(x)} I(X; Y)$ of the discrete memoryless channel $p(y|x)$ is the maximum rate at which data can be transmitted reliably
 - Lossless source coding theorem: The *entropy* $H(X)$ of a discrete memoryless source $X \sim p(x)$ is the minimum rate at which the source can be compressed (described) losslessly
 - Lossy source coding theorem: The *rate-distortion* function $R(D) = \min_{p(\hat{x}|x): E(d(x, \hat{x})) \leq D} I(X; \hat{X})$ for the source $X \sim p(x)$ and distortion measure $d(x, \hat{x})$ is the minimum rate at which the source can be compressed (described) within distortion D

- Separation theorem: To send a discrete memoryless source over a discrete memoryless channel, it suffices to perform source coding and channel coding separately. Thus, a standard binary interface between the source and the channel can be used without any loss in performance
- Until recently, these results were considered (by most) an esoteric theory with no apparent relation to the “real world”
- With advances in technology (signal processing, algorithms, hardware, software), practical data compression, modulation, and error correction techniques that approach the Shannon limits have been developed and are widely used in communication and multimedia applications

Network Information Theory

- The simplistic model of a network as consisting of separate links and naive forwarding nodes, however, does not capture many important aspects of real world networked systems:
 - Real world networks involve multiple sources with various messaging requirements, e.g., multicasting, multiple unicast, etc.
 - Real world information sources have redundancies, time and space correlations, and time variations
 - Real world wireless networks suffer from interference, node failure, delay, and time variation
 - The wireless medium is inherently a shared, broadcast medium, naturally allowing for multicasting, but creating complex tradeoffs between competition for resources (bandwidth, energy) and cooperation for the common good
 - Real world communication nodes allow for more complex node operations than forwarding
 - The goal in many information processing systems is not to merely communicate source information, but to make a decision, compute a function, or coordinate an action

- Network information theory aims to answer the fundamental information flow questions while capturing some of these aspects of real-world networks by studying network models with:
 - Multiple sources and destinations
 - Multi-accessing
 - Broadcasting
 - Interference
 - Relaying
 - Interactive communication
 - Distributed coding and computing
- The first paper on network information theory was (again) by Shannon, titled "two-way communication channels" [5]
 - He didn't find the optimal rates
 - Problem remains open

- Significant research activities occurred in the 70s and early 80s with many new results and techniques, but
 - Many basic problems remain open
 - Little interest from the information theory community and absolutely no interest from communication practitioners
- Wireless communications and the Internet (and advances in technology) have revived interest in this area since the mid 90s
 - Lots of research is going on
 - Some work on old open problems but many new models and problems as well

State of the Theory

- Most work has been on compression and communication
- Most work assumes *discrete memoryless* (DM) or *Gaussian* source and channel models
- Most results are for separate source–channel settings, where the goal is to establish a coding theorem that determines the set of *achievable rate tuples*, i.e.,
 - the capacity region when sending independent *messages* over a noisy channel, or
 - the optimal rate/rate-distortion region when sending source descriptions over a noiseless channel
- Computable characterizations of capacity/optimal rate regions are known only for few settings. For most other settings, inner and outer bounds are known
- There are some results on joint source–channel coding and on applications such as communication for computing, secrecy, and models involving random data arrivals and asynchronous communication

- Several of the coding techniques developed, such as superposition coding, successive cancellation decoding, Slepian–Wolf coding, Wyner–Ziv coding, successive refinement, writing on dirty paper, network coding, decode–forward, and compress–forward are beginning to have an impact on real world networks

About the Lecture Notes

- The lecture notes aim to provide a broad coverage of key results, techniques, and open problems in network information theory:
 - We attempt to organize the field in a “top-down” manner
 - The organization balances the introduction of new techniques and new models
 - We discuss extensions (if any) to many users and large networks throughout
 - We unify, simplify, and formalize the achievability proofs
 - The proofs use elementary tools and techniques
 - We attempt to use clean and unified notation and terminology
- We neither aim to be comprehensive, nor claim to have captured all important results in the field. The explosion in the number of papers on the subject in recent years makes it almost impossible to provide a complete coverage of the field

Outline of the Lecture Notes

Part I. Background (Lectures 2,3): We review basic information measures, typicality, Shannon’s point-to-point communication theorems. We also introduce key lemmas that will be used throughout

Part II. Single-hop networks (Lectures 4–15): We study networks with single-round, one-way communication. The material is grouped into:

- Sending independent (maximally compressed) messages over noisy channels
- Sending (uncompressed) correlated sources over noiseless networks
- Sending correlated sources over noisy channels

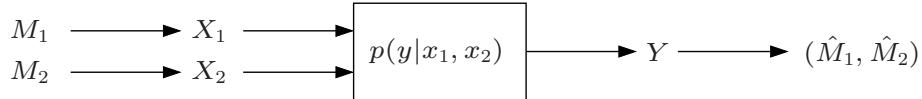
Part III. Multi-hop networks (Lectures 16–21): We study networks with relaying and multiple communication rounds. The material is grouped into:

- Sending independent messages over noiseless networks
- Sending independent messages into noisy networks
- Sending correlated sources over noiseless networks

Part IV. Extensions (Lectures 22–24): We present extensions of the theory to distributed computing, secrecy, and asynchronous communication

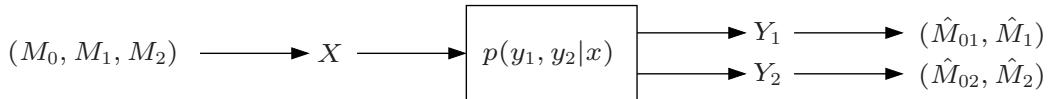
II. Single-hop Networks: Messages over Noisy Channels

- Lecture 4: Multiple access channels:



Problem solved; successive cancellation; time sharing

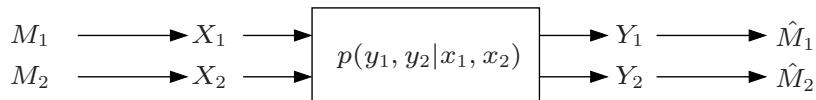
- Lecture 5: Degraded broadcast channels:



Problem solved; superposition coding

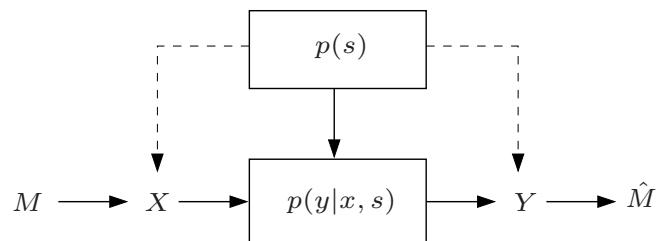
II. Single-hop Networks: Messages over Noisy Channels

- Lecture 6: Interference channels:



Problem open in general; strong interference; weak interference;
Han–Kobayashi rate region; deterministic approximations

- Lecture 7: Channels with state:



Shannon strategy; Gelfand–Pinsker; multicoding; writing on dirty paper

II. Single-hop Networks: Messages over Noisy Channels

- Lecture 8: Fading channels:

Water-filling; broadcast strategy; adaptive coding; outage capacity

- Lecture 9: General broadcast channels:

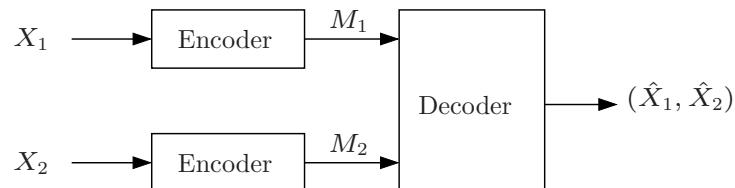
Problem open; Marton coding; mutual covering

- Lecture 10: Gaussian vector (MIMO) channels:

Vector writing-on-dirty-paper coding; MAC–BC duality; convex optimization

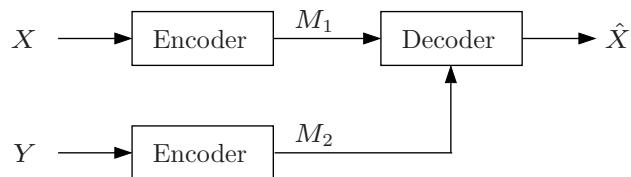
II. Single-hop Networks: Sources over Noiseless Channels

- Lecture 11: Distributed lossless source coding:



Problem solved; Slepian–Wolf; Cover's random binning;
lossless source coding with helper

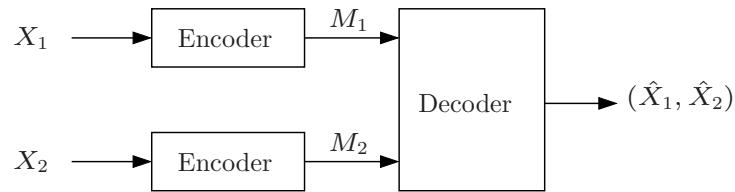
- Lecture 12: Source coding with side information:



Problem mostly solved; Wyner–Ziv; deterministic binning; Markov lemma

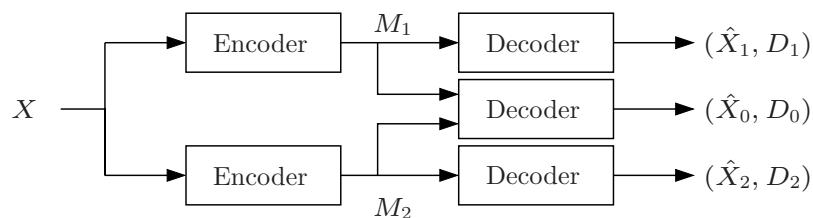
II. Single-hop Networks: Sources over Noiseless Channels

- Lecture 13: Distributed lossy source coding:



Problem open in general; Berger–Tung; Markov lemma;
optimal for quadratic Gaussian

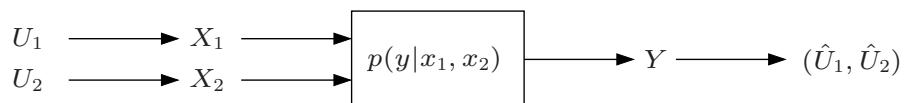
- Lecture 14: Multiple descriptions:



Problem open in general; multivariate mutual covering;
successive refinement

II. Single-hop Networks: Sources over Noisy Channels

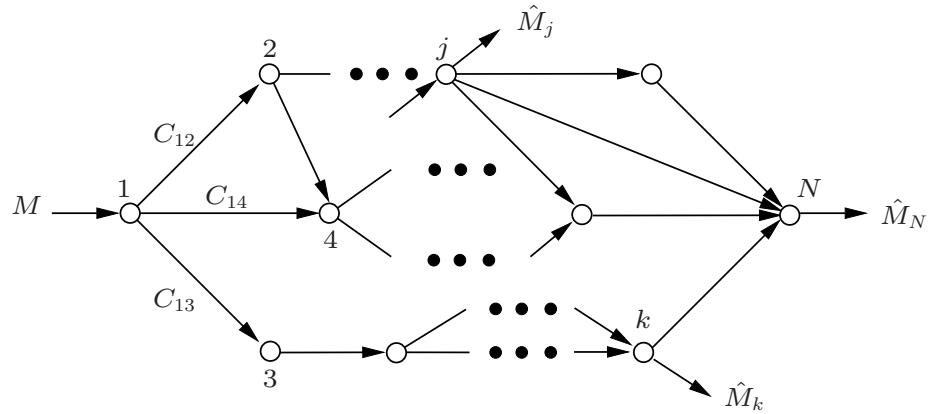
- Lecture 15: Joint source–channel coding:



Separation theorem does not hold in general; common information

III. Multi-hop networks: Messages over Noiseless Networks

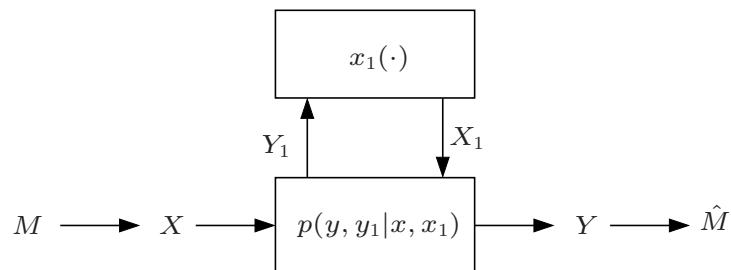
- Lecture 16: Noiseless networks:



Max-flow min-cut; network coding; multi-commodity flow

III. Multi-hop Networks: Messages over Noisy Networks

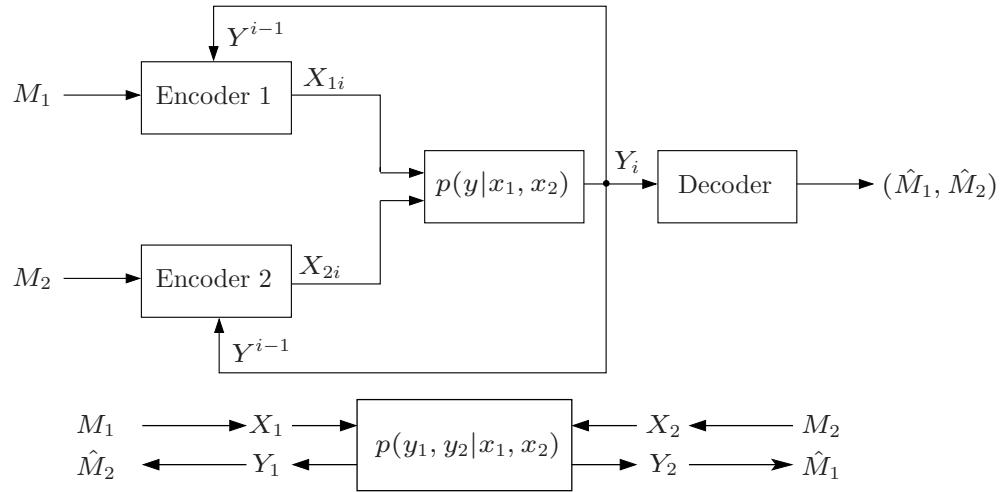
- Lecture 17: Relay channels:



Problem open in general; cutset bound; decode-forward;
compress-forward; amplify-forward

III. Multi-hop Networks: Messages over Noisy Networks

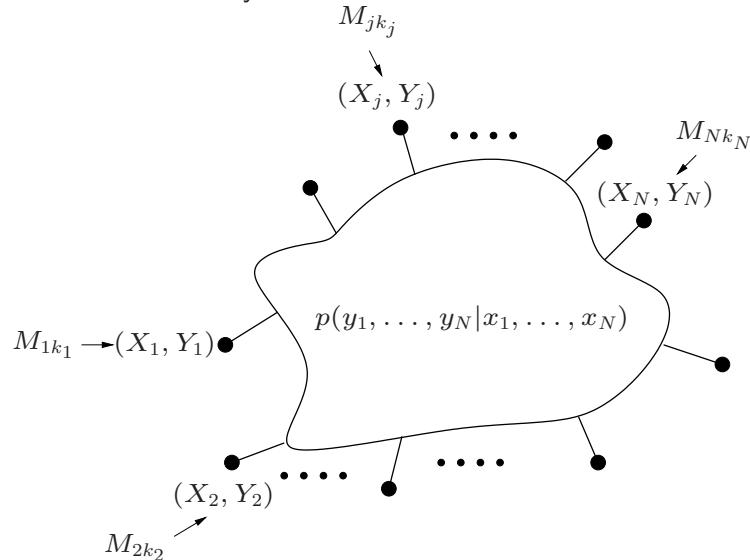
- Lecture 18: Interactive communication:



Feedback can increase capacity of multiple user channels;
iterative refinement (Schalkwijk–Kailath, Horstein); two-way channel (open)

III. Multi-hop Networks: Messages over Noisy Networks

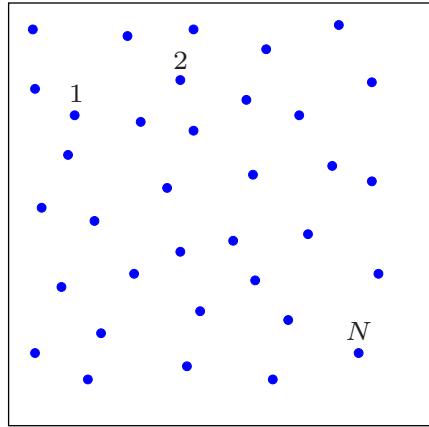
- Lecture 19: Discrete memoryless networks:



Cutset outer bound; network decode-forward; noisy network coding

III. Multi-hop Networks

- Lecture 20: Gaussian networks:



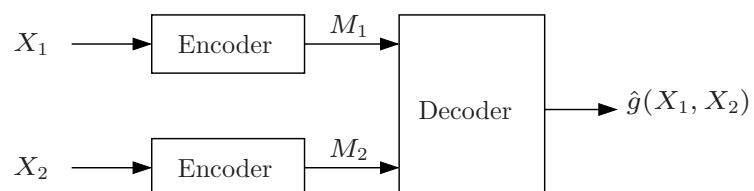
Gupta–Kumar random network model; scaling laws

- Lecture 21: Source coding over noiseless networks:

Multiple descriptions network; CFO; interactive source coding

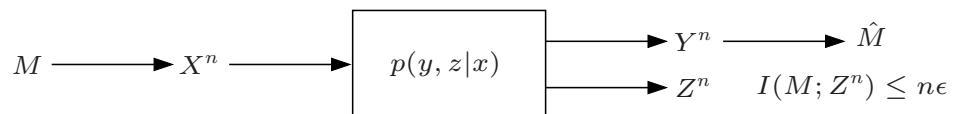
IV. Extensions

- Lecture 22: Communication for computing:



Orlitsky–Roche; μ -sum problem; distributed consensus

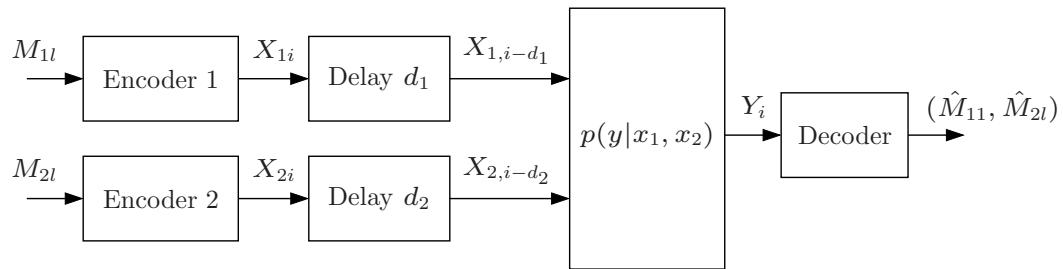
- Lecture 23: Information theoretic secrecy:



Wiretap channel; key generation from common randomness

IV. Extensions

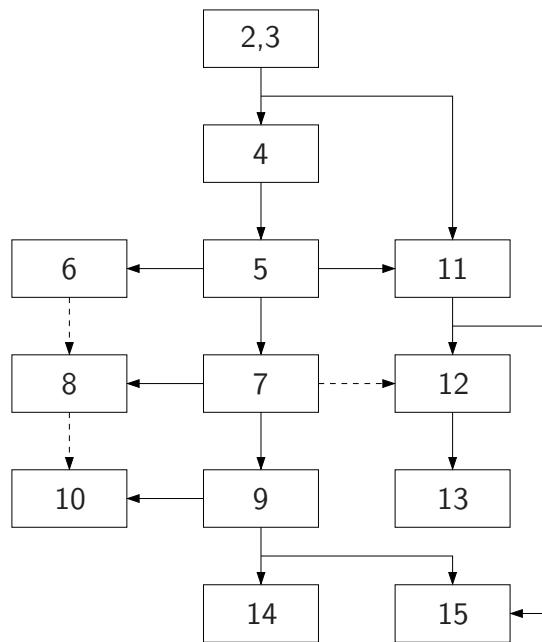
- Lecture 24: Information theory and networking:



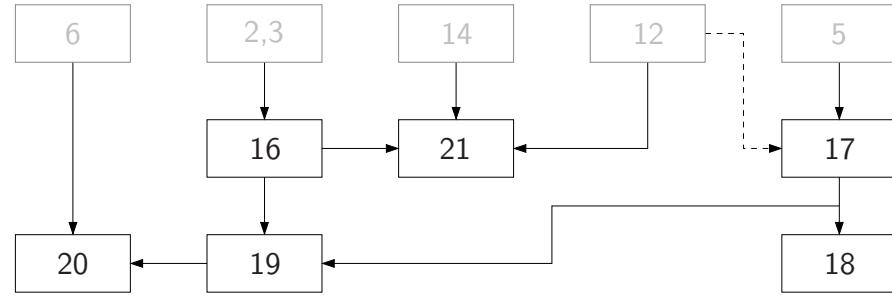
Asynchronous MAC; random arrivals; random access

Dependency Graph

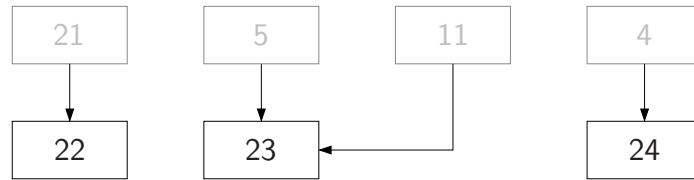
- Part II: Single-hop networks (solid: required / dashed: recommended)



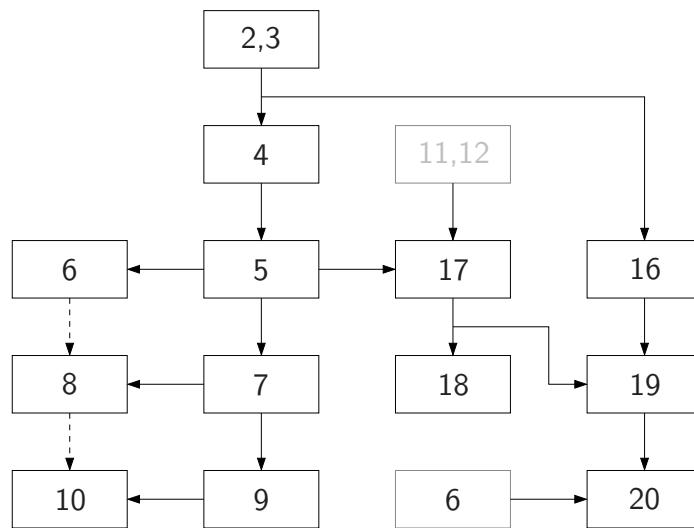
- Part III: Multi-hop networks



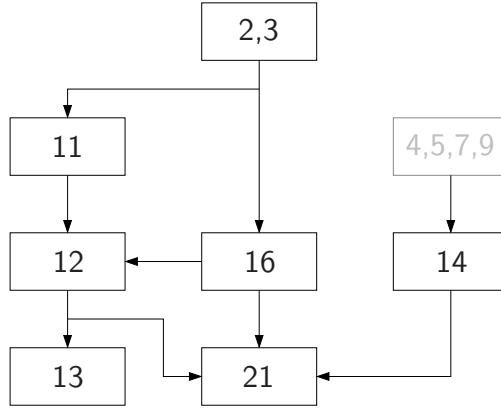
- Part IV: Extensions



- Channel coding



- Source coding



Notation: Sets, Scalars, and Vectors

- For constants and values of random variables, we use lower case letters x, y, \dots
- For $1 \leq i \leq j$, $x_i^j := (x_i, x_{i+1}, \dots, x_j)$ denotes an $(j - i + 1)$ -sequence/vector
For $i = 1$, we always drop the subscript and use $x^j := (x_1, x_2, \dots, x_j)$
- Lower case $\mathbf{x}, \mathbf{y}, \dots$ also refer to values of random (column) vectors with specified dimensions. $\mathbf{1} = (1, \dots, 1)$ denotes a vector of all ones
- x_j is the j -th component of \mathbf{x}
- $\mathbf{x}(i)$ is a vector indexed by time i , $x_j(i)$ is the j -th component of $\mathbf{x}(i)$
- $\mathbf{x}^n = (\mathbf{x}(1), \mathbf{x}(2), \dots, \mathbf{x}(n))$
- Let $\alpha, \beta \in [0, 1]$. Define $\bar{\alpha} := (1 - \alpha)$ 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 mod 2 sum of the two vectors
- Script letters $\mathcal{X}, \mathcal{Y}, \dots$ refer exclusively to finite sets
 $|\mathcal{X}|$ is the cardinality of the finite set \mathcal{X}

- \mathbb{R}^d is the d -dimensional real Euclidean space
- \mathbb{C}^d is the d -dimensional complex Euclidean space
- \mathbb{F}_q^d is the d -dimensional base- q finite field
- Script letters $\mathcal{C}, \mathcal{R}, \mathcal{P}, \dots$ refer to subsets of \mathbb{R}^d or \mathbb{C}^d
- For integers $i \leq j$, we define $[i : j] := \{i, i+1, \dots, j\}$
- We also define for $a \geq 0$ and integer $i \leq 2^a$
 - $[i : 2^a] := \{i, i+1, \dots, 2^{\lfloor a \rfloor}\}$, where $\lfloor a \rfloor$ is the integer part of a
 - $[i : 2^a] := \{i, i+1, \dots, 2^{\lceil a \rceil}\}$, where $\lceil a \rceil$ is the smallest integer $\geq a$

Probability and Random Variables

- $P(\mathcal{A})$ denotes the probability of an event \mathcal{A}
 $P(\mathcal{A}|\mathcal{B})$ is the conditional probability of \mathcal{A} given \mathcal{B}
- We use upper case letters X, Y, \dots to denote random variables. The random variables may take values from finite sets $\mathcal{X}, \mathcal{Y}, \dots$, from the real line \mathbb{R} , or from the complex plane \mathbb{C} . By convention, $X = \emptyset$ means that X is a degenerate random variable (unspecified constant) regardless of its support
- $P\{X \in \mathcal{A}\}$ is the probability of the event $\{X \in \mathcal{A}\}$
- For $1 \leq i \leq j$, $X_i^j := (X_i, X_{i+1}, \dots, X_j)$ denotes an $(j-i+1)$ -sequence/vector of random variables
For $i=1$, we always drop the subscript and use $X^j := (X_1, X_2, \dots, X_j)$
- Let $(X_1, X_2, \dots, X_k) \sim p(x_1, x_2, \dots, x_k)$ and $\mathcal{J} \subseteq [1 : k]$. Define the subset of random variables $X(\mathcal{J}) := \{X_j : j \in \mathcal{J}\}$
 $X^n(\mathcal{J}) := (X_1(\mathcal{J}), X_2(\mathcal{J}), \dots, X_n(\mathcal{J}))$
- Upper case $\mathbf{X}, \mathbf{Y}, \dots$ refer to random (column) vectors with specified dimensions

- X_j is the j -th component of \mathbf{X}
- $\mathbf{X}(i)$ is a random vector indexed by time i , $X_j(i)$ is the j -th component of $\mathbf{X}(i)$
- $\mathbf{X}^n = (\mathbf{X}(1), \mathbf{X}(2), \dots, \mathbf{X}(n))$
- $\{X_i\} := \{X_1, X_2, \dots\}$ refers to a discrete-time random process (or sequence)
- $X^n \sim p(x^n)$: Probability mass function (pmf) of the 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., $p_{X^n}(\tilde{x}^n) := P\{X^n = \tilde{x}^n\}$ for all $\tilde{x}^n \in \mathcal{X}^n$. The function $p(x^n)$ without subscript is understood as the pmf of the random vector X^n defined on $\mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_n$
- $X^n \sim f(x^n)$: Probability density function (pdf) of X^n
- $X^n \sim F(x^n)$: Cumulative distribution function (cdf) of X^n
- $(X^n, Y^n) \sim p(x^n, y^n)$: Joint pmf of X^n and Y^n
- $Y^n | \{X^n \in \mathcal{A}\} \sim p(y^n | X^n \in \mathcal{A})$ is the pmf of Y^n conditioned on $\{X^n \in \mathcal{A}\}$
- $Y^n | \{X^n = x^n\} \sim p(y^n | x^n)$: Conditional pmf of Y^n given $\{X^n = x^n\}$
- $p(y^n | x^n)$: 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 distributions

- $X \rightarrow Y \rightarrow Z$ form a Markov chain if $p(x, y, z) = p(x)p(y|x)p(z|y)$
 $X_1 \rightarrow X_2 \rightarrow X_3 \rightarrow \dots$ form a Markov chain if $p(x_i | x^{i-1}) = p(x_i | x_{i-1})$ for $i = 2, 3, \dots$
- $E_X(g(X))$, or $E(g(X))$ in short, denotes the expected value of $g(X)$
 $E(X|Y)$ denotes the conditional expectation of X given Y
- $\text{Var}(X) = E[(X - E(X))^2]$ denotes the variance of X
 $\text{Var}(X|Y) = E[(X - E(X|Y))^2 | Y]$ denotes the conditional variance of X given Y
- For random vectors $\mathbf{X} = X^n$ and $\mathbf{Y} = Y^k$:
 - $K_{\mathbf{X}} = E((\mathbf{X} - E\mathbf{X})(\mathbf{X} - E\mathbf{X})^T)$: Covariance matrix of \mathbf{X}
 - $K_{\mathbf{XY}} = E((\mathbf{X} - E\mathbf{X})(\mathbf{Y} - E\mathbf{Y})^T)$: Cross covariance matrix of (\mathbf{X}, \mathbf{Y})
 - $K_{\mathbf{X}|\mathbf{Y}} = E\left((\mathbf{X} - E(\mathbf{X}|\mathbf{Y}))(\mathbf{X} - E(\mathbf{X}|\mathbf{Y}))^T\right) = K_{\mathbf{X}-E(\mathbf{X}|\mathbf{Y})}$: Covariance matrix of the minimum mean square error (MMSE) for estimating \mathbf{X} given \mathbf{Y}

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

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

- $X \sim \text{Binom}(n, p)$: X is a binomial random variable with parameters $n \geq 1$ and $p \in [0, 1]$, i.e., $p_X(k) = \binom{n}{k} p^k (1-p)^{n-k}$ for $k \in [0 : n]$
- $X \sim \text{Unif}[i : j]$ for integers $j > i$: X is a discrete uniform random variable
- $X \sim \text{Unif}[a, b]$ for $b > a$: X is a continuous uniform random variable
- $X \sim \mathcal{N}(\mu, \sigma^2)$: X is a Gaussian random variable with mean μ and variance σ^2

$$Q(x) := \mathbb{P}\{X > x\}, x \in \mathbb{R}, \text{ where } X \sim \mathcal{N}(0, 1)$$
- $X^n \sim \mathcal{N}(\boldsymbol{\mu}, K)$: X^n is a Gaussian random vector with mean vector $\boldsymbol{\mu}$ and covariance matrix K

- $\{X_i\}$ is a $\text{Bern}(p)$ process means that X_1, X_2, \dots is a sequence of i.i.d. $\text{Bern}(p)$ random variables
- $\{X_i, Y_i\}$ is a DSBS(p) process means that $(X_1, Y_1), (X_2, Y_2), \dots$ is a sequence of i.i.d. pairs of binary random variables such that $X_1 \sim \text{Bern}(1/2)$, $Y_1 = X_1 \oplus Z_1$, where $\{Z_i\}$ is a $\text{Bern}(p)$ process independent of $\{X_i\}$ (or equivalently, $Y_1 \sim \text{Bern}(1/2)$, $X_1 = Y_1 \oplus Z_1$, and $\{Z_i\}$ is independent of $\{Y_i\}$)
- $\{X_i\}$ is a WGN(P) process means that X_1, X_2, \dots is a sequence of i.i.d. $\mathcal{N}(0, P)$ random variables
- $\{X_i, Y_i\}$ is a 2-WGN(P, ρ) process means that $(X_1, Y_1), (X_2, Y_2), \dots$ is a sequence of i.i.d. pairs of jointly Gaussian random variables such that $E(X_1) = E(Y_1) = 0$, $E(X_1^2) = E(Y_1^2) = P$, and the correlation coefficient between X_1 and Y_1 is ρ
- In general $\{\mathbf{X}(i)\}$ is a r -dimensional vector WGN(K) process means that $\mathbf{X}(1), \mathbf{X}(2), \dots$ is a sequence of i.i.d. Gaussian random vectors with zero mean and covariance matrix K

Common Functions

- \log is base 2, unless specified otherwise
- $C(x) := \frac{1}{2} \log(1 + x)$ for $x \geq 0$
- $R(x) := (1/2) \log(x)$ for $x \geq 1$, and 0, otherwise

$\epsilon-\delta$ Notation

- Throughout ϵ, ϵ' are nonnegative constants and $\epsilon' < \epsilon$
- We often use $\delta(\epsilon) > 0$ to denote a function of ϵ such that $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$
- When there are multiple functions $\delta_1(\epsilon), \delta_2(\epsilon), \dots, \delta_k(\epsilon) \rightarrow 0$, we denote them all by a generic $\delta(\epsilon) \rightarrow 0$ with the implicit understanding that $\delta(\epsilon) = \max\{\delta_1(\epsilon), \dots, \delta_k(\epsilon)\}$
- Similarly, ϵ_n denotes a generic sequence of nonnegative numbers that approaches zero as $n \rightarrow \infty$
- We say $a_n \doteq 2^{nb}$ for some constant b if there exists $\delta(\epsilon)$ such that $2^{n(b-\delta(\epsilon))} \leq a_n \leq 2^{n(b+\delta(\epsilon))}$

Matrices

- For matrices we use upper case $A, B, G \dots$
- $|A|$ is the determinant of the matrix A
- $\text{diag}(a_1, a_2, \dots, a_d)$ is a $d \times d$ diagonal matrix with diagonal elements a_1, a_2, \dots, a_d
- I_d is the $d \times d$ identity matrix. The subscript d is omitted when it is clear from the context
- For a symmetric matrix A , $A \succ 0$ means that A is positive definite, i.e., $\mathbf{x}^T A \mathbf{x} > 0$ for all $\mathbf{x} \neq 0$; $A \succeq 0$ means that A is positive semidefinite, i.e., $\mathbf{x}^T A \mathbf{x} \geq 0$ for all x
For symmetric matrices A and B of 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 as $G = \Phi \Gamma \Psi^T$, 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 $\Gamma = \text{diag}(\gamma_1, \dots, \gamma_d)$ 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 the symmetric square root of K as $K^{1/2} = \Phi \Lambda^{1/2} \Phi^T$, where $\Lambda^{1/2}$ is a diagonal matrix with diagonal elements $\sqrt{\lambda_i}$. 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 $K \succ 0$ as the symmetric square root of K^{-1}

Order Notation

- $g_1(N) = o(g_2(N))$ means that $g_1(N)/g_2(N) \rightarrow 0$ as $N \rightarrow \infty$
- $g_1(N) = O(g_2(N))$ means that there exist a constant a and integer n_0 such that $g_1(N) \leq ag_2(N)$ 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 $g_2(N) = O(g_1(N))$

References

- [1] L. R. Ford, Jr. and D. R. Fulkerson, “Maximal flow through a network,” *Canad. J. Math.*, vol. 8, pp. 399–404, 1956.
- [2] P. Elias, A. Feinstein, and C. E. Shannon, “A note on the maximum flow through a network,” *IRE Trans. Inf. Theory*, vol. 2, no. 4, pp. 117–119, Dec. 1956.
- [3] C. E. Shannon, “A mathematical theory of communication,” *Bell System Tech. J.*, vol. 27, pp. 379–423, 623–656, 1948.
- [4] ———, “Coding theorems for a discrete source with a fidelity criterion,” in *IRE Int. Conv. Rec., part 4*, 1959, vol. 7, pp. 142–163, reprinted with changes in *Information and Decision Processes*, R. E. Machol, Ed. New York: McGraw-Hill, 1960, pp. 93–126.
- [5] ———, “Two-way communication channels,” in *Proc. 4th Berkeley Sympos. Math. Statist. Prob.* Berkeley, Calif.: Univ. California Press, 1961, vol. I, pp. 611–644.

Part I. Background

Lecture Notes 2

Entropy, Mutual Information, and Typicality

- Entropy
- Differential Entropy
- Mutual Information
- Typical Sequences
- Jointly Typical Sequences
- Multivariate Typical Sequences
- Appendix: Weak Typicality
- Appendix: Proof of Lower Bound on Typical Set Cardinality

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Entropy

- Entropy of a discrete random variable $X \sim p(x)$:

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

- $H(X)$ is nonnegative and concave function of $p(x)$

- $H(X) \leq \log |\mathcal{X}|$

This (as well as many other information theoretic inequalities) follows by Jensen's inequality

- Binary entropy function: For $p \in [0, 1]$

$$H(p) := -p \log p - (1-p) \log(1-p),$$

$$H(0) = H(1) = 0$$

Throughout we use $0 \cdot \log 0 = 0$ by convention (recall $\lim_{x \rightarrow 0} x \log x = 0$)

- Conditional entropy: Let $X \sim F(x)$ and $Y|X=x$ be discrete for every x , then

$$H(Y|X) := -\mathbb{E}_{X,Y}(\log p(Y|X))$$

◦ $H(Y|X) \leq H(Y)$. Note that equality holds if X and Y are independent

- Joint entropy for random variables $(X, Y) \sim p(x, y)$ is

$$\begin{aligned} H(X, Y) &:= -\mathbb{E}(\log p(X, Y)) \\ &= -\mathbb{E}(\log p(X)) - \mathbb{E}(\log p(Y|X)) = H(X) + H(Y|X) \\ &= -\mathbb{E}(\log p(Y)) - \mathbb{E}(\log p(X|Y)) = H(Y) + H(X|Y) \end{aligned}$$

◦ $H(X, Y) \leq H(X) + H(Y)$, with equality iff X and Y are independent

- *Chain rule for entropy*: Let X^n be a discrete random vector. Then

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

◦ $H(X^n) \leq \sum_{i=1}^n H(X_i)$ with equality iff X_1, X_2, \dots, X_n are independent

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

$$H(g(X)) \leq H(X)$$

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

- *Fano's inequality*: If $(X, Y) \sim p(x, y)$ for $X, Y \in \mathcal{X}$ and $P_e := \mathbb{P}\{X \neq Y\}$, then

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

- *Mrs. Gerber's Lemma (MGL)* [1]: Let $H^{-1} : [0, 1] \rightarrow [0, 1/2]$ be the inverse of the binary entropy function, that is, $H(H^{-1}(u)) = u$

◦ *Scalar MGL*: Let X be a binary-valued 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

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

The proof follows by the convexity of the function $H(H^{-1}(u) * p)$ in u

◦ *Vector MGL*: Let X^n be a binary-valued random vectors and let U be an arbitrary random variable. If Z^n is i.i.d. $\text{Bern}(p)$ random variables

independent of (X^n, U) and $Y^n = X^n \oplus Z^n$, then

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

The proof follows using the scalar Mrs. Gerber's lemma and by induction

- Extensions of Mrs. Gerber's lemmas are given in [2, 3, 4]
- *Entropy rate:* Let $X = \{X_i\}$ be a stationary random process with X_i taking values in a finite alphabet \mathcal{X} . The entropy rate of the process X is defined as

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

Differential Entropy

- Differential entropy for continuous random variable $X \sim f(x)$ (pdf):

$$h(X) := - \int f(x) \log f(x) dx = - \mathbb{E}_X(\log f(X))$$

- $h(X)$ is concave function of $f(x)$ (but not necessarily nonnegative)
- Translation: For any constant a , $h(X + a) = h(X)$
- Scaling: For any constant a , $h(aX) = h(X) + \log |a|$

- Conditional differential entropy: Let $X \sim F(x)$ and $Y|X=x \sim f(y|x)$. Define conditional differential entropy as $h(Y|X) := - \mathbb{E}_{X,Y}(\log f(Y|X))$

- $h(Y|X) \leq h(Y)$

- If $X \sim N(\mu, \sigma^2)$, then

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

- Maximum differential entropy under average power constraint:

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

and is achieved for $X \sim N(0, P)$. Thus, for any $X \sim f(x)$,

$$h(X) = h(X - E(X)) \leq \frac{1}{2} \log(2\pi e \operatorname{Var}(X))$$

- Joint differential entropy of random vector X^n :

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

- Translation: For any constant vector a^n , $h(X^n + a^n) = h(X^n)$

- Scaling: For any nonsingular $n \times n$ matrix A ,

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

- If $X^n \sim N(\mu, K)$, i.e., a Gaussian random n -vector, then

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

- Maximum differential entropy lemma: Let $(\mathbf{X}, \mathbf{Y}) = (X^n, Y^k) \sim f(x^n, y^k)$ be a pair of random vectors with covariance matrices $K_{\mathbf{X}} = E[(\mathbf{X} - E\mathbf{X})(\mathbf{X} - E\mathbf{X})^T]$ and $K_{\mathbf{Y}} = E[(\mathbf{Y} - E\mathbf{Y})(\mathbf{Y} - E\mathbf{Y})^T]$. Let $K_{\mathbf{X}|\mathbf{Y}}$ be the covariance matrix of the minimum mean square error (MMSE) for estimating X^n given Y^k .

Then

$$h(X^n | Y^k) \leq \frac{1}{2} \log((2\pi e)^n |K_{\mathbf{X}|\mathbf{Y}}|),$$

with equality iff (X^n, Y^k) are jointly Gaussian. In particular,

$$h(X^n) \leq \frac{1}{2} \log((2\pi e)^n |K_{\mathbf{X}}|) \leq \frac{1}{2} \log(2\pi e)^n |E(\mathbf{X}\mathbf{X}^T)|,$$

where $E(\mathbf{X}\mathbf{X}^T)$ is the correlation matrix of X^n .

The upper bound on the differential entropy can be further relaxed to

$$h(X^n) \leq \frac{n}{2} \log \left(2\pi e \left(\frac{1}{n} \sum_{i=1}^n \operatorname{Var}(X_i) \right) \right) \leq \frac{n}{2} \log \left(2\pi e \left(\frac{1}{n} \sum_{i=1}^n E(X_i^2) \right) \right).$$

This can be proved using Hadamard's inequality [5, 6], or more directly using the inequality $h(X^n) \leq \sum_{i=1}^n h(X_i)$, the scalar maximum entropy result, and convexity

- *Entropy Power Inequality (EPI)* [7, 8, 9]:

- *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 iff 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 iff X^n and Z^n are Gaussian with $K_X = aK_Z$ for some scalar $a > 0$

The proof follows by the EPI, convexity of the function $\log(2^u + 2^v)$ in (u, v) , and induction

- *Conditional EPI*: Let X^n and Z^n be conditionally independent given an arbitrary random variable U , with conditional densities $f(x^n|u)$ and $f(z^n|u)$, then

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

The proof follows from the above

- *Differential entropy rate*: Let $X = \{X_i\}$ be a stationary continuous-valued random process. The differential entropy rate of the process X is defined as

$$\bar{h}(X) := \lim_{n \rightarrow \infty} \frac{1}{n} h(X^n) = \lim_{n \rightarrow \infty} h(X_n | X^{n-1})$$

Mutual Information

- Mutual information for discrete random variables $(X, Y) \sim p(x, y)$ is defined as

$$I(X; Y) := \sum_{(x,y) \in \mathcal{X} \times \mathcal{Y}} p(x, y) \log \frac{p(x, y)}{p(x)p(y)}$$

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

Mutual information is a nonnegative function of $p(x, y)$, concave in $p(x)$ for fixed $p(y|x)$, and convex in $p(y|x)$ for fixed $p(x)$

- For continuous random variables $(X, Y) \sim f(x, y)$ is defined as

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

- In general, mutual information can be defined for any random variables [10] 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 taken over all such functions

- This general definition can be shown to be consistent with above definitions of mutual information for discrete and continuous random variables [11, Section 5]. In this case,

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

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 quantization errors for all $x, y, x - \hat{x}_j(x), y - \hat{y}_k(y) \rightarrow 0$ as $j, k \rightarrow \infty$

- If $X \sim p(x)$ is discrete and $Y|X=x \sim f(y|x)$ is continuous for each x , then

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

- 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 $\{Z = z\}$ as $I(X; Y|Z = z)$. The conditional mutual information is defined as

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

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

$$I(X; Y|Z) = H(X|Z) - H(X|Y, Z) = H(Y|Z) - H(Y|X, Z)$$

- Note that no general inequality relationship exists between $I(X; Y|Z)$ and $I(X; Y)$

Two important special cases:

- If $p(x, y, z) = p(x)p(z)p(y|x, z)$, then $I(X; Y|Z) \geq I(X; Y)$
This follows by the convexity of $I(X; Y)$ in $p(y|x)$ for fixed $p(x)$
- If $Z \rightarrow X \rightarrow Y$ 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 fixed $p(y|x)$

- Chain rule:

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

- *Data processing inequality*: If $X \rightarrow Y \rightarrow Z$ form a Markov chain, then $I(X; Z) \leq I(Y; Z)$

To show this, we use the chain rule to expand $I(X; Y, Z)$ in two ways

$$I(X; Y, Z) = I(X; Y) + I(X; Z|Y) = I(X; Y), \text{ and}$$

$$I(X; Y, Z) = I(X; Z) + I(X; Y|Z) \geq I(X; Z)$$

- *Csiszár Sum Identity* [12]: Let X^n and Y^n be two random vectors with arbitrary joint probability distribution, then

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

where $X_{n+1}, Y_0 = \emptyset$

This lemma can be proved by induction, or more simply using the chain rule for mutual information

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

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

- Let X_1, X_2, \dots be i.i.d. with $X_i \sim p_X(x_i)$. For each $x \in \mathcal{X}$,

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

This is a consequence of the (weak) law of large numbers (LLN)

Thus most likely the random empirical pmf $\pi(x|X^n)$ does not deviate much from the true pmf $p(x)$

- *Typical set* [13]: For $X \sim p(x)$ and $\epsilon \in (0, 1)$, define the set $\mathcal{T}_\epsilon^{(n)}(X)$ of typical sequences x^n (the ϵ -typical set or the typical set in short) as

$$\mathcal{T}_\epsilon^{(n)}(X) := \{x^n : |\pi(x|x^n) - p(x)| \leq \epsilon \cdot p(x) \text{ for all } x \in \mathcal{X}\}$$

When it is clear from the context, we shall use $\mathcal{T}_\epsilon^{(n)}$ instead of $\mathcal{T}_\epsilon^{(n)}(X)$

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

$$(1 - \epsilon) \mathbb{E}(g(X)) \leq \frac{1}{n} \sum_{i=1}^n g(x_i) \leq (1 + \epsilon) \mathbb{E}(g(X))$$

Proof: From the definition of the typical set,

$$\begin{aligned} \left| \frac{1}{n} \sum_{i=1}^n g(x_i) - \mathbb{E}(g(X)) \right| &= \left| \sum_x \pi(x|x^n) g(x) - \sum_x p(x) g(x) \right| \\ &\leq \sum_x \epsilon p(x) g(x) \\ &= \epsilon \cdot \mathbb{E}(g(X)) \end{aligned}$$

- Properties of typical sequences:

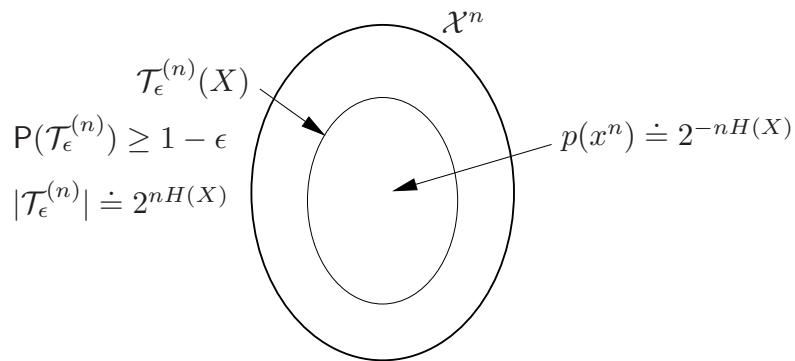
1. Let $p(x^n) = \prod_{i=1}^n p_X(x_i)$. Then, for each $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$

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

where $\delta(\epsilon) = \epsilon \cdot H(X) \rightarrow 0$ as $\epsilon \rightarrow 0$. This follows from the typical average lemma by taking $g(x) = -\log p_X(x)$

2. The cardinality of the typical set $|\mathcal{T}_\epsilon^{(n)}| \leq 2^{n(H(X)+\delta(\epsilon))}$. This can be shown by summing the lower bound in the previous property over the typical set
3. If X_1, X_2, \dots are i.i.d. with $X_i \sim p_X(x_i)$, then by the LLN
 $P\{X^n \in \mathcal{T}_\epsilon^{(n)}\} \rightarrow 1$
4. The cardinality of the typical set $|\mathcal{T}_\epsilon^{(n)}| \geq (1 - \epsilon)2^{n(H(X)-\delta(\epsilon))}$ for n sufficiently large. This follows by property 3 and the upper bound in property 1

- The above properties are illustrated in the following figure



Jointly Typical Sequences

- We generalize the notion of typicality 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

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

- Let $(X, Y) \sim p(x, y)$. The set $\mathcal{T}_\epsilon^{(n)}(X, Y)$ (or $\mathcal{T}_\epsilon^{(n)}$ in short) of jointly ϵ -typical n -sequences (x^n, y^n) is defined as:
- $$\mathcal{T}_\epsilon^{(n)} := \{(x^n, y^n) : |\pi(x, y|x^n, y^n) - p(x, y)| \leq \epsilon \cdot p(x, y) \text{ for all } (x, y) \in (\mathcal{X}, \mathcal{Y})\},$$
- In other words, $\mathcal{T}_\epsilon^{(n)}(X, Y) = \mathcal{T}_\epsilon^{(n)}((X, Y))$

Properties of Jointly Typical Sequences

- Let $p(x^n, y^n) = \prod_{i=1}^n p_{X,Y}(x_i, y_i)$. If $(x^n, y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)$, then
 1. $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$ and $y^n \in \mathcal{T}_\epsilon^{(n)}(Y)$
 2. $p(x^n, y^n) \doteq 2^{-nH(X, Y)}$
 3. $p(x^n) \doteq 2^{-nH(X)}$ and $p(y^n) \doteq 2^{-nH(Y)}$
 4. $p(x^n|y^n) \doteq 2^{-nH(X|Y)}$ and $p(y^n|x^n) \doteq 2^{-nH(Y|X)}$
- As in the single random variable case, for n sufficiently large

$$|\mathcal{T}_\epsilon^{(n)}(X, Y)| \doteq 2^{nH(X, Y)}$$

- Let $\mathcal{T}_\epsilon^{(n)}(Y|x^n) := \{y^n : (x^n, y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\}$. Then

$$|\mathcal{T}_\epsilon^{(n)}(Y|x^n)| \leq 2^{n(H(Y|X) + \delta(\epsilon))},$$

where $\delta(\epsilon) = \epsilon \cdot H(Y|X)$

- 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 $i \in [1 : n]$

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

$$\mathbb{P}\{(x^n, Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\} \rightarrow 1 \text{ as } n \rightarrow \infty$$

This follows by the LLN. Note that the condition $\epsilon > \epsilon'$ is crucial to apply the LLN (why?)

The conditional typicality lemma implies that for all $x^n \in \mathcal{T}_{\epsilon'}^{(n)}(X)$

$$|\mathcal{T}_\epsilon^{(n)}(Y|x^n)| \geq (1 - \epsilon) 2^{n(H(Y|X) - \delta(\epsilon))} \text{ for } n \text{ sufficiently large}$$

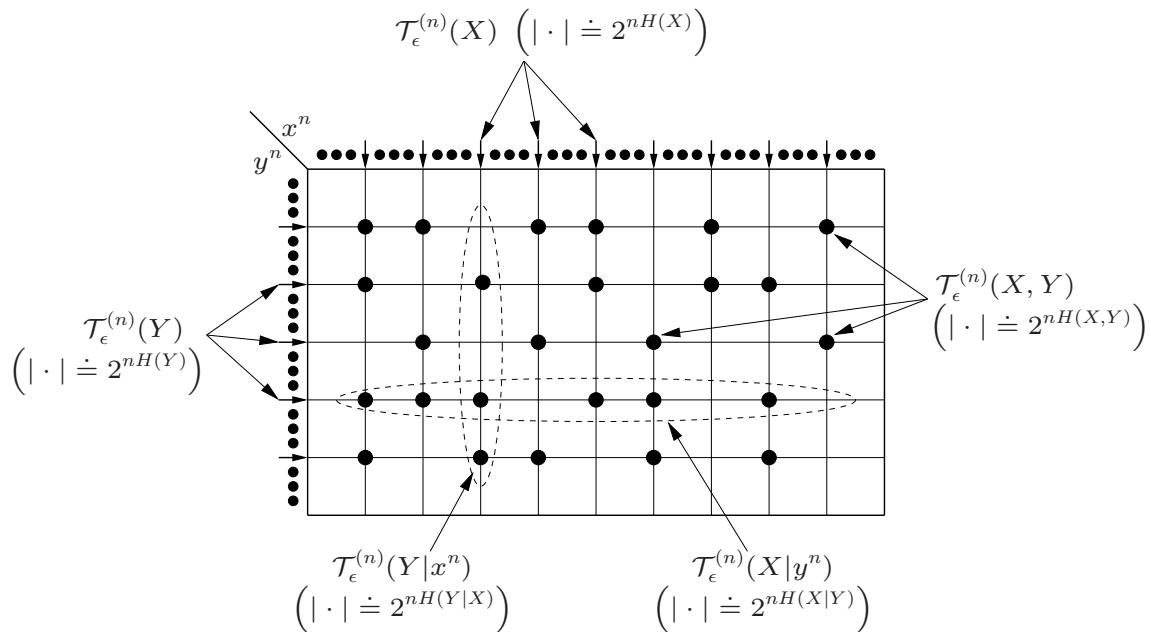
- In fact, a stronger statement holds: For every $x^n \in \mathcal{T}_\epsilon^{(n)}(X)$ and n sufficiently large,

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

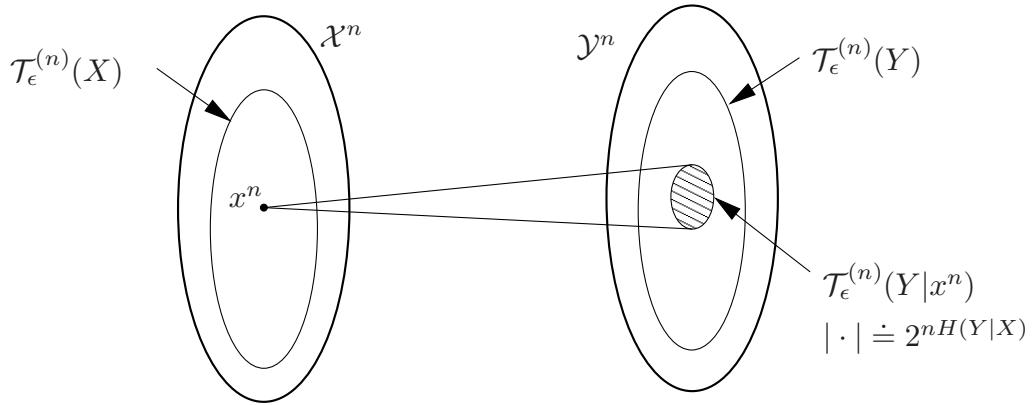
for some $\delta'(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$

This can be proved by counting jointly typical y^n sequences (the method of types [12]) as shown in the Appendix

Useful Picture



Another Useful Picture



Joint Typicality for Random Triples

- Let $(X, Y, Z) \sim p(x, y, z)$. The set $\mathcal{T}_\epsilon^{(n)}(X_1, X_2, X_3)$ of ϵ -typical n -sequences is defined by

$$\{(x^n, y^n, z^n) : |\pi(x, y, z | x^n, y^n, z^n) - p(x, y, z)| \leq \epsilon \cdot p(x, y, z)$$

for all $(x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z}\}$

- Since this is equivalent to the typical set of a single “large” random variable (X, Y, Z) or a pair of random variables $((X, Y), Z)$, the properties of joint typical sequences continue to hold
- For example, if $p(x^n, y^n, z^n) = \prod_{i=1}^n p_{X,Y,Z}(x_i, y_i, z_i)$ and $(x^n, y^n, z^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y, Z)$, 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. $|\mathcal{T}_\epsilon^{(n)}(X | y^n, z^n)| \doteq 2^{nH(X | Y, Z)}$ for n sufficiently large

- Similarly, suppose $X \rightarrow Y \rightarrow Z$ form a Markov chain and $(x^n, y^n) \in \mathcal{T}_{\epsilon'}^{(n)}(X, Y)$. If $p(z^n|y^n) = \prod_{i=1}^n p_{Z|Y}(z_i|y_i)$, then for every $\epsilon > \epsilon'$,

$$\mathbb{P}\{(x^n, y^n, Z^n) \in \mathcal{T}_{\epsilon}^{(n)}(X, Y, Z)\} \rightarrow 1 \quad \text{as } n \rightarrow \infty$$

This result [14] follows from the conditional typicality lemma since the Markov condition implies that

$$p(z^n|y^n) = \prod_{i=1}^n p_{Z|X,Y}(z_i|x_i, y_i),$$

i.e., Z^n is distributed according to the correct conditional pmf

Joint Typicality Lemma

- Let $(X, Y, Z) \sim p(x, y, z)$. Then there exists $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$ such that the following statements hold:

- Given $(x^n, y^n) \in \mathcal{T}_{\epsilon}^{(n)}(X, Y)$, let \tilde{Z}^n be distributed according to $\prod_{i=1}^n p_{Z|X}(\tilde{z}_i|x_i)$ (instead of $p_{Z|X,Y}(\tilde{z}_i|x_i, y_i)$). Then,

$$(a) \mathbb{P}\{(x^n, y^n, \tilde{Z}^n) \in \mathcal{T}_{\epsilon}^{(n)}(X, Y, Z)\} \leq 2^{-n(I(Y;Z|X)-\delta(\epsilon))}, \text{ and}$$

(b) for sufficiently large n ,

$$\mathbb{P}\{(x^n, y^n, \tilde{Z}^n) \in \mathcal{T}_{\epsilon}^{(n)}(X, Y, Z)\} \geq (1 - \epsilon)2^{-n(I(Y;Z|X)+\delta(\epsilon))}$$

- If $(\tilde{X}^n, \tilde{Y}^n)$ is distributed according to an arbitrary pmf $p(\tilde{x}^n, \tilde{y}^n)$ and $\tilde{Z}^n \sim \prod_{i=1}^n p_{Z|X}(\tilde{z}_i|\tilde{x}_i)$, conditionally independent of \tilde{Y}^n given \tilde{X}^n , then

$$\mathbb{P}\{(\tilde{X}^n, \tilde{Y}^n, \tilde{Z}^n) \in \mathcal{T}_{\epsilon}^{(n)}(X, Y, Z)\} \leq 2^{-n(I(Y;Z|X)-\delta(\epsilon))}$$

To prove the first statement, consider

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

Similarly, for n sufficiently large

$$\begin{aligned}
P\{(\tilde{x}^n, \tilde{y}^n, \tilde{Z}^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y, Z)\} &\geq |\mathcal{T}_\epsilon^{(n)}(Z|\tilde{x}^n, \tilde{y}^n)| \cdot 2^{-n(H(Z|X)+\epsilon H(Z|X))} \\
&\geq 2^{n(H(Z|X,Y)-\delta'(\epsilon))} \cdot 2^{-n(H(Z|X)+\epsilon H(Z|X))} \\
&= 2^{-n(I(Y;Z|X)+\delta(\epsilon))}
\end{aligned}$$

The proof of the second statement follows similarly.

Multivariate Typical Sequences

- Let $(X_1, X_2, \dots, X_k) \sim p(x_1, x_2, \dots, x_k)$ and \mathcal{J} be a non-empty subset of $[1 : k]$. Define the ordered subset of random variables $X(\mathcal{J}) := (X_j : j \in \mathcal{J})$
Example: Let $k = 3$, $\mathcal{J} = \{1, 3\}$; then $X(\mathcal{J}) = (X_1, X_3)$

- The set of ϵ -typical n -sequences $(x_1^n, x_2^n, \dots, x_k^n)$ is defined by

$$\mathcal{T}_\epsilon^{(n)}(X_1, X_2, \dots, X_k) = \mathcal{T}_\epsilon^{(n)}((X_1, X_2, \dots, X_k))$$

(same as the typical set for a single “large” random variable (X_1, X_2, \dots, X_k))

- One can similarly define $\mathcal{T}_\epsilon^{(n)}(X(\mathcal{J}))$ for every $\mathcal{J} \subseteq [1 : k]$

- We can easily check that the properties of jointly typical sets continue to hold by considering $X(\mathcal{J})$ as a single random variable

For example, if $p(x_1^n, x_2^n, \dots, x_k^n) = \prod_{i=1}^n p_{X_1, X_2, \dots, X_k}(x_{1i}, x_{2i}, \dots, x_{ki})$ and $(x_1^n, x_2^n, \dots, x_k^n) \in \mathcal{T}_\epsilon^{(n)}(X_1, X_2, \dots, X_k)$, 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. $|\mathcal{T}_\epsilon^{(n)}(X(\mathcal{J})|x^n(\mathcal{J}'))| \doteq 2^{nH(X(\mathcal{J})|X(\mathcal{J}'))}$ for n sufficiently large

- The conditional and joint typicality lemmas can be readily generalized to subsets $X(\mathcal{J}_1), X(\mathcal{J}_2), X(\mathcal{J}_3)$ for $\mathcal{J}_1, \mathcal{J}_2, \mathcal{J}_3 \subseteq [1 : k]$ and sequences $x^n(\mathcal{J}_1), x^n(\mathcal{J}_2), \tilde{x}^n(\mathcal{J}_3)$ satisfying similar conditions

References

- [1] A. D. Wyner and J. Ziv, "A theorem on the entropy of certain binary sequences and applications—I," *IEEE Trans. Inf. Theory*, vol. 19, pp. 769–772, 1973.
- [2] H. S. Witsenhausen, "Entropy inequalities for discrete channels," *IEEE Trans. Inf. Theory*, vol. 20, pp. 610–616, 1974.
- [3] H. S. Witsenhausen and A. D. Wyner, "A conditional entropy bound for a pair of discrete random variables," *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 493–501, 1975.
- [4] S. Shamai and A. D. Wyner, "A binary analog to the entropy-power inequality," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1428–1430, 1990.
- [5] R. Bellman, *Introduction to Matrix Analysis*, 2nd ed. New York: McGraw-Hill, 1970.
- [6] A. W. Marshall and I. Olkin, "A convexity proof of Hadamard's inequality," *Amer. Math. Monthly*, vol. 89, no. 9, pp. 687–688, 1982.
- [7] C. E. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, vol. 27, pp. 379–423, 623–656, 1948.
- [8] A. J. Stam, "Some inequalities satisfied by the quantities of information of Fisher and Shannon," *Inf. Control*, vol. 2, pp. 101–112, 1959.
- [9] N. M. Blachman, "The convolution inequality for entropy powers," *IEEE Trans. Inf. Theory*, vol. 11, pp. 267–271, 1965.
- [10] M. S. Pinsker, *Information and Information Stability of Random Variables and Processes*. San Francisco: Holden-Day, 1964.
- [11] R. M. Gray, *Entropy and Information Theory*. New York: Springer, 1990.

- [12] I. Csiszár and J. Körner, *Information Theory*. Budapest: Akadémiai Kiadó, 1981.
- [13] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, 2001.
- [14] T. Berger, "Multiterminal source coding," in *The Information Theory Approach to Communications*, G. Longo, Ed. New York: Springer-Verlag, 1978.
- [15] B. McMillan, "The basic theorems of information theory," *Ann. Math. Statist.*, vol. 24, pp. 196–219, 1953.
- [16] L. Breiman, "The individual ergodic theorem of information theory," *Ann. Math. Statist.*, vol. 28, pp. 809–811, 1957, with correction in *Ann. Math. Statist.*, vol. 31, pp. 809–810, 1960.
- [17] A. R. Barron, "The strong ergodic theorem for densities: Generalized Shannon–McMillan–Breiman theorem," *Ann. Probab.*, vol. 13, no. 4, pp. 1292–1303, 1985.
- [18] W. Feller, *An Introduction to Probability Theory and its Applications*, 3rd ed. New York: Wiley, 1968, vol. I.

Appendix: Weak Typicality

- There is another widely used definition for typicality, namely, *weakly* typical sequences:

$$\mathcal{A}_\epsilon^{(n)}(X) := \left\{ x^n : \left| -\frac{1}{n} \log p(x^n) - H(X) \right| \leq \epsilon \right\}$$

- If X_1, X_2, \dots are i.i.d. random variables with $X_i \sim p_X(x_i)$, then
 1. $\mathbb{P} \left\{ X^n \in \mathcal{A}_\epsilon^{(n)} \right\} \rightarrow 1$ as $n \rightarrow \infty$
 2. $|\mathcal{A}_\epsilon^{(n)}| \leq 2^{n(H(X)+\epsilon)}$
 3. $|\mathcal{A}_\epsilon^{(n)}| \geq (1-\epsilon)2^{n(H(X)-\epsilon)}$ for n sufficiently large

- Our notion of typicality is stronger than weak typicality, since

$$\mathcal{T}_\epsilon^{(n)} \subseteq \mathcal{A}_\delta^{(n)} \text{ for } \delta = \epsilon \cdot H(X),$$

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 w.r.t. the $\text{Bern}(1/2)$ pmf, but not all of them are typical)

- Weak typicality can be handy when dealing with stationary ergodic and/or continuous processes

- For a discrete stationary ergodic process $\{X_i\}$

$$-\frac{1}{n} \log p(X^n) \rightarrow \overline{H}(X),$$

where $\overline{H}(X)$ is the entropy rate of the process

- Similarly, for a continuous stationary ergodic process

$$-\frac{1}{n} \log f(X^n) \rightarrow \overline{h}(X),$$

where $h(X)$ is the differential entropy rate of the process

This is a consequence of the ergodic theorem and is referred to as the asymptotic equipartition property (AEP) or Shannon–McMillan–Breiman theorem [7, 15, 16, 17]

- However, we shall encounter several coding techniques that require the use of strong typicality, and hence we shall use strong typicality in all following lectures notes

Appendix: Proof of Lower Bound on Typical Set Cardinality

- Let $(x^n, y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y)$ and define

$$n_{xy} := n\pi(x, y|x^n, y^n),$$

$$n_x := n\pi(x|x^n) = \sum_{y \in \mathcal{Y}} n_{xy}$$

for all $(x, y) \in \mathcal{X} \times \mathcal{Y}$. Then $\mathcal{T}_\epsilon^{(n)}(Y|x^n) \supseteq \{\tilde{y}^n \in \mathcal{Y}^n : \pi(x, y|x^n, \tilde{y}^n) = n_{xy}/n\}$ and thus

$$|\mathcal{T}_\epsilon^{(n)}(Y|x^n)| \geq \prod_{x \in \mathcal{X}} \frac{n_x!}{\prod_{y \in \mathcal{Y}} (n_{xy})!}$$

- We now use Stirling's approximation [18]:

$$\log(k!) = k \log k - k \log e + k\epsilon_k,$$

where $\epsilon_k \rightarrow 0$ as $k \rightarrow \infty$, and consider

$$\begin{aligned}
\frac{1}{n} \log |\mathcal{T}_\epsilon^{(n)}(Y|x^n)| &\geq \frac{1}{n} \sum_{x \in \mathcal{X}} \left(\log(n_x!) - \sum_{y \in \mathcal{Y}} \log(n_{xy}!) \right) \\
&= \frac{1}{n} \sum_{x \in \mathcal{X}} \left(n_x \log n_x - \sum_{y \in \mathcal{Y}} n_{xy} \log n_{xy} - n_x \epsilon_n \right) \\
&= \sum_{x \in \mathcal{X}} \sum_{y \in \mathcal{Y}} \frac{n_{xy}}{n} \log \left(\frac{n_x}{n_{xy}} \right) - \epsilon_n
\end{aligned}$$

- Note that by definition,

$$\left| \frac{1}{n} n_{xy} - p(x, y) \right| < \epsilon p(x, y) \text{ for every } (x, y)$$

- Substituting, we obtain

$$\begin{aligned}
\frac{1}{n} \log |\mathcal{T}_\epsilon^{(n)}(Y|x^n)| &\geq \sum_{p(x,y)>0} (1-\epsilon)p(x, y) \log \frac{\sum_{y \in \mathcal{Y}} (1-\epsilon)p(x, y)}{((1+\epsilon)p(x, y))} - \epsilon_n \\
&= \sum_{p(x,y)>0} (1-\epsilon)p(x, y) \log \frac{(1-\epsilon)p(x)}{(1+\epsilon)p(x, y)} - \epsilon_n \\
&= \sum_{p(x,y)>0} p(x, y) \log \frac{p(x)}{p(x, y)} - \sum_{p(x,y)>0} \epsilon p(x, y) \log \frac{p(x)}{p(x, y)} - \epsilon_n \\
&\quad - (1-\epsilon) \log \left(\frac{1+\epsilon}{1-\epsilon} \right) - \epsilon_n \\
&\geq H(Y|X) - \delta'(\epsilon)
\end{aligned}$$

for n sufficiently large

Lecture Notes 3

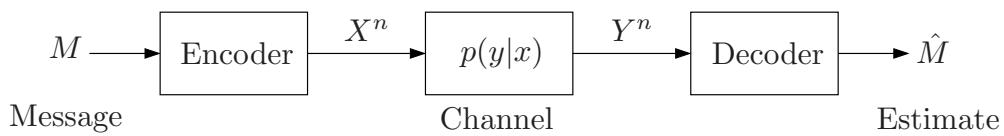
Point-to-Point Communication

- Channel Coding
- Packing Lemma
- Channel Coding with Cost
- Additive White Gaussian Noise Channel
- Lossless Source Coding
- Lossy Source Coding
- Covering Lemma
- Quadratic Gaussian Source Coding
- Joint Source–Channel Coding
- Key Ideas and Techniques
- Appendix: Proof of Lemma 2

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Channel Coding

- Sender X wishes to send a message reliably to a receiver Y over a communication channel
- A *discrete (stationary) memoryless channel* (DMC) $(\mathcal{X}, p(y|x), \mathcal{Y})$ consists of two finite sets \mathcal{X} , \mathcal{Y} , and a collection of conditional pmfs $p(y|x)$ on \mathcal{Y}
- By memoryless, we mean that when the DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ is used over n transmissions with message M and input X^n , the output Y_i at time $i \in [1 : n]$ is distributed according to $p(y_i|x^i, y^{i-1}, m) = p(y_i|x_i)$



- A $(2^{nR}, n)$ code with rate $R \geq 0$ bits/transmission for the DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ consists of:
 1. A message set $[1 : 2^{nR}] = \{1, 2, \dots, 2^{\lceil nR \rceil}\}$
 2. An encoding function (encoder) $x^n : [1 : 2^{nR}] \rightarrow \mathcal{X}^n$ that assigns a codeword $x^n(m)$ to each message $m \in [1 : 2^{nR}]$. The set $\mathcal{C} := \{x^n(1), \dots, x^n(2^{\lceil nR \rceil})\}$ is referred to as the *codebook*

- 3. A decoding function (decoder) $\hat{m} : \mathcal{Y}^n \rightarrow [1 : 2^{nR}] \cup \{e\}$ that assigns a message $\hat{m} \in [1 : 2^{nR}]$ or an error message e to each received sequence y^n
- Note that under the above definition of a code, the memoryless property reduces to

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

- Remark: When the channel is used with feedback, i.e., $x_i(m, y^{i-1})$, we need to use the more general definition of the memoryless property
- We assume the message $M \sim \text{Unif}[1 : 2^{nR}]$, i.e., it is chosen uniformly at random from the message set
- Probability of error: Let $\lambda_m(\mathcal{C}) = P\{\hat{M} \neq m | M = m\}$ be the conditional probability of error given that message m is sent

The *average probability of error* $P_e^{(n)}(\mathcal{C})$ for a $(2^{nR}, n)$ code is defined as

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

- A rate R is said to be *achievable* if there exists a sequence of $(2^{nR}, n)$ codes with probability of error $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$

- The *capacity* C of a discrete memoryless channel is the supremum of all achievable rates

Channel Coding Theorem

- *Shannon's Channel Coding Theorem* [1]: The capacity of the DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ is given by $C = \max_{p(x)} I(X; Y)$
- Examples:

- Binary symmetric channel with crossover probability p (BSC(p)):

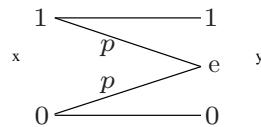


Here binary input symbols are flipped with probability p . Equivalently, $Y = X \oplus Z$, where the noise $Z \sim \text{Bern}(p)$ is independent of X . The capacity

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

and is achieved by $X \sim \text{Bern}(1/2)$

- Binary erasure channel with erasure probability p (BEC(p))



Here binary input symbols are erased with probability p and mapped to an erasure e . The receiver knows the location of erasures, but the sender does not. The capacity

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

- Product DMC: Let $(\mathcal{X}_1, p(y_1|x_1), \mathcal{Y}_1)$ and $(\mathcal{X}_2, p(y_2|x_2), \mathcal{Y}_2)$ be two DMCs with capacities C_1 and C_2 , respectively. Consider 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 symbols Y_1 and Y_2 are distributed according to $p(y_1, y_2|x_1, x_2) = p(y_1|x_1)p(y_2|x_2)$.

Then the capacity of this *product* DMC is

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

where (a) follows since $I(X_1, X_2; Y_1) = I(X_1; Y_1)$ by the Markovity of $X_2 \rightarrow X_1 \rightarrow Y_1$, and $I(X_1, X_2; Y_2|Y_1) = I(Y_1, X_1, X_2; Y_2) = I(X_2; Y_2)$ by the Markovity of $(X_1, Y_1) \rightarrow X_2 \rightarrow Y_2$

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

The capacity of the product DMC is

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

Proof of Channel Coding Theorem

- Achievability: We show that any rate $R < C$ is achievable, i.e., there exists a sequence of $(2^{nR}, n)$ codes with average probability of error $P_e^{(n)} \rightarrow 0$

The proof of achievability uses random coding and joint typicality decoding

- Weak converse: We show that given any sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$, then $R \leq C$

The proof of converse uses Fano's inequality and properties of mutual information

Proof of Achievability

- We show that any rate $R < C$ is achievable, i.e., there exists a sequence of $(2^{nR}, n)$ codes with average probability of error $P_e^{(n)} \rightarrow 0$. For simplicity of presentation, we assume throughout the proof that nR is an integer
- Random codebook generation (random coding): Fix $p(x)$ that achieves 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 sender and receiver before any transmission takes place
- Encoding: To send a 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 a message $\hat{m} \in [1 : 2^{nR}]$ is sent if it is the unique message such that $(x^n(\hat{m}), y^n) \in \mathcal{T}_\epsilon^{(n)}$; otherwise an error e is declared

- Analysis of the probability of error: Assuming m is sent, there is a decoding error if $(x^n(m), y^n) \notin \mathcal{T}_\epsilon^{(n)}$ or if there is an index $m' \neq m$ such that $(x^n(m'), y^n) \in \mathcal{T}_\epsilon^{(n)}$
- Consider the probability of error averaged over M and over all codebooks

$$\begin{aligned} P(\mathcal{E}) &= \sum_{\mathcal{C}} p(\mathcal{C}) P_e^{(n)}(\mathcal{C}) \\ &= \sum_{\mathcal{C}} p(\mathcal{C}) 2^{-nR} \sum_{m=1}^{2^{nR}} \lambda_m(\mathcal{C}) \\ &= 2^{-nR} \sum_{m=1}^{2^{nR}} \sum_{\mathcal{C}} p(\mathcal{C}) \lambda_m(\mathcal{C}) \\ &= \sum_{\mathcal{C}} p(\mathcal{C}) \lambda_1(\mathcal{C}) = P(\mathcal{E} | M = 1) \end{aligned}$$

Thus, assume without loss of generality that $M = 1$ is sent

The decoder makes an error iff

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

Thus, by the union of events bound

$$P(\mathcal{E}) = P(\mathcal{E}|M=1) = P(\mathcal{E}_1 \cup \mathcal{E}_2) \leq P(\mathcal{E}_1) + P(\mathcal{E}_2)$$

We bound each term:

- o For the first term, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ by the LLN
- o For the second term, since for $m \neq 1$,
 $(X^n(m), X^n(1), Y^n) \sim \prod_{i=1}^n p_X(x_i(m))p_{X,Y}(x_i(1), y_i)$,
 $(X^n(m), Y^n) \sim \prod_{i=1}^n p_X(x_i)p_Y(y_i)$. Thus, by the joint typicality lemma,

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

By the union of events bound

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

which $\rightarrow 0$ as $n \rightarrow \infty$ if $R < C - \delta(\epsilon)$

- To complete the proof, note that since the probability of error averaged over the codebooks $P(\mathcal{E}) \rightarrow 0$, there must exist a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$. This proves that $R < I(X; Y)$ is achievable

- Note that to bound $P(\mathcal{E})$, we divided \mathcal{E} into events each of which has the same (X^n, Y^n) pmf. This observation will prove useful when we analyze more complex error events

Remarks

- The above achievability proof is based on Shannon's original arguments, which was later made rigorous by Forney [2]. We will use the similar idea of "random packing" of codewords in subsequent multiple-user channel and source coding problems
- There are several alternative proofs, e.g.,
 - Feinstein's maximal coding theorem [3]
 - Gallager's random coding exponent [4]
- The capacity for the *maximal* probability of error $\lambda^* = \max_m \lambda_m$ is equal to that for the average probability of error $P_e^{(n)}$. This can be shown by throwing away the worst half of the codewords (in terms of error probability) from each of the sequence of $(2^{nR}, n)$ codes that achieve R . The maximal probability of error for the codes with the remaining codewords is $\leq 2P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$. As we shall see, this is not always the case for multiple-user channels
- It can be shown (e.g., see [5]) that the probability of error decays exponentially in n . The optimal error exponent is referred to as the *reliability function*. Very good bounds exist on the reliability function

Achievability with 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. It can be used to show that the capacity of a BSC can be achieved using *linear* codes
 - Consider a BSC(p). Let $k = \lceil nR \rceil$ and $(u_1, u_2, \dots, u_k) \in \{0, 1\}^k$ be the binary expansion of the message $m \in [1 : 2^k]$
 - Random *linear* codebook generation: 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

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

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

- Now we can easily check that:
 1. $X_1(u^k), \dots, X_n(u^k)$ are i.i.d. $\text{Bern}(1/2)$ for each u^k , and
 2. $X^n(u^k)$ and $X^n(\tilde{u}^k)$ are independent for each $u^k \neq \tilde{u}^k$
- Repeating the same arguments as before, it can be shown that the error probability of joint typicality decoding $\rightarrow 0$ as $n \rightarrow \infty$ if $R < 1 - H(p) - \delta(\epsilon)$
- This proves that for a BSC there exists not only a good code, but also a good *linear* code
- Remarks:
 - It can be similarly shown that random linear codes achieve the capacity of the binary erasure channel or more generally channels for which input alphabet is a finite field and capacity is achieved by the uniform pmf
 - Even though the (random) linear code constructed above allows efficient encoding (by simply multiply the message by the *generator matrix* G), the 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. For example, Gallager's low density parity check (LDPC) codes [6] have much sparser *parity check* matrices. Efficient iterative decoding algorithms on the graphical representation of LDPC codes have been developed, achieving close to capacity [7]

Proof of Weak Converse

- We need to show that for any sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$, $R \leq \max_{p(x)} I(X; Y)$
- Again for simplicity of presentation, we assume that nR is an integer
- Each $(2^{nR}, n)$ code induces the joint pmf

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

- By Fano's inequality

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

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$ by the assumption that $P_e^{(n)} \rightarrow 0$

- From the data processing inequality,

$$H(M|Y^n) \leq H(M|\hat{M}) \leq n\epsilon_n$$

- Now consider

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

where (a) follows by the fact that channel is memoryless, which implies that $(M, Y^{i-1}) \rightarrow X_i \rightarrow Y_i$ form a Markov chain. Since $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$, $R \leq C$

Packing Lemma

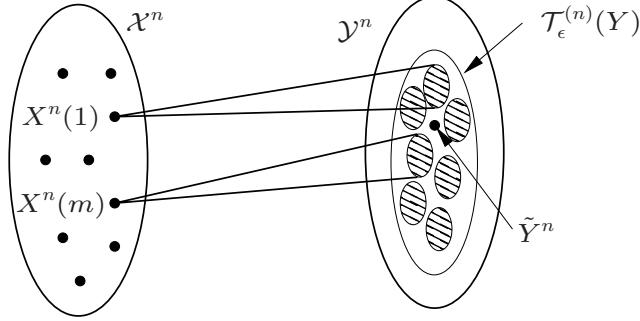
- We generalize the bound on the probability of decoding error, $P(\mathcal{E}_2)$, in the proof of achievability for the channel capacity theorem for subsequent use in achievability proofs for multiple user source and channel settings
- *Packing Lemma:* Let $(U, X, Y) \sim p(u, x, y)$. Let $(\tilde{U}^n, \tilde{Y}^n) \sim p(\tilde{u}^n, \tilde{y}^n)$ be a pair of arbitrarily distributed random sequences (not necessarily according to $\prod_{i=1}^n p_{U,Y}(\tilde{u}_i, \tilde{y}_i)$). Let $X^n(m)$, $m \in \mathcal{A}$, where $|\mathcal{A}| \leq 2^{nR}$, be random sequences, each distributed according to $\prod_{i=1}^n p_{X|U}(x_i | \tilde{u}_i)$. 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 $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$ such that

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

as $n \rightarrow \infty$, if $R < I(X; Y|U) - \delta(\epsilon)$

- The lemma is illustrated in the figure with $U = \emptyset$. The random sequences $X^n(m)$, $m \in \mathcal{A}$, represent codewords. The \tilde{Y}^n sequence represents the received sequence as a result of sending a codeword not in this set. The lemma shows that under any pmf on \tilde{Y}^n the probability that some codeword in \mathcal{A} is jointly typical with $\tilde{Y}^n \rightarrow 0$ as $n \rightarrow \infty$ if the rate of the code $R < I(X; Y|U)$



- For the bound on $P(\mathcal{E}_2)$ in the proof of achievability: $\mathcal{A} = [2 : 2^{nR}]$, $U = \emptyset$, for $m \neq 1$, the $X^n(m)$ sequences are i.i.d. each distributed according to $\prod_{i=1}^n p_X(x_i)$ and independent of $\tilde{Y}^n \sim \prod_{i=1}^n p_Y(\tilde{y}_i)$
- In the linear coding case, however, the $X^n(m)$ sequences are only pairwise independent. The packing lemma readily applies to this case
- We will encounter settings where $U \neq \emptyset$ and \tilde{Y}^n is not generated i.i.d.

- Proof: Define the events

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

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

$$P\left(\bigcup_{m \in \mathcal{A}} \mathcal{E}_m\right) \leq \sum_{m \in \mathcal{A}} P(\mathcal{E}_m)$$

Now, consider

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

where (a) follows by the conditional joint typicality lemma, since $(\tilde{u}^n, \tilde{y}^n) \in \mathcal{T}_\epsilon^{(n)}$ and $X^n(m) \sim \prod_{i=1}^n p_{X|U}(x_i|\tilde{u}_i)$, and $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$. Hence

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

which tends to 0 as $n \rightarrow \infty$ if $R < I(X; Y|U) - \delta(\epsilon)$

Channel Coding with Cost

- Suppose that there is a nonnegative cost $b(x)$ associated with each input symbol $x \in \mathcal{X}$. Without loss of generality, we assume that there exists an $x_0 \in \mathcal{X}$ such that $b(x_0) = 0$
 - Assume that the following cost constraint B is imposed on the codebook:
For every codeword $x^n(m)$, $\sum_{i=1}^n b(x_i(m)) \leq nB$
 - *Theorem 2:* The capacity of the DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ with cost constraint B is given by
- $$C(B) = \max_{p(x): E(b(X)) \leq B} I(X; Y),$$
- Note: As a function of the cost constraint B , the function $C(B)$ is sometimes called the *capacity-cost function*. $C(B)$ is nondecreasing, concave, and continuous in B

- Proof of achievability: Fix $p(x)$ that achieves $C(B/(1 + \epsilon))$. Randomly and independently generate 2^{nR} ϵ -typical codewords $x^n(m)$, $m \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_X(x_i)/P(\mathcal{T}_\epsilon^{(n)}(X))$
Remark: This can be done as follows. A sequence is generated according to $\prod_{i=1}^n p_X(x_i)$. If it is typical, we accept it as a codeword. Otherwise, we discard it and generate another sequence according to $\prod_{i=1}^n p_X(x_i)$. This process is continued until we obtain a codebook with only typical codewords
Since each codeword $x^n(m) \in \mathcal{T}_\epsilon^{(n)}(X)$ with $E(b(X)) \leq B/(1 + \epsilon)$, by the typical average lemma (Lecture Notes 2), each codeword satisfies the cost constraint $\sum_{i=1}^n b(x_i(m)) \leq nB$
Following similar lines to the proof of achievability for the coding theorem without cost constraint, we can show that any $R < I(X; Y) = C(B/(1 + \epsilon))$ is achievable (check!)
Finally, by the continuity of $C(B)$ in B , we have $C(B/(1 + \epsilon)) \rightarrow C(B)$ as $\epsilon \rightarrow 0$, which implies the achievability of any rate $R < C(B)$

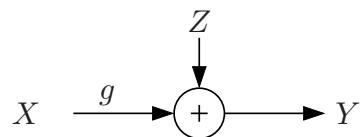
- Proof of converse: Consider any sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ such that for every n , the cost constraint $\sum_{i=1}^n b(x_i(m)) \leq nB$ is satisfied for every $m \in [1 : 2^{nR}]$ and thus $\sum_{i=1}^n E_M[b(X_i(M))] \leq nB$. As before,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

$$\begin{aligned} nR &\leq \sum_{i=1}^n I(X_i; Y_i) + n\epsilon_n \\ &\stackrel{(a)}{\leq} \sum_{i=1}^n C(E(b(X_i))) + n\epsilon_n \\ &\stackrel{(b)}{\leq} nC\left(\frac{1}{n} \sum_{i=1}^n E(b(X_i))\right) + n\epsilon_n \\ &\stackrel{(c)}{\leq} nC(B) + n\epsilon_n, \end{aligned}$$

where (a) follows from the definition of $C(B)$, (b) follows from concavity of $C(B)$ in B , and (c) follows from monotonicity of $C(B)$

Additive White Gaussian Noise Channel

- Consider the following discrete-time AWGN channel model



At transmission (time) i : $Y_i = gX_i + Z_i$, where g is the channel gain (also referred to as the *path loss*), and the receiver noise $\{Z_i\}$ is a white Gaussian noise process with average power $N_0/2$ (WGN($N_0/2$)), independent of $\{X_i\}$

Average transmit power constraint: For every codeword $x^n(m)$,
 $\sum_{i=1}^n x_i^2(m) \leq nP$

We assume throughout that $N_0/2 = 1$ and label the received power g^2P as S (for signal-to-noise ratio (SNR))

- Remark: If there is causal feedback from the receiver to the sender, then X_i depends only on the message M and 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 independent

Capacity of the AWGN Channel

- *Theorem 3* (Shannon [1]): The capacity of the AWGN channel with average received SNR S is given by

$$C = \frac{1}{2} \log(1 + S) =: C(S) \text{ bits/transmission}$$

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

- Proof of achievability: There are several ways to prove achievability for the AWGN channel under power constraint [5, 8]. Here we prove the achievability by extending the achievability proof for the DMC with input cost constraint

Set $X \sim N(0, P)$, then $Y = gX + Z \sim N(0, S + 1)$, where $S = g^2P$. Consider

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

For every $j = 1, 2, \dots$, let

$[X]_j \in \{-j\Delta, -(j-1)\Delta, \dots, -\Delta, 0, \Delta, \dots, (j-1)\Delta, j\Delta\}$, $\Delta = 1/\sqrt{j}$, be a quantized version of X , obtained by mapping X to the closest quantization point $[X]_j = \hat{x}_j(X)$ such that $|[X]_j| \leq |X|$. Clearly, $E([X]_j^2) \leq E(X^2) = P$. 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

Using the achievability proof for the DMC with cost constraint, we can show that for each j, k , $I([X]_j; [Y_j]_k)$ is achievable for the channel with input $[X]_j$ and output $[Y_j]_k$ under power constraint P

We now prove that $I([X]_j; [Y_j]_k)$ can be made as close as desired to $I(X; Y)$ by taking j, k sufficiently large

Lemma 2:

$$\liminf_{j \rightarrow \infty} \lim_{k \rightarrow \infty} I([X]_j; [Y_j]_k) \geq I(X; Y)$$

The proof of the lemma is given in the Appendix

On the other hand, by the data processing inequality,

$I([X]_j; [Y_j]_k) \leq I([X]_j; Y_j) = h(Y_j) - h(Z)$. Since $\text{Var}(Y_j) \leq S + 1$, $h(Y_j) \leq h(Y)$ for all j . Thus, $I([X]_j; [Y_j]_k) \leq I(X; Y)$. Combining this bound with Lemma 2 shows that

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

- Remark: This procedure [9] shows how we can extend results for DMCs to Gaussian or other well-behaved continuous-alphabet channels. Subsequently, we shall assume that a coding theorem for a channel with finite alphabets can be extended to an equivalent Gaussian model without providing a formal proof
- Proof of converse: As before, by Fano's inequality and the data processing inequality

$$\begin{aligned}
nR &= H(M) \leq I(X^n; Y^n) + n\epsilon_n \\
&= h(Y^n) - h(Z^n) + n\epsilon_n \\
&= h(Y^n) - \frac{n}{2} \log(2\pi e) + n\epsilon_n \\
&\leq \frac{n}{2} \log \left(2\pi e \left(\frac{1}{n} \sum_{i=1}^n g^2 \text{Var}(X_i) + 1 \right) \right) - \frac{n}{2} \log(2\pi e) + n\epsilon_n \\
&\leq \frac{n}{2} \log(2\pi e(S+1)) - \frac{n}{2} \log(2\pi e) + n\epsilon_n = nC(S) + n\epsilon_n
\end{aligned}$$

- Note that the converse for the DM case applies to arbitrary memoryless channels (not necessarily discrete). As such, the converse for the AWGN channel can be proved alternatively by optimizing $I(X; Y)$ over $F(x)$ with the power constraint $E(X^2) \leq P$

- The discrete-time AWGN channel models a continuous-time bandlimited AWGN channel with bandwidth $W = 1/2$, noise psd $N_0/2$, average transmit power P (area under psd of signal), and channel gain g . If the channel has bandwidth W and average power $2WP$, then it is equivalent to $2W$ parallel discrete-time AWGN channels (per second) and capacity is given (see [10]) by

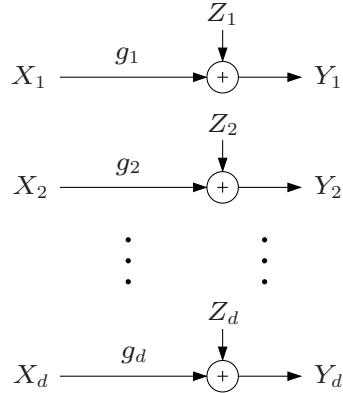
$$C = W \log \left(1 + \frac{2g^2 WP}{WN_0} \right) = W C(S) \text{ bits/second}$$

where $S = 2g^2 P/N_0$. For a wideband channel, $C \rightarrow (S/2) \ln 2$ as $W \rightarrow \infty$

Thus the capacity grows linearly with S and can be achieved via simple binary code [11]

Gaussian Product Channel

- The Gaussian product channel consists of a set of parallel AWGN channels:



At time i : $Y_{ji} = g_j X_{ji} + Z_{ji}$, $j \in [1 : d]$, $i \in [1 : n]$

where g_j is the gain of the j -th channel component and $\{Z_{1i}\}, \{Z_{2i}\}, \dots, \{Z_{di}\}$ are independent WGN processes with common average power $N_0/2 = 1$

- Average power constraint: For any codeword,

$$\frac{1}{n} \sum_{i=1}^n \sum_{j=1}^d x_{ji}^2(m) \leq P$$

- This models a continuous-time waveform Gaussian channel; the parallel channels may represent different frequency bands or time instances, or in general “degrees of freedom”
- The capacity is

$$C = \max_{F(X^d): \sum_{j=1}^d \mathbb{E}(X_j^2) \leq P} I(X^d; Y^d) = \max_{F(X^d): \sum_{j=1}^d \mathbb{E}(X_j^2) \leq P} \sum_{j=1}^d I(X_j; Y_j)$$

- Each mutual information term is maximized by a zero-mean Gaussian input distribution. Denote $P_j = \mathbb{E}(X_j^2)$. Then

$$C = \max_{\substack{P_1, P_2, \dots, P_d \\ \sum_{j=1}^d P_j \leq P}} \sum_{j=1}^d C(g_j^2 P_j)$$

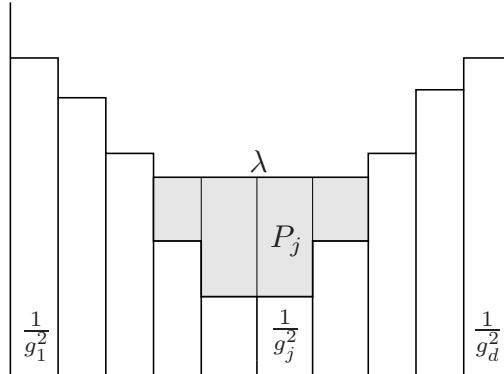
- *Water-filling solution:* This optimization problem can be solved using a Lagrange multiplier, and we obtain

$$P_j = \left(\lambda - \frac{1}{g_j^2} \right)^+ = \max \left\{ \lambda - \frac{1}{g_j^2}, 0 \right\},$$

where the Lagrange multiplier λ is chosen to satisfy

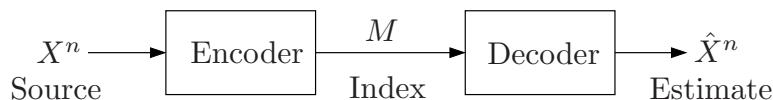
$$\sum_{j=1}^d \left(\lambda - \frac{1}{g_j^2} \right)^+ = P$$

The optimal solution has the following water-filling interpretation:



Lossless Source Coding

- A *discrete (stationary) memoryless source* (DMS) $(\mathcal{X}, p(x))$, informally referred to as X , consists of a finite alphabet \mathcal{X} and a pmf $p(x)$ over \mathcal{X} . (Throughout the phrase “discrete memoryless (DM)” will refer to “finite-alphabet and stationary memoryless”)
- The DMS $(\mathcal{X}, p(x))$ generates an i.i.d. random process $\{X_i\}$ with $X_i \sim p_X(x_i)$
- The DMS X is to be described losslessly to a decoder over a noiseless communication link. We wish to find the minimum required communication rate in bits/sec required



- Formally, a $(2^{nR}, n)$ fixed-length source code consists of:
 1. An encoding function (encoder) $m : \mathcal{X}^n \rightarrow [1 : 2^{nR}] = \{1, 2, \dots, 2^{\lfloor nR \rfloor}\}$ that assigns an index $m(x^n)$ (a codeword of length nR bits) to each source n -sequence x^n . Hence R is the rate of the code in bits/source symbol
 2. A decoding function (decoder) $\hat{x}^n : [1 : 2^{nR}] \rightarrow \mathcal{X}^n$ that assigns to each index $m \in [1 : 2^{nR}]$ an estimate $\hat{x}^n(m) \in \mathcal{X}^n$
- The probability of decoding error is defined as $P_e^{(n)} = P\{\hat{X}^n \neq X^n\}$
- A rate R is achievable if there exists a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ (so the coding is asymptotically lossless)
- The optimal lossless compression rate R^* is the infimum of all achievable rates
The lossless source coding problem is to find R^*

Lossless Source Coding Theorem

- Shannon's Lossless Source Coding Theorem [1]: The optimal lossless compression rate for a DMS $(\mathcal{X}, p(x))$ is $R^* = H(X)$
- Example: A $\text{Bern}(p)$ source X generates a $\text{Bern}(p)$ random process $\{X_i\}$. Then $H(X) = H(p)$ is the optimal rate for lossless source coding
- To establish the theorem, we need to prove the following:
 - Achievability: If $R > R^* = H(X)$, then there exists a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$
 - Weak converse: For any sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$, $R \geq R^* = H(X)$
- Proof of achievability: For simplicity of presentation, assume nR is an integer
 - For any $\epsilon > 0$, let $R = H(X) + \delta(\epsilon)$ with $\delta(\epsilon) = \epsilon \cdot H(X)$. Thus, $|\mathcal{T}_\epsilon^{(n)}| \leq 2^{n(H(X)+\delta(\epsilon))} = 2^{nR}$
 - Encoding: Assign an 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 correctly decoded. Thus the probability of error is $P_e^{(n)} = 1 - P(\mathcal{T}_\epsilon^{(n)}) \rightarrow 0$ as $n \rightarrow \infty$
 - Proof of converse: Given a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$, let M be the random variable corresponding to the index of the $(2^{nR}, n)$ encoder
- By Fano's inequality

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

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$ by the assumption $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$. Now consider

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

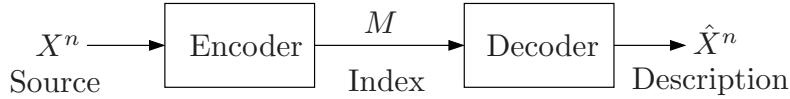
By taking $n \rightarrow \infty$, we conclude that $R \geq H(X)$

- Remark: The above source coding theorem holds for any discrete stationary ergodic (not necessarily i.i.d.) source [1]

- Error-free data compression: In many applications, one cannot afford to have any errors introduced by compression. Error-free compression ($P\{X^n \neq \hat{X}^n\} = 0$) for fixed-length codes, however, requires $R \geq \log |\mathcal{X}|$
Using *variable-length* codes ($m : \mathcal{X}^n \rightarrow [0, 1]^*$, $\hat{x}^n : [0, 1]^* \rightarrow \hat{\mathcal{X}}^n$), it can be easily shown that error-free compression is possible if the average rate of the code is $> H(X)$
Hence, the limit on the average achievable rate is the same for both lossless and error-free compression [1] (this is not true in general for distributed coding of multiple sources)

Lossy Source Coding

- A DMS X is encoded (described) at rate R by the encoder. The decoder receives the description index over a noiseless link and generates a reconstruction (estimate) \hat{X} of the source with a prescribed distortion D . What is the optimal tradeoff between the communication rate R and distortion between X and the estimate \hat{X}



- The distortion criterion is defined as follows. Let $\hat{\mathcal{X}}$ be a *reproduction alphabet* and define a *distortion measure* as a mapping

$$d : \mathcal{X} \times \hat{\mathcal{X}} \rightarrow [0, \infty)$$

It measures the cost of representing the symbol x by the symbol \hat{x}

The average per-letter distortion between x^n and \hat{x}^n is defined as

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

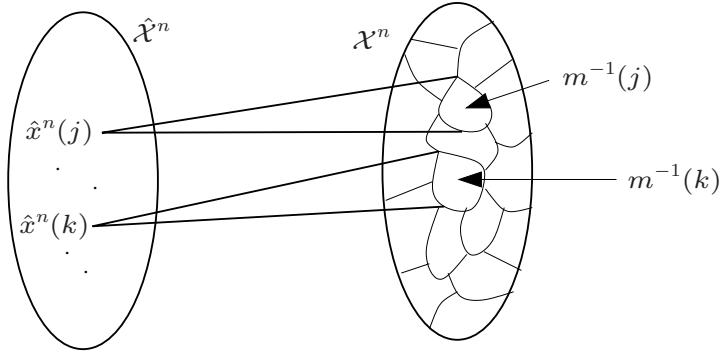
- Example: *Hamming distortion (loss)*: Assume $\mathcal{X} = \hat{\mathcal{X}}$. The Hamming distortion is the indicator for an error, i.e.,

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

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

- Formally, a $(2^{nR}, n)$ *rate-distortion code* consists of:
 1. An encoder that assigns to each sequence $x^n \in \mathcal{X}^n$ an index $m(x^n) \in [1 : 2^{nR}]$, and
 2. A decoder that assigns to each index $m \in [1 : 2^{nR}]$ an estimate $\hat{x}^n(m) \in \hat{\mathcal{X}}^n$

The set $\mathcal{C} = \{\hat{x}^n(1), \dots, \hat{x}^n(2^{\lfloor nR \rfloor})\}$ constitutes the *codebook*, and the sets $m^{-1}(1), \dots, m^{-1}(2^{\lfloor nR \rfloor}) \in \mathcal{X}^n$ are the associated *assignment regions*



- The distortion associated with the $(2^{nR}, n)$ code is

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

- A rate-distortion pair (R, D) is said to be *achievable* if there exists a sequence of $(2^{nR}, n)$ rate-distortion codes with $\limsup_{n \rightarrow \infty} E(d(X^n, \hat{X}^n)) \leq D$
- The *rate-distortion function* $R(D)$ is the infimum of rates R such that (R, D) is achievable

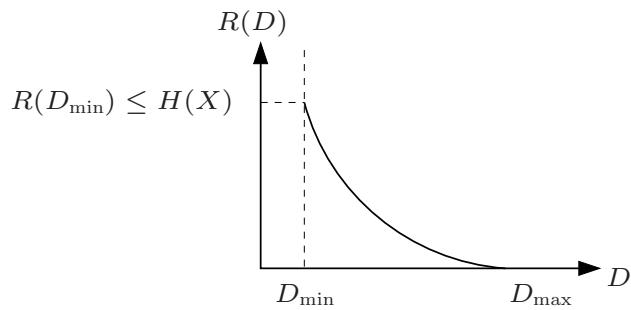
Lossy Source Coding Theorem

- Shannon's Lossy Source Coding Theorem* [12]: The *rate-distortion function* for a DMS $(\mathcal{X}, p(x))$ and a distortion measure $d(x, \hat{x})$ is

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

for $D \geq D_{\min} := E(\min_{\hat{x}} d(X, \hat{x}))$

- $R(D)$ is nonincreasing and convex (and thus continuous) in $D \in [D_{\min}, D_{\max}]$, where $D_{\max} := \min_{\hat{x}} E(d(X, \hat{x}))$ (check!)



- Without loss of generality we assume throughout that $D_{\min} = 0$, i.e., for every $x \in \mathcal{X}$ there exists an $\hat{x} \in \hat{\mathcal{X}}$ such that $d(x, \hat{x}) = 0$

Bernoulli Source with Hamming Distortion

- The rate-distortion function for a $\text{Bern}(p)$ source X , $p \in [0, 1/2]$, with Hamming distortion (loss) is

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

- Proof: Recall that

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

If we want $D \geq p$, we can simply set $\hat{X} = 0$. Thus $R(D) = 0$

If $D < p$, we find a lower bound and then show that there exists a test channel $p(\hat{x}|x)$ that achieves it

For any joint pmf that satisfies the distortion constraint,

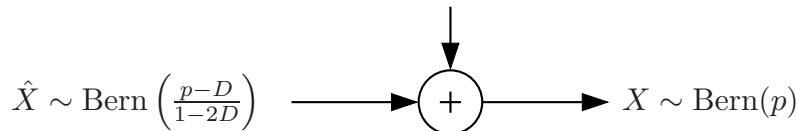
$$\begin{aligned} I(X; \hat{X}) &= H(X) - H(X|\hat{X}) \\ &= H(p) - H(X \oplus \hat{X}|\hat{X}) \\ &\geq H(p) - H(X \oplus \hat{X}) \\ &\geq H(p) - H(D) \end{aligned}$$

The last step follows since $P\{X \neq \hat{X}\} \leq D$. Thus

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

It is easy to show (check!) that this bound is achieved by the following backward BSC (with \hat{X} and Z independent)

$$Z \sim \text{Bern}(D)$$



and the associated expected distortion is D

Proof of Achievability

- Random codebook generation: Fix $p(\hat{x}|x)$ that achieves $R(D/(1+\epsilon))$, where D is the desired distortion, and calculate $p(\hat{x}) = \sum_x p(x)p(\hat{x}|x)$. Assume that nR is an integer

Randomly and independently generate 2^{nR} sequences $\hat{x}^n(m)$, $m \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_{\hat{X}}(\hat{x}_i)$

The randomly generated codebook is revealed to both the encoder and decoder

- Encoding: We use *joint typicality encoding*

Given a sequence x^n , choose an index m such that $(x^n, \hat{x}^n(m)) \in \mathcal{T}_\epsilon^{(n)}$

If there is more than one such m , choose the smallest index

If there is no such m , choose $m = 1$

- Decoding: Upon receiving the index m , the decoder chooses the reproduction sequence $\hat{x}^n(m)$

- Analysis of the expected distortion: We bound the distortion averaged over X^n and the random choice of the codebook \mathcal{C}

- Define the “encoding error” event

$$\mathcal{E} := \{(X^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m \in [1 : 2^{nR}]\},$$

and partition it into 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,

$$P(\mathcal{E}) \leq P(\mathcal{E}_1) + P(\mathcal{E}_2)$$

We bound each term:

- For the first term, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ by the LLN

- Consider the second term

$$\begin{aligned}
P(\mathcal{E}_2) &= \sum_{x^n \in \mathcal{T}_\epsilon^{(n)}} p(x^n) P\{(x^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m | X^n = x^n\} \\
&= \sum_{x^n \in \mathcal{T}_\epsilon^{(n)}} p(x^n) \prod_{m=1}^{2^{nR}} P\{(x^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)}\} \\
&= \sum_{x^n \in \mathcal{T}_\epsilon^{(n)}} p(x^n) \left[P\{(x^n, \hat{X}^n(1)) \notin \mathcal{T}_\epsilon^{(n)}\} \right]^{2^{nR}}
\end{aligned}$$

Since $x^n \in \mathcal{T}_\epsilon^{(n)}$ and $\hat{X}^n \sim \prod_{i=1}^n p_{\hat{X}}(\hat{x}_i)$, by the joint typicality lemma,

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

where $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$

Using the inequality $(1 - x)^k \leq e^{-kx}$, we have

$$\begin{aligned}
\sum_{x^n \in \mathcal{T}_\epsilon^{(n)}} p(x^n) \left[P\{(x^n, \hat{X}^n(1)) \notin \mathcal{T}_\epsilon^{(n)}\} \right]^{2^{nR}} &\leq \left[1 - 2^{-n(I(X; \hat{X}) + \delta(\epsilon))} \right]^{2^{nR}} \\
&\leq e^{-\left(2^{nR} \cdot 2^{-n(I(X; \hat{X}) + \delta(\epsilon))} \right)} \\
&= e^{-\left(2^{n(R - I(X; \hat{X}))} - \delta(\epsilon) \right)},
\end{aligned}$$

which goes to zero as $n \rightarrow \infty$, provided that $R > I(X; \hat{X}) + \delta(\epsilon)$

- Now, denote the reproduction sequence for X^n by $\hat{X}^n \in \mathcal{C}$. Then by the law of total expectation and the typical average lemma

$$\begin{aligned}
E_{\mathcal{C}, X^n}(d(X^n, \hat{X}^n)) &= P(\mathcal{E}) E_{\mathcal{C}, X^n}(d(X^n, \hat{X}^n) | \mathcal{E}) + P(\mathcal{E}^c) E_{\mathcal{C}, X^n}(d(X^n, \hat{X}^n) | \mathcal{E}^c) \\
&\leq P(\mathcal{E}) d_{\max} + P(\mathcal{E}^c)(1 + \epsilon) E(d(X, \hat{X})),
\end{aligned}$$

where $d_{\max} := \max_{(x, \hat{x}) \in \mathcal{X} \times \hat{\mathcal{X}}} d(x, \hat{x})$

Hence, by the assumption $E(d(X, \hat{X})) \leq D/(1 + \epsilon)$, we have shown that

$$\limsup_{n \rightarrow \infty} E_{\mathcal{C}, X^n}(d(X^n, \hat{X}^n)) \leq D,$$

if $R > I(X; \hat{X}) + \delta(\epsilon) = R(D/(1 + \epsilon)) + \delta(\epsilon)$

- Since the average per-letter distortion (over all random codebooks) is asymptotically $\leq D$, there must exist at least one sequence of codes with asymptotic distortion $\leq D$, which proves the achievability of $(R(D/(1 + \epsilon)) + \delta(\epsilon), D)$
 Finally since $R(D)$ is continuous in D , $R(D/(1 + \epsilon)) + \delta(\epsilon) \rightarrow R(D)$ as $\epsilon \rightarrow 0$, which completes the proof of achievability
- Remark: The lossy source coding theorem can be extended to stationary ergodic sources [5] with the following characterization of the rate-distortion function:

$$R(D) = \lim_{n \rightarrow \infty} \min_{p(\hat{X}^k | X^k) : E(d(X^k, \hat{X}^k)) \leq D} \frac{1}{k} I(X^k; \hat{X}^k)$$

Proof of Converse

- We need to show that for any sequence of $(2^{nR}, n)$ rate-distortion codes with $\limsup_{n \rightarrow \infty} E(d(X^n, \hat{X}^n)) \leq D$, we must have $R \geq R(D)$

Consider

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

where (a) follows by the fact that the source is memoryless, (b) follows from the definition of $R(D) = \min I(X; \hat{X})$ and (c) follows from convexity of $R(D)$

Since $R(D)$ is nonincreasing in D , $R \geq R(D)$ as $n \rightarrow \infty$

Lossless Source Coding Revisited

- We show that the lossless source coding theorem is a special case of the lossy source coding theorem. This leads to an alternative *covering proof* of achievability for the lossless source coding theorem
- Consider the lossy source coding problem for a DMS X , reproduction alphabet $\hat{\mathcal{X}} = \mathcal{X}$, and Hamming distortion measure. If we let $D = 0$, we obtain $R(0) = \min_{p(\hat{x}|x): E(d(X, \hat{X}))=0} I(X; \hat{X}) = I(X; X) = H(X)$, which is the optimal lossless source coding rate
- We show that $R^* = R(0)$
- To prove the converse ($R^* \geq R(D)$), 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 per-symbol error probability $(1/n) \sum_{i=1}^n P\{\hat{X}_i \neq X_i\} \rightarrow 0$, then $R \geq H(X)$. Since the average per-symbol error probability is less than or equal to the block error probability $P\{\hat{X}^n \neq X^n\}$ (why?), this also establishes the converse for the lossless case
- As for achievability ($R^* \leq R(0)$), we can still use random coding and joint typicality encoding!

We fix a test channel $p(\hat{x}|x) = 1$ if $x = \hat{x}$ and 0, otherwise, and define $\mathcal{T}_\epsilon^{(n)}(X, \hat{X})$ in the usual way. Note that if $(x^n, \hat{x}^n) \in \mathcal{T}_\epsilon^{(n)}$, then $x^n = \hat{x}^n$

Following the proof of the lossy source coding theorem, we generate a random code $\hat{x}^n(m)$, $m \in [1 : 2^{nR}]$

By the covering lemma if $R > I(X; \hat{X}) + \delta(\epsilon) = H(X) + \delta(\epsilon)$, the probability of decoding error averaged over the codebooks $P\{\hat{X}^n \neq X^n\} \rightarrow 0$ as $n \rightarrow \infty$.

Thus there exists a sequence of $(2^{nR}, n)$ lossless source codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$

- Remarks:
 - Of course we already know how to construct a sequence of optimal lossless source codes by uniquely labeling each typical sequence
 - The covering proof for the lossless source coding theorem, however, will prove useful later (see Lecture Notes 12). It also shows that random coding can be used for *all* information theoretic settings. Such unification shows the power of random coding and is aesthetically pleasing

Covering Lemma

- We generalize the bound on the probability of encoding error, $P(\mathcal{E})$, in the proof of achievability for subsequent use in achievability proofs for multiple user source and channel settings
- Let $(U, X, \hat{X}) \sim p(u, x, \hat{x})$. Let $(U^n, X^n) \sim p(u^n, x^n)$ be a pair of arbitrarily distributed random sequences such that $P\{(U^n, X^n) \in \mathcal{T}_\epsilon^{(n)}(U, X)\} \rightarrow 1$ as $n \rightarrow \infty$ and let $\hat{X}^n(m), m \in \mathcal{A}$, where $|\mathcal{A}| \geq 2^{nR}$, be random sequences, conditionally independent of each other and of X^n given U^n , each distributed according to $\prod_{i=1}^n p_{\hat{X}|U}(\hat{x}_i|u_i)$

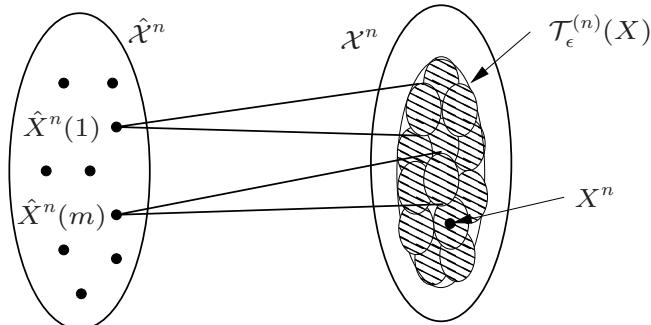
Then, there exists $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$ such that

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

as $n \rightarrow \infty$, if $R > I(X; \hat{X}|U) + \delta(\epsilon)$

- Remark: For the lossy source coding case, we have $U = \emptyset$

- The lemma is illustrated in the figure with $U = \emptyset$. The random sequences $\hat{X}^n(m), m \in \mathcal{A}$, represent reproduction sequences and X^n represents the source sequence. The lemma shows that if $R > I(X; \hat{X}|U)$ then there is at least one reproduction sequence that is jointly typical with X^n . This is the dual setting to the packing lemma, where we wanted none of the wrong codewords to be jointly typical with the received sequence



- Remark: The lemma continues to hold even when independence among all $\hat{X}^n(m), m \in \mathcal{A}$ is replaced with pairwise independence (cf. the mutual covering lemma in Lecture Notes 9)

- Proof: Define the event

$$\mathcal{E}_0 := \{(U^n, X^n) \notin \mathcal{T}_\epsilon^{(n)}\}$$

The probability of the event of interest can be upper bounded as

$$P(\mathcal{E}) \leq P(\mathcal{E}_0) + P(\mathcal{E} \cap \mathcal{E}_0^c)$$

By the condition of the lemma, $P(\mathcal{E}_0) \rightarrow 0$ as $n \rightarrow \infty$

For the second term, recall from the joint typicality lemma that if $(u^n, x^n) \in \mathcal{T}_\epsilon^{(n)}$, then

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

for each $m \in \mathcal{A}$, where $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$. Hence

$$\begin{aligned} & P(\mathcal{E} \cap \mathcal{E}_0^c) \\ &= \sum_{(u^n, x^n) \in \mathcal{T}_\epsilon^{(n)}} p(u^n, x^n) P\{(u^n, x^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m | U^n = u^n, X^n = x^n\} \\ &= \sum_{(u^n, x^n) \in \mathcal{T}_\epsilon^{(n)}} p(u^n, x^n) \prod_{m \in \mathcal{A}} P\{(u^n, x^n, \hat{X}^n(m)) \notin \mathcal{T}_\epsilon^{(n)} | U^n = u^n\} \\ &\leq \left[1 - 2^{-n(I(X; \hat{X}|U) + \delta(\epsilon))}\right]^{|\mathcal{A}|} \leq e^{-\left(|\mathcal{A}| \cdot 2^{-n(I(X; \hat{X}|U) + \delta(\epsilon))}\right)} \leq e^{-\left(2^{n(R - I(X; \hat{X}|U) - \delta(\epsilon))}\right)}, \end{aligned}$$

which goes to zero as $n \rightarrow \infty$, provided that $R > I(X; \hat{X}|U) + \delta(\epsilon)$

Quadratic Gaussian Source Coding

- Let X be a $\text{WGN}(P)$ source, that is, a source that generates a $\text{WGN}(P)$ random process $\{X_i\}$
- Consider a lossy source coding problem for the source X with *quadratic (squared error) distortion*

$$d(x, \hat{x}) = (x - \hat{x})^2$$

This is the most popular continuous-alphabet lossy source coding setting

- *Theorem 6:* The rate-distortion function for a $\text{WGN}(P)$ source with quadratic distortion is

$$R(D) = \begin{cases} \frac{1}{2} \log \left(\frac{P}{D} \right) & \text{for } 0 \leq D < P, \\ 0 & \text{for } D \geq P \end{cases}$$

Define $R(x) := (1/2) \log(x)$, if $x \geq 1$, and 0, otherwise. Then $R(D) = R(P/D)$

- Proof of converse: By the rate-distortion theorem, we have

$$R(D) = \min_{F(\hat{x}|x): E((\hat{x}-x)^2) \leq D} I(X; \hat{X})$$

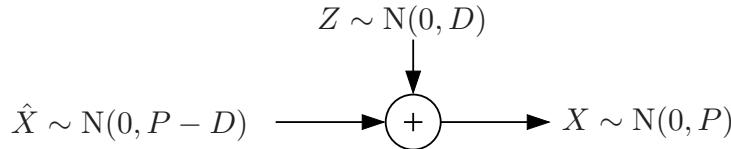
If we want $D \geq P$, then we set $\hat{X} = E(X) = 0$. Thus $R(D) = 0$

If $0 \leq D < P$, we first find a lower bound on the rate-distortion function and then prove that there exists a test channel that achieves it. Consider

$$\begin{aligned} I(X; \hat{X}) &= h(X) - h(X | \hat{X}) \\ &= \frac{1}{2} \log(2\pi e P) - h(X - \hat{X} | \hat{X}) \\ &\geq \frac{1}{2} \log(2\pi e P) - h(X - \hat{X}) \\ &\geq \frac{1}{2} \log(2\pi e P) - \frac{1}{2} \log(2\pi e E[(X - \hat{X})^2]) \\ &\geq \frac{1}{2} \log(2\pi e P) - \frac{1}{2} \log(2\pi e D) = \frac{1}{2} \log \frac{P}{D} \end{aligned}$$

The last step follows since $E[(X - \hat{X})^2] \leq D$

It is easy to show that this bound is achieved by the following “backward” AWGN test channel and that the associated expected distortion is D



- Proof of achievability: There are several ways to prove achievability for continuous sources and unbounded distortion measures [13, 14, 15, 8]. We show how the achievability for finite sources can be extended to the case of a Gaussian source with quadratic distortion [9]

- Let D be the desired distortion and let (X, \hat{X}) be a pair of jointly Gaussian random variables achieving $R((1 - 2\epsilon)D)$ with distortion $E[(X - \hat{X})^2] = (1 - 2\epsilon)D$

Let $[X]$ and $[\hat{X}]$ be finitely quantized versions of X and \hat{X} , respectively, such that

$$E[(X - [X])^2] \leq (1 - \epsilon)^2 D \text{ and } E[(X - [X])^2] \leq \epsilon^2 D$$

- Define $R'(D)$ to be the rate-distortion function for the finite alphabet source $[X]$ with reproduction random variable $[\hat{X}]$ and quadratic distortion. Then, by the data processing inequality

$$R'((1 - \epsilon)^2 D) \leq I([X]; [\hat{X}]) \leq I(X; \hat{X}) = R((1 - 2\epsilon)D)$$

- Hence, by the achievability proof for DMSs, there exists a sequence of $(2^{nR}, n)$ rate-distortion codes with asymptotic distortion

$$\limsup_{n \rightarrow \infty} (1/n) E[d([X]^n, [\hat{X}]^n)] \leq (1 - \epsilon^2) D$$

if $R > R((1 - 2\epsilon)D) \geq R'((1 - \epsilon)^2 D)$

- We use this sequence of codes for the original source X by mapping each x^n to the codeword $[\hat{x}]^n$ assigned to $[x]^n$. Thus

$$\begin{aligned}
\mathbb{E} \left(d(X^n, [\hat{X}]^n) \right) &= \frac{1}{n} \sum_{i=1}^n \mathbb{E} \left[(X_i - [\hat{X}]_i)^2 \right] \\
&= \frac{1}{n} \sum_{i=1}^n \mathbb{E} \left[\left((X_i - [X_i]) + ([X_i] - [\hat{X}]_i) \right)^2 \right] \\
&\leq \frac{1}{n} \sum_{i=1}^n \left[\mathbb{E} \left((X_i - [X_i])^2 \right) + \mathbb{E} \left(([X_i] - [\hat{X}]_i)^2 \right) \right] \\
&\quad + \frac{2}{n} \sum_{i=1}^n \sqrt{\mathbb{E} \left[(X_i - [X_i])^2 \right] \mathbb{E} \left[([X_i] - [\hat{X}]_i)^2 \right]} \\
&\leq \epsilon^2 D + (1 - \epsilon)^2 D + 2\epsilon(1 - \epsilon)D = D
\end{aligned}$$

- Thus $R > R((1 - 2\epsilon)D)$ is achievable for distortion D , and hence by the continuity of $R(D)$, we have the desired proof of achievability

Joint Source–Channel Coding

- Let $(\mathcal{U}, p(u))$ be a DMS, $(\mathcal{X}, p(y|x), \mathcal{Y})$ be a DMC with capacity C , and $d(x, \hat{x})$ be a distortion measure
- We wish to send the source U over the DMC at a rate of r source symbols per channel transmission ($k/n = r$ in the figure) so that the decoder can reconstruct it with average distortion D



- A $(|\mathcal{U}|^k, n)$ joint source–channel code of rate $r = k/n$ consists of:
 1. An encoder that assigns a sequence $x^n(u^k) \in \mathcal{X}^n$ to each sequence $u^k \in \mathcal{U}^k$, and
 2. 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
$$\limsup_{k \rightarrow \infty} \mathbb{E}[d(U^k, \hat{U}^k(Y^n))] \leq D$$

- *Shannon's Source–Channel Separation Theorem* [12]: Given a DMS $(\mathcal{U}, p(u))$, DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$, and distortion measure $d(u, \hat{u})$:
 - if $rR(D) < C$, then (r, D) is achievable, and
 - if (r, D) is achievable, then $rR(D) \leq C$
- Outline 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 $R(D) + \delta(\epsilon)$ that achieve average distortion $\leq D$
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 transmitted over the channel provided $r(R(D) + \delta(\epsilon)) \leq C - \delta'(\epsilon)$
 - The source decoder finds the reconstruction sequence corresponding to the received index. If the channel decoder makes an error, the distortion is $\leq d_{\max}$. Because the probability of error approaches 0 with n , the overall average distortion is $\leq D$

- Proof of converse: We wish to show that if a sequence of codes that achieves the rate–distortion pair (r, D) , then $rR(D) \leq C$

From the converse of the rate–distortion theorem, we know that

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

Now, by the data processing inequality and steps of the converse of the channel coding theorem (we do not need Fano's inequality here), we have

$$\begin{aligned} \frac{1}{k} I(U^k; \hat{U}^k) &\leq \frac{1}{k} I(X^n; Y^n) \\ &\leq \frac{1}{r} C \end{aligned}$$

Combining the above inequalities completes the proof of the converse

- Remarks:
 - A special case of the separation theorem for sending U losslessly over a DMC, i.e., with probability of error $P\{\hat{U}^k \neq U^k\} \rightarrow 0$, yields the requirement that $rH(U) \leq C$
 - Moral: There is no benefit in terms of highest achievable rate r of *jointly* coding for the source and channel. In a sense, “bits” can be viewed as a universal currency for point-to-point communication. This is not, in general, the case for multiple user source–channel coding
 - The separation theorem holds for sending any stationary ergodic source over a DMC

Uncoded Transmission

- Sometimes joint source–channel coding simplifies coding
Example: Consider sending a $\text{Bern}(1/2)$ source over a $\text{BSC}(p)$ at rate $r = 1$ with Hamming distortion $\leq D$
Separation theorem gives that $1 - H(D) < 1 - H(p)$, or $D > p$ can be achieved using separate source and channel coding
Uncoded transmission: Simply send the binary sequence over the channel
Average distortion $D \leq p$ is achieved
Similar uncoded transmission works also for sending a WGN source over an AWGN channel with quadratic distortion (with proper scaling to satisfy the power constraint)
- General conditions for optimality of uncoded transmission [16]: A DMS $(\mathcal{U}, p(u))$ can be optimally sent over a DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ uncoded, i.e., $C = R(D)$, if
 1. the test channel $p_{Y|X}(\hat{u}|u)$ achieves the rate–distortion function $R(D) = \min_{p(\hat{u}|u)} I(U; \hat{U})$ of the source, and
 2. $X \sim p_U(x)$ achieves the capacity $C = \max_{p(x)} I(X; Y)$ of the channel

Key Ideas and Techniques

- Digital communication system architecture
- Channel capacity is the limit on channel coding
- Random codebook generation
- Joint typicality decoding
- Packing lemma
- Fano's inequality
- Capacity with cost
- Capacity of AWGN channel (how to go from discrete to continuous alphabet)
- 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 of WGN source with quadratic distortion
- Lossless source coding is a special case of lossy source coding
- Source–channel separation
- Uncoded transmission can be optimal

References

- [1] C. E. Shannon, "A mathematical theory of communication," *Bell System Tech. J.*, vol. 27, pp. 379–423, 623–656, 1948.
- [2] G. D. Forney, Jr., "Information theory," 1972, unpublished course notes, Stanford University, 1972.
- [3] A. Feinstein, "A new basic theorem of information theory," *IRE Trans. Inf. Theory*, vol. 4, pp. 2–22, 1954.
- [4] R. G. Gallager, "A simple derivation of the coding theorem and some applications," *IEEE Trans. Inf. Theory*, vol. 11, pp. 3–18, 1965.
- [5] ———, *Information Theory and Reliable Communication*. New York: Wiley, 1968.
- [6] ———, *Low-Density Parity-Check Codes*. Cambridge, MA: MIT Press, 1963.
- [7] T. Richardson and R. Urbanke, *Modern Coding Theory*. Cambridge: Cambridge University Press, 2008.
- [8] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley, 2006.
- [9] R. J. McEliece, *The Theory of Information and Coding*. Reading, MA: Addison-Wesley, 1977.
- [10] A. D. Wyner, "The capacity of the band-limited Gaussian channel," *Bell System Tech. J.*, vol. 45, pp. 359–395, Mar. 1966.
- [11] M. J. E. Golay, "Note on the theoretical efficiency of information reception with PPM," *Proc. IRE*, vol. 37, no. 9, p. 1031, Sept. 1949.

- [12] C. E. Shannon, "Coding theorems for a discrete source with a fidelity criterion," in *IRE Int. Conv. Rec., part 4*, 1959, vol. 7, pp. 142–163, reprinted with changes in *Information and Decision Processes*, R. E. Machol, Ed. New York: McGraw-Hill, 1960, pp. 93–126.
- [13] T. Berger, "Rate distortion theory for sources with abstract alphabets and memory." *Inf. Control*, vol. 13, pp. 254–273, 1968.
- [14] J. G. Dunham, "A note on the abstract-alphabet block source coding with a fidelity criterion theorem," *IEEE Trans. Inf. Theory*, vol. 24, no. 6, p. 760, 1978.
- [15] J. A. Bucklew, "The source coding theorem via Sanov's theorem," *IEEE Trans. Inf. Theory*, vol. 33, no. 6, pp. 907–909, 1987.
- [16] M. Gastpar, B. Rimoldi, and M. Vetterli, "To code, or not to code: lossy source-channel communication revisited," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1147–1158, 2003.

Appendix: Proof of Lemma 2

- We first note that $I([X]_j; [Y_j]_k) \rightarrow I([X]_j; Y_j) = h(Y_j) - h(Z)$ as $k \rightarrow \infty$. This follows since $([Y_j]_k - Y_j) \rightarrow 0$ as $k \rightarrow \infty$ (cf. Lecture Notes 2)
- Hence it suffices to show that

$$\liminf_{j \rightarrow \infty} h(Y_j) \geq h(Y)$$

- The pdf of Y_j converges pointwise to that of $Y \sim N(0, S + 1)$. To prove this, note that

$$f_{Y_j}(y) = \int f_Z(y - x) dF_{[X]_j}(x) = E(f_Z(y_j - [X]_j))$$

Since the Gaussian pdf $f_Z(z)$ is continuous and bounded, $f_{Y_j}(y)$ converges to $f_Y(y)$ by the weak convergence of $[X]_j$ to X

- Furthermore, we have

$$f_{Y_j}(y) = E[f_Z(y - X_j)] \leq \max_z f_Z(z) = \frac{1}{\sqrt{2\pi}}$$

Hence, for each $T > 0$, by the dominated convergence theorem (Appendix A),

$$\begin{aligned} h(Y_j) &= \int_{-\infty}^{\infty} -f_{Y_j}(y) \log f_{Y_j}(y) dy \\ &\geq \int_{-T}^T -f_{Y_j}(y) \log f_{Y_j}(y) dy + P\{|Y_j| \geq T\} \cdot \left(\min_y (-\log f_{Y_j}(y)) \right) \\ &\rightarrow \int_{-T}^T -f(y) \log f(y) dy + P\{|Y| \geq T\} \cdot \left(\min_y (-\log f(y)) \right) \end{aligned}$$

as $j \rightarrow \infty$. Taking $T \rightarrow \infty$, we obtain the desired result

Part II. Single-hop Networks

Lecture Notes 4

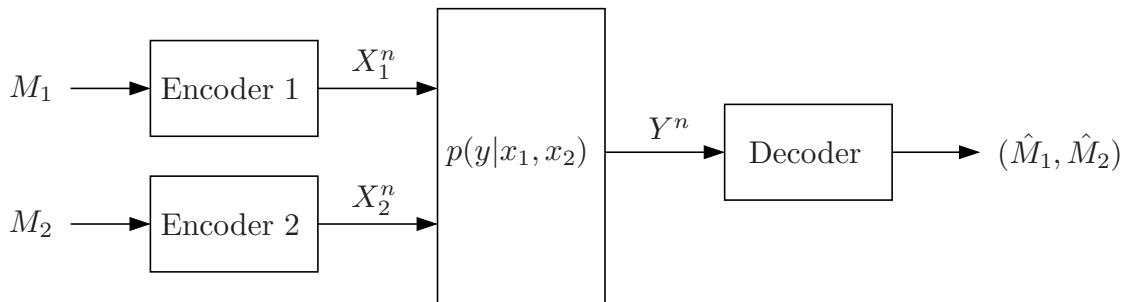
Multiple Access Channels

- Problem Setup
- Simple Inner and Outer Bounds on the Capacity Region
- Multi-letter Characterization of the Capacity Region
- Time Sharing
- Single-Letter Characterization of the Capacity Region
- AWGN Multiple Access Channel
- Comparison to Point-to-Point Coding Schemes
- Extension to More Than Two Senders
- Key New Ideas and Techniques

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- A 2-sender *discrete memoryless multiple access channel* (DM-MAC) $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$ consists of three finite sets \mathcal{X}_1 , \mathcal{X}_2 , \mathcal{Y} , and a collection of conditional pmfs $p(y|x_1, x_2)$ on \mathcal{Y}
- The senders X_1 and X_2 wish to send independent messages M_1 and M_2 , respectively, to the receiver Y



- A $(2^{nR_1}, 2^{nR_2}, n)$ code for a DM-MAC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$ consists of:
 1. Two message sets $[1 : 2^{nR_1}]$ and $[1 : 2^{nR_2}]$

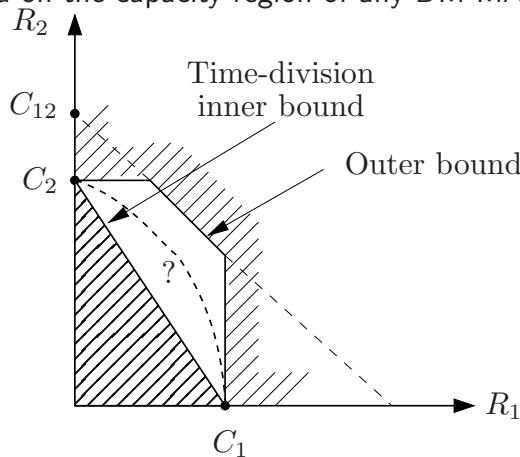
2. Two encoders: Encoder 1 assigns a codeword $x_1^n(m_1)$ to each message $m_1 \in [1 : 2^{nR_1}]$ and encoder 2 assigns a codeword $x_2^n(m_2)$ to each message $m_2 \in [1 : 2^{nR_2}]$
 3. A decoder that assigns an estimate $(\hat{m}_1, \hat{m}_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$ or an error message e to each received sequence y^n
- We assume that the message pair (M_1, M_2) is uniformly distributed over $[1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$. Thus, $x_1^n(M_1)$ and $x_2^n(M_2)$ are independent
 - The average probability of error is defined as
- $$P_e^{(n)} = P\{(\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\}$$
- A rate pair (R_1, R_2) is said to be *achievable* for the DM-MAC if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
 - The *capacity region* \mathcal{C} of the DM-MAC is the closure of the set of achievable rate pairs (R_1, R_2)

Simple Inner and Outer Bounds on the Capacity Region

- Note that the maximum achievable individual rates are:
$$C_1 := \max_{x_2, p(x_1)} I(X_1; Y | X_2 = x_2), \quad C_2 := \max_{x_1, p(x_2)} I(X_2; Y | X_1 = x_1)$$
- Also following similar steps to the converse proof of the point-to-point channel coding theorem, we can show that the maximum sum rate is upper bounded by

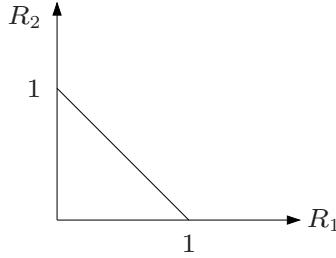
$$R_1 + R_2 \leq C_{12} := \max_{p(x_1)p(x_2)} I(X_1, X_2; Y)$$

- Using these rates, we can derive the following *time-division* inner bound and general outer bound on the capacity region of any DM-MAC



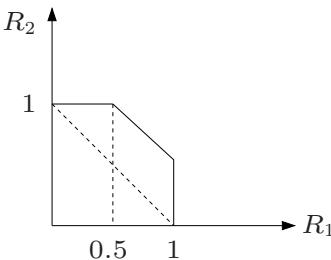
Examples

- *Binary multiplier DM-MAC*: X_1, X_2 are binary, $Y = X_1 \cdot X_2$ is binary



Inner and outer bounds coincide

- *Binary erasure DM-MAC*: X_1, X_2 are binary, $Y = X_1 + X_2$ is ternary



Inner and outer bounds do not coincide (the outer bound is the capacity region)

- The above inner and outer bounds are *not* tight in general

Multi-letter Characterization of the Capacity Region

- *Theorem 1 [1]*: Let \mathcal{C}_k , $k \geq 1$, be the set of rate pairs (R_1, R_2) such that

$$R_1 \leq \frac{1}{k} I(X_1^k; Y^k), \quad R_2 \leq \frac{1}{k} I(X_2^k; Y^k)$$

for some joint pmf $p(x_1^k)p(x_2^k)$. Then the capacity region \mathcal{C} of the DM-MAC is $\mathcal{C} = \cup_k \mathcal{C}_k$

- Proof of achievability: We use k symbols of \mathcal{X}_1 and \mathcal{X}_2 (super-letters) together and code over them. Fix $p(x_1^k)p(x_2^k)$. Using a random coding argument with randomly and independently generated codeword pairs $(x_1^{nk}(m_1), x_2^{nk}(m_2))$, $(m_1, m_2) \in [1 : 2^{nkR_1}] \times [1 : 2^{nkR_2}]$, each according to $\prod_{i=1}^n p_{X_1^k}(x_{1,(i-1)k+1}^k) p_{X_2^k}(x_{2,(i-1)k+1}^k)$, and joint typicality decoding, it can be readily shown that any rate pair (R_1, R_2) such that $kR_1 < I(X_1^k; Y^k)$ and $kR_2 < I(X_2^k; Y^k)$ is achievable

- Proof of converse: Using Fano's inequality, we can show that

$$R_1 \leq \frac{1}{n} I(X_1^n; Y^n) + \epsilon_n, \quad R_2 \leq \frac{1}{n} I(X_2^n; Y^n) + \epsilon_n,$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$. This shows that (R_1, R_2) must be in \mathcal{C}

- Even though the above “multi-letter” (or “infinite-letter”) characterization of the capacity region is well-defined, it is not clear how to compute it. Further, this characterization does not provide any insight into how to best code for a multiple access channel
- Such “multi-letter” expressions can be readily obtained for other multiple user channels and sources, leading to a fairly complete but generally unsatisfactory theory
- Consequently information theorists seek computable “single-letter” characterizations of capacity, such as Shannon’s capacity expression for the point-to-point channel, that shed light on practical coding techniques
- Single-letter characterizations, however, have been difficult to find for most multiple user channels and sources. The DM-MAC is one of the few channels for which a complete “single-letter” characterization has been found

Time Sharing

- Suppose the rate pairs (R_1, R_2) and (R'_1, R'_2) are achievable for a DM-MAC. We use the following *time sharing* argument to show that $(\alpha R_1 + \bar{\alpha} R'_1, \alpha R_2 + \bar{\alpha} R'_2)$ is achievable for any $\alpha \in [0, 1]$
 - Consider two sequences of codes, one achieving (R_1, R_2) and the other achieving (R'_1, R'_2)
 - For any block length n , let $k = \lfloor \alpha n \rfloor$ and $k' = n - k$. The $(2^{kR_1+k'R'_1}, 2^{kR_2+k'R'_2}, n)$ “time sharing” code is obtained by using the $(2^{kR_1}, 2^{kR_2}, k)$ code from the first sequence in the first k transmissions and the $(2^{k'R'_1}, 2^{k'R'_2}, k')$ code from the second in the remaining k' transmissions
 - Decoding: y^k is decoded using the decoder for the $(2^{kR_1}, 2^{kR_2}, k)$ code and y_{k+1}^n is decoded using the decoder for the $(2^{k'R'_1}, 2^{k'R'_2}, k')$ code
 - Clearly $(\alpha R_1 + \bar{\alpha} R'_1, \alpha R_2 + \bar{\alpha} R'_2)$ is achievable

- Remarks:
 - This time-sharing argument shows that the capacity region of the DM-MAC is convex. Note that this proof uses the *operational* definition of the capacity region (as opposed to the information definition in terms of mutual information)
 - Similar time sharing arguments can be used to show the convexity of the capacity region of *any* (synchronous) channel for which capacity is defined as the optimal rate of block codes, e.g., capacity with cost constraint, as well as optimal rate regions for source coding problems, e.g., rate-distortion function in Lecture Notes 3. As we show later in Lecture Notes 24, the capacity region of the DM-MAC may not be convex when the sender transmissions are not synchronized because time sharing cannot be used
 - Time-division and frequency-division multiple access are special cases of time sharing, where in each transmission only one sender is allowed to transmit at a nonzero rate, i.e., time sharing between $(R_1, 0)$ and $(0, R_2)$

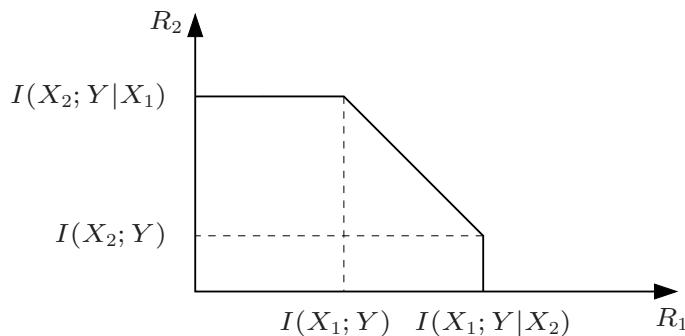
Single-Letter Characterization of the Capacity Region

- Let $(X_1, X_2) \sim p(x_1)p(x_2)$. Define $\mathcal{R}(X_1, X_2)$ as the set of (R_1, R_2) rate pairs such that

$$\begin{aligned} R_1 &\leq I(X_1; Y | X_2), \quad R_2 \leq I(X_2; Y | X_1), \\ R_1 + R_2 &\leq I(X_1, X_2; Y) \end{aligned}$$

- This set is in general a pentagon with a 45° side because

$$\max\{I(X_1; Y | X_2), I(X_2; Y | X_1)\} \leq I(X_1, X_2; Y) \leq I(X_1; Y | X_2) + I(X_2; Y | X_1)$$



- *Theorem 2* (Ahlswede [2], Liao [3]): The capacity region \mathcal{C} for the DM-MAC is the *convex closure* of the union of the regions $\mathcal{R}(X_1, X_2)$ over all $p(x_1)p(x_2)$

- For example, consider the binary erasure MAC. It can be easily shown that the simple outer bound is the capacity region and is attained by setting X_1, X_2 as $\text{Bern}(1/2)$ (check)

Proof of Achievability

- Fix $(X_1, X_2) \sim p(x_1)p(x_2)$. We show that any rate pair (R_1, R_2) in the interior of $\mathcal{R}(X_1, X_2)$ is achievable

The rest of the capacity region can be achieved using time sharing

- Assume nR_1 and nR_2 to be integers
- Codebook generation: Randomly and independently generate 2^{nR_1} sequences $x_1^n(m_1)$, $m_1 \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{X_1}(x_{1i})$. Similarly generate 2^{nR_2} sequences $x_2^n(m_2)$, $m_2 \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_{X_2}(x_{2i})$

These codewords form the codebook, which is revealed to the encoders and the decoder

- Encoding: To send message m_1 , encoder 1 transmits $x_1^n(m_1)$
Similarly, to send m_2 , encoder 2 transmits $x_2^n(m_2)$
- In the following, we consider two decoding rules

Successive Cancellation Decoding

- This decoding rule aims to achieve the two *corner points* of the pentagon $\mathcal{R}(X_1, X_2)$, e.g., $R_1 < I(X_1; Y)$, $R_2 < I(X_2; Y|X_1)$
- Decoding is performed in two steps:
 1. The decoder declares that \hat{m}_1 is sent if it is the unique message such that $(x_1^n(\hat{m}_1), y^n) \in \mathcal{T}_\epsilon^{(n)})$; otherwise it declares an error
 2. If such \hat{m}_1 is found, the decoder finds the unique \hat{m}_2 such that $(x_1^n(\hat{m}_1), x_2^n(\hat{m}_2), y^n) \in \mathcal{T}_\epsilon^{(n)})$; otherwise it declares an error
- Analysis of the probability of error: We bound the probability of error averaged over codebooks and messages. By symmetry of code generation

$$P(\mathcal{E}) = P(\mathcal{E}|M_1 = 1, M_2 = 1)$$

- A decoding error occurs only if

$$\begin{aligned}\mathcal{E}_1 &:= \{(X_1^n(1), X_2^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \text{ or} \\ \mathcal{E}_2 &:= \{(X_1^n(m_1), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1\}, \text{ or} \\ \mathcal{E}_3 &:= \{(X_1^n(1), X_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_2 \neq 1\}\end{aligned}$$

Then, by the union of events bound $P(\mathcal{E}) \leq P\{\mathcal{E}_1\} + P(\mathcal{E}_2) + P(\mathcal{E}_3)$

- By the LLN, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$
- Since for $m \neq 1$, $(X_1^n(m_1), Y^n) \sim \prod_{i=1}^n p_{X_1}(x_{1i})p_Y(y_i)$, by the packing lemma (with $|\mathcal{A}| = 2^{nR_1} - 1$, $U = \emptyset$), $P(\mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X_1; Y) - \delta(\epsilon)$
- Since for $m_2 \neq 1$, $X_2^n(m_2) \sim \prod_{i=1}^n p_{X_2}(x_{2i})$ is independent of $(X_1^n(1), Y^n) \sim \prod_{i=1}^n p_{X_1,Y}(x_{1i}, y_i)$, by the packing lemma (with $|\mathcal{A}| = 2^{nR_2} - 1$, $Y \leftarrow (X_1, Y)$, $U = \emptyset$), $P(\mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$ if $R_2 < I(X_2; Y|X_1) - \delta(\epsilon) = I(X_2; Y|X_1) - \delta(\epsilon)$, since X_1, X_2 are independent
- Thus the total average probability of decoding error $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X_1; Y) - \delta(\epsilon)$ and $R_2 < I(X_2; Y|X_1) - \delta(\epsilon)$
- Achievability of the other corner point follows by changing the decoding order
- To show achievability of other points in $\mathcal{R}(X_1, X_2)$, we use time sharing between corner points and points on the axes
- Finally, to show achievability of points not in any $\mathcal{R}(X_1, X_2)$, we use time sharing between points in different $\mathcal{R}(X_1, X_2)$ regions

Simultaneous Joint Typicality Decoding

- We can prove achievability of every rate pair in the interior of $\mathcal{R}(X_1, X_2)$ without time sharing
- The decoder declares that (\hat{m}_1, \hat{m}_2) is sent if it is the unique message pair such that $(x_1^n(\hat{m}_1), x_2^n(\hat{m}_2), y^n) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error
- Analysis of the probability of error: We bound the probability of error averaged over codebooks and messages
- To divide the error event, let's look at all possible pmfs for the triple $(X_1^n(m_1), X_2^n(m_2), Y^n)$

m_1	m_2	Joint pmf
1	1	$p(x_1^n)p(x_2^n)p(y^n x_1^n, x_2^n)$
*	1	$p(x_1^n)p(x_2^n)p(y^n x_2^n)$
1	*	$p(x_1^n)p(x_2^n)p(y^n x_1^n)$
*	*	$p(x_1^n)p(x_2^n)p(y^n)$

* here means $\neq 1$

- Then, the error event \mathcal{E} occurs iff

$$\begin{aligned}\mathcal{E}_1 &:= \{(X_1^n(1), X_2^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \text{ or} \\ \mathcal{E}_2 &:= \{(X_1^n(m_1), X_2^n(1), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1\}, \text{ or} \\ \mathcal{E}_3 &:= \{(X_1^n(1), X_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_2 \neq 1\}, \text{ or} \\ \mathcal{E}_4 &:= \{(X_1^n(m_1), X_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1, m_2 \neq 1\}\end{aligned}$$
 Thus, $P(\mathcal{E}) \leq \sum_{j=1}^4 P(\mathcal{E}_j)$
- We now bound each term:
 - By the LLN, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$
 - By the packing lemma, $P(\mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X_1; Y|X_2) - \delta(\epsilon)$
 - Similarly, $P(\mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$ if $R_2 < I(X_2; Y|X_1) - \delta(\epsilon)$
 - Finally, since for $m_1 \neq 1, m_2 \neq 1$, $(X_1^n(m_1), X_2^n(m_2))$ is independent of $(X_1^n(1), X_2^n(1), Y^n)$, again by the packing lemma, $P(\mathcal{E}_4) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 + R_2 < I(X_1, X_2; Y) - \delta(\epsilon)$
 - Therefore, simultaneous decoding is more powerful than successive cancellation decoding because we don't need time sharing to achieve points in $\mathcal{R}(X_1, X_2)$

- As in successive cancellation decoding, to show achievability of points not in any $\mathcal{R}(X_1, X_2)$, we use time sharing between points in different $\mathcal{R}(X_1, X_2)$ regions
- Since the probability of error averaged over all codebooks $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$, there must exist a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^{(n)} \rightarrow 0$
- Remarks:
 - Unlike the capacity of a DMC, the capacity region of a DM-MAC for maximal probability of error can be strictly smaller than the capacity region for average probability of error (see Dueck [4]). However, by allowing randomization at the encoders, the maximal probability of error capacity region can be shown to be equal to the average probability of error capacity region

Proof of Converse

- We need to show that given any sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^{(n)} \rightarrow 0$, $(R_1, R_2) \in \mathcal{C}$ as defined in Theorem 2
- Each code induces the joint pmf

$$(M_1, M_2, X_1^n, X_2^n, Y^n) \sim 2^{-n(R_1+R_2)} \cdot p(x_1^n | m_1)p(x_2^n | m_2)p(y^n | x_1^n, x_2^n)$$

- By Fano's inequality,

$$H(M_1, M_2 | Y^n) \leq n(R_1 + R_2)P_e^{(n)} + 1 \leq n\epsilon_n,$$

where $\epsilon_n \rightarrow 0$ as $P_e^{(n)} \rightarrow 0$

- Using similar steps to those used in the converse proof for the DMC coding theorem, it is easy to show that

$$n(R_1 + R_2) \leq \sum_{i=1}^n I(X_{1i}, X_{2i}; Y_i) + n\epsilon_n$$

- Next note that

$$H(M_1 | Y^n, M_2) \leq H(M_1, M_2 | Y^n) \leq n\epsilon_n$$

Consider

$$\begin{aligned}
nR_1 &= H(M_1) = H(M_1|M_2) = I(M_1; Y^n|M_2) + H(M_1|Y^n, M_2) \\
&\leq I(M_1; Y^n|M_2) + n\epsilon_n \\
&= \sum_{i=1}^n I(M_1; Y_i|Y^{i-1}, M_2) + n\epsilon_n \\
&\stackrel{(a)}{=} \sum_{i=1}^n I(M_1; Y_i|Y^{i-1}, M_2, X_{2i}) + n\epsilon_n \\
&\leq \sum_{i=1}^n I(M_1, M_2, Y^{i-1}; Y_i|X_{2i}) + n\epsilon_n \\
&\stackrel{(b)}{=} \sum_{i=1}^n I(X_{1i}, M_1, M_2, Y^{i-1}; Y_i|X_{2i}) + n\epsilon_n \\
&= \sum_{i=1}^n I(X_{1i}; Y_i|X_{2i}) + \sum_{i=1}^n I(M_1, M_2, Y^{i-1}; Y_i|X_{1i}, X_{2i}) + n\epsilon_n \\
&\stackrel{(c)}{=} \sum_{i=1}^n I(X_{1i}; Y_i|X_{2i}) + n\epsilon_n,
\end{aligned}$$

where (a) and (b) follow because X_{ji} is a function of M_j for $j = 1, 2$, respectively, and (c) follows by the memoryless property of the channel, which implies that $(M_1, M_2, Y^{i-1}) \rightarrow (X_{1i}, X_{2i}) \rightarrow Y_i$ form a Markov chain

- Hence, we have

$$\begin{aligned}
R_1 &\leq \frac{1}{n} \sum_{i=1}^n I(X_{1i}; Y_i|X_{2i}) + \epsilon_n, \\
R_2 &\leq \frac{1}{n} \sum_{i=1}^n I(X_{2i}; Y_i|X_{1i}) + \epsilon_n, \\
R_1 + R_2 &\leq \frac{1}{n} \sum_{i=1}^n I(X_{1i}, X_{2i}; Y_i) + \epsilon_n
\end{aligned}$$

Since M_1 and M_2 are independent, so are $X_{1i}(M_1)$ and $X_{2i}(M_2)$ for all i

- Remark: Bounding each of the above terms by its corresponding capacity, i.e., C_1 , C_2 , and C_{12} , respectively, yields the simple outer bound we presented earlier, which is in general larger than the inner bound we established

- Let the random variable $Q \sim \text{Unif}[1 : n]$ be independent of (X_1^n, X_2^n, Y^n) . Then, we can write

$$\begin{aligned} R_1 &\leq \frac{1}{n} \sum_{i=1}^n I(X_{1i}; Y_i | X_{2i}) + \epsilon_n \\ &= \frac{1}{n} \sum_{i=1}^n I(X_{1i}; Y_i | X_{2i}, Q = i) + \epsilon_n \\ &= I(X_{1Q}; Y_Q | X_{2Q}, Q) + \epsilon_n \end{aligned}$$

We now observe that $Y_Q | \{X_{1Q} = x_1, X_{2Q} = x_2\} \sim p_{Y|X_1, X_2}(y|x_1, x_2)$, i.e., it is distributed according to the channel conditional pmf. Hence we identify $X_1 := X_{1Q}$, $X_2 := X_{2Q}$, and $Y := Y_Q$ to obtain

$$R_1 \leq I(X_1; Y | X_2, Q) + \epsilon_n$$

- Thus (R_1, R_2) must be in the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y | X_2, Q) + \epsilon_n,$$

$$R_2 \leq I(X_2; Y | X_1, Q) + \epsilon_n,$$

$$R_1 + R_2 \leq I(X_1, X_2; Y | Q) + \epsilon_n$$

for some $Q \sim \text{Unif}[1 : n]$ and pmf $p(x_1|q)p(x_2|q)$ and hence for some joint pmf $p(q)p(x_1|q)p(x_2|q)$ with Q taking values in some finite set

- Since $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$, we have shown that (R_1, R_2) must be in the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y | X_2, Q),$$

$$R_2 \leq I(X_2; Y | X_1, Q),$$

$$R_1 + R_2 \leq I(X_1, X_2; Y | Q)$$

for some joint pmf $p(q)p(x_1|q)p(x_2|q)$ with Q in some finite set

- Remark: Q is referred to as a *time sharing* random variable. It is an *auxiliary* random variable, that is, a random variable that is not part of the channel variables
- Denote the above region by \mathcal{C}' . To complete the proof of the converse, we need to show that $\mathcal{C}' = \mathcal{C}$
- We already know that $\mathcal{C} \subseteq \mathcal{C}'$ (because we proved that any achievable rate pair must be in \mathcal{C}'). We can also see this directly:
 - \mathcal{C}' contains all $\mathcal{R}(X_1, X_2)$ sets
 - \mathcal{C}' also contains all points (R_1, R_2) in the convex closure of the union of these sets, since any such point can be represented as a convex combination of points in these sets using the time-sharing random variable Q

- It can be also shown that $\mathcal{C}' \subseteq \mathcal{C}$
 - Any joint pmf $p(q)p(x_1|q)p(x_2|q)$ defines a pentagon region with a 45° side. Thus it suffices to check whether the corner points of the pentagon are in \mathcal{C}
 - Consider the corner point $(R_1, R_2) = (I(X_1; Y|Q), I(X_2; Y|X_1, Q))$. It is easy to see that (R_1, R_2) belongs to \mathcal{C} , since it is a finite convex combination of $(I(X_1; Y|Q = q), I(X_2; Y|X_1, Q = q))$ points, each of which in turn belongs to $\mathcal{R}(X_{1q}, X_{2q})$ with $(X_{1q}, X_{2q}) \sim p(x_1|q)p(x_2|q)$. We can similarly show that the other corner points of the pentagon also belong to \mathcal{C}
- This shows that $\mathcal{C}' = \mathcal{C}$, which completes the proof of the converse
- But there is a problem. Neither \mathcal{C} nor \mathcal{C}' seems to be “computable”:
 - How many $\mathcal{R}(X_1, X_2)$ sets do we need to consider in computing each point on the boundary of \mathcal{C} ?
 - How large must the cardinality of \mathcal{Q} be to compute each point on the boundary of \mathcal{C}' ?

Bounding the Cardinality of \mathcal{Q}

- *Theorem 3 [5]:* The capacity region of the DM-MAC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$ is the set of (R_1, R_2) pairs satisfying

$$\begin{aligned} R_1 &\leq I(X_1; Y|X_2, Q), \\ R_2 &\leq I(X_2; Y|X_1, Q), \\ R_1 + R_2 &\leq I(X_1, X_2; Y|Q) \end{aligned}$$

for some $p(q)p(x_1|q)p(x_2|q)$ with the cardinality of Q bounded as $|\mathcal{Q}| \leq 2$

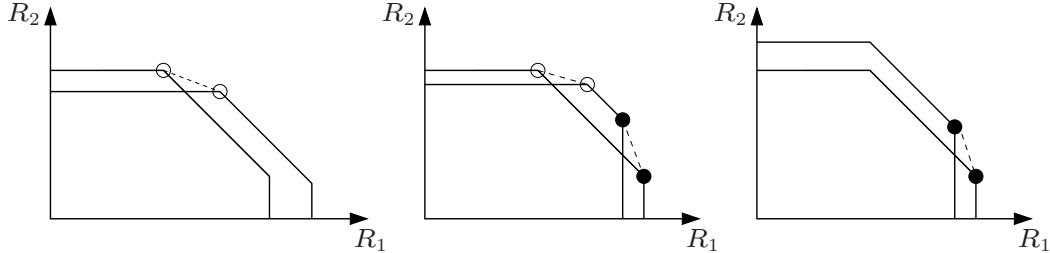
- Proof: We already know that the region \mathcal{C}' of Theorem 3 without the bound on the cardinality of Q is the capacity region. To establish the bound on $|\mathcal{Q}|$, we first consider some properties of the region \mathcal{C} in Theorem 2:
 1. Any pair (R_1, R_2) in \mathcal{C} is in the convex closure of the union of no more than two $\mathcal{R}(X_1, X_2)$ sets

To prove this, we use the Fenchel–Eggleston–Carathéodory theorem in Appendix A

Since the union of the $\mathcal{R}(X_1, X_2)$ sets is a connected compact set in \mathbb{R}^2 (why?), each point in its convex closure can be represented as a convex

combination of at most 2 points in the union, and thus each point is in the convex closure of the union of no more than two $\mathcal{R}(X_1, X_2)$ sets

2. Any point on the boundary of \mathcal{C} is either a boundary point of some $\mathcal{R}(X_1, X_2)$ set or a convex combination of the “upper-diagonal” or “lower-diagonal” corner points of two $\mathcal{R}(X_1, X_2)$ sets as shown below



- This shows that $|\mathcal{Q}| \leq 2$ suffices (why?)

- Remarks:

- It can be shown that time sharing is required for some DM-MACs, i.e., choosing $|\mathcal{Q}| = 1$ is not sufficient in general. An example is the push-to-talk MAC in the homework
- The maximum sum rate (sum capacity) for a DM-MAC can be written as

$$\begin{aligned} C &= \max_{p(q)p(x_1|q)p(x_2|q)} I(X_1, X_2; Y|Q) \\ &\stackrel{(a)}{=} \max_{p(x_1)p(x_2)} I(X_1, X_2; Y), \end{aligned}$$

where (a) follows since the average is upper bounded by the maximum. Thus the sum capacity is “computable” without cardinality bound on \mathcal{Q} . However, the second maximization problem is not convex in general, so there does not exist an efficient algorithm to compute C from it. In comparison, the first maximization problem is convex and can be solved efficiently

Coded Time Sharing

- Can we achieve the capacity region characterization in Theorem 3 directly without explicit time sharing?
- The answer turns out to be yes and it involves *coded time sharing* [6]. We outline the achievability proof using coded time sharing
- Codebook generation: Fix $p(q)p(x_1|q)p(x_2|q)$
Randomly generate a *time sharing* sequence q^n according to $\prod_{i=1}^n p_Q(q_i)$
Randomly and conditionally independently generate 2^{nR_1} sequences $x_1^n(m_1)$, $m_1 \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{X_1|Q}(x_{1i}|q_i)$. Similarly generate 2^{nR_2} sequences $x_2^n(m_2)$, $m_2 \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_{X_2|Q}(x_{2i}|q_i)$
The chosen codebook, including q^n , is revealed to the encoders and decoder
- Encoding: To send (m_1, m_2) , transmit $x_1^n(m_1)$ and $x_2^n(m_2)$
- Decoding: The decoder declares that (\hat{m}_1, \hat{m}_2) is sent if it is the unique message pair such that $(q^n, x_1^n(\hat{m}_1), x_2^n(\hat{m}_2), y^n) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error

- Analysis of the probability of error: The error event \mathcal{E} occurs iff

$$\mathcal{E}_1 := \{(Q^n, X_1^n(1), X_2^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \text{ or}$$

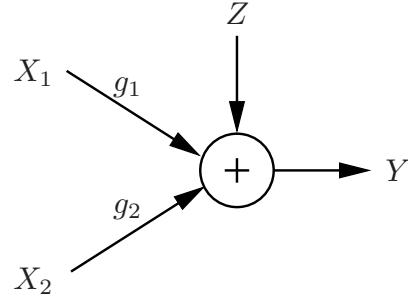
$$\mathcal{E}_2 := \{(Q^n, X_1^n(m_1), X_2^n(1), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1\}, \text{ or}$$

$$\mathcal{E}_3 := \{(Q^n, X_1^n(1), X_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_2 \neq 1\}, \text{ or}$$

$$\mathcal{E}_4 := \{(Q^n, X_1^n(m_1), X_2^n(m_2), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1, m_2 \neq 1\}$$
- Then, $P(\mathcal{E}) \leq \sum_{j=1}^4 P(\mathcal{E}_j)$
- By the LLN, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$
- Since for $m_1 \neq 1$, $X_1^n(m_1)$ is conditionally independent of $(X_2^n(1), Y^n)$ given Q^n , by the packing lemma ($|\mathcal{A}| = 2^{nR_1} - 1$, $Y \leftarrow (X_2, Y)$, $U \leftarrow Q$), $P(\mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X_1; X_2, Y|Q) - \delta(\epsilon) = I(X_1; Y|X_2, Q) - \delta(\epsilon)$
- Similarly, $P(\mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$ if $R_2 < I(X_2; Y|X_1, Q) - \delta(\epsilon)$
- Finally, since for $m_1 \neq 1, m_2 \neq 1$, $(X_1^n(m_1), X_2^n(m_2))$ is conditionally independent of $(X_1^n(1), X_2^n(1), Y^n)$ given Q^n , again by the packing lemma, $P(\mathcal{E}_4) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X_1, X_2; Y|Q) - \delta(\epsilon)$

AWGN Multiple Access Channel

- Consider an AWGN-MAC with two senders X_1 and X_2 , and a single receiver Y



At time i : $Y_i = g_1 X_{1i} + g_2 X_{2i} + Z_i$, where g_1, g_2 are the channel gains and $\{Z_i\}$ is a $\text{WGN}(N_0/2)$ process, independent of $\{X_{1i}, X_{2i}\}$ (when no feedback is present)

Assume the average transmit power constraints

$$\frac{1}{n} \sum_{i=1}^n x_{ji}^2(m_j) \leq P, \quad m_j \in [1 : 2^{nR_j}], \quad j = 1, 2$$

- Assume without loss of generality that $N_0/2 = 1$ and define the received powers (SNRs) as $S_j := g_j^2 P$, $j = 1, 2$

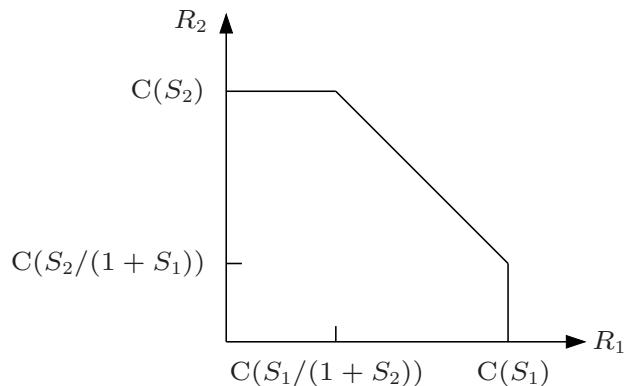
Capacity Region of AWGN-MAC

- Theorem 4: ([7], [8]):* The capacity region of the AWGN-MAC is the set of (R_1, R_2) rate pairs satisfying

$$R_1 \leq C(S_1),$$

$$R_2 \leq C(S_2),$$

$$R_1 + R_2 \leq C(S_1 + S_2)$$



- Remark: The capacity region coincides with the simple outer bound and no convexification via time-sharing random variable Q is required

- Proof of achievability: Consider the $\mathcal{R}(X_1, X_2)$ region with $X_1 \sim N(0, P)$ and $X_2 \sim N(0, P)$ are independent of each other. Then,

$$\begin{aligned}
I(X_1; Y|X_2) &= h(Y|X_2) - h(Y|X_1, X_2) \\
&= h(g_1 X_1 + g_2 X_2 + Z|X_2) - h(g_1 X_1 + g_2 X_2 + Z|X_1, X_2) \\
&= h(g_1 X_1 + Z) - h(Z) \\
&= \frac{1}{2} \log(2\pi e(S_1 + 1)) - \frac{1}{2} \log(2\pi e) = C(S_1)
\end{aligned}$$

The other two mutual information terms follow similarly

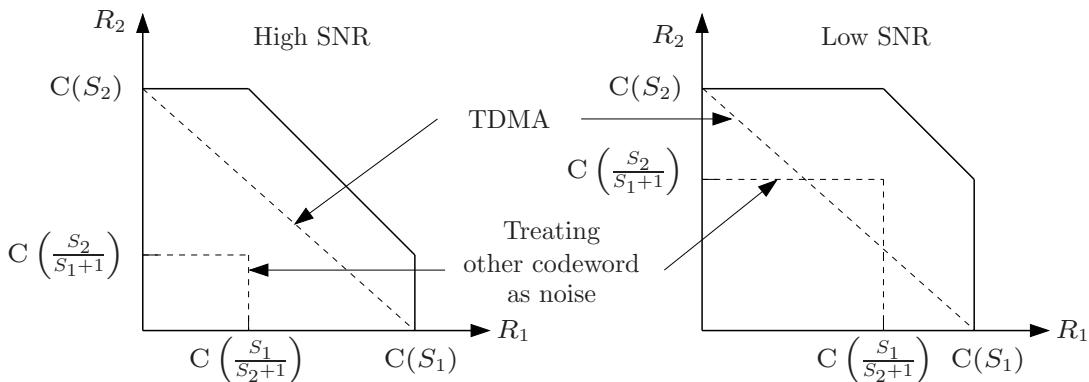
The rest of the achievability proof follows by discretizing the code and the channel output as in the achievability proof of the point-to-point AWGN channel, applying the achievability of the DM-MAC with cost on x_1 and x_2 to the discretized problem, and taking appropriate limits

Note that no time sharing is required here

- The converse proof is similar to that for the AWGN channel (check!)

Comparison to Point-to-Point Coding Schemes

- Treating other codeword as noise:* Consider the practically motivated coding scheme where Gaussian random codes are used but each message is decoded while treating the other codeword as noise. This scheme achieves the set of (R_1, R_2) pairs such that $R_1 < C(S_1/(S_2 + 1))$, $R_2 < C(S_2/(S_1 + 1))$
- TDMA:* A straightforward TDMA scheme achieves the set of (R_1, R_2) pairs such that $R_1 < \alpha C(S_1)$, $R_2 < \bar{\alpha} C(S_2)$ for some $\alpha \in [0, 1]$
- Note that when SNRs are sufficiently low, treating the other codeword as noise can outperform TDMA for some rate pairs



TDMA With Power Control

- The average power used by the senders in TDMA is strictly lower than the average power constraint P for $\alpha \in (0, 1)$
- If the senders are allowed to vary their powers with the rates, we can do strictly better. Divide the block length n into two subblocks, one of length αn and the other of length $\bar{\alpha}n$

During the first subblock, the first sender transmits using Gaussian random codes at average power P/α and the second sender does not transmit (i.e., transmits zeros)

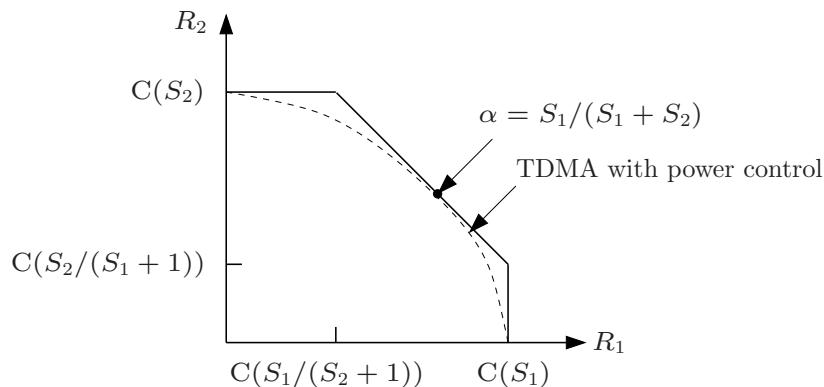
During the second subblock, the second sender transmits at average power $P/\bar{\alpha}$ and the first sender does not transmit

Note that the average power constraints are satisfied

- The resulting time-division inner bound is given by the set of rate pairs (R_1, R_2) such that

$$R_1 \leq \alpha C(S_1/\alpha), \quad R_2 \leq \bar{\alpha} C(S_2/\bar{\alpha}) \quad \text{for some } \alpha \in [0, 1]$$

- Now choose $\alpha = S_1/(S_1 + S_2)$. Substituting and adding, we find a point (R_1, R_2) on the boundary of the time-division inner bound that coincides with a point on the sum capacity line $R_1 + R_2 = C(S_1 + S_2)$



- Note that TDMA with power control *always* outperforms treating the other codeword as noise

Successive Cancellation Decoding

- As in the DM case, the corner points of the AWGN-MAC capacity region can be achieved using successive cancellation decoding:
 - Upon receiving $y^n = x_2^n(m_2) + x_1^n(m_1) + z^n$, the receiver decodes the second sender's message m_2 considering the first sender's codeword $x_1^n(m_1)$ as part of the noise. This probability of error for this step $\rightarrow 0$ as $n \rightarrow \infty$ if $R_2 < C(S_2/(S_1 + 1))$
 - The second sender's codeword is then subtracted from y^n and the first sender's message m_1 is decoded from $(y^n - x_2^n(m_2)) = (x_1^n(m_1) + z^n)$. The probability of error for this step $\rightarrow 0$ as $n \rightarrow \infty$ if the first decoding step is successful and $R_1 < C(S_1)$
- Remark: To make the above argument rigorous, we can follow a similar procedure to that used to prove the achievability for the AWGN channel
- Any point on the $R_1 + R_2 = C(S_1 + S_2)$ line can be achieved by time sharing between the two corner points
- Note that with successive cancellation decoding and time sharing, the entire capacity region can be achieved simply by using good point-to-point AWGN channel codes

Extension to More Than Two Senders

- Consider a k -sender DM-MAC $(\mathcal{X}_1 \times \mathcal{X}_2 \cdots \times \mathcal{X}_k, p(y|x_1, x_2, \dots, x_k), \mathcal{Y})$
- Theorem 5:* The capacity region of the k -sender DM-MAC is the set of (R_1, R_2, \dots, R_k) tuples satisfying

$$\sum_{j \in \mathcal{J}} R_j \leq I(X(\mathcal{J}); Y|X(\mathcal{J}^c), Q) \text{ for all } \mathcal{J} \subseteq [1 : k]$$

and some joint pmf $p(q)p_1(x_1|q)p_2(x_2|q)\cdots p_k(x_k|q)$ with $|\mathcal{Q}| \leq k$, where $X(\mathcal{J})$ is the ordered vector of X_j , $j \in \mathcal{J}$

- For a k -sender AWGN-MAC with average power constraint P on each sender and equal channel gains (thus equal SNRs $S_1 = S_2 = \dots = S$) the capacity region is the set of rate tuples satisfying

$$\sum_{j \in \mathcal{J}} R_j \leq C(|\mathcal{J}| \cdot S) \text{ for all } \mathcal{J} \subseteq [1 : k]$$

Note that as the sum capacity $C(kS) \rightarrow \infty$ as $k \rightarrow \infty$

However, the maximum rate per user $C(kS)/k \rightarrow 0$ as $k \rightarrow \infty$

Key New Ideas and Techniques

- Capacity region
- Time sharing: used to show that capacity region is convex
- Single-letter versus multi-letter characterization of the capacity region
- Successive cancellation decoding
- Simultaneous decoding: More powerful than successive cancellation
- Coded time sharing: More powerful than time sharing
- Time-sharing random variable
- Bounding cardinality of the time-sharing random variable

References

- [1] E. C. van der Meulen, "The discrete memoryless channel with two senders and one receiver," in *Proc. 2nd Int. Symp. Inf. Theory*, Tsahkadsor, Armenian S.S.R., 1971, pp. 103–135.
- [2] R. Ahlswede, "Multiway communication channels," in *Proc. 2nd Int. Symp. Inf. Theory*, Tsahkadsor, Armenian S.S.R., 1971, pp. 23–52.
- [3] H. H. J. Liao, "Multiple access channels," Ph.D. Thesis, University of Hawaii, Honolulu, Sept. 1972.
- [4] G. Dueck, "Maximal error capacity regions are smaller than average error capacity regions for multi-user channels," *Probl. Control Inf. Theory*, vol. 7, no. 1, pp. 11–19, 1978.
- [5] D. Slepian and J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell System Tech. J.*, vol. 52, pp. 1037–1076, Sept. 1973.
- [6] T. S. Han and K. Kobayashi, "A new achievable rate region for the interference channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, 1981.
- [7] T. M. Cover, "Some advances in broadcast channels," in *Advances in Communication Systems*, A. J. Viterbi, Ed. San Francisco: Academic Press, 1975, vol. 4, pp. 229–260.
- [8] A. D. Wyner, "Recent results in the Shannon theory," *IEEE Trans. Inf. Theory*, vol. 20, pp. 2–10, 1974.

Lecture Notes 5

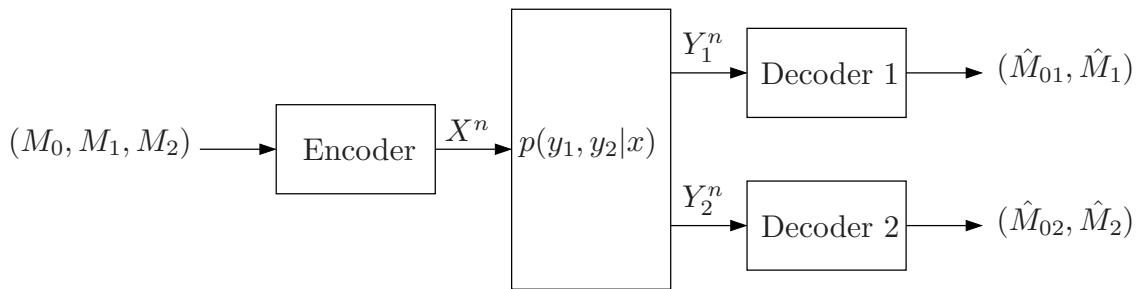
Degraded Broadcast Channels

- Problem Setup
- Simple Inner and Outer Bounds on the Capacity Region
- Superposition Coding Inner Bound
- Degraded Broadcast Channels
- AWGN Broadcast Channels
- Less Noisy and More Capable Broadcast Channels
- Extensions
- Key New Ideas and Techniques

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- A 2-receiver *discrete memoryless broadcast channel* (DM-BC) $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$ consists of three finite sets \mathcal{X} , \mathcal{Y}_1 , \mathcal{Y}_2 , and a collection of conditional pmfs $p(y_1, y_2|x)$ on $\mathcal{Y}_1 \times \mathcal{Y}_2$
- The sender X wishes to send a common message M_0 to both receivers, a private messages M_1 and M_2 to receivers Y_1 and Y_2 , respectively



- A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for a DM-BC consists of:
 1. Three message sets $[1 : 2^{nR_0}]$, $[1 : 2^{nR_1}]$, and $[1 : 2^{nR_2}]$
 2. An encoder that assigns a codeword $x^n(m_0, m_1, m_2)$ to each message triple $(m_0, m_1, m_2) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$
 3. Two decoders: Decoder 1 assigns an estimate $(\hat{m}_{01}, \hat{m}_1)(y_1^n) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$ or an error message e to each received sequence y_1^n , and decoder 2 assigns an estimate $(\hat{m}_{02}, \hat{m}_2)(y_2^n) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_2}]$ or an error message e to each received sequence y_2^n
- We assume that the message triple (M_0, M_1, M_2) is uniformly distributed over $[1 : 2^{nR_0}] \times [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$
- The average probability of error is defined as

$$P_e^{(n)} = P\{(\hat{M}_{01}, \hat{M}_1) \neq (M_0, M_1) \text{ or } (\hat{M}_{02}, \hat{M}_2) \neq (M_0, M_2)\}$$
- A rate triple (R_0, R_1, R_2) is said to be *achievable* for the DM-BC if there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The *capacity region* \mathcal{C} of the DM-BC is the closure of the set of achievable rate triples (R_0, R_1, R_2) —a closed set in \mathbb{R}^3

- *Lemma 1:* The capacity region of the DM-BC depends on $p(y_1, y_2|x)$ only through the conditional marginal pmfs $p(y_1|x)$ and $p(y_2|x)$

Proof: Consider the individual probabilities of error

$$P_{ej}^{(n)} = P\{(\hat{M}_{0j}, \hat{M}_j)(Y_j^n) \neq (M_0, M_j)\} \text{ for } j = 1, 2$$

Note that each term depends only on its corresponding conditional marginal pmf $p(y_j|x)$, $j = 1, 2$

By the union of events bound,

$$P_e^{(n)} \leq P_{e1}^{(n)} + P_{e2}^{(n)}$$

Also,

$$P_e^{(n)} \geq \max\{P_{e1}^{(n)}, P_{e2}^{(n)}\}$$

Hence $P_e^{(n)} \rightarrow 0$ iff $P_{e1}^{(n)} \rightarrow 0$ and $P_{e2}^{(n)} \rightarrow 0$, which implies that the capacity region for a DM-BC depends only on the conditional marginal pmfs

- Remark: The above lemma does not hold in general when feedback is present
- The capacity region of the DM-BC is not known in general
- There are inner and outer bounds on the capacity region that coincide in several cases, including:

- *Common message* only: If $R_1 = R_2 = 0$, the *common-message* capacity is

$$C_0 = \max_{p(x)} \min\{I(X; Y_1), I(X; Y_2)\}$$

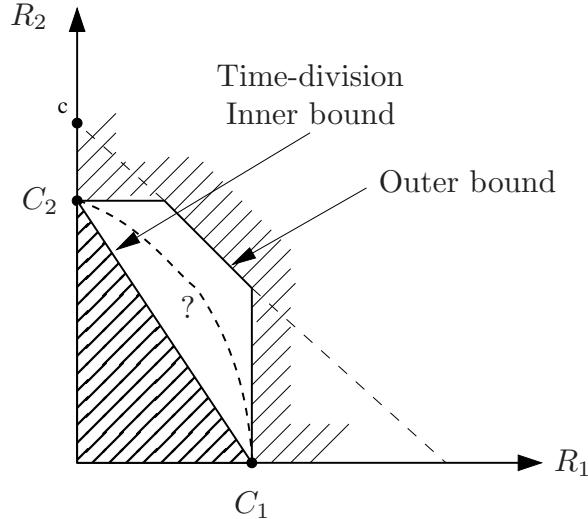
Note that this is in general smaller than the minimum of the individual capacities of the channels $p(y_1|x)$ and $p(y_2|x)$

- *Degraded message sets*: If $R_2 = 0$ (or $R_1 = 0$) [1], the capacity region is known. We will discuss this scenario in detail in Lecture Notes 9
- Several classes of DM-BCs with restrictions on their channel structures, e.g., degraded, less noisy, and more capable BC
- In this lecture notes we present the superposition coding inner bound and discuss several special classes of BCs where it is optimal. Specifically, we establish the capacity region for the class of degraded broadcast channels, which is an important class because it includes the binary symmetric and AWGN channel models. We then discuss extensions of this result to more general classes of broadcast channels
- For simplicity of presentation, we focus the discussion on *private-message* capacity region, i.e., when $R_0 = 0$. We then show how the results can be readily extended to the case of both common and private messages

- Other inner and outer bounds on the capacity region for general broadcast channels will be discussed later in Lecture Notes 9

Simple Inner and Outer Bounds on the Capacity Region

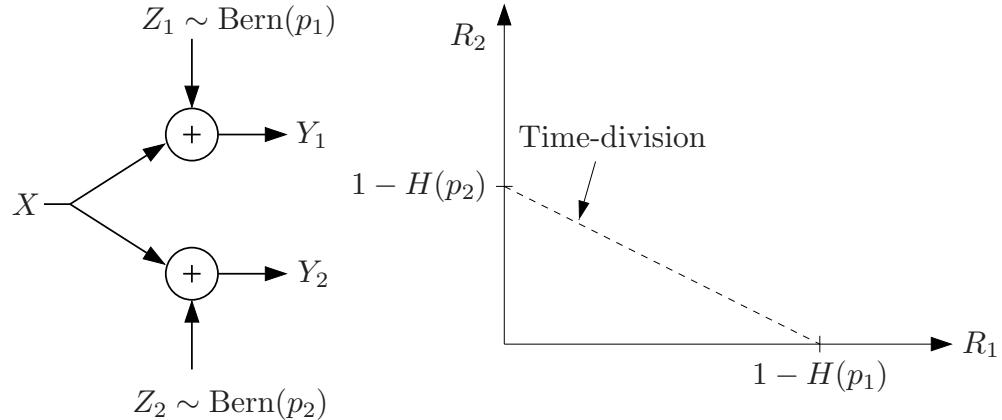
- Consider the individual channel capacities $C_j = \max_{p(x)} I(X; Y_j)$ for $j = 1, 2$. These define a time-division inner bound and a general outer bound on the capacity region



- Examples:
 - Consider a symmetric DM-BC, where $\mathcal{Y}_1 = \mathcal{Y}_2$ and $p_{Y_1|X}(y|x) = p_{Y_2|X}(y|x)$
For this example $C_1 = C_2 = \max_{p(x)} I(X; Y)$
Since the capacity region depends only on the marginals of $p(y_1, y_2|x)$, we can assume that $Y_1 = Y_2 = Y$. Thus $R_1 + R_2 \leq C_1$ and the time-division inner bound is tight
 - Consider a DM-BC with separate channels, where $\mathcal{X} = \mathcal{X}_1 \times \mathcal{X}_2$ and $p(y_1, y_2|x_1, x_2) = p(y_1|x_1)p(y_2|x_2)$
For this example the outer bound is tight
- Neither bound is tight in general, however

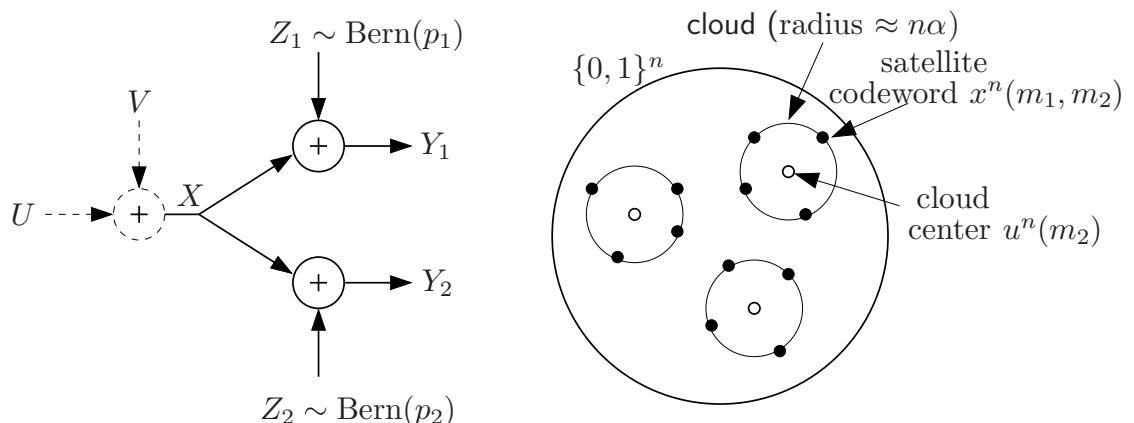
Binary Symmetric Broadcast Channel

- The binary symmetric BC (BS-BC) consists of a $\text{BSC}(p_1)$ and a $\text{BSC}(p_2)$.
Assume $p_1 < p_2 < 1/2$



- Can we do better than time division?

- Consider the following *superposition coding* technique [1]
- Codebook generation: For $\alpha \in [0, 1/2]$, let $U \sim \text{Bern}(1/2)$ and $V \sim \text{Bern}(\alpha)$ be independent and $X = U \oplus V$
Randomly and independently generate 2^{nR_2} $u^n(m_2)$ sequences, each i.i.d. $\text{Bern}(1/2)$ (cloud centers)
Randomly and independently generate 2^{nR_1} $v^n(m_1)$ sequences, each i.i.d. $\text{Bern}(\alpha)$



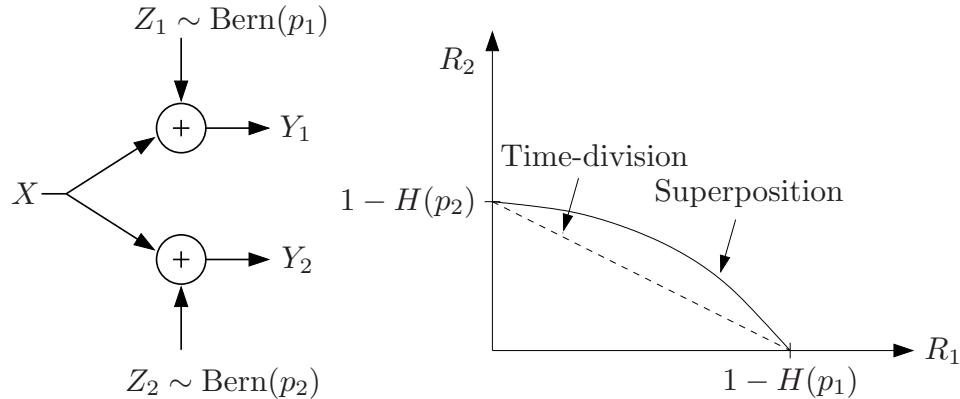
- Encoding: To send (m_1, m_2) , transmit $x^n(m_1, m_2) = u^n(m_2) \oplus v^n(m_1)$ (satellite codeword)
- Decoding:
 - Decoder 2 decodes m_2 from $y_2^n = u^n(m_2) \oplus (v^n(m_1) \oplus z_2^n)$ considering $v^n(m_1)$ as noise
 m_2 can be decoded with probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if $R_2 < 1 - H(\alpha * p_2)$, where $\alpha * p_2 := \alpha \bar{p}_2 + \bar{\alpha} p_2$, $\bar{\alpha} := 1 - \alpha$
 - Decoder 1 uses successive cancellation: It first decodes m_2 from $y_1^n = u^n(m_2) \oplus (v^n(m_1) \oplus z_1^n)$, subtracts off $u^n(m_2)$, then decodes m_1 from $(v^n(m_1) \oplus z_1^n)$
 m_1 can be decoded with probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(V; V \oplus Z_1) = H(\alpha * p_1) - H(p_1)$ and $R_2 < 1 - H(\alpha * p_1)$, which is already satisfied from the rate constraint for decode 2 because $p_1 < p_2$

- Thus superposition coding leads to an inner bound consisting of the set of rate pairs (R_1, R_2) such that

$$R_1 \leq H(\alpha * p_1) - H(p_1),$$

$$R_2 \leq 1 - H(\alpha * p_2)$$

for some $\alpha \in [0, 1/2]$. This inner bound is larger than the time-division inner bound and is the capacity region for this channel as will be proved later



Superposition Coding Inner Bound

- The superposition coding technique illustrated in the BS-BC example can be generalized to obtain the following inner bound to the capacity region of the general DM-BC
- *Theorem 1* (Superposition Coding Inner Bound) [2, 3]: A rate pair (R_1, R_2) is achievable for a DM-BC $(\{\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2\})$ if it satisfies the conditions

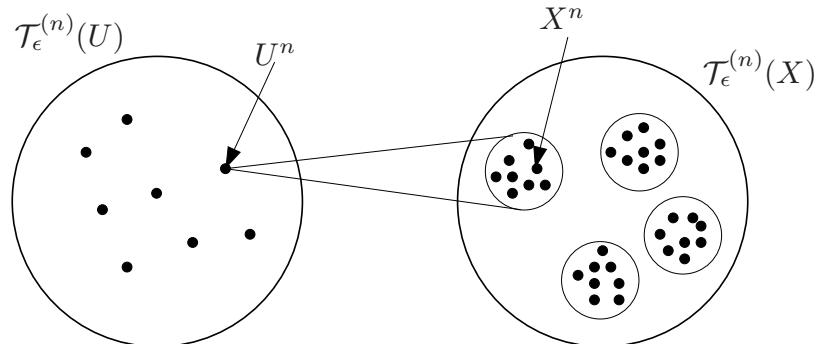
$$\begin{aligned} R_1 &< I(X; Y_1|U), \\ R_2 &< I(U; Y_2), \\ R_1 + R_2 &< I(X; Y_1) \end{aligned}$$

for some $p(u, x)$

- It can be shown that this set is convex and therefore there is no need for convexification using a time-sharing random variable (check!)

Outline of Achievability

- Fix $p(u)p(x|u)$. Generate 2^{nR_2} independent $u^n(m_2)$ “cloud centers.” For each $u^n(m_2)$, generate 2^{nR_1} conditionally independent $x^n(m_1, m_2)$ “satellite” codewords



- Decoder 2 decodes the cloud center $u^n(m_2)$
- Decoder 1 decodes the satellite codeword

Proof of Achievability

- Codebook generation: Fix $p(u)p(x|u)$
Randomly and independently generate 2^{nR_2} sequences $u^n(m_2)$, $m_2 \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_U(u_i)$
For each sequence $u^n(m_2)$, randomly and conditionally independently generate 2^{nR_1} sequences $x^n(m_1, m_2)$, $m_1 \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{X|U}(x_i|u_i(m_2))$
- Encoding: To send the message pair (m_1, m_2) , transmit $x^n(m_1, m_2)$
- Decoding: Decoder 2 declares that a message \hat{m}_2 is sent if it is the unique message such that $(u^n(\hat{m}_2), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error
Decoder 1 declares that a message \hat{m}_1 is sent if it is the unique message such that $(u^n(m_2), x^n(\hat{m}_1, m_2), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$ for some m_2 ; otherwise it declares an error
- Analysis of the probability of error: Without loss of generality, assume that $(M_1, M_2) = (1, 1)$ is sent

- First consider the average probability of error for decoder 2. Define the events

$$\mathcal{E}_{21} := \{(U^n(1), Y_2^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\mathcal{E}_{22} := \{(U^n(m_2), Y_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_2 \neq 1\}$$

The probability of error for decoder 2 is then upper bounded by

$$P(\mathcal{E}_2) = P(\mathcal{E}_{21} \cup \mathcal{E}_{22}) \leq P(\mathcal{E}_{21}) + P(\mathcal{E}_{22})$$

Now by the LLN, the first term $P(\mathcal{E}_{21}) \rightarrow 0$ as $n \rightarrow \infty$. On the other hand, since for $m_2 \neq 1$, $U^n(m_2)$ is independent of $(U^n(1), Y_2^n)$, by the packing lemma $P(\mathcal{E}_{22}) \rightarrow 0$ as $n \rightarrow \infty$ if $R_2 < I(U; Y_2) - \delta(\epsilon)$

- Next consider the average probability of error for decoder 1

Let's look at the pmfs for the triple $(U^n(m_2), X^n(m_1, m_2), Y_1^n)$

m_1	m_2	Joint pmf
1	1	$p(u^n, x^n)p(y_1^n x^n)$
*	1	$p(u^n, x^n)p(y_1^n u^n)$
*	*	$p(u^n, x^n)p(y_1^n)$
1	*	$p(u^n, x^n)p(y_1^n)$

The last case does not result in an error, so we divide the error event into the 3 events

$$\mathcal{E}_{11} := \{(U^n(1), X^n(1, 1), Y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\mathcal{E}_{12} := \{(U^n(1), X^n(m_1, 1), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1\},$$

$$\mathcal{E}_{13} := \{(U^n(m_2), X^n(m_1, m_2), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_2 \neq 1, m_1 \neq 1\}$$

The probability of error for decoder 1 is then bounded by

$$P(\mathcal{E}_1) = P(\mathcal{E}_{11} \cup \mathcal{E}_{12} \cup \mathcal{E}_{13}) \leq P(\mathcal{E}_{11}) + P(\mathcal{E}_{12}) + P(\mathcal{E}_{13})$$

1. By the LLN, $P(\mathcal{E}_{11}) \rightarrow 0$ as $n \rightarrow \infty$
2. Next consider the event \mathcal{E}_{12} . For $m_1 \neq 1$, $X^n(m_1, 1)$ is conditionally independent of $(X^n(1, 1), Y_1^n)$ given $U^n(1)$ and is distributed according to $\prod_{i=1}^n p_{X|U}(x_i|u_i)$. Hence, by the packing lemma, $P(\mathcal{E}_{12}) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X; Y_1|U) - \delta(\epsilon)$
3. Finally, consider the event \mathcal{E}_{13} . For $m_2 \neq 1$ (and any m_1), $(U^n(m_2), X^n(m_1, m_2))$ is independent of $(U^n(1), X^n(1, 1), Y_1^n)$. Hence, by the packing lemma, $P(\mathcal{E}_{13}) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 + R_2 < I(U, X; Y_1) - \delta(\epsilon) = I(X; Y_1) - \delta(\epsilon)$ (recall that $U \rightarrow X \rightarrow Y_1$ form a Markov chain)
 - o This completes the proof of achievability

- Remarks:

- o Consider the error event

$$\mathcal{E}_{14} := \{(U^n(m_2), X^n(1, m_2), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_2 \neq 1\}$$

Then, by the packing lemma, $P(\mathcal{E}_{14}) \rightarrow 0$ as $R_2 < I(U, X; Y_1) - \delta(\epsilon) = I(X; Y_1) - \delta(\epsilon)$, which is already satisfied

Therefore, the inner bound does not change if we require decoder 1 to also reliably decode M_2

- o We can obtain a similar inner bound by having Y_1 decode the cloud center (which would now represent M_1) and Y_2 decode the satellite codeword. This gives the set of rate pairs (R_1, R_2) satisfying

$$R_1 < I(U; Y_1),$$

$$R_2 < I(X; Y_2|U),$$

$$R_1 + R_2 < I(X; Y_2)$$

for some $p(u, x)$

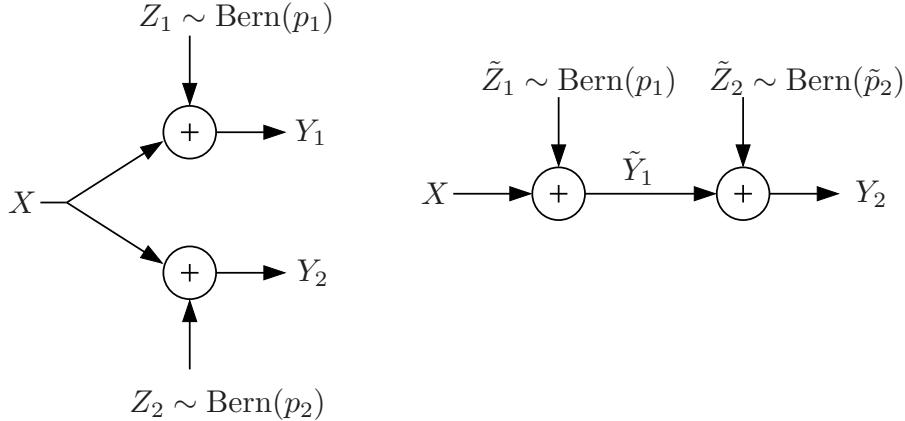
The convex closure of the union of these two inner bounds also constitutes an inner bound to the capacity region of the general BC

- Superposition coding is optimal for several classes of DM-BC that we discuss in the following sections
- However, it is not optimal in general because it assume that one of the receivers is “better” than the other, and hence can decode both messages. This is not always the case as we will see in Lecture Notes 9

Degraded Broadcast Channels

- A DM-BC is said to be *physically degraded* if $p(y_1, y_2|x) = p(y_1|x)p(y_2|y_1)$, i.e., $X \rightarrow Y_1 \rightarrow Y_2$ form a Markov chain
- A DM-BC is said to be *stochastically degraded* (or simply degraded) if there exists a random variable \tilde{Y}_1 such that
 1. $\tilde{Y}_1|\{X = x\} \sim p_{Y_1|X}(\tilde{y}_1|x)$, i.e., \tilde{Y}_1 has the same conditional pmf as Y_1 (given X), and
 2. $X \rightarrow \tilde{Y}_1 \rightarrow Y_2$ form a Markov chain
- Since the capacity region of a DM-BC depends only on the conditional marginals, the capacity region of the stochastically degraded DM-BC is the same as that of the corresponding physically degraded channel (key observation for proving the converse)

- Example: The BS-BC is degraded. Again assume that $p_1 < p_2 < 1/2$



The channel is degraded since we can write $Y_2 = X \oplus \tilde{Z}_1 \oplus \tilde{Z}_2$, where $\tilde{Z}_1 \sim \text{Bern}(p_1)$ and $\tilde{Z}_2 \sim \text{Bern}(\tilde{p}_2)$ are independent, and

$$\tilde{p}_2 := \frac{(p_2 - p_1)}{(1 - 2p_1)}$$

The capacity region for the BS-BC is the same as that of the physically degraded BS-BC

Capacity Region of the Degraded Broadcast Channel

- *Theorem 2 [2, 3, 4]:* The private-message capacity region of the degraded DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$ is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X; Y_1|U), \\ R_2 \leq I(U; Y_2)$$

for some $p(u, x)$, where the cardinality of the auxiliary random variable U satisfies $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\} + 1$

- Achievability follows from the superposition coding inner bound. To show this, note that the sum of the first two inequalities in the inner bound characterization gives $R_1 + R_2 < I(U; Y_2) + I(X; Y_1|U)$. Since the channel is degraded, $I(U; Y_1) \geq I(U; Y_2)$ for all $p(u, x)$. Hence, $I(U; Y_2) + I(X; Y_1|U) \leq I(U; Y_1) + I(X; Y_1|U) = I(X; Y_1)$ and the third inequality is automatically satisfied

Proof of Converse

- We need to show that for any sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^{(n)} \rightarrow 0$, $R_1 \leq I(X; Y_1|U)$, $R_2 \leq I(U; Y_2)$ for some $p(u, x)$ such that $U \rightarrow X \rightarrow (Y_1, Y_2)$
- The key is to identify U in the converse
- Each $(2^{nR_1}, 2^{nR_2}, n)$ code induces the joint pmf

$$(M_1, M_2, X^n, Y_1^n, Y_2^n) \sim 2^{-n(R_1+R_2)} p(x^n | m_1, m_2) \prod_{i=1}^n p_{Y_1, Y_2 | X}(y_{1i}, y_{2i} | x_i)$$

- As usual, by Fano's inequality

$$\begin{aligned} H(M_1 | Y_1^n) &\leq nR_1 P_e^{(n)} + 1 \leq n\epsilon_n, \\ H(M_2 | Y_2^n) &\leq nR_2 P_e^{(n)} + 1 \leq n\epsilon_n, \end{aligned}$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$

- So we have

$$\begin{aligned} nR_1 &\leq I(M_1; Y_1^n) + n\epsilon_n, \\ nR_2 &\leq I(M_2; Y_2^n) + n\epsilon_n \end{aligned}$$

- A first attempt: Take $U := M_2$ (satisfies $U \rightarrow X_i \rightarrow (Y_{1i}, Y_{2i})$)

$$\begin{aligned} I(M_1; Y_1^n) &\leq I(M_1; Y_1^n | M_2) \\ &= I(M_1; Y_1^n | U) \\ &= \sum_{i=1}^n I(M_1; Y_{1i} | U, Y_1^{i-1}) \\ &\leq \sum_{i=1}^n I(M_1, Y_1^{i-1}; Y_{1i} | U) \\ &\leq \sum_{i=1}^n I(X_i, M_1, Y_1^{i-1}; Y_{1i} | U) \\ &= \sum_{i=1}^n I(X_i; Y_{1i} | U) \end{aligned}$$

So far so good. Now let's try the second inequality

$$I(M_2; Y_2^n) = \sum_{i=1}^n I(M_2; Y_{2i} | Y_2^{i-1}) = \sum_{i=1}^n I(U; Y_{2i} | Y_2^{i-1})$$

But $I(U; Y_{2i} | Y_2^{i-1})$ is not necessarily $\leq I(U; Y_{2i})$, so $U = M_2$ does not work

- Ok, let's try $U_i := (M_2, Y_1^{i-1})$ (satisfies $U_i \rightarrow X_i \rightarrow (Y_{1i}, Y_{2i})$), so

$$I(M_1; Y_1^n | M_2) \leq \sum_{i=1}^n I(X_i; Y_{1i} | U_i)$$

Now, let's consider the other term

$$\begin{aligned} I(M_2; Y_2^n) &\leq \sum_{i=1}^n I(M_2, Y_2^{i-1}; Y_{2i}) \\ &\leq \sum_{i=1}^n I(M_2, Y_2^{i-1}, Y_1^{i-1}; Y_{2i}) \end{aligned}$$

But $I(M_2, Y_2^{i-1}, Y_1^{i-1}; Y_{2i})$ is not necessarily equal to $I(M_2, Y_1^{i-1}; Y_{2i})$

- Key insight: Since the capacity region is the same as the corresponding physically degraded BC, we can assume that $X \rightarrow Y_1 \rightarrow Y_2$ form a Markov chain, thus $Y_2^{i-1} \rightarrow (M_2, Y_1^{i-1}) \rightarrow Y_{2i}$ also form a Markov chain, and

$$I(M_2; Y_2^n) \leq \sum_{i=1}^n I(U_i; Y_{2i})$$

- Remark: Proof also works with $U_i := (M_2, Y_2^{i-1})$ or $U_i := (M_2, Y_1^{i-1}, Y_2^{i-1})$ (both satisfy $U_i \rightarrow X_i \rightarrow (Y_{1i}, Y_{2i})$)

- Define the time-sharing random variable Q independent of $(M_1, M_2, X^n, Y_1^n, Y_2^n)$ and uniformly distributed over $[1 : n]$ and let $U := (Q, U_Q)$, $X := X_Q$, $Y_1 := Y_{1Q}$, $Y_2 := Y_{2Q}$. Clearly, $U \rightarrow X \rightarrow (Y_1, Y_2)$; therefore

$$nR_1 \leq \sum_{i=1}^n I(X_i; Y_{1i} | U_i) + n\epsilon_n = nI(X; Y_1 | U) + n\epsilon_n,$$

$$nR_2 \leq \sum_{i=1}^n I(U_i; Y_{2i}) + n\epsilon_n = nI(U_Q; Y_2 | Q) + n\epsilon_n \leq nI(U; Y_2) + n\epsilon_n$$

- The bound on the cardinality of U was established in [4] (see Appendix C)

Capacity Region of the Binary Symmetric BC

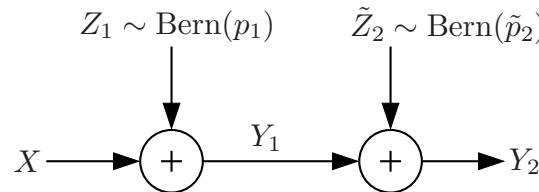
- *Proposition:* The capacity region of the binary symmetric BC is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq H(\alpha * p_1) - H(p_1),$$

$$R_2 \leq 1 - H(\alpha * p_2)$$

for some $\alpha \in [0, 1/2]$

- We have already argued that this is achievable via superposition coding by taking (U, X) as DSBS(α)
- Let's show that the characterization for the capacity region of the degraded DM-BC reduces to the above characterization
- First note that the capacity region is the same as that of the physically degraded DM-BC $X \rightarrow \tilde{Y}_1 \rightarrow Y_2$. Thus we assume that it is physically degraded



Consider the term

$$I(U; Y_2) = H(Y_2) - H(Y_2|U) \leq 1 - H(Y_2|U)$$

Now, $1 \geq H(Y_2|U) \geq H(Y_2|X) = H(p_2)$. Thus there exists $\alpha \in [0, 1/2]$ such that

$$H(Y_2|U) = H(\alpha * p_2)$$

Next consider

$$I(X; Y_1|U) = H(Y_1|U) - H(Y_1|X) = H(Y_1|U) - H(p_1)$$

Now, let $0 \leq H^{-1} \leq 1/2$ be the inverse of the binary entropy function

By physical degradedness and the scalar Mrs. Gerber's lemma, we have

$$H(Y_2|U) = H(Y_1 \oplus \tilde{Z}_2|U) \geq H(H^{-1}(H(Y_1|U)) * \tilde{p}_2)$$

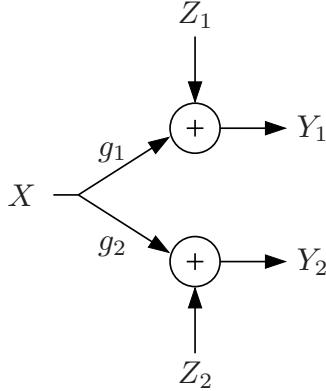
But, $H(Y_2|U) = H(\alpha * p_2) = H(\alpha * p_1 * \tilde{p}_2)$, and thus

$$H(Y_1|U) \leq H(\alpha * p_1)$$

This complete the proof

AWGN Broadcast Channels

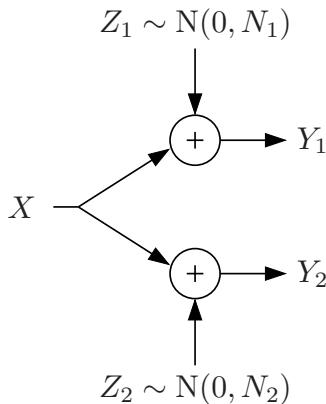
- General AWGN-BC: Consider a 2-receiver AWGN-BC



At time i : $Y_{1i} = g_1 X_i + Z_{1i}$, $Y_{2i} = g_2 X_i + Z_{2i}$, where $\{Z_{1i}\}, \{Z_{2i}\}$ are WGN($N_0/2$) processes, independent of $\{X_i\}$, and g_1, g_2 are channel gains. Without loss of generality, assume that $|g_1| \geq |g_2|$ and $N_0/2 = 1$. Assume average power constraint P on X

- Remark: The joint distribution of Z_{1i} and Z_{2i} does not affect the capacity region (Why?)

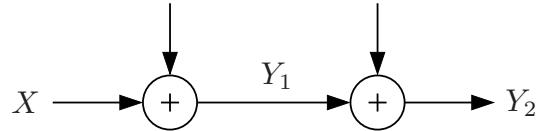
- An equivalent model: For notational convenience, we consider the equivalent AWGN-BC channel $Y_{1i} = X_i + Z_{1i}$, $Y_{2i} = X_i + Z_{2i}$, where channel gains are normalized to 1 and the “transmitter-referred” noise $\{Z_{1i}\}, \{Z_{2i}\}$ are WGN(N_1) and WGN(N_2) processes, respectively, with $N_1 := 1/g_1^2$ and $N_2 := 1/g_2^2 \geq N_1$
The equivalence can be seen by first multiplying both sides of the equations of the original channel model by $1/g_1$ and $1/g_2$, respectively, and then scaling the resulting channel outputs by g_1 and g_2



- The channel is stochastically degraded (Why?)

- The capacity region of the equivalent AWGN-BC is the same as that of a physically degraded AWGN-BC with $Y_{1i} = X_i + Z_{1i}$ and $Y_{2i} = Y_{1i} + \tilde{Z}_{2i}$, where $\{Z_{1i}\}$, $\{\tilde{Z}_{2i}\}$ are independent WGN(N_1) and WGN($(N_2 - N_1)$) processes, respectively, and power constraint P on X (why?)

$$Z_1 \sim \mathcal{N}(0, N_1) \quad \tilde{Z}_2 \sim \mathcal{N}(0, N_2 - N_1)$$



Capacity Region of AWGN Broadcast Channel

- Theorem 3:* The capacity of the AWGN-BC is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq C(\alpha S_1),$$

$$R_2 \leq C\left(\frac{\bar{\alpha}S_2}{\alpha S_2 + 1}\right)$$

for some $\alpha \in [0, 1]$, where $S_1 := P/N_1$ and $S_2 := P/N_2$ denote the received SNRs

- Outline of achievability: Use superposition coding. Let $U \sim \mathcal{N}(0, \bar{\alpha}P)$ and $V \sim \mathcal{N}(0, \alpha P)$ be independent and $X = U + V \sim \mathcal{N}(0, P)$. With this choice of (U, X) it is not difficult to show that

$$I(X; Y_1 | U) = C\left(\frac{\alpha P}{N_1}\right) = C(\alpha S_1),$$

$$I(U; Y_2) = C\left(\frac{\bar{\alpha}P}{\alpha P + N_2}\right) = C\left(\frac{\bar{\alpha}S_2}{\alpha S_2 + 1}\right),$$

which are the expressions in the capacity region characterization

Randomly and independently generate 2^{nR_2} sequences $u^n(m_2)$, $m_2 \in [1 : 2^{nR_2}]$, each i.i.d. $N(0, \bar{\alpha}P)$, and 2^{nR_1} $v^n(m_1)$ sequences, $m_1 \in [1 : 2^{nR_1}]$, each i.i.d. $N(0, \alpha P)$

Encoding: To send the message pair (m_1, m_2) , the encoder transmits
 $x^n(m_1, m_2) = u^n(m_2) + v^n(m_1)$

Decoding: Decoder 2 treats $v^n(m_1)$ as noise and decodes m_2 from
 $y_2^n = u^n(m_2) + v^n + z_2^n$

Decoder 1 uses successive cancellation; it first decodes m_2 , subtracts off $u^n(m_2)$ from $y_1^n = u^n(m_2) + v^n(m_1) + z_1^n$, and then decodes m_1 from $(v^n(m_1) + z_1^n)$

- Remarks:

- To make the above argument rigorous, one can follow a similar procedure to that used in the achievability for the point-to-point AWGN channel
- Much like the AWGN-MAC, with successive cancellation decoding, the entire capacity region can be achieved simply by using good point-to-point AWGN channel codes and superposition

Converse [5]

- Since the capacity of the AWGN-BC is the same as that of the corresponding physically degraded AWGN-BC, we prove the converse for the physically degraded AWGN-BC

$$\begin{aligned} Y_1^n &= X^n + Z_1^n, \\ Y_2^n &= X^n + Z_2^n = Y_1^n + \tilde{Z}_2^n \end{aligned}$$

- By Fano's inequality, we have

$$\begin{aligned} nR_1 &\leq I(M_1; Y_1^n | M_2) + n\epsilon_n, \\ nR_2 &\leq I(M_2; Y_2^n) + n\epsilon_n \end{aligned}$$

We need to show that there exists an $\alpha \in [0, 1]$ such that

$$\begin{aligned} I(M_1; Y_1^n | M_2) &\leq n C(\alpha S_1) = n C\left(\frac{\alpha P}{N_1}\right), \\ I(M_2; Y_2^n) &\leq n C\left(\frac{\bar{\alpha} S_2}{\alpha S_2 + 1}\right) = n C\left(\frac{\bar{\alpha} P}{\alpha P + N_2}\right) \end{aligned}$$

- Consider

$$\begin{aligned} I(M_2; Y_2^n) &= h(Y_2^n) - h(Y_2^n | M_2) \\ &\leq \frac{n}{2} \log(2\pi e(P + N_2)) - h(Y_2^n | M_2) \end{aligned}$$

Now we show that

$$\frac{n}{2} \log(2\pi e N_2) \leq h(Y_2^n | M_2) \leq \frac{n}{2} \log(2\pi e(P + N_2))$$

The lower bound is obtained as follows

$$\begin{aligned} h(Y_2^n | M_2) &= h(X^n + Z_2^n | M_2) \\ &\geq h(X^n + Z_2^n | M_2, X^n) \\ &= h(Z_2^n) = \frac{n}{2} \log(2\pi e N_2) \end{aligned}$$

The upper bound follows from $h(Y_2^n | M_2) \leq h(Y_2^n) \leq \frac{n}{2} \log(2\pi e(P + N_2))$
Thus there must exist an $\alpha \in [0, 1]$ such that

$$h(Y_2^n | M_2) = \frac{n}{2} \log(2\pi e(\alpha P + N_2))$$

- Next consider

$$\begin{aligned} I(M_1; Y_1^n | M_2) &= h(Y_1^n | M_2) - h(Y_1^n | M_1, M_2) \\ &\leq h(Y_1^n | M_2) - h(Y_1^n | M_1, M_2, X^n) \\ &= h(Y_1^n | M_2) - h(Y_1^n | X^n) \\ &= h(Y_1^n | M_2) - \frac{n}{2} \log(2\pi e N_1) \end{aligned}$$

- Now using a conditional version of the vector EPI, we obtain

$$\begin{aligned} h(Y_2^n | M_2) &= h(Y_1^n + \tilde{Z}_2^n | M_2) \\ &\geq \frac{n}{2} \log \left(2^{\frac{2}{n}h(Y_1^n | M_2)} + 2^{\frac{2}{n}h(\tilde{Z}_2^n | M_2)} \right) \\ &= \frac{n}{2} \log \left(2^{\frac{2}{n}h(Y_1^n | M_2)} + 2\pi e(N_2 - N_1) \right) \end{aligned}$$

But since $h(Y_2^n | M_2) = \frac{n}{2} \log(2\pi e(\alpha P + N_2))$,

$$2\pi e(\alpha P + N_2) \geq 2^{\frac{2}{n}h(Y_1^n | M_2)} + 2\pi e(N_2 - N_1)$$

Thus, $h(Y_1^n | M_2) \leq \frac{n}{2} \log(2\pi e(\alpha P + N_1))$, which implies that

$$I(M_1; Y_1^n | M_2) \leq \frac{n}{2} \log(2\pi e(\alpha P + N_1)) - \frac{n}{2} \log(2\pi e N_1) = n C \left(\frac{\alpha P}{N_1} \right)$$

This completes the proof of converse

- Remarks:
 - The converse can be proved also directly from the single-letter description $R_2 \leq I(U; Y_2)$, $R_1 \leq I(X; Y_1|U)$ (without the cardinality bound) with the power constraint $E(X^2) \leq P$ following similar step to the above converse and using the conditional scalar EPI
 - Note the similarity between the above converse and the converse for the BS-BC. In a sense Mrs. Gerber's lemma can be viewed as the binary analog of the entropy power inequality

Less Noisy and More Capable Broadcast Channels

- Superposition coding is optimal for the following two classes of broadcast channels, which are more general than degraded BCs
- *Less noisy* DM-BC [6]: A DM-BC is said to be *less noisy* if $I(U; Y_1) \geq I(U; Y_2)$ for all $p(u, x)$. In this case we say that receiver Y_1 is less noisy than receiver Y_2 . The private-message capacity region for this class is the set of (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq I(X; Y_1|U), \\ R_2 &\leq I(U; Y_2) \end{aligned}$$

for some $p(u, x)$, where $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_2|\} + 1$

- *More capable* DM-BC [6]: A DM-BC is said to be more capable if $I(X; Y_1) \geq I(X; Y_2)$ for all $p(x)$. In this case we say that receiver Y_1 is more capable than receiver Y_2

The private-message capacity region for this class [7] is the set of (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq I(X; Y_1 | U), \\ R_2 &\leq I(U; Y_2), \\ R_1 + R_2 &\leq I(X; Y_1) \end{aligned}$$

for some $p(u, x)$, where $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1| \cdot |\mathcal{Y}_2|\} + 2$

- It can be easily shown that if a DM-BC is degraded then it is less noisy, and that if a DM-BC is less noisy then it is more capable. The converse to these statements do not hold in general as illustrated in the following example

Example (*a BSC and a BEC*) [8]: Consider a DM-BC with sender $X \in \{0, 1\}$ and receivers $Y_1 \in \{0, 1\}$ and $Y_2 \in \{0, 1, e\}$, where the channel from X to Y_1 is a $\text{BSC}(p)$, $p \in [0, 1/2]$, and the channel from X to Y_2 is a $\text{BEC}(\epsilon)$, $\epsilon \in [0, 1]$. Then it can be shown that:

1. For $0 \leq \epsilon \leq 2p$: Y_1 is a *degraded* version of Y_2
2. For $2p < \epsilon \leq 4p(1 - p)$: Y_2 is *less noisy* than Y_1 , but not degraded
3. For $4p(1 - p) < \epsilon \leq H(p)$: Y_2 is *more capable* than Y_1 , but not less noisy
4. For $H(p) < \epsilon \leq 1$: The channel does not belong to *any* of the three classes

The capacity regions for cases 1–3 are achieved via superposition coding. The capacity region of the case 4 is also achieved via superposition coding. The converse will be given in Lecture Notes 9

Proof of Converse for More Capable DM-BC [7]

- Trying to prove the converse directly for the above capacity region characterization does not appear to be feasible mainly because it is difficult to find an identification of the auxiliary random variable that works for the first two inequalities
- Instead, we prove the converse for the alternative region consisting of the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_2 &\leq I(U; Y_2), \\ R_1 + R_2 &\leq I(X; Y_1|U) + I(U; Y_2), \\ R_1 + R_2 &\leq I(X; Y_1) \end{aligned}$$

for some $p(u, x)$

It can be shown that this region is equal to the capacity region (check!). The proof of the converse for this alternative region involves a tricky identification of the auxiliary random variable and the application of the Csiszár sum identity (cf. Lecture Notes 2)

- By Fano's inequality, it is straightforward to show that

$$\begin{aligned} nR_2 &\leq I(M_2; Y_2^n) + n\epsilon_n, \\ n(R_1 + R_2) &\leq I(M_1; Y_1^n|M_2) + I(M_2; Y_2^n) + n\epsilon_n, \\ n(R_1 + R_2) &\leq I(M_1; Y_1^n) + I(M_2; Y_2^n|M_1) + n\epsilon_n \end{aligned}$$

- Consider the mutual information terms in the second inequality

$$\begin{aligned} &I(M_1; Y_1^n|M_2) + I(M_2; Y_2^n) \\ &= \sum_{i=1}^n I(M_1; Y_{1i}|M_2, Y_1^{i-1}) + \sum_{i=1}^n I(M_2; Y_{2i}|Y_{2,i+1}^n) \\ &\leq \sum_{i=1}^n I(M_1, Y_{2,i+1}^n; Y_{1i}|M_2, Y_1^{i-1}) + \sum_{i=1}^n I(M_2, Y_{2,i+1}^n; Y_{2i}) \\ &= \sum_{i=1}^n I(M_1, Y_{2,i+1}^n; Y_{1i}|M_2, Y_1^{i-1}) + \sum_{i=1}^n I(M_2, Y_{2,i+1}^n, Y_1^{i-1}; Y_{2i}) \\ &\quad - \sum_{i=1}^n I(Y_1^{i-1}; Y_{2i}|M_2, Y_{2,i+1}^n) \end{aligned}$$

$$\begin{aligned}
&= \sum_{i=1}^n I(M_1; Y_{1i} | M_2, Y_1^{i-1}, Y_{2,i+1}^n) + \sum_{i=1}^n I(M_2, Y_{2,i+1}^n, Y_1^{i-1}; Y_{2i}) \\
&\quad - \sum_{i=1}^n I(Y_1^{i-1}; Y_{2i} | M_2, Y_{2,i+1}^n) + \sum_{i=1}^n I(Y_{2,i+1}^n; Y_{1i} | M_2, Y_1^{i-1}) \\
&\stackrel{(a)}{=} \sum_{i=1}^n (I(M_1; Y_{1i} | U_i) + I(U_i; Y_{2i})) \leq \sum_{i=1}^n (I(X_i; Y_{1i} | U_i) + I(U_i; Y_{2i})),
\end{aligned}$$

where $Y_1^0 = Y_{2,n+1}^n = \emptyset$, (a) follows by the Csiszár sum identity, and the auxiliary random variable $U_i := (M_2, Y_1^{i-1}, Y_{2,i+1}^n)$

- Next, consider the mutual information term in the first inequality

$$\begin{aligned}
I(M_2; Y_2^n) &= \sum_{i=1}^n I(M_2; Y_{2i} | Y_{2,i+1}^n) \\
&\leq \sum_{i=1}^n I(M_2, Y_{2,i+1}^n; Y_{2i}) \\
&\leq \sum_{i=1}^n I(M_2, Y_1^{i-1}, Y_{2,i+1}^n; Y_{2i}) \leq \sum_{i=1}^n I(U_i; Y_{2i})
\end{aligned}$$

- For the third inequality, define $V_i := (M_1, Y_1^{i-1}, Y_{2,i+1}^n)$. Following similar steps to the bound for the second inequality, we have

$$\begin{aligned}
I(M_1; Y_1^n) + I(M_2; Y_2^n | M_1) &\leq \sum_{i=1}^n (I(V_i; Y_{1i}) + I(X_i; Y_{2i} | V_i)) \\
&\stackrel{(a)}{\leq} \sum_{i=1}^n (I(V_i; Y_{1i}) + I(X_i; Y_{1i} | V_i)) \\
&\leq \sum_{i=1}^n I(X_i; Y_{1i}),
\end{aligned}$$

where (a) follows by the more capable condition, which implies that $I(X; Y_2 | V) \leq I(X; Y_1 | V)$ whenever $V \rightarrow X \rightarrow (Y_1, Y_2)$ form a Markov chain

- The rest of the proof follows by introducing a time-sharing random variable $Q \sim \text{Unif}[1 : n]$ independent of $(M_1, M_2, X^n, Y_1^n, Y_2^n)$ and defining $U := (Q, U_Q)$, $X := X_Q$, $Y_1 := Y_{1Q}$, $Y_2 := Y_{2Q}$
- The bound on the cardinality of U uses the standard technique in Appendix C

- Remark: The converse for the less noisy case can be proved similarly by considering the alternative characterization consisting of the set of (R_1, R_2) such that

$$R_2 \leq I(U; Y_2),$$

$$R_1 + R_2 \leq I(X; Y_1|U) + I(U; Y_2)$$

for some $p(u, x)$

Extensions

- So far, our discussion has been focused on the private-message capacity region

However, as remarked before, in superposition coding the “better” receiver Y_1 can reliably decode the message for the “worse” receiver Y_2 without changing the inner bound. In other words, if (R_1, R_2) is achievable for private messages, then $(R_0, R_1, R_2 - R_0)$ is achievable for private and common messages

For example, the capacity region for the more capable DM-BC is the set of rate triples (R_0, R_1, R_2) such that

$$R_1 \leq I(X; Y_1|U),$$

$$R_0 + R_2 \leq I(U; Y_2),$$

$$R_0 + R_1 + R_2 \leq I(X; Y_1)$$

The proof of converse follows similarly to that for the private-message capacity region (but unlike the achievability, is not implied automatically by the latter)

- Degraded BC with more than 2 receivers: Consider a k -receiver degraded DM-BC $(\mathcal{X}, p(y_1, y_2, \dots, y_k|x), \mathcal{Y}_1 \times \mathcal{Y}_2 \times \dots \times \mathcal{Y}_k)$, where $X \rightarrow Y_1 \rightarrow Y_2 \rightarrow \dots \rightarrow Y_k$ form a Markov chain. The private message capacity region is the set of rate tuples (R_1, R_2, \dots, R_k) such that

$$R_1 \leq I(X; Y_1|U_2),$$

$$R_j \leq I(U_j; Y_j|U_{j+1}) \text{ for } j \in [2 : k]$$

for some $p(u_k, u_{k-1})p(u_{k-2}|u_{k-1}) \cdots p(u_1|u_2)p(x|u_1)$ and $U_{k+1} = \emptyset$

- The capacity region for the 2-receiver AWGN-BC also extends to > 2 receivers
- Capacity for the less noisy is not known in general for $k > 3$ (see [9] for $k = 3$ case)
- Capacity for the more capable broadcast channels is not known in general for $k > 2$

Key New Ideas and Techniques

- Superposition coding
- Identification of the auxiliary random variable in converse
- Mrs. Gerber's Lemma in the proof of converse for the BS-BC
- Bounding cardinality of auxiliary random variables
- Entropy power inequality in the proof of the converse for AWGN-BCs
- Csiszár sum identity in the proof of converse (less noisy, more capable)
- Open problems:
 - What is the capacity region for less noisy BC with more than 3 receivers?
 - What is the capacity region of the more capable BC with more than 2 receivers?

References

- [1] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 60–64, 1977.
- [2] T. M. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 2–14, Jan. 1972.
- [3] P. P. Bergmans, "Random coding theorem for broadcast channels with degraded components," *IEEE Trans. Inf. Theory*, vol. 19, no. 2, pp. 197–207, 1973.
- [4] R. G. Gallager, "Capacity and coding for degraded broadcast channels," *Probl. Inf. Transm.*, vol. 10, no. 3, pp. 3–14, 1974.
- [5] P. P. Bergmans, "A simple converse for broadcast channels with additive white Gaussian noise," *IEEE Trans. Inf. Theory*, vol. 20, pp. 279–280, 1974.
- [6] J. Körner and K. Marton, "Comparison of two noisy channels," in *Topics in Information Theory (Second Colloq., Keszthely, 1975)*. Amsterdam: North-Holland, 1977, pp. 411–423.
- [7] A. El Gamal, "The capacity of a class of broadcast channels," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 166–169, 1979.
- [8] C. Nair, "Capacity regions of two new classes of 2-receiver broadcast channels," 2009. [Online]. Available: <http://arxiv.org/abs/0901.0595>
- [9] C. Nair and Z. V. Wang, "The capacity region of a class of broadcast channels with a sequence of less noisy receivers," 2010. [Online]. Available: <http://arxiv.org/abs/1001.1799>

Lecture Notes 6

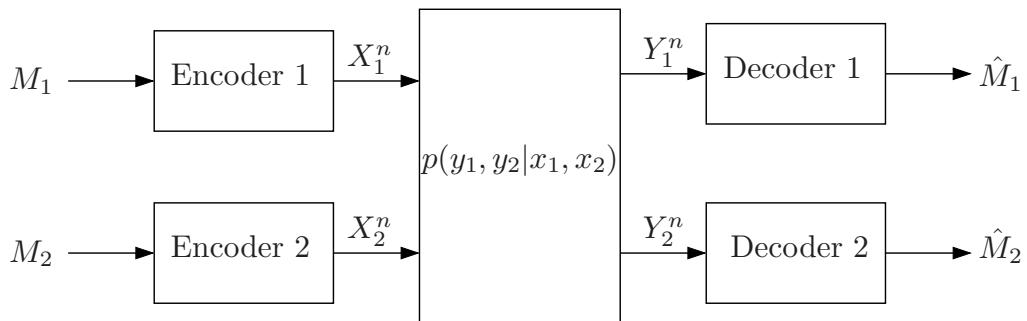
Interference Channels

- Problem Setup
- Inner and Outer Bounds on the Capacity Region
- Strong Interference
- AWGN Interference Channel
- Capacity Region of AWGN-IC Under Strong Interference
- Han–Kobayashi Inner Bound
- Capacity Region of a Class of Deterministic IC
- Sum-Capacity of AWGN-IC Under Weak Interference
- Capacity Region of AWGN-IC Within Half a Bit
- Deterministic Approximation of AWGN-IC
- Extensions to More than 2 User Pairs
- Key New Ideas and Techniques

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- Sender $j = 1, 2$ wishes to send an independent message M_j to its respective receiver Y_j
- A 2-user pair discrete memoryless *interference channel* (DM-IC) $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ 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 $\mathcal{Y}_1 \times \mathcal{Y}_2$

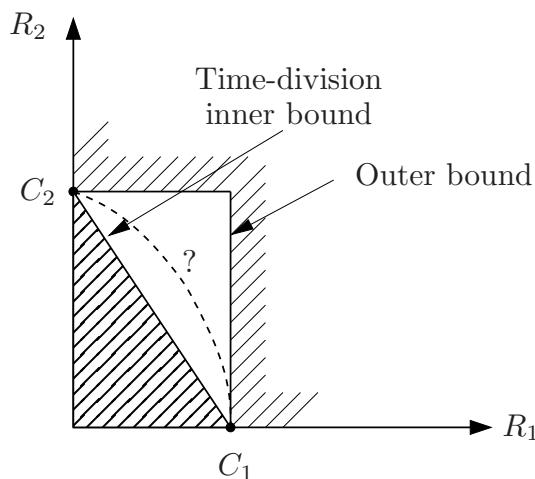


- A $(2^{nR_1}, 2^{nR_2}, n)$ code for the interference channel consists of:
 1. Two message sets $[1 : 2^{nR_1}]$ and $[1 : 2^{nR_2}]$

2. Two encoders: 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 $m_2 \in [1 : 2^{nR_2}]$
 3. Two decoders: Decoder 1 assigns an estimate $\hat{m}_1(y_1^n)$ 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 by
$$P_e^{(n)} = P\{(\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\}$$
 - 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 with $P_e^{(n)} \rightarrow 0$
 - The *capacity region* of the DM-IC is the closure of the set of achievable rate pairs (R_1, R_2)
 - As for the broadcast channel, the capacity region of the DM-IC depends on $p(y_1, y_2 | x_1, x_2)$ only through the 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

Simple Outer and Inner Bounds

- The maximum achievable individual rates are
$$C_1 := \max_{p(x_1), x_2} I(X_1; Y_1 | X_2 = x_2), \quad C_2 := \max_{p(x_2), x_1} I(X_2; Y_2 | X_1 = x_1)$$
- Using these rates, we obtain a general outer bound and a time-division inner bound



- Example (Modulo-2 sum IC): Consider an IC with $X_1, X_2, Y_1, Y_2 \in \{0, 1\}$ and $Y_1 = Y_2 = X_1 \oplus X_2$. The capacity region coincides with the time-division inner bound (why?)
- By treating interference as noise, we obtain the inner bound consisting of the set of rate pairs (R_1, R_2) such that

$$R_1 < I(X_1; Y_1|Q),$$

$$R_2 < I(X_2; Y_2|Q)$$

for some $p(q)p(x_1|q)p(x_2|q)$

- A better outer bound: By not maximizing rates individually, we obtain the outer bound consisting of the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y_1|X_2, Q),$$

$$R_2 \leq I(X_2; Y_2|X_1, Q)$$

for some $p(q)p(x_1|q)p(x_2|q)$

- Sato's Outer Bound [1]: By adding a sum rate constraint, and using the fact that capacity depends only on the marginals of $p(y_1, y_2|x_1, x_2)$, we obtain a generally tighter outer bound as follows. Let $\tilde{p}(y_1, y_2|x_1, x_2)$ have the same marginals as $p(y_1, y_2|x_1, x_2)$. It is easy to establish an outer bound $\mathcal{R}(\tilde{p}(y_1, y_2|x_1, x_2))$ that consists of the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y_1|X_2, Q),$$

$$R_2 \leq I(X_2; Y_2|X_1, Q),$$

$$R_1 + R_2 \leq I(X_1, X_2; Y_1, Y_2|Q)$$

for some $p(q)p(x_1|q)p(x_2|q)\tilde{p}(y_1, y_2|x_1, x_2)$

Therefore, the intersection of the sets $\mathcal{R}(\tilde{p}(y_1, y_2|x_1, x_2))$ over all $\tilde{p}(y_1, y_2|x_1, x_2)$ with the same marginals as $p(y_1, y_2|x_1, x_2)$ constitutes an outer bound on the capacity region of the DM-IC

- The above bounds are not tight in general

Simultaneous Decoding Inner Bound

- By having each receiver decode both messages, we obtain the inner bound [2] consisting of the set of rate pairs (R_1, R_2) such that

$$R_1 \leq \min\{I(X_1; Y_1|X_2, Q), I(X_1; Y_2|X_2, Q)\},$$

$$R_2 \leq \min\{I(X_2; Y_1|X_1, Q), I(X_2; Y_2|X_1, Q)\},$$

$$R_1 + R_2 \leq \min\{I(X_1, X_2; Y_1|Q), I(X_1, X_2; Y_2|Q)\}$$

for some $p(q)p(x_1|q)p(x_2|q)$

- Example: Consider a DM-IC with $p(y_1|x_1, x_2) = p(y_2|x_1, x_2)$. The Sato outer bound shows that the capacity region for this IC is the same as the capacity region of the DM-MAC with inputs X_1 and X_2 and output Y_1 (why?)
- A tighter inner bound: By not requiring that each receiver correctly decode the message for the other receiver, we can obtain a better inner bound consisting of the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y_1|X_2, Q),$$

$$R_2 \leq I(X_2; Y_2|X_1, Q),$$

$$R_1 + R_2 \leq \min\{I(X_1, X_2; Y_1|Q), I(X_1, X_2; Y_2|Q)\}$$

for some $p(q)p(x_1|q)p(x_2|q)$

Proof:

- Let $\mathcal{R}(X_1, X_2)$ be the set of rate pairs (R_1, R_2) such as

$$R_1 \leq I(X_1; Y_1|X_2),$$

$$R_2 \leq I(X_2; Y_2|X_1),$$

$$R_1 + R_2 \leq \min\{I(X_1, X_2; Y_1), I(X_1, X_2; Y_2)\}$$

for some $p(x_1)p(x_2)$

Note that the inner bound involving Q can be strictly larger than the convex closure of the union of the sets $\mathcal{R}(X_1, X_2)$ over all $p(x_1)p(x_2)$. Thus showing achievability for points in each $\mathcal{R}(X_1, X_2)$ and then using time-sharing, as we did in the proof of the DM-MAC achievability, does not necessarily establish the achievability of all rate pairs in the stated region

- Instead, we use the *coded time-sharing* technique described in Lecture Notes 4

- Codebook generation: Fix $p(q)p(x_1|q)p(x_2|q)$. Randomly generate a sequence $q^n \sim \prod_{i=1}^n p_Q(q_i)$. For q^n , 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 $\prod_{i=1}^n p_{X_2|Q}(x_{2i}|q_i)$
- Encoding: To send (m_1, m_2) , decoder j transmits $x_j^n(m_k)$ for $j = 1, 2$
- Decoding: Decoder 1 declares that \hat{m}_1 is sent if it is the unique message 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 ; otherwise it declares an error. Similarly, decoder 2 declares that \hat{m}_2 is sent if it is the unique message 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 ; otherwise it declares an error
- Analysis of the probability of error: Assume $(M_1, M_2) = (1, 1)$
For decoder 1, define the error events

$$\mathcal{E}_{11} := \{(Q^n, X_1^n(1), X_2^n(1), Y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\mathcal{E}_{12} := \{(Q^n, X_1^n(m_1), X_2^n(1), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1\},$$

$$\mathcal{E}_{13} := \{(Q^n, X_1^n(m_1), X_2^n(m_2), Y_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_1 \neq 1, m_2 \neq 1\}$$

Then, $P(\mathcal{E}_1) \leq P(\mathcal{E}_{11}) + P(\mathcal{E}_{12}) + P(\mathcal{E}_{13})$

By the LLN, $P(\mathcal{E}_{11}) \rightarrow 0$ as $n \rightarrow \infty$

Since for $m_1 \neq 1$, $X_1^n(m_1)$ is conditionally independent of $(X_1^n(1), X_2^n(1), Y_1^n)$ given Q^n , by the packing lemma $P(\mathcal{E}_{12}) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X_1; Y_1, X_2|Q) = I(X_1; Y_1|X_2, Q) - \delta(\epsilon)$

Similarly, by the packing lemma, $P(\mathcal{E}_{13}) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 + R_2 < I(X_1, X_2; Y|Q) - \delta(\epsilon)$

We can similarly bound the probability of error for decoder 2

Strong Interference

- A DM-IC is said to have *very strong interference* [3, 4] if

$$I(X_1; Y_1 | X_2) \leq I(X_1; Y_2), \\ I(X_2; Y_2 | X_1) \leq I(X_2; Y_1)$$

for all $p(x_1)p(x_2)$

- The capacity of the DM-IC with very strong interference is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y_1 | X_2, Q), \\ R_2 \leq I(X_2; Y_2 | X_1, Q)$$

for some $p(q)p(x_1|q)p(x_2|q)$

Note that this can be achieved via successive (interference) cancellation decoding and time sharing. Each decoder first decodes the other message, then decodes its own. Because of the very strong interference condition, only the requirements on achievable rates for the second decoding step matters

- The channel is said to have *strong interference* [5] if

$$I(X_1; Y_1 | X_2) \leq I(X_1; Y_2 | X_2), \\ I(X_2; Y_2 | X_1) \leq I(X_2; Y_1 | X_1)$$

for all $p(x_1)p(x_2)$

Note that this is an extension of the more capable notion for DM-BC (given X_2 , Y_2 is more capable than Y_1, \dots)

- Clearly, if the channel has very strong interference, it also has strong interference (the converse is not necessarily true)

Example: Consider the DM-IC with binary inputs and ternary outputs, where $Y_1 = Y_2 = X_1 + X_2$. Then

$$I(X_1; Y_1 | X_2) = I(X_1; Y_2 | X_2) = H(X_1), \\ I(X_2; Y_2 | X_1) = I(X_2; Y_1 | X_1) = H(X_2)$$

Therefore, this DM-IC has strong interference. However,

$$I(X_1; Y_1 | X_2) = H(X_1) \geq H(X_1) - H(X_1 | Y_2) = I(X_1; Y_2), \\ I(X_2; Y_2 | X_1) = H(X_2) \geq H(X_2) - H(X_2 | Y_1) = I(X_2; Y_1)$$

with strict inequality for some $p(x_1)p(x_2)$ easily established

Therefore, this channel does not satisfy the definition of very strong interference

Capacity Region Under Strong Interference

- *Theorem 1 [5]:* The capacity region of the DM-IC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with strong interference is the set of rate pairs (R_1, R_2) such as

$$R_1 \leq I(X_1; Y_1|X_2, Q),$$

$$R_2 \leq I(X_2; Y_2|X_1, Q),$$

$$R_1 + R_2 \leq \min\{I(X_1, X_2; Y_1|Q), I(X_1, X_2; Y_2|Q)\}$$

for some $p(q, x_1, x_2) = p(q)p(x_1|q)p(x_2|q)$, where $|\mathcal{Q}| \leq 4$

- Achievability follows from the simultaneous decoding inner bound discussed earlier
- Proof of converse: The first two inequalities are easy to establish. By symmetry it suffices to show that $R_1 + R_2 \leq I(X_1, X_2; Y_2|Q)$. Consider

$$\begin{aligned} n(R_1 + R_2) &= H(M_1) + H(M_2) \\ &\stackrel{(a)}{\leq} I(M_1; Y_1^n) + I(M_2; Y_2^n) + n\epsilon_n \\ &\stackrel{(b)}{\leq} I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) + n\epsilon_n \end{aligned}$$

$$\begin{aligned} &\leq I(X_1^n; Y_1^n|X_2^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\ &\stackrel{(c)}{\leq} I(X_1^n; Y_2^n|X_2^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\ &= I(X_1^n, X_2^n; Y_2^n) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(X_{1i}, X_{2i}; Y_{2i}) + n\epsilon_n = nI(X_1, X_2; Y_2|Q) + n\epsilon_n, \end{aligned}$$

where (a) follows by Fano's inequality, (b) follows by the fact that $M_j \rightarrow X_j^n \rightarrow Y_j^n$ form a Markov chain for $j = 1, 2$ (by independence of M_1, M_2), and (c) follows by the following

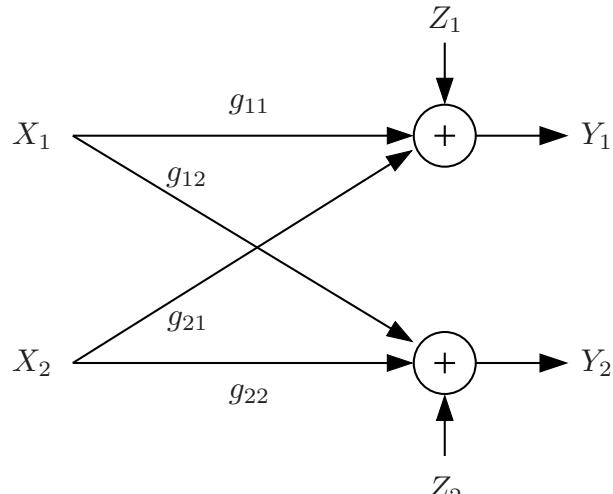
Lemma 1 [5]: For a DM-IC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with strong interference, $I(X_1^n; Y_1^n|X_2^n) \leq I(X_1^n; Y_2^n|X_2^n)$ for all $(X_1^n, X_2^n) \sim p(x_1^n)p(x_2^n)$ and all $n \geq 1$

The lemma can be proved by noting that the strong interference condition implies that $I(X_1; Y_1|X_2, U) \leq I(X_1; Y_2|X_2, U)$ for all $p(u)p(x_1|u)p(x_2|u)$ and using induction on n

The other bound follows similarly

AWGN Interference Channel

- Consider the following AWGN interference channel (AWGN-IC) model:



At time i , $Y_{1i} = g_{11}X_{1i} + g_{21}X_{2i} + Z_{1i}$, $Y_{2i} = g_{12}X_{1i} + g_{22}X_{2i} + Z_{2i}$, where $\{Z_{1i}\}$ and $\{Z_{2i}\}$ are discrete-time WGN processes with average power $N_0/2 = 1$ (independent of $\{X_{1i}\}$ and $\{X_{2i}\}$), and g_{jk} , $j, k = 1, 2$, are channel gains

Assume average power constraint P on X_1 and on X_2

- Define the *signal-to-noise* ratios $S_1 = g_{11}^2 P$, $S_2 = g_{22}^2 P$ and the *interference-to-noise* ratios $I_1 = g_{21}^2 P$ and $I_2 = g_{12}^2 P$
- The capacity region of the AWGN-IC is not known in general

Simple Inner Bounds

- *Time-division-with-power-control inner bound:* Set of all (R_1, R_2) such that

$$R_1 < \alpha C(S_1/\alpha),$$

$$R_2 < \bar{\alpha} C(S_2/\bar{\alpha})$$

for some $\alpha \in [0, 1]$

- *Treat-interference-as-noise inner bound:* Set of all (R_1, R_2) such that

$$R_1 < C(S_1/(1 + I_1)),$$

$$R_2 < C(S_2/(1 + I_2))$$

Note that this inner bound can be further improved via power control and time sharing

- *Simultaneous decoding inner bound:* Set of all (R_1, R_2) such that

$$R_1 < C(S_1),$$

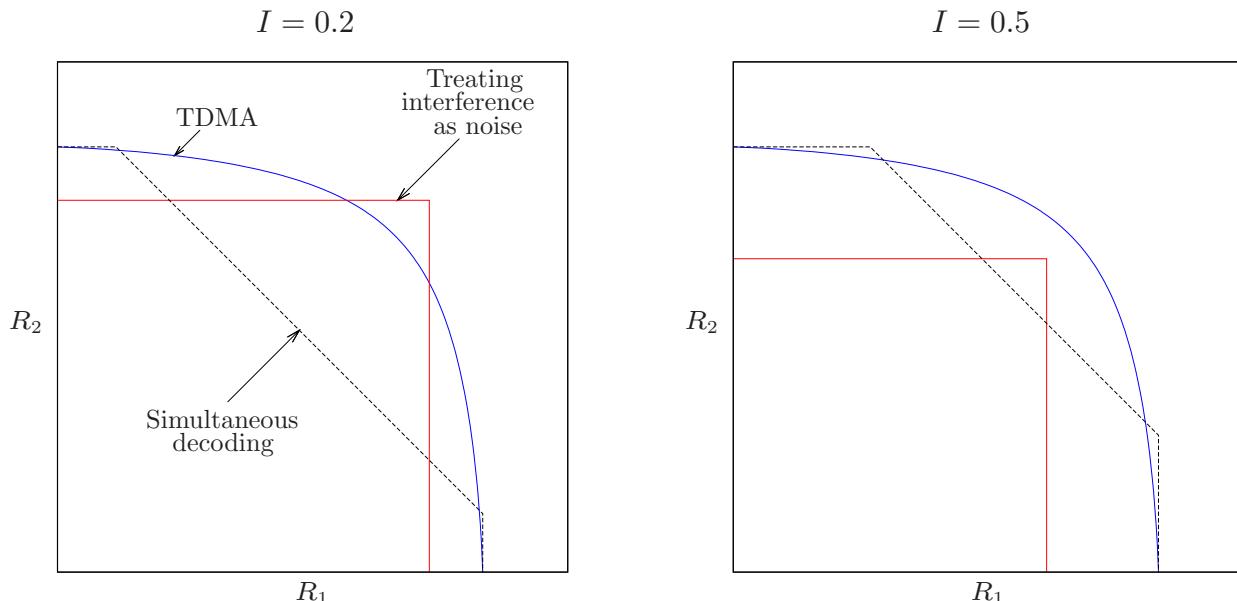
$$R_2 < C(S_2),$$

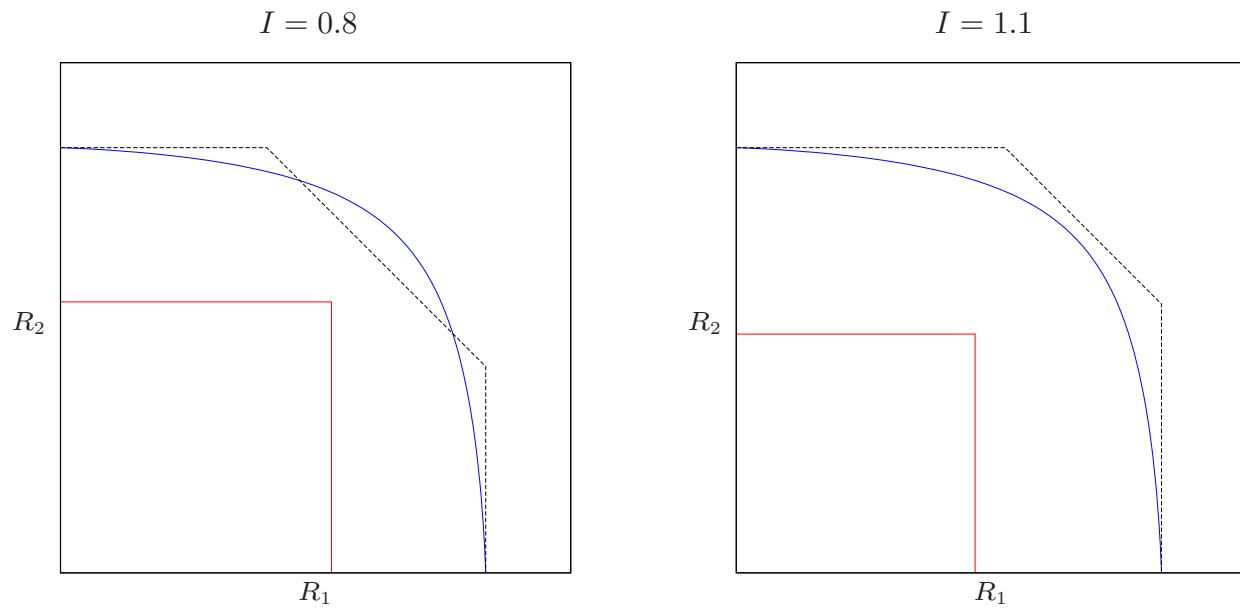
$$R_1 + R_2 < \min\{C(S_1 + I_1), C(S_2 + I_2)\}$$

- Remark: These inner bounds are achieved by using good point-to-point AWGN codes. In the simultaneous decoding inner bound, however, sophisticated decoders are needed

Comparison of the Bounds

- We consider the symmetric case ($S_1 = S_2 = S = 1$ and $I_1 = I_2 = I$)





Capacity Region of AWGN-IC Under Strong Interference

- The AWGN-IC is said to have *strong interference* if $I_2 \geq S_1$ and $I_1 \geq S_2$
- Theorem 2 [4]:* The capacity region of the AWGN-IC with strong interference is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq C(S_1), \\ R_2 &\leq C(S_2), \\ R_1 + R_2 &\leq \min\{C(S_1 + I_1), C(S_2 + I_2)\} \end{aligned}$$

- Achievability follows by the simultaneous decoding scheme
- The converse follows by noting that the above conditions are equivalent to the conditions for strong interference for the DM-IC and showing that $X_1, X_2 \sim N(0, P)$ optimize the mutual information terms

To show that the above conditions are equivalent to
 $I(X_1 : Y_1 | X_2) \leq I(X_1; Y_2 | X_2)$ and $I(X_2 : Y_2 | X_1) \leq I(X_2; Y_1 | X_1)$ for all
 $F(x_1)F(x_2)$

- If $I_2 \geq S_1$ and $I_1 \geq S_2$, then it is easy to see that both AWGN-BCs X_1 to $(Y_2 - \sqrt{S_2}X_2, Y_1 - \sqrt{I_1}X_2)$ and X_2 to $(Y_1 - \sqrt{S_1}X_1, Y_2 - \sqrt{I_2}X_1)$ are degraded, thus they are more capable. This proves one direction of the equivalence
- To prove the other direction, assume that $h(g_{11}X_1 + Z_1) \leq h(g_{12}X_1 + Z_2)$ and $h(g_{22}X_2 + Z_2) \leq h(g_{21}X_2 + Z_1)$. Substituting $X_1 \sim N(0, P)$ and $X_2 \sim N(0, P)$ shows that $I_2 \geq S_1$ and $I_1 \geq S_2$, respectively
- Remark: The conditions for *very strong interference* are $S_2 \leq I_1/(1 + S_1)$ and $S_1 \leq I_2/(1 + S_2)$. It can be shown that these conditions are equivalent to the conditions for very strong interference for the DM-IC. Under these conditions, interference does not impair communication and the capacity region is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq C(S_1), \\ R_2 &\leq C(S_2) \end{aligned}$$

Han–Kobayashi Inner Bound

- The Han–Kobayashi inner bound introduced in [6] is the best known bound on the capacity region of the DM-IC. It is tight for all cases in which the capacity region is known. We present a recent description of this inner bound in [7]
- *Theorem 4 (Han–Kobayashi Inner Bound):* A rate pair (R_1, R_2) is achievable for a general DM-IC if it satisfies the inequalities

$$R_1 < I(X_1; Y_1 | U_2, Q),$$

$$R_2 < I(X_2; Y_2 | U_1, Q),$$

$$R_1 + R_2 < I(X_1, U_2; Y_1 | Q) + I(X_2; Y_2 | U_1, U_2, Q),$$

$$R_1 + R_2 < I(X_1; Y_1 | U_1, U_2, Q) + I(X_2, U_1; Y_2 | Q),$$

$$R_1 + R_2 < I(X_1, U_2; Y_1 | U_1, Q) + I(X_2, U_1; Y_2 | U_2, Q),$$

$$2R_1 + R_2 < I(X_1, U_2; Y_1 | Q) + I(X_1; Y_1 | U_1, U_2, Q) + I(X_2, U_1; Y_2 | U_2, Q),$$

$$R_1 + 2R_2 < I(X_2, U_1; Y_2 | Q) + I(X_2; Y_2 | U_1, U_2, Q) + I(X_1, U_2; Y_1 | U_1, Q)$$

for some $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$, where $|\mathcal{U}_1| \leq |\mathcal{X}_1| + 4$, $|\mathcal{U}_2| \leq |\mathcal{X}_2| + 4$, $|\mathcal{Q}| \leq 7$

- Outline of Achievability: Split message M_j , $j = 1, 2$, into independent “public” message at rate R_{j0} and “private” message at rate R_{jj} . Thus, $R_j = R_{j0} + R_{jj}$. Superposition coding is used, whereby each public message, represented by U_j , is superimposed onto its corresponding private message. The public messages are decoded by both receivers, while each private message is decoded 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 $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$

- Codebook generation: Fix $p(q)p(u_1, x_1|q)p(u_2, x_2|q)$
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 $u_j^n(m_{j0})$, 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 the message $m_j = (m_{j0}, m_{jj})$, encoder $j = 1, 2$ transmits $x_j^n(m_{j0}, m_{jj})$
- 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 $m_{20} \in [1 : 2^{nR_{20}}]$. If no such unique pair exists, the decoder declares an error
Decoder 2 decodes 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
- We have 8 cases to consider (conditioning on q^n suppressed)

	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	$p(u_1^n, x_1^n)p(u_2^n)p(y_1^n x_1^n)$

- Cases 3,4 and 6,7 share same pmf, and case 8 does not cause an error

- We are left with only 5 error events:

$$\begin{aligned}
 \mathcal{E}_{10} &:= \{(Q^n, U_1^n(1), U_2^n(1), X_1^n(1, 1), Y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \\
 \mathcal{E}_{11} &:= \{(Q^n, U_1^n(1), U_2^n(1), X_1^n(1, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \\
 &\quad \text{for some } m_{11} \neq 1\}, \\
 \mathcal{E}_{12} &:= \{(Q^n, U_1^n(m_{10}), U_2^n(1), X_1^n(m_{10}, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \\
 &\quad \text{for some } m_{10} \neq 1, m_{11}\}, \\
 \mathcal{E}_{13} &:= \{(Q^n, U_1^n(1), U_2^n(m_{20}), X_1^n(1, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \\
 &\quad \text{for some } m_{20} \neq 1, m_{11} \neq 1\}, \\
 \mathcal{E}_{14} &:= \{(Q^n, U_1^n(m_{10}), U_2^n(m_{20}), X_1^n(m_{10}, m_{11}), Y_1^n) \in \mathcal{T}_\epsilon^{(n)} \\
 &\quad \text{for some } m_{10} \neq 1, m_{20} \neq 1, m_{11}\}
 \end{aligned}$$

Then, the average probability of error for decoder 1 is

$$P(\mathcal{E}_1) \leq \sum_{j=0}^4 P(\mathcal{E}_{1j})$$

- Now, we bound each probability of error term
 1. By the LLN, $P(\mathcal{E}_{10}) \rightarrow 0$ as $n \rightarrow \infty$

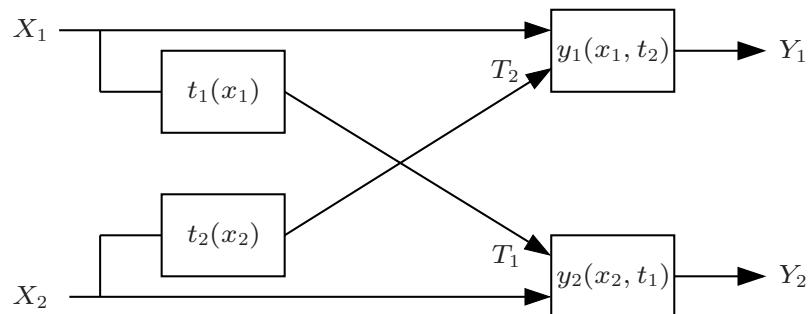
2. By the packing lemma, $P(\mathcal{E}_{11}) \rightarrow 0$ as $n \rightarrow \infty$ if
 $R_{11} < I(X_1; Y_1|U_1, U_2, Q) - \delta(\epsilon)$
 3. By the packing lemma, $P(\mathcal{E}_{12}) \rightarrow 0$ as $n \rightarrow \infty$ if
 $R_{11} + R_{10} < I(X_1; Y_1|U_2, Q) - \delta(\epsilon)$
 4. By the packing lemma, $P(\mathcal{E}_{13}) \rightarrow 0$ as $n \rightarrow \infty$ if
 $R_{11} + R_{20} < I(X_1, U_2; Y_1|U_1, Q) - \delta(\epsilon)$
 5. By the packing lemma, $P(\mathcal{E}_{14}) \rightarrow 0$ as $n \rightarrow \infty$ if
 $R_{11} + R_{10} + R_{20} < I(X_1, U_2; Y_1|Q) - \delta(\epsilon)$
- The average probability of error for decoder 2 can be bounded similarly
 - Finally, we use the Fourier–Motzkin procedure with the constraints
 $R_{j0} = R_j - R_{jj}$, $0 \leq R_{jj} \leq R_j$ for $j = 1, 2$, to eliminate R_{11}, R_{22} and obtain the region given in the theorem (see Appendix D for details)
 - Remark: The Han–Kobayashi region is tight for the class of DM-IC with strong and very strong interference. In these cases both messages are public and we obtain the capacity regions by setting $U_1 = X_1$ and $U_2 = X_2$

Capacity Region of a Class of Deterministic IC

- Consider the following deterministic interference channel: At time i

$$\begin{aligned} T_{1i} &= t_1(X_{1i}), \quad T_{2i} = t_2(X_{2i}), \\ Y_{1i} &= y_1(X_{1i}, T_{2i}), \quad Y_{2i} = y_2(X_{2i}, T_{1i}), \end{aligned}$$

where the functions y_1, y_2 satisfy the conditions 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 . For example, y_1, y_2 could be additions. Note that these conditions imply that $H(Y_1|X_1) = H(T_2)$ and $H(Y_2|X_2) = H(T_1)$



- *Theorem 5* [8]: The capacity region of the class of deterministic interference channel is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq H(Y_1|T_2),$$

$$R_2 \leq H(Y_2|T_1),$$

$$R_1 + R_2 \leq H(Y_1) + H(Y_2|T_1, T_2),$$

$$R_1 + R_2 \leq H(Y_1|T_1, T_2) + H(Y_2),$$

$$R_1 + R_2 \leq H(Y_1|T_1) + H(Y_2|T_2),$$

$$2R_1 + R_2 \leq H(Y_1) + H(Y_1|T_1, T_2) + H(Y_2|T_2),$$

$$R_1 + 2R_2 \leq H(Y_2) + H(Y_2|T_1, T_2) + H(Y_1|T_1)$$

for some $p(x_1)p(x_2)$

- Note that the region is convex
- Achievability follows by noting that the region coincides with the Han–Kobayashi achievable rate region (take $U_1 = T_1$, $U_2 = T_2$, $Q = \emptyset$)

- Note that by the conditions on the functions y_1, y_2 , each receiver knows, after decoding its own codeword, the interference caused by the other sender exactly, i.e., decoder 1 knows T_2^n after decoding its intended codeword X_1^n , and similarly decoder 2 knows T_1^n after decoding X_2^n . Thus T_1 and T_2 can be naturally considered as the common messages in the Han–Kobayashi scheme

Proof of Converse

- Consider the first two inequalities. By evaluating the simple outer bound we discussed earlier, we have

$$\begin{aligned}
 nR_1 &\leq nI(X_1; Y_1 | X_2, Q) + n\epsilon_n \\
 &= nH(Y_1 | T_2, Q) + n\epsilon_n \leq nH(Y_1 | T_2) + n\epsilon_n, \\
 nR_2 &\leq nH(Y_1 | T_2) + n\epsilon_n,
 \end{aligned}$$

where Q is the usual time-sharing random variable

- Consider the third inequality. By Fano's inequality

$$\begin{aligned}
 n(R_1 + R_2) &\leq I(M_1; Y_1^n) + I(M_2; Y_2^n) + n\epsilon_n \\
 &\stackrel{(a)}{\leq} I(M_1; Y_1^n) + I(M_2; Y_2^n, T_2^n) + n\epsilon_n \\
 &\leq I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n, T_2^n) + n\epsilon_n \\
 &\stackrel{(b)}{\leq} I(X_1^n; Y_1^n) + I(X_2^n; T_2^n, Y_2^n | T_1^n) + n\epsilon_n \\
 &= H(Y_1^n) - H(Y_1^n | X_1^n) + I(X_2^n; T_2^n | T_1^n) + I(X_2^n; Y_2^n | T_1^n, T_2^n) + n\epsilon_n \\
 &\stackrel{(c)}{=} H(Y_1^n) + H(Y_2^n | T_1^n, T_2^n) + n\epsilon_n
 \end{aligned}$$

$$\begin{aligned}
 &\leq \sum_{i=1}^n (H(Y_{1i}) + H(Y_{2i} | T_{1i}, T_{2i})) + n\epsilon_n \\
 &= n(H(Y_1 | Q) + H(Y_2 | T_1, T_2, Q)) + n\epsilon_n \\
 &\leq n(H(Y_1) + H(Y_2 | T_1, T_2)) + n\epsilon_n
 \end{aligned}$$

Step (a) is the key step in the proof. Even if a “genie” gives receiver Y_2 its common message T_2 as side information to help it decode 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, we have

$$n(R_1 + R_2) \leq n(H(Y_2 | Q) + H(Y_1 | T_1, T_2, Q)) + n\epsilon_n$$

- Consider the fifth inequality,

$$\begin{aligned}
 n(R_1 + R_2) &\leq I(X_1^n; Y_1^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\
 &\leq I(X_1^n; Y_1^n | T_1^n) + I(X_2^n; Y_2^n | T_2^n) + n\epsilon_n \\
 &= H(Y_1^n | T_1^n) + H(Y_2^n | T_2^n) + n\epsilon_n \\
 &\leq n(H(Y_1 | T_1) + H(Y_2 | T_2)) + n\epsilon_n,
 \end{aligned}$$

where (a) follows by the independence of X_j^n and T_j^n for $j = 1, 2$

- Following similar steps, consider the sixth inequality,

$$\begin{aligned}
n(2R_1 + R_2) &\leq 2I(M_1; Y_1^n) + I(M_2; Y_2^n) + n\epsilon_n \\
&\leq I(X_1^n; Y_1^n) + I(X_1^n; Y_1^n, T_1^n | T_2^n) + I(X_2^n; Y_2^n) + n\epsilon_n \\
&= H(Y_1^n) - H(T_2^n) + H(T_1^n) + H(Y_1^n | T_1^n, T_2^n) + H(Y_2^n) - H(T_1^n) + n\epsilon_n \\
&= H(Y_1^n) - H(T_2^n) + H(Y_1^n | T_1^n, T_2^n) + H(Y_2^n) + n\epsilon_n \\
&\leq H(Y_1^n) + H(Y_1^n | T_1^n, T_2^n) + H(Y_2^n | T_2^n) + n\epsilon_n \\
&\leq n(H(Y_1) + H(Y_1 | T_1, T_2) + H(Y_2 | T_2)) + n\epsilon_n
\end{aligned}$$

- Similarly, for the last inequality, we have

$$n(R_1 + 2R_2) \leq n(H(Y_2) + H(Y_2 | T_1, T_2) + H(Y_1 | T_1)) + n\epsilon_n$$

- This completes the proof of the converse
- The idea of a genie giving receivers side information will be subsequently used to establish outer bounds on the capacity region of the AWGN interference channel (see [9])

Sum-Capacity of AWGN-IC Under Weak Interference

- Define the *sum capacity* C_{sum} of the AWGN-IC as the supremum over the sum rate $(R_1 + R_2)$ such that (R_1, R_2) is achievable
- *Theorem 3* [10, 11, 12]: For the AWGN-IC, if the *weak interference* conditions $\sqrt{I_1/S_2}(1+I_2) \leq \rho_2\sqrt{1-\rho_1^2}$ and $\sqrt{I_2/S_1}(1+I_1) \leq \rho_1\sqrt{1-\rho_2^2}$ hold for some $\rho_1, \rho_2 \in [0, 1]$, then the sum capacity is

$$C_{\text{sum}} = C\left(\frac{S_1}{1+I_1}\right) + C\left(\frac{S_2}{1+I_2}\right)$$

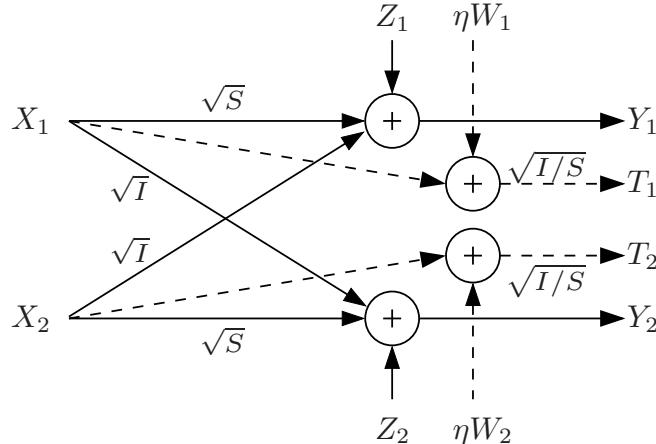
- Achievability follows by treating interference as Gaussian noise
- The interesting part of the proof is the converse. It involves using a *genie* to establish an outer bound on the capacity region of the AWGN-IC
- For simplicity of presentation, we consider the symmetric case with $I_1 = I_2 = I$ and $S_1 = S_2 = S$. In this case, the *weak interference* condition reduces to $\sqrt{I/S}(1+I) \leq 1/2$ and the sum capacity is $C_{\text{sum}} = 2C(S/(1+I))$

Proof of Converse

- Consider the AWGN-IC with side information T_{1i} at Y_{1i} and T_{2i} at Y_{2i} at each time i , where

$$T_{1i} = \sqrt{I/S} (X_{1i} + \eta W_{1i}), \quad T_{2i} = \sqrt{I/S} (X_{2i} + \eta W_{2i}),$$

and $\{W_{1i}\}$ and $\{W_{2i}\}$ are independent WGN(1) processes random variables with $E(Z_{1i}W_{1i}) = E(Z_{2i}W_{2i}) = \rho$ and $\eta \geq 0$



- Clearly, the sum capacity of this channel $\tilde{C}_{\text{sum}} \geq C_{\text{sum}}$

- Proof outline:
 - We first show that if $\eta^2 I \leq (1 - \rho^2)S$ (useful genie), then the sum capacity of the genie aided channel is achieved via Gaussian inputs and by treating interference as noise
 - We then show that if in addition, $\eta\rho\sqrt{S} = 1 + I$ (smart genie), then the sum capacity of the genie aided channel is the same as if there were no genie. Since $\tilde{C}_{\text{sum}} \geq C_{\text{sum}}$, this also shows that C_{sum} is achieved via Gaussian signals and by treating interference as noise
 - Using the second condition to eliminate η from the first condition gives $\sqrt{I/S}(1 + I) \leq \rho^2\sqrt{1 - \rho^2}$. Taking $\rho = 1/2$, 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 worst noise with a given average power in an additive noise channel with Gaussian input, and properties of jointly Gaussian random variables

- *Lemma 2* (Useful genie): Suppose that

$$\eta^2 I \leq (1 - \rho^2)S.$$

Then the sum capacity of the above genie aided channel is

$$\tilde{C}_{\text{sum}} = I(X_1^*; Y_1^*, T_1^*) + I(X_2^*; Y_2^*, T_2^*),$$

where the superscript * indicates zero mean Gaussian random variable with appropriate average power, and \tilde{C}_{sum} is achieved by treating interference as noise

- Remark: If $\rho = 0$, $\eta = 1$ and $I \leq S$, the genie is always useful. This gives a general outer bound on the capacity region (not just an upper bound on the sum capacity) under weak interference [13]

- Proof of Lemma 2:

The sum capacity is achieved by treating interference as Gaussian noise.

Therefore, we only need to prove the converse

- Let $(T_1, T_2, Y_1, Y_2) := (T_{1i}, T_{2i}, Y_{1i}, Y_{2i})$ with probability $1/n$ for $i \in [1 : n]$. In other words, for time-sharing random variable $Q \sim \text{Unif}[1 : n]$, independent of all other random variables, $T_1 = T_{1Q}$ and so on

Suppose a rate pair $(\tilde{R}_1, \tilde{R}_2)$ is achievable for the genie aided channel. Then by Fano's inequality,

$$\begin{aligned} n\tilde{R}_1 &\leq I(X_1^n; Y_1^n, T_1^n) + n\epsilon_n \\ &= I(X_1^n; T_1^n) + I(X_1^n; Y_1^n | T_1^n) + n\epsilon_n \\ &= h(T_1^n) - h(T_1^n | X_1^n) + h(Y_1^n | T_1^n) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\leq h(T_1^n) - h(T_1^n | X_1^n) + \sum_{i=1}^n h(Y_{1i} | T_1^n) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\stackrel{(a)}{\leq} h(T_1^n) - h(T_1^n | X_1^n) + \sum_{i=1}^n h(Y_{1i} | T_1) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\stackrel{(b)}{\leq} h(T_1^n) - h(T_1^n | X_1^n) + nh(Y_1^* | T_1^*) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\stackrel{(c)}{=} h(T_1^n) - nh(T_1^* | X_1^*) + nh(Y_1^* | T_1^*) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n \\ &\leq h(T_1^n) - nh(T_1^* | X_1^*) + nh(Y_1^* | T_1^*) - h(Y_1^n | T_1^n, X_1^n) + n\epsilon_n, \end{aligned}$$

where (a) follows since $h(Y_{1i} | T_1^n) = h(Y_{1i} | T_1^n, Q) \leq h(Y_{1i} | T_{1Q}, Q) \leq h(Y_{1i} | T_{1Q})$, (b) follows by the maximum differential entropy lemma and concavity of Gaussian entropy in power, and (c) follows by the fact that

$$h(T_1^n|X_1^n) = h\left(\eta\sqrt{I/S} W_1^n\right) = nh\left(\eta\sqrt{I/S} W_1\right) = nh(T_1^*|X_1^*)$$

Similarly,

$$n\tilde{R}_2 \leq h(T_2^n) - nh(T_2^*|X_2^*) + nh(Y_2^*|T_2^*) - h(Y_2^n|T_2^n, X_2^n) + n\epsilon_n$$

- o Thus, we can upper bound the sum rate $\tilde{R}_1 + \tilde{R}_2$ by

$$\begin{aligned}\tilde{R}_1 + \tilde{R}_2 &\leq h(T_1^n) - h(Y_2^n|T_2^n, X_2^n) - nh(T_1^*|X_1^*) + nh(Y_1^*|T_1^*) \\ &\quad + h(T_2^n) - h(Y_1^n|T_1^n, X_1^n) - nh(T_2^*|X_2^*) + nh(Y_2^*|T_2^*) + n\epsilon_n\end{aligned}$$

- o Evaluating the first two terms

$$\begin{aligned}h(T_1^n) - h(Y_2^n|T_2^n, X_2^n) &= h\left(\sqrt{I/S}X_1^n + \eta\sqrt{I}W_1^n\right) - h\left(\sqrt{I/S}X_1^n + Z_2^n|W_2^n\right) \\ &= h\left(\sqrt{I/S}X_1^n + V_1^n\right) - h\left(\sqrt{I/S}X_1^n + V_2^n\right),\end{aligned}$$

where $V_1^n := \eta\sqrt{I/S} W_1^n$ is i.i.d. $N(0, \eta^2 I/S)$, $V_2^n := E(Z_2^n|W_2^n)$ is i.i.d. $N(0, 1 - \rho^2)$

- o Assuming $\eta^2 I/S \leq 1 - \rho^2$, let $V_2^n = V_1^n + V^n$, where V^n is i.i.d. $N(0, 1 - \rho^2 - \eta^2 I/S)$ and independent of V_1^n

As before, define $(V, V_1, V_2, X_1) := (V_Q, V_{1Q}, V_{2Q}, X_{1Q})$ and consider

$$h(T_1^n) - h(Y_2^n|T_1^n, X_1^n) = h\left(\sqrt{I/S}X_1^n + V_1^n\right) - h\left(\sqrt{I/S}X_1^n + V_2^n\right)$$

$$\begin{aligned}&= -I(V^n; \sqrt{I/S}X_1^n + V_1^n + V^n) \\ &= -nh(V) + h(V^n | \sqrt{I/S}X_1^n + V_1^n + V^n) \\ &\leq -nh(V) + \sum_{i=1}^n h(V_i | \sqrt{I/S}X_1^n + V_1^n + V^n) \\ &\leq -nh(V) + \sum_{i=1}^n h(V_i | \sqrt{I/S}X_1 + V_1 + V) \\ &\leq -nh(V) + nh(V | \sqrt{I/S}X_1 + V_1 + V) \\ &\stackrel{(b)}{\leq} -nI(V; \sqrt{I/S}X_1^* + V_1 + V) \\ &= -nh(\sqrt{I/S}X_1^* + V_1 + V) + nh(\sqrt{I/S}X_1^* + V_1) \\ &= nh(T_1^*) - nh(Y_2^*|T_2^*, X_2^*),\end{aligned}$$

where (b) follows from the fact that Gaussian is the worst noise with a given average power in an additive noise channel with Gaussian input

- The $(h(T_2^n) - h(Y_1^n|T_1^n, X_1^n))$ terms can be bounded in the same manner.
This complete the proof of the lemma
- *Proof of Theorem 3:* Suppose that the following *smart genie* condition

$$\eta\rho\sqrt{S} = I + 1$$

holds. Combined with the (useful genie) condition for the lemma, this gives the weak interference condition

$$\sqrt{I/S}(1+I) \leq \frac{1}{2}$$

From the smart genie condition, the MMSE estimate of X_1^* given $(\sqrt{S}X_1^* + \sqrt{I}X_2^* + Z_1)$ and $(X_1^* + \eta W_1)$ can be shown to be the same as the MMSE estimate of X_1^* given only $(\sqrt{S}X_1^* + \sqrt{I}X_2^* + Z_1)$, i.e.,

$$\mathbb{E} \left[\eta\sqrt{S} W_1 (\sqrt{I}X_2^* + Z_1) \right] = \mathbb{E} \left[(\sqrt{I}X_2^* + Z_1)^2 \right]$$

Since all random variables involved are jointly Gaussian, this implies that $X_1^* \rightarrow (\sqrt{S}X_1^* + \sqrt{I}X_2^* + Z_1) \rightarrow \sqrt{S}(X_1^* + \eta W_1)$ form a Markov chain, or equivalently,

$$\begin{aligned} I(X_1^*; T_1^*|Y_1^*) &= I(X_1^*; X_1^* + \eta W_1 | \sqrt{S}X_1^* + \sqrt{I}X_2^* + Z_1) \\ &= I(X_1^*; \sqrt{S}X_1^* + \eta\sqrt{S}W_1 | \sqrt{S}X_1^* + \sqrt{I}X_2^* + Z_1) = 0 \end{aligned}$$

Simiarly $I(X_2^*; T_2^*|Y_2^*) = 0$

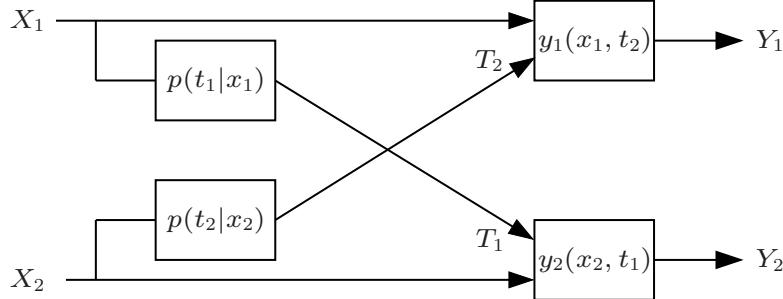
Now from lemma, we have

$$\begin{aligned} C_{\text{sum}} &\leq I(X_1^*; Y_1^*, T_1^*) + I(X_2^*; Y_2^*, T_2^*) \\ &= I(X_1^*; Y_1^*) + I(X_2^*; Y_2^*), \end{aligned}$$

which completes the proof of converse

Class of Semideterministic DM-IC

- We establish inner and outer bounds on the capacity region of the AWGN-IC that differ by no more than 1/2-bit [13] per user using the method in [14]
- Consider the following class of interference channels, which is a generalization of the class of deterministic interference channels discussed earlier



Here again the functions y_1, y_2 satisfy the condition that for $x_1 \in \mathcal{X}_1$, $y_1(x_1, t_2)$ is a one-to-one function of t_2 and for $x_2 \in \mathcal{X}_2$, $y_2(x_2, t_1)$ 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

- Note that the AWGN interference channel is a special case of this class, where $T_1 = g_{12}X_1 + Z_2$ and $T_2 = g_{21}X_2 + Z_1$

Outer Bound

- *Lemma 3* [14]: Every achievable rate pair (R_1, R_2) must satisfy the inequalities

$$R_1 \leq H(Y_1|X_2, Q) - H(T_2|X_2),$$

$$R_2 \leq H(Y_2|X_1, Q) - H(T_1|X_1),$$

$$R_1 + R_2 \leq H(Y_1|Q) + H(Y_2|U_2, X_1, Q) - H(T_1|X_1) - H(T_2|X_2),$$

$$R_1 + R_2 \leq H(Y_1|U_1, X_2, Q) + H(Y_2|Q) - H(T_1|X_1) - H(T_2|X_2),$$

$$R_1 + R_2 \leq H(Y_1|U_1, Q) + H(Y_2|U_2, Q) - H(T_1|X_1) - H(T_2|X_2),$$

$$2R_1 + R_2 \leq H(Y_1|Q) + H(Y_1|U_1, X_2, Q) + H(Y_2|U_2, Q)$$

$$- H(T_1|X_1) - 2H(T_2|X_2),$$

$$R_1 + 2R_2 \leq H(Y_2|Q) + H(Y_2|U_2, X_1, Q) + H(Y_1|U_1, Q)$$

$$- 2H(T_1|X_1) - H(T_2|X_2)$$

for some Q, X_1, X_2, U_1, U_2 such that $p(q, x_1, x_2) = p(q)p(x_1|q)p(x_2|q)$ and $p(u_1, u_2|q, x_1, x_2) = p_{T_1|X_1}(u_1|x_1)p_{T_2|X_2}(u_2|x_2)$

- Note that this outer bound is *not* tight under the strong interference condition
- Denote the above outer bound for a fixed $p(q)p(x_1|q)p(x_2|q)$ by $\mathcal{R}_o(Q, X_1, X_2)$

- For the AWGN-IC, we have the corresponding outer bound with differential entropies in place of entropies
- The proof of the outer bound again uses the genie argument with U_j conditionally independent of T_j given X_j , $j = 1, 2$. The details are given in the Appendix

Inner Bound

- 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 set of rate pairs (R_1, R_2) such that

$$R_1 \leq H(Y_1|U_2, Q) - H(T_2|U_2, Q),$$

$$R_2 \leq H(Y_2|U_1, Q) - H(T_1|U_1, Q),$$

$$R_1 + R_2 \leq H(Y_1|Q) + H(Y_2|U_1, U_2, Q) - H(T_1|U_1, Q) - H(T_2|U_2, Q),$$

$$R_1 + R_2 \leq H(Y_1|U_1, U_2, Q) + H(Y_2|Q) - H(T_1|U_1, Q) - H(T_2|U_2, Q),$$

$$R_1 + R_2 \leq H(Y_1|U_1, Q) + H(Y_2|U_2, Q) - H(T_1|U_1, Q) - H(T_2|U_2, Q),$$

$$\begin{aligned} 2R_1 + R_2 &\leq H(Y_1|Q) + H(Y_1|U_1, U_2, Q) + H(Y_2|U_2, Q) \\ &\quad - H(T_1|U_1, Q) - 2H(T_2|U_2, Q), \end{aligned}$$

$$\begin{aligned} R_1 + 2R_2 &\leq H(Y_2|Q) + H(Y_2|U_1, U_2, Q) + H(Y_1|U_1, Q) \\ &\quad - 2H(T_1|U_1, Q) - H(T_2|U_2, Q) \end{aligned}$$

for some Q, X_1, X_2, U_1, U_2 such that $p(q, x_1, x_2) = p(q)p(x_1|q)p(x_2|q)$ and $p(u_1, u_2|q, x_1, x_2) = p_{T_1|X_1}(u_1|x_1) p_{T_2|X_2}(u_2|x_2)$

- This inner bound coincides with the outer bound for the class of deterministic interference channels 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 $U_2 = T_2$)
- Denote the above inner bound for a fixed $p(q)p(x_1|q)p(x_2|q)$ by $\mathcal{R}_i(Q, X_1, X_2)$
- For the AWGN-IC, we have the corresponding inner bound with differential entropies in place of entropies

Gap Between Inner and Outer Bounds

- *Proposition 5 [14]:* If $(R_1, R_2) \in \mathcal{R}_o(Q, X_1, X_2)$, then $(R_1 - I(X_2; T_2|U_2, Q), R_2 - I(X_1; T_1|U_1, Q))$ is achievable
- Proof:
 - Construct a larger rate region $\overline{\mathcal{R}}_o(Q, X_1, X_2)$ from $\mathcal{R}_o(Q, X_1, X_2)$, by replacing every X_j in a positive conditioning entropy term in the outer bound by U_j . Clearly $\overline{\mathcal{R}}_o(Q, X_1, X_2) \supseteq \mathcal{R}_o(Q, X_1, X_2)$
 - Observing that for $j = 1, 2$, $I(X_j; T_j|U_j) = H(T_j|U_j) - H(T_j|X_j)$ and comparing the equivalent achievable region $\mathcal{R}_i(Q, X_1, X_2)$ to $\overline{\mathcal{R}}_o(Q, X_1, X_2)$, we see that $\overline{\mathcal{R}}_o(Q, X_1, X_2)$ can be equivalently described as the set of (R_1, R_2) such that $(R_1 - I(X_2; T_2|U_2, Q), R_2 - I(X_1; T_1|U_1, Q)) \in \mathcal{R}_i(Q, X_1, X_2)$

Half-Bit Theorem for AWGN-IC

- Using the inner and outer bound on the capacity region of the semideterministic DM-IC, we provide an outer bound on the capacity region of the general AWGN-IC and show that this outer bound is achievable within 1/2 bit
- The outer bound for the semideterministic DM-IC gives the outer bound consisting of the set of (R_1, R_2) such that

$$R_1 \leq C(S_1),$$

$$R_2 \leq C(S_2),$$

$$R_1 + R_2 \leq C\left(\frac{S_1}{1+I_2}\right) + C(I_2 + S_2),$$

$$R_1 + R_2 \leq C\left(\frac{S_2}{1+I_1}\right) + C(I_1 + S_1),$$

$$R_1 + R_2 \leq C\left(\frac{S_1 + I_1 + I_1 I_2}{1+I_2}\right) + C\left(\frac{S_2 + I_2 + I_1 I_2}{1+I_1}\right),$$

$$2R_1 + R_2 \leq C\left(\frac{S_1}{1+I_2}\right) + C(S_1 + I_1) + C\left(\frac{S_2 + I_2 + I_1 I_2}{1+I_1}\right),$$

$$R_1 + 2R_2 \leq C\left(\frac{S_2}{1+I_1}\right) + C(S_2 + I_2) + C\left(\frac{S_1 + I_1 + I_1 I_2}{1+I_2}\right)$$

Denote this outer bound by $\mathcal{R}_0^{\text{AWGN-IC}}$

- For the general AWGN-IC, we have $T_1 = g_{12}X_1 + Z_2$, $U_1 = g_{12}X_1 + Z'_2$, $T_2 = g_{21}X_2 + Z_1$, and $U_2 = g_{21}X_2 + Z'_1$, where Z_j and Z'_j are independent $N(0, 1)$ for $j = 1, 2$
- Proposition 5 now leads to the following approximation on the capacity region
- *Half-Bit Theorem* [13]: For the AWGN-IC, if $(R_1, R_2) \in \mathcal{R}_0^{\text{AWGN-IC}}$, then $(R_1 - 1/2, R_2 - 1/2)$ is achievable
- Proof: For $j = 1, 2$, consider

$$\begin{aligned} I(X_j; T_j | U_j, Q) &= h(T_j | U_j, Q) - h(T_j | U_j, X_j, Q) \\ &\leq h(T_j - U_j) - h(Z_j) \\ &= 1/2 \text{ bit} \end{aligned}$$

Symmetric Degrees of Freedom

- Consider the symmetric Gaussian case where

$$S_1 = S_2 = S \quad \text{and} \quad I_1 = I_2 = I$$

Note that S and I fully characterize the channel

- We are interested in the maximum achievable symmetric rate ($C_{\text{sym}} = R_1 = R_2$)
- Specializing the outer bound $\mathcal{R}_{\text{o}}^{\text{AWGN-IC}}$ to the symmetric case yields

$$C_{\text{sym}} \leq \bar{R} := \min \left\{ C(S), \frac{1}{2} C\left(\frac{S}{1+I}\right) + \frac{1}{2} C(S+I), \right. \\ \left. C\left(\frac{S+I+I^2}{1+I}\right), \frac{2}{3} C\left(\frac{S}{1+I}\right) + \frac{1}{3} C(S+2I+I^2) \right\}$$

- Normalizing C_{sym} by the interference-free capacity, let

$$d_{\text{sym}} := \frac{C_{\text{sym}}}{C(S)}$$

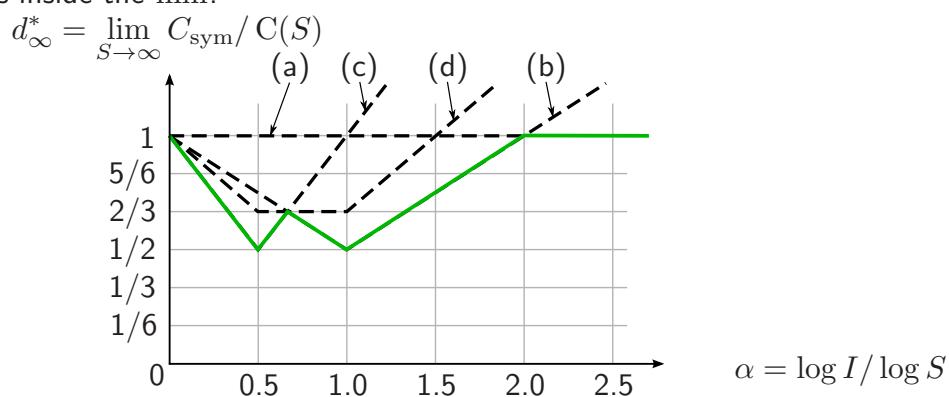
- From the 1/2-bit result, $(\bar{R} - 1/2)/C(S) \leq d_{\text{sym}} \leq \bar{R}/C(S)$, and the difference between the upper and lower bounds converges to zero as $S \rightarrow \infty$. Thus,

$d_{\text{sym}} \rightarrow d^*$, “the degrees of freedom” (DoF), which depends on how I scales as $S \rightarrow \infty$

- Let $\alpha := \log I / \log S$ (i.e., $I = S^\alpha$). Then, as $S \rightarrow \infty$,

$$d_{\text{sym}} \rightarrow d^*(\alpha) = \lim_{S \rightarrow \infty} \frac{\bar{R}(S, I = S^\alpha)}{C(S)} \\ = \min \{1, \max\{\alpha/2, 1 - \alpha/2\}, \max\{\alpha, 1 - \alpha\}, \\ \max\{2/3, 2\alpha/3\} + \max\{1/3, 2\alpha/3\} - 2\alpha/3\}$$

This is plotted in the figure, where (a), (b), (c), and (d) correspond to the bounds inside the min:



- Remarks:
 - Note that constraint (d) is redundant (only tight at $\alpha = 2/3$, but so are bounds (b) and (c)). This simplifies the DoF expression to

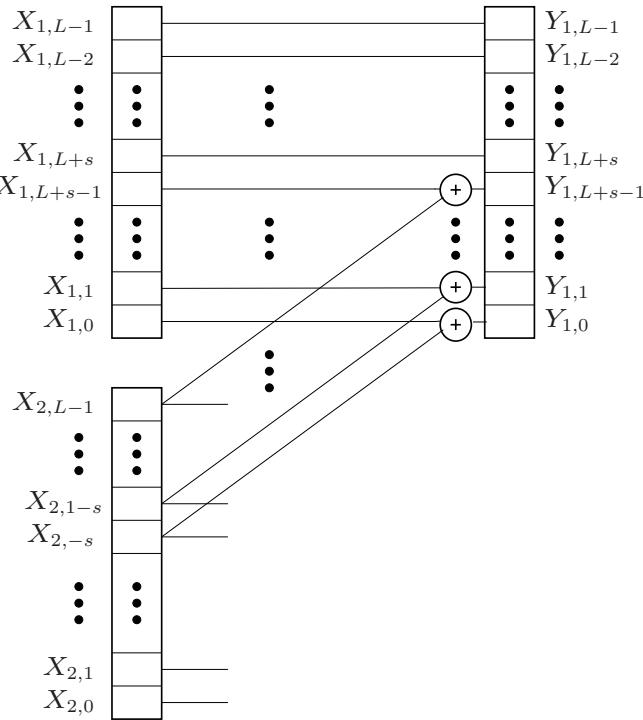
$$d^*(\alpha) = \min \{1, \max\{\alpha, 1 - \alpha\}, \max\{\alpha/2, 1 - \alpha/2\}\}$$
 - $\alpha \rightarrow 0$: negligible interference
 - $\alpha < 1/2$: treating interference as noise is optimal
 - $1/2 < \alpha < 1$: partial decoding of other message (a la H-K) is optimal (note the surprising “W” shape with maximum at $\alpha = 2/3$)
 - $\alpha = 1/2$ and $\alpha = 1$: time division is optimal
 - $1 < \alpha \leq 2$: strong interference
 - $\alpha \geq 2$: very strong interference; interference does not impair capacity
- High SNR regime: In the above results the channel gains are scaled. Alternatively, we can fix the channel coefficients and scale the power $P \rightarrow \infty$. It is not difficult to see that $\lim_{P \rightarrow \infty} d^* = 1/2$, independent of the values of the channel gains. Thus time-division is asymptotically optimal

Deterministic Approximation of AWGN-IC

- Consider the q -ary expansion deterministic interference channel (QED-IC) proposed by Avestimehr, Diggavi, and Tse 2007 [15] as an approximation to the Gaussian interference channel in the high SNR regime
- The inputs to the QED-IC are q -ary L -vectors X_1, X_2 for some “qit-pipe” number L . So, we can express X_1 as $[X_{1,L-1}, X_{1,L-2}, X_{1,L-3}, \dots, X_{1,0}]^T$, 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 $\alpha \in [0, 2]$, where $\alpha L \in \mathbb{Z}$. 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., $0 \leq \alpha < 1$, and Y_1 is a q -ary L -vector with

$$Y_{1l} = \begin{cases} X_{1l} & \text{if } L + s \leq l \leq L - 1, \\ X_{1l} + X_{2,l-s} \mod q & \text{if } 0 \leq l \leq L + s - 1 \end{cases}$$

This case is depicted in the figure below



The outputs of the channel can be represented as

$$Y_1 = X_1 + G_s X_2,$$

$$Y_2 = G_s X_1 + X_2,$$

where G_s denotes the $L \times L$ (down)shift matrix with $G_s(j, k) = 1$ if $k = j - s$ and $G_s(j, k) = 0$, otherwise

- *Upshift:* Here $s \geq 0$, i.e., $1 \leq \alpha \leq 2$, and Y_1 is a q -ary αL -vector with

$$Y_{1l} = \begin{cases} X_{2,l-s} & \text{if } L \leq l \leq L + s - 1, \\ X_{1l} + X_{2,l-s} \pmod{q} & \text{if } s \leq l \leq L - 1, \\ X_{1l} & \text{if } 0 \leq l \leq s - 1 \end{cases}$$

Again the outputs of the channel can be represented as

$$Y_1 = X_1 + G_s X_2,$$

$$Y_2 = G_s X_1 + X_2,$$

where G_s denotes the $(L + s) \times L$ (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 is obtained by a straightforward evaluation of the capacity region for the class of deterministic IC. Let $R'_j := R_j/(L \log q)$, $j = 1, 2$. The “normalized” capacity region \mathcal{C}' is the set of rate pairs (R'_1, R'_2) such that:

$$\begin{aligned} R'_1 &\leq 1, \\ R'_2 &\leq 1, \\ R'_1 + R'_2 &\leq \max\{2\alpha, 2 - 2\alpha\}, \\ R'_1 + R'_2 &\leq \max\{\alpha, 2 - \alpha\}, \\ 2R'_1 + R'_2 &\leq 2, \\ R'_1 + 2R'_2 &\leq 2 \end{aligned}$$

for $\alpha \in [1/2, 1]$, and

$$\begin{aligned} R'_1 &\leq 1, \\ R'_2 &\leq 1, \\ R'_1 + R'_2 &\leq \max\{2\alpha, 2 - 2\alpha\}, \\ R'_1 + R'_2 &\leq \max\{\alpha, 2 - \alpha\} \end{aligned}$$

for $\alpha \in [0, 1/2) \cup (1, 2]$

- The capacity region of the symmetric QED-IC can be achieved with zero error using a simple single-letter linear coding technique [16, 17]. To illustrate this, we consider the normalized symmetric capacity $C'_{\text{sym}} = \max\{R : (R, R) \in \mathcal{C}'\}$
Each sender represents its “single-letter” message by an LC'_{sym} -qit vector U_j , $j = 1, 2$, and sends $X_j = AU_j$, where A is an $L \times LC'_{\text{sym}}$ binary matrix A .
Each decoder multiplies each received symbol Y_j by a corresponding $LC'_{\text{sym}} \times L$ matrix B to recover U_j perfectly!

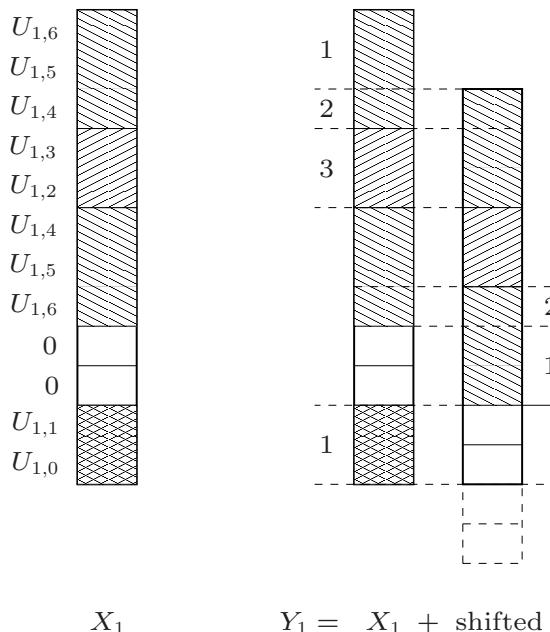
For example, consider a binary expansion deterministic IC with $L = 12$ and $\alpha = 5/6$. The symmetric capacity $C_{\text{sym}} = 7$ bits/transmission

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 the figure



X_1

$Y_1 = X_1 + \text{shifted } X_2$

Decoding of U_1 can also be done sequentially as follows (see the figure):

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 procedure corresponds to the decoding matrix

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

Note that $BA = I$ and $BAG_s = 0$, so the interference is canceled out while the intended signal can be recovered

Similar coding procedures can be readily developed for any q -ary alphabet, dimension L , and $\alpha \in [0, 2]$

The symmetric capacity can be written as

$$C_{\text{sym}} = H(U_j) = I(U_j; Y_j) = I(X_j; Y_j), \quad j = 1, 2$$

under the given choice of input $X_j = AU_j$, where U_j is uniform over the set of q -ary C_{sym} vectors. Hence, the capacity is achieved (with zero error) by simply treating interference as noise !!

In fact, it can be shown [17] that the same linear coding technique can achieve the entire capacity region. Thus, the capacity region for this channel is achieved by treating interference as noise and is characterized as the set of rate pairs such that

$$R_1 < I(X_1; Y_1),$$

$$R_2 < I(X_2; Y_2)$$

for some $p(x_1)p(x_2)$

QED-IC Approximation of the AWGN-IC

- Note that the normalized symmetric capacity of the QED-IC (check!) is

$$C'_{\text{sym}} = \min \{1, \max\{\alpha, 1 - \alpha\}, \max\{\alpha/2, 1 - \alpha/2\}\}$$

- This matches the DoF, $d^*(\alpha)$, of the Gaussian channel exactly !
- It turned out that in the limit, the symmetric AWGN-IC is equivalent to the QED-IC. We only sketch achievability, i.e., show that achievability carries over from a q -ary expansion deterministic IC to the AWGN-IC [16]:
 - Express the inputs and outputs of the AWGN-IC in base- q representation, e.g., $X_1 = X_{1,L-1}X_{1,L-2}X_{1,L-3}\dots X_{11}X_{10}X_{1,-1}X_{1,-2}\dots$, where $X_{1l} \in [0 : q - 1]$ are *q-ary digits*
 - Assuming $P = 1$, the channel output can be expressed as $Y_1 = \sqrt{S}X_1 + \sqrt{I}X_2 + Z_1$. Assuming \sqrt{S} and \sqrt{I} are powers of q , the digits of X_1 , X_2 , Y_1 , and Y_2 align with each other
 - Model the noise Z_1 as peak-power-constrained. Then, only the least-significant digits of Y_1 are affected by the noise. These digits are considered unusable for transmission

- Restrict each input qit to values from $[0 : \lfloor (q - 1)/2 \rfloor]$. Thus, signal additions at the qit-level are independent of each other (no carry-overs), and effectively modulo- q . Note that this assumption does not significantly affect the rate because $\log(\lfloor (q - 1)/2 \rfloor) / \log q$ can be made arbitrarily close to 1 by choosing q large enough
- Under the above assumptions, we arrive at a q -ary expansion deterministic IC, and the (random coding) achievability results for the deterministic IC carry over to the AWGN-IC
- Showing that the converse to the QED-IC carries over to the AWGN-IC is given in [18]
- Remark: 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 for the AWGN-IC can be also achieved simply by treating interference as noise. The resulting approximation gap is, however, larger than $1/2$ bit [18]
- Approximations for other AWGN channels are discussed in [15]

Extensions to More than 2 User Pairs

- Interference channels with more than 2 user pairs are far less understood. For example, the notion of strong interference does not extend to 3 users in a straightforward manner
- These channels exhibit the interesting property that decoding at each receiver is impaired by the *joint* effect of interference from all 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 the *interference alignment*, e.g., [19, 20], whereby the code is designed so that the combined interference signal at each receiver is confined (*aligned*) to a subset of the receiver signal space. Depending on the specific channel, this alignment may be achieved via linear subspaces [19], signal scale levels [21], time delay slots [20], or number-theoretic irrational bases [22]. In each case, the subspace that contains the combined interference is disregarded, while the desired signal is reconstructed from the orthogonal subspace

- Example (k -user symmetric QED-IC): Let

$$Y_j = X_j + G_s \sum_{j' \neq j} X_{j'}, \quad j \in [1 : k],$$

where X_1, \dots, X_k are q -ary L vectors, Y_1, \dots, Y_k are q -ary $L+s$ vectors, and G_s is the 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 by 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 !!! (Note that this is the best possible—why?)

To show this, consider the single-letter linear coding technique [16] described before for the 2 user-pair case. Then it is easy to check that the symmetric capacity is achievable (with zero error), since the interfering signals from other senders are aligned in the same subspace and filtered out simultaneously

- Using the same approximation procedure for the 2-user case, this deterministic IC example shows that the symmetric DoF of the symmetric Gaussian IC is

$$d^*(\alpha) = \begin{cases} 1/k & \text{if } \alpha = 1 \\ \min \{1, \max\{\alpha, 1 - \alpha\}, \max\{\alpha/2, 1 - \alpha/2\}\} & \text{otherwise} \end{cases}$$

Approximations for the AWGN-IC with more than 2 users by the QED-ID are discussed in [23, 16, 24]

- Interference alignment has been applied to several classes of Gaussian [20, 25, 26, 22, 27] and QED interference channels [16, 21, 24]. In all these cases, the achievable rate tuple is given by

$$R_j = I(X_j; Y_j), \quad j \in [1 : k]$$

for some symmetric $\prod_{j=1}^k p_X(x_j)$, which is simply treating interference as noise for a carefully chosen input pmf

- There are a few coding techniques for more than 2 user pairs beyond interference alignment. A straightforward extension of the Han–Kobayashi coding scheme is shown to be optimal for a class of deterministic IC [28], where the received signal is one-to-one to *all* interference signals given the intended signal

More interestingly, each receiver can decode the combined (not individual) interference, which is achieved by using structured codes for the many-to-one AWGN IC [23]. Decoding the combined interference can be also applied to deterministic ICs [29]

Key New Ideas and Techniques

- Coded time-sharing can be better than naive time-sharing
- Strong interference
- Rate splitting
- Fourier–Motzkin elimination
- Genie-based converse; weak interference
- Interference alignment
- Equivalence of AWGN-IC to deterministic IC in high SNR limit
- Open problems:
 - What is the generalization of the strong interference result to more than 2 sender–receiver pairs ?
 - What is the capacity of the AWGN interference channel ?

References

- [1] H. Sato, “Two-user communication channels,” *IEEE Trans. Inf. Theory*, vol. 23, no. 3, pp. 295–304, 1977.
- [2] R. Ahlswede, “The capacity region of a channel with two senders and two receivers,” *Ann. Probability*, vol. 2, pp. 805–814, 1974.
- [3] A. B. Carleial, “A case where interference does not reduce capacity,” *IEEE Trans. Inf. Theory*, vol. 21, no. 5, pp. 569–570, 1975.
- [4] H. Sato, “The capacity of the Gaussian interference channel under strong interference,” *IEEE Trans. Inf. Theory*, vol. 27, no. 6, pp. 786–788, Nov. 1981.
- [5] M. H. M. Costa and A. El Gamal, “The capacity region of the discrete memoryless interference channel with strong interference,” *IEEE Trans. Inf. Theory*, vol. 33, no. 5, pp. 710–711, 1987.
- [6] T. S. Han and K. Kobayashi, “A new achievable rate region for the interference channel,” *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 49–60, 1981.
- [7] H.-F. Chong, M. Motani, H. K. Garg, and H. El Gamal, “On the Han–Kobayashi region for the interference channel,” *IEEE Trans. Inf. Theory*, vol. 54, no. 7, pp. 3188–3195, July 2008.
- [8] A. El Gamal and M. H. M. Costa, “The capacity region of a class of deterministic interference channels,” *IEEE Trans. Inf. Theory*, vol. 28, no. 2, pp. 343–346, 1982.
- [9] G. Kramer, “Outer bounds on the capacity of Gaussian interference channels,” *IEEE Trans. Inf. Theory*, vol. 50, no. 3, pp. 581–586, 2004.
- [10] X. Shang, G. Kramer, and B. Chen, “A new outer bound and the noisy-interference sum-rate

- capacity for Gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 689–699, Feb. 2009.
- [11] V. S. Annapureddy and V. V. Veeravalli, "Gaussian interference networks: Sum capacity in the low interference regime and new outer bounds on the capacity region," *IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3032–3050, July 2009.
 - [12] A. S. Motahari and A. K. Khandani, "Capacity bounds for the Gaussian interference channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 620–643, Feb. 2009.
 - [13] R. Etkin, D. Tse, and H. Wang, "Gaussian interference channel capacity to within one bit," *IEEE Trans. Inf. Theory*, vol. 54, no. 12, pp. 5534–5562, Dec. 2008.
 - [14] I. E. Telatar and D. N. C. Tse, "Bounds on the capacity region of a class of interference channels," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007.
 - [15] S. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow," 2007, submitted to *IEEE Trans. Inf. Theory*, 2007. [Online]. Available: <http://arxiv.org/abs/0710.3781/>
 - [16] S. A. Jafar and S. Vishwanath, "Generalized degrees of freedom of the symmetric K user Gaussian interference channel," 2008. [Online]. Available: <http://arxiv.org/abs/cs.IT/0608070/>
 - [17] B. Bandemer, "Capacity region of the 2-user-pair symmetric deterministic IC," 2009. [Online]. Available: <http://www.stanford.edu/~bandemer/detic/detic2/>
 - [18] G. Bresler and D. N. C. Tse, "The two-user Gaussian interference channel: A deterministic view," *Euro. Trans. Telecomm.*, vol. 19, no. 4, pp. 333–354, June 2008.
 - [19] M. A. Maddah-Ali, A. S. Motahari, and A. K. Khandani, "Communication over MIMO X

- channels: Interference alignment, decomposition, and performance analysis," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3457–3470, 2008.
- [20] V. Cadambe and S. A. Jafar, "Interference alignment and degrees of freedom of the K -user interference channel," *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.
 - [21] V. Cadambe, S. A. Jafar, and S. Shamai, "Interference alignment on the deterministic channel and application to fully connected Gaussian interference channel," *IEEE Trans. Inf. Theory*, vol. 55, no. 1, pp. 269–274, Jan. 2009.
 - [22] A. S. Motahari, S. O. Gharan, M. A. Maddah-Ali, and A. K. Khandani, "Real interference alignment: Exploring the potential of single antenna systems," 2009, submitted to *IEEE Trans. Inf. Theory*, 2009. [Online]. Available: <http://arxiv.org/abs/0908.2282/>
 - [23] G. Bresler, A. Parekh, and D. N. C. Tse, "The approximate capacity of the many-to-one and one-to-many Gaussian interference channel," 2008. [Online]. Available: <http://arxiv.org/abs/0809.3554/>
 - [24] B. Bandemer, G. Vazquez-Vilar, and A. El Gamal, "On the sum capacity of a class of cyclically symmetric deterministic interference channels," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 2622–2626.
 - [25] T. Gou and S. A. Jafar, "Degrees of freedom of the K user $M \times N$ MIMO interference channel," 2008. [Online]. Available: <http://arxiv.org/abs/0809.0099/>
 - [26] A. Ghasemi, A. S. Motahari, and A. K. Khandani, "Interference alignment for the K user MIMO interference channel," 2009. [Online]. Available: <http://arxiv.org/abs/0909.4604/>
 - [27] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath, "Ergodic interference alignment," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 1769–1773.

- [28] T. Gou and S. A. Jafar, "Capacity of a class of symmetric SIMO Gaussian interference channels within $O(1)$," 2009. [Online]. Available: <http://arxiv.org/abs/0905.1745/>
- [29] B. Bandemer and A. El Gamal, "Interference decoding for deterministic channels," 2010.

Appendix: Proof of Lemma 3

- Consider a sequence of $(2^{nR_1}, 2^{nR_2})$ codes with $P_e^{(n)} \rightarrow 0$. 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 $p_{T_j|X_j}(u|x_{ji})$, conditionally independent of T_{ji} given X_{ji} for every $j = 1, 2$ and every $i \in [1 : n]$
- Fano's inequality implies for $j = 1, 2$ that

$$\begin{aligned} nR_j &= H(M_j) = I(M_j; Y_j^n) + H(M_j | Y_j^n) \\ &\leq I(M_j; Y_j^n) + n\epsilon_n \\ &\leq I(X_j^n; Y_j^n) + n\epsilon_n \end{aligned}$$

This directly yields a multi-letter outer bound of the capacity region. We are looking for a nontrivial single-letter upper bound

- Observe that

$$\begin{aligned}
I(X_1^n; Y_1^n) &= H(Y_1^n) - H(Y_1^n | X_1^n) \\
&= H(Y_1^n) - H(T_2^n | X_1^n) \\
&= H(Y_1^n) - H(T_2^n) \\
&\leq \sum_{i=1}^n H(Y_{1i}) - \boxed{H(T_2^n)}
\end{aligned}$$

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

$$\begin{aligned}
I(X_1^n; Y_1^n) &\leq I(X_1^n; Y_1^n, U_1^n, X_2^n) \\
&= I(X_1^n; U_1^n) + I(X_1^n; X_2^n | U_1^n) + I(X_1^n; Y_1^n | U_1^n, X_2^n) \\
&= H(U_1^n) - H(U_1^n | X_1^n) + H(Y_1^n | U_1^n, X_2^n) - H(Y_1^n | X_1^n, U_1^n, X_2^n) \\
&\stackrel{(a)}{=} H(T_1^n) - H(U_1^n | X_1^n) + H(Y_1^n | U_1^n, X_2^n) - H(T_2^n | X_2^n) \\
&\leq \boxed{H(T_1^n)} - \sum_{i=1}^n H(U_{1i} | X_{1i}) + \sum_{i=1}^n H(Y_{1i} | U_{1i}, X_{2i}) - \sum_{i=1}^n H(T_{2i} | X_{2i})
\end{aligned}$$

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

$$\begin{aligned}
I(X_1^n; Y_1^n) &\leq I(X_1^n; Y_1^n, U_1^n) \\
&= I(X_1^n; U_1^n) + I(X_1^n; Y_1^n | U_1^n) \\
&= H(U_1^n) - H(U_1^n | X_1^n) + H(Y_1^n | U_1^n) - H(Y_1^n | X_1^n, U_1^n) \\
&= H(T_1^n) - H(U_1^n | X_1^n) + H(Y_1^n | U_1^n) - H(T_2^n) \\
&\leq \boxed{H(T_1^n)} - \boxed{H(T_2^n)} - \sum_{i=1}^n H(U_{1i} | X_{1i}) + \sum_{i=1}^n H(Y_{1i} | U_{1i}),
\end{aligned}$$

$$\begin{aligned}
I(X_1^n; Y_1^n) &\leq I(X_1^n; Y_1^n, X_2^n) \\
&= I(X_1^n; X_2^n) + I(X_1^n; Y_1^n | X_2^n) \\
&= H(Y_1^n | X_2^n) - H(Y_1^n | X_1^n, X_2^n) \\
&= H(Y_1^n | X_2^n) - H(T_2^n | X_2^n) \leq \sum_{i=1}^n H(Y_{1i} | X_{2i}) - \sum_{i=1}^n H(T_{2i} | X_{2i})
\end{aligned}$$

- By symmetry, similar bounds can be established for $I(X_2^n; Y_2^n)$, namely

$$I(X_2^n; Y_2^n) \leq \sum_{i=1}^n H(Y_{2i}) - \boxed{H(T_1^n)}$$

$$I(X_2^n; Y_2^n) \leq \boxed{H(T_2^n)} - \sum_{i=1}^n H(U_{2i}|X_{2i}) + \sum_{i=1}^n H(Y_{2i}|U_{2i}, X_{1i}) - \sum_{i=1}^n H(T_{1i}|X_{1i})$$

$$I(X_2^n; Y_2^n) \leq \boxed{H(T_2^n)} - \boxed{H(T_1^n)} - \sum_{i=1}^n H(U_{2i}|X_{2i}) + \sum_{i=1}^n H(Y_{2i}|U_{2i})$$

$$I(X_2^n; Y_2^n) \leq \sum_{i=1}^n H(Y_{2i}|X_{1i}) - \sum_{i=1}^n H(T_{1i}|X_{1i})$$

- Now consider linear combinations of the above inequalities where all boxed terms are cancelled. Combining them with the bounds using Fano's inequality and using a time-sharing variable Q uniformly distributed on $[1 : n]$ completes the proof of the outer bound

Lecture Notes 7

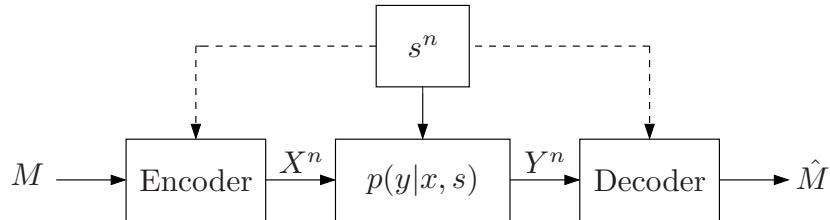
Channels with State

- Problem Setup
- Compound Channel
- Arbitrarily Varying Channel
- Channels with Random State
- Causal State Information Available at the Encoder
- Noncausal State Information Available at the Encoder
- Costa's Writing on Dirty Paper
- Coded State Information
- Key New Ideas and Techniques

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- A discrete-memoryless *channel with state* $(\mathcal{X} \times \mathcal{S}, p(y|x, s), \mathcal{Y})$ consists of a finite input alphabet \mathcal{X} , a finite output alphabet \mathcal{Y} , a finite *state* alphabet \mathcal{S} , and a collection of conditional pmfs $p(y|x, s)$ on \mathcal{Y}



- The channel is memoryless in the sense that, without feedback,

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

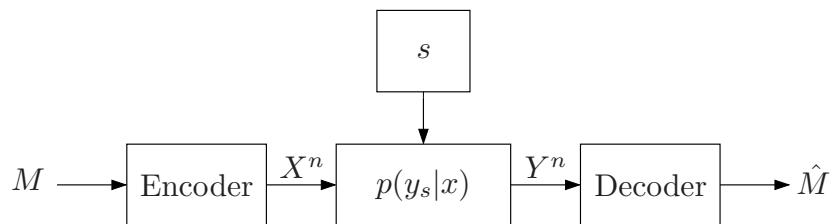
- The message $M \in [1 : 2^{nR}]$ is to be sent reliably from the sender X to the receiver Y with possible complete or partial side information about the state S available at the encoder and/or decoder

- The state can be used to model many practical scenarios such as:
 - Uncertainty about channel (compound channel)
 - Jamming (arbitrarily varying channel)
 - Channel fading
 - Write-Once-Memory (WOM)
 - Memory with defects
 - Host image in digital watermarking
 - Feedback from the receiver
 - Finite state channels ($p(y_i, s_i | x_i, s_{i-1})$)
- Three general classes of channels with state:
 - Compound channel: State is fixed throughout transmission
 - Arbitrarily varying channel (AVC): Here s^n is an arbitrary sequence
 - Random state: The state sequence $\{S_i\}$ is a stationary ergodic random process, e.g., i.i.d.

Compound Channel

- The compound channel models a communication situation where the channel is not known, but is one of several possible DMCs
- Formally, a compound channel (CC) consists of a set of DMCs $(\mathcal{X}, p(y_s|x), \mathcal{Y})$, where $y_s \in \mathcal{Y}$ for every s in the finite set \mathcal{S} . The transmission is over an unknown yet fixed DMC $p(y_s|x)$. In the framework of channels with state, the compound channel corresponds to the case in which the state s is the same throughout the transmission block, i.e.,

$$p(y^n|x^n, s^n) = \prod_{i=1}^n p_{Y_s|X}(y_i|x_i) = \prod_{i=1}^n p_{Y|X,S}(y_i|x_i, s)$$
- The sender X wishes to send a message reliably to the receiver



- A $(2^{nR}, n)$ code for the compound channel is defined as before, while the average probability of error is defined as

$$P_e^{(n)} = \max_{s \in \mathcal{S}} \mathbb{P}\{M \neq \hat{M} | s \text{ is the actual channel state}\}$$

Achievability and capacity are also defined as before

- *Theorem 1 [1]:* The capacity of the compound channel $(\mathcal{X}, \{p(y_s|x) : s \in \mathcal{S}\}, \mathcal{Y})$ is

$$C_{\text{CC}} = \max_{p(x)} \min_{s \in \mathcal{S}} I(X; Y_s),$$

- The capacity does not increase if the decoder knows the state s
- Note the similarity between this setup and the DM-BC with common message
- Clearly, $C_{\text{CC}} \leq \min_{s \in \mathcal{S}} C_s$, where $C_s = \max_{p(x)} I(X; Y_s)$ is the capacity of each channel $p(y_s|x)$, and this inequality can be strict. Note that $\min_{s \in \mathcal{S}} C_s$ is the capacity when the encoder knows the state s

- Proof of converse: From Fano's inequality, we have for each $s \in \mathcal{S}$, $H(M|Y_s^n) \leq n\epsilon_n$ with $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$. As in the proof for the DMC,

$$\begin{aligned} nR &\leq I(M; Y_s^n) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(X_i; Y_{s,i}) + n\epsilon_n \end{aligned}$$

Now we introduce the time-sharing random variable $Q \sim [1 : n]$ independent of (M, X^n, Y_s^n, s) and let $X := X_Q$ and $Y_s := Y_{s,Q}$. Then $Q \rightarrow X \rightarrow Y_s$ form a Markov chain and

$$\begin{aligned} nR &\leq nI(X_Q; Y_{s,Q}|Q) + n\epsilon_n \\ &\leq nI(X, Q; Y_s) + n\epsilon_n \\ &= nI(X; Y_s) + n\epsilon_n \end{aligned}$$

for every $s \in \mathcal{S}$. By taking $n \rightarrow \infty$, we have

$$R \leq \min_{s \in \mathcal{S}} I(X; Y_s)$$

for some $p(x)$

- Proof of achievability
 - Codebook generation and encoding: Fix $p(x)$ and 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 the message m , transmit $x^n(m)$
 - Decoding: Upon receiving y^n , the decoder finds a unique message \hat{m} such that $(x^n(\hat{m}), y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y_s)$ for some $s \in \mathcal{S}$
 - Analysis of the probability of error: Without loss of generality, assume that $M = 1$ is sent. Define the following error events

$$\mathcal{E}_1 := \{(X^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}(X, Y_{s'}) \text{ for all } s' \in \mathcal{S}\},$$

$$\mathcal{E}_2 := \{(X^n(m), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y_{s'}) \text{ for some } m \neq 1, s' \in \mathcal{S}\}$$

Then, the average probability of error $P(\mathcal{E}) \leq P(\mathcal{E}_1) + P(\mathcal{E}_2)$

- By LLN, $P((X^n(1), Y^n) \notin \mathcal{T}_\epsilon^{(n)}(X, Y_s)) \rightarrow 0$ as $n \rightarrow \infty$. Thus $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$
 - By the packing lemma, for each $s' \in \mathcal{S}$,
- $$P\{(X^n(m), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y_{s'}) \text{ for some } m \neq 1\} \rightarrow 0$$
- as $n \rightarrow \infty$, if $R < I(X; Y_{s'}) - \delta(\epsilon)$. (Recall that the packing lemma is universal w.r.t. an arbitrary output pmf $p(y)$.)

Hence, by the union of events bound,

$$\begin{aligned} P(\mathcal{E}_2) &= P\{(X^n(m), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y_{s'}) \text{ for some } m \neq 1, s' \in \mathcal{S}\} \\ &\leq |\mathcal{S}| \cdot \max_{s' \in \mathcal{S}} P\{(X^n(m), Y^n) \in \mathcal{T}_\epsilon^{(n)}(X, Y_{s'}) \text{ for some } m \neq 1\} \rightarrow 0 \end{aligned}$$

as $n \rightarrow \infty$, if $R < I(X; Y_{s'}) - \delta(\epsilon)$ for all $s' \in \mathcal{S}$, or equivalently,
 $R < \min_{s' \in \mathcal{S}} I(X; Y_{s'}) - \delta(\epsilon)$

- In general, when \mathcal{S} is arbitrary (not necessarily finite),

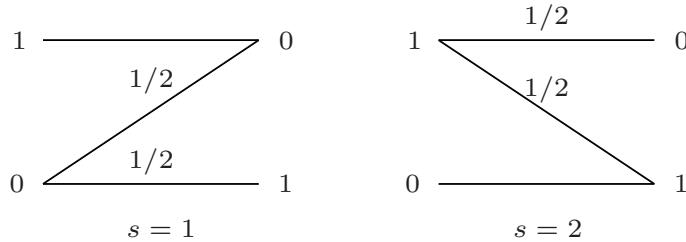
$$C_{CC} = \max_{p(x)} \inf_{s \in \mathcal{S}} I(X; Y_s)$$

Intuitively, this can be proved by noting that the probability of error for the packing lemma decays exponentially fast in n and the effective number of states is polynomial in n (there are only polynomially many empirical pmfs $p(y_s^n | x^n)$). This heuristic argument can be made rigorous [1]. Alternatively, one can use maximum empirical mutual information decoding to prove achievability [2, 3]

- Examples

- Consider the compound BSC(s) with $s \in [0, p]$, $p < 1/2$. Then,
 $C_{CC} = 1 - H(p)$, which is achieved by $X \sim \text{Bern}(1/2)$
If $p = 1/2$, then $C_{CC} = 0$

- Suppose $s \in \{1, 2\}$. If $s = 1$, then the channel is the Z -channel with parameter $1/2$. If $s = 2$, then the channel is the inverted Z -channel with parameter $1/2$



The capacity is

$$C_{CC} = H(1/4) - 1/2 = 0.3113$$

and is achieved by $X \sim \text{Bern}(1/2)$, which is strictly less than

$$C_1 = C_2 = H(1/5) - 2/5 = 0.3219$$

- As demonstrated by the first example above, the compound channel model is quite pessimistic, being robust against the worst-case channel uncertainty

- Compound channel with state available at encoder: Suppose that the encoder knows the state before communication commences, for example, by sending a training sequence that allows the decoder to estimate the state and feeding back the estimated state to the encoder. In this case, we can *adapt* the code to the selected channel and capacity becomes

$$C_{CC-E} = \inf_{s \in \mathcal{S}} \max_{p(x)} I(X; Y_s) = \inf_{s \in \mathcal{S}} C_s$$

Arbitrarily Varying Channel

- The arbitrarily varying channel (AVC) [4] is a channel with state where the state sequence s^n is chosen arbitrarily
- The AVC models a communication situation in which the channel may vary with time in an unknown and potentially adversarial manner
- The capacity of the AVC depends on the problem formulation (and is unknown in some cases):
 - availability of common randomness shared between the encoder and decoder (randomized code vs. deterministic code),
 - performance criterion (average vs. maximum probability of error),
 - knowledge of the adversary (codebook and/or the actual codeword transmitted)

- Example: Suppose X, S are binary and $Y = X + S$ is ternary
 - If the adversary knows the codebook, then it can always choose S^n to be one of the codewords. Given the sum of two codewords, the decoder has no way of differentiating the true codeword from the interference. Hence, the probability of error is essentially 1/2 and the capacity is zero
 - If the encoder and decoder can use common randomness, they can use a random code to combat the adversary. In this case, the capacity is 1/2 bit, which is the capacity of a BEC(1/2), for both average and maximum error probability criteria
 - If the adversary, however, has the knowledge of the actual codeword transmitted, the shared randomness becomes useless again since the adversary can make the output sequence all “1”s. Therefore, the capacity is zero again
- Here we review the capacity of the simplest setup in which the encoder and decoder can use shared common randomness to randomize the encoding and decoding operation, and the adversary has no knowledge of the actual codeword transmitted. In this case, the performance criterion of average or maximum probability of error does not affect the capacity

Theorem 2 [4]: The randomized code capacity of the AVC is

$$C_{\text{AVC}} = \max_{p(x)} \min_{p(s)} I(X; Y_S) = \min_{p(s)} \max_{p(x)} I(X; Y_S)$$

- In a sense, the capacity is the saddle point of the game played by the encoder and the state selector with randomized strategies $p(x)$ and $p(s)$
- Proofs of the theorem and capacities of different setups can be found in [4, 5, 6, 7, 8, 9, 2, 10, 3]
- The AVC model is even more pessimistic than the compound channel model with $C_{\text{AVC}} \leq C_{\text{CC}}$. (The randomized code under the average probability of error is the AVC setup with the highest capacity)

Channels with Random State

- Consider a *DMC with DM state* $(\mathcal{X} \times \mathcal{S}, p(y|x, s)p(s), \mathcal{Y})$, where the state sequence $\{S_i\}$ is an i.i.d. process with $S_i \sim p_S(s_i)$. Here the uncertainty about the channel state plays a less adversarial role than in the compound channel and AVC models
- There are *many* possible scenarios of encoder and/or decoder state information availability, including:
 - State information not available at either the encoder or decoder
 - State information fully or partially available at both the encoder and decoder
 - State information fully or partially available only at the decoder
 - State information fully or partially available only at the encoder
- The state information may be available at the encoder in several ways, e.g.:
 - Noncausal: The entire sequence of the channel state is known in advance and can be used for encoding from time $i = 1$
 - Causal: The state sequence known only up to the present time, i.e., it is revealed on the fly

- For each set of assumptions, a $(2^{nR}, n)$ code, achievability, and capacity can be defined in the usual way
- Note that having the state available causally at the decoder yields the same capacity as having it available noncausally, independent of whether the state is available at the encoder or not (why?)

This is, however, not the case for state availability at the encoder as we will see

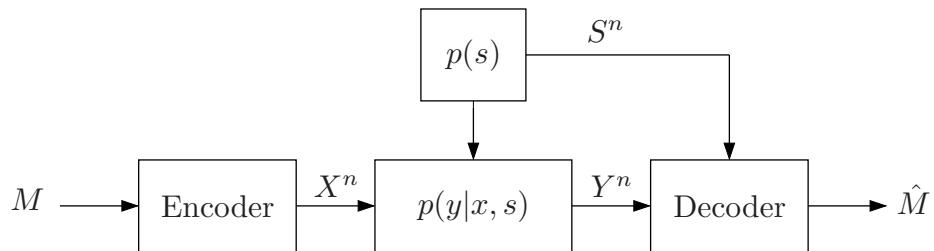
Simple Special Cases

- Consider a DMC with DM state $(\mathcal{X} \times \mathcal{S}, p(y|x, s)p(s), \mathcal{Y})$
- No state information available at either the encoder or the decoder: The capacity is

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

where $p(y|x) = \sum_s p(s)p(y|x, s)$

- The state sequence is available only at the decoder:

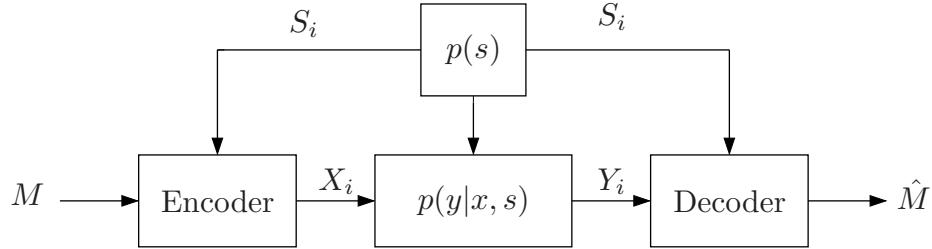


The capacity is

$$C_{\text{SI-D}} = \max_{p(x)} I(X; Y, S) = \max_{p(x)} I(X; Y|S),$$

and is achieved by treating (Y^n, S^n) as the output of the channel $p(y, s|x) = p(s)p(y|x, s)$. The converse is straightforward

- The state sequence is available (causally or noncausally) at both the encoder and decoder:



The capacity is

$$C_{\text{SI-ED}} = \max_{p(x|s)} I(X; Y|S)$$

for both the causal and noncausal cases

- Achievability can be proved by treating S^n as a time-sharing sequence [11] as follows:

- Codebook generation: Let $0 < \epsilon < 1$. Fix $p(x|s)$ and generate $|\mathcal{S}|$ random codebooks \mathcal{C}_s , $s \in \mathcal{S}$. For each $s \in \mathcal{S}$, randomly and independently generate 2^{nR_s} sequences $x^n(m_s)$, $m_s \in [1 : 2^{nR_s}]$, each according to $\prod_{i=1}^n p_{X|S}(x_i|s)$. These sequences constitute the codebook \mathcal{C}_s . Set $R = \sum_s R_s$
- Encoding: To send a message $m \in [1 : 2^{nR}]$, express it as a unique set of messages $\{m_s : s \in \mathcal{S}\}$ and consider the set of codewords $\{x^n(m_s, s) : s \in \mathcal{S}\}$. Store each codeword in a FIFO buffer of length n . A multiplexer is used to choose a symbol at each transmission time $i \in [1 : n]$ from one of the FIFO buffers according to the state s_i . The chosen symbol is then transmitted
- Decoding: The decoder demultiplexes the received sequence into subsequences $\{y^{n_s}(s), s \in \mathcal{S}\}$, where $\sum_s n_s = n$. Assuming $s^n \in \mathcal{T}_\epsilon^{(n)}$, and thus $n_s \geq n(1 - \epsilon)p(s)$ for all $s \in \mathcal{S}$, it finds for each s , a unique \hat{m}_s such that the codeword subsequence $x^{n(1-\epsilon)p(s)}(\hat{m}_s, s)$ is jointly typical with $y^{np(s)(1-\epsilon)}(s)$. By the LLN and the packing lemma, the probability of error for each decoding step $\rightarrow 0$ as $n \rightarrow \infty$ if $R_s < (1 - \epsilon)p(s)I(X; Y|S = s) - \delta(\epsilon)$. Thus, the total probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if $R < (1 - \epsilon)I(X; Y|S) - \delta(\epsilon)$

- The converse for the noncausal case is quite straightforward. This also establishes optimality for the causal case
- In Lecture Notes 8, we discuss the application of the above coding theorems to fading channels, which are the most popular channel models in wireless communication

Extensions to MAC with State

- The above coding theorems can be extended to some multiple user channels with known capacity regions
- For example, consider a DM-MAC with DM state $(\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{S}, p(y|x_1, x_2, s)p(s), \mathcal{Y})$
 - When no state information is available at the encoders or the decoder, the capacity region is the one for the regular DM-MAC
 $p(y|x_1, x_2) = \sum_s p(s)p(y|x_1, x_2, s)$
 - When the state sequence is available only at the decoder, the capacity region $\mathcal{C}_{\text{SI-D}}$ is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y|X_2, Q, S),$$

$$R_2 \leq I(X_2; Y|X_1, Q, S),$$

$$R_1 + R_2 \leq I(X_1, X_2; Y|Q, S)$$

for some $p(q)p(x_1|q)p(x_2|q)$

- When the state sequence is available at both the encoders and the decoder, the capacity region $\mathcal{C}_{\text{SI-ED}}$ is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y | X_2, Q, S),$$

$$R_2 \leq I(X_2; Y | X_1, Q, S),$$

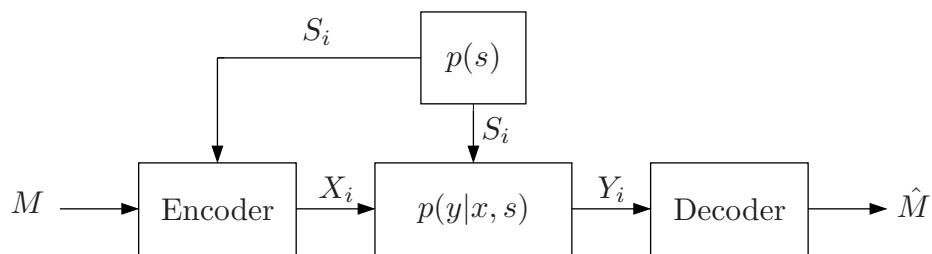
$$R_1 + R_2 \leq I(X_1, X_2; Y | Q, S)$$

for some $p(q)p(x_1|s, q)p(x_2|s, q)$ and the encoders can adapt their codebooks according to the state sequence

- In Lecture Notes 8, we discuss results for multiple user fading channels

Causal State Information Available at the Encoder

- We consider yet another special case of state availability. Suppose the state sequence is available only at the encoder
- Here the capacity depends on whether the state information is available causally or noncausally at the encoder. First, we consider the causal case
- Consider a DMC with DM state $(\mathcal{X} \times \mathcal{S}, p(y|x, s)p(s), \mathcal{Y})$. Assume that the state is available causally only at the encoder. In other words, a $(2^{nR}, n)$ code is defined by an encoder $x_i(m, s^i)$, $i \in [1 : n]$, and a decoder $\hat{m}(y^n)$



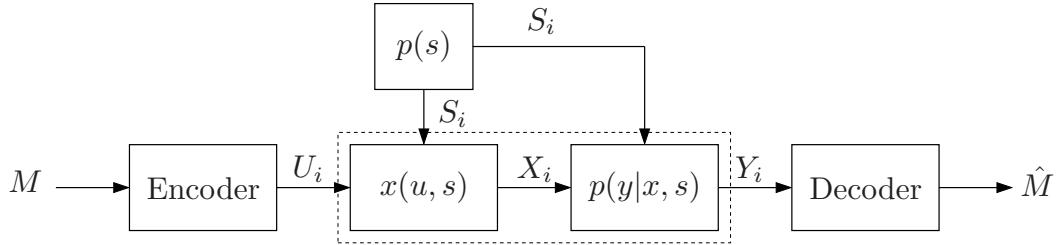
- *Theorem 3 [12]:* The capacity of the DMC with DM state available causally at the encoder is

$$C_{\text{CSI-E}} = \max_{p(u), x(u,s)} I(U; Y),$$

where U is an auxiliary random variable independent of S and with cardinality $|\mathcal{U}| \leq \min\{(|\mathcal{X}| - 1) \cdot |\mathcal{S}| + 1, |\mathcal{Y}|\}$

- Proof of achievability:

- Suppose we attach a “physical device” $x(u, s)$ with two inputs U and S , and one output X in front of the actual channel input



- This induces a new DMC $p(y|u) = \sum_s p(y|x(s, u), s)p(s)$ with input U and output Y (it is still memoryless because the state S is i.i.d.)
- Now, using the channel coding theorem for the DMC, we see that $I(U; Y)$ is achievable for arbitrary $p(u)$ and $x(u, s)$

- Remark: We can view the encoding as being done over the space $|\mathcal{X}|^{|\mathcal{S}|}$ of all functions $x_u(s)$ indexed by u (the cardinality bound shows that we need only $\min\{(|\mathcal{X}| - 1) \cdot |\mathcal{S}| + 1, |\mathcal{Y}|\}$ functions). This technique of coding over functions onto \mathcal{X} instead of actual symbols in \mathcal{X} is referred to as the *Shannon strategy*
- Proof of converse: The key is to identify the auxiliary random variable. We would like X_i to be a function of (U_i, S_i) . In general, X_i is a function of (M, S^{i-1}, S_i) . So we define $U_i = (M, S^{i-1})$. This identification also satisfies the requirements that U_i be independent of S_i and $U_i \rightarrow (X_i, S_i) \rightarrow Y_i$ form a Markov chain for every $i \in [1 : n]$. Now, by Fano’s inequality,

$$\begin{aligned} nR &\leq I(M; Y^n) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(M; Y_i | Y^{i-1}) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(M, Y^{i-1}; Y_i) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(M, S^{i-1}, Y^{i-1}; Y_i) + n\epsilon_n \end{aligned}$$

$$\begin{aligned}
&\stackrel{(a)}{=} \sum_{i=1}^n I(M, S^{i-1}, X^{i-1}, Y^{i-1}; Y_i) + n\epsilon_n \\
&\stackrel{(b)}{=} \sum_{i=1}^n I(M, S^{i-1}, X^{i-1}; Y_i) + n\epsilon_n \\
&\stackrel{(c)}{=} \sum_{i=1}^n I(U_i; Y_i) + n\epsilon_n \\
&\leq n \max_{p(u), x(u,s)} I(U; Y) + n\epsilon_n,
\end{aligned}$$

where (a) and (c) follow since X^{i-1} is a function of (M, S^{i-1}) and (b) follows since $Y^{i-1} \rightarrow (X^{i-1}, S^{i-1}) \rightarrow Y_i$ form a Markov chain

This completes the proof of the converse

- Let's revisit the scenario in which the state is available causally at both the encoder and decoder:
 - Treating (Y^n, S^n) as the equivalent channel output, the above theorem reduces to

$$C_{\text{SI-ED}} = \max_{p(u), x(u,s)} I(U; Y, S)$$

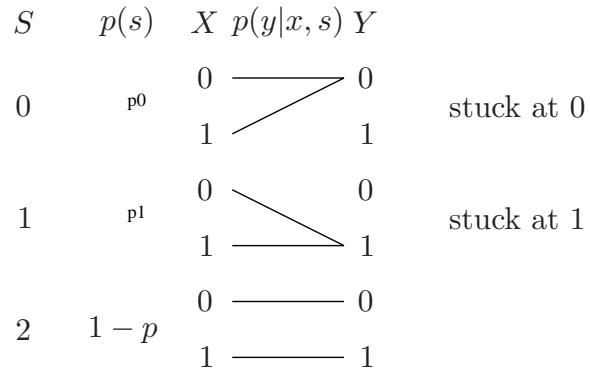
$$\begin{aligned}
&\stackrel{(a)}{=} \max_{p(u), x(u,s)} I(U; Y|S) \\
&\stackrel{(b)}{=} \max_{p(u), x(u,s)} I(X; Y|S) \\
&\stackrel{(c)}{=} \max_{p(x|s)} I(X; Y|S),
\end{aligned}$$

where (a) follows by the independence of U and S , (b) follows since X is a function of (U, S) and $U \rightarrow (S, X) \rightarrow Y$ form a Markov chain, and (c) follows since any conditional pmf $p(x|s)$ can be represented as some function $x(u, s)$, where U is independent of S as shown in the functional representation lemma in Appendix B

- Remark: The Shannon strategy for this case gives an alternative capacity-achieving coding scheme to the time-sharing scheme discussed earlier

Noncausal State Information Available at the Encoder

- Again consider a DMC with DM state $(\mathcal{X} \times \mathcal{S}, p(y|x, s)p(s), \mathcal{Y})$. Suppose that the state sequence is available noncausally only at the encoder. In other words, a $(2^{nR}, n)$ code is defined by a message set $[1 : 2^{nR}]$, an encoder $x^n(m, s^n)$, and a decoder $\hat{m}(y^n)$. The definitions of probability of error, achievability, and the capacity $C_{\text{SI-E}}$ are as before
- Example (Memory with defects) [13]: Model a memory with stuck-at faults as a DMC with DM state:



This is also a model for a Write-once memory (WOM), such as a ROM or a

CD-ROM. The stuck-at faults in this case are locations where a “1” is stored

- The writer (encoder) who knows the locations of the faults (by first reading the memory) wishes to reliably store information in a way that does not require the reader (decoder) to know the locations of the faults

How many bits can be reliably stored?
- Note that:
 - If neither the writer nor the reader knows the fault locations, we can store up to $\max_{p(x)} I(X; Y) = 1 - H(p/2)$ bits/cell
 - If both the writer and the reader know the fault locations, we can store up to $\max_{p(x|s)} I(X; Y|S) = 1 - p$ bits/cell
 - If the reader knows the fault locations (erasure channel), we can also store $\max_{p(x)} I(X; Y|S) = 1 - p$ bits/cell
- Answer: Even if only the writer knows the fault locations we can still reliably store up to $1 - p$ bits/cell !!

- Coding scheme: Assume that the memory has n cells
 - Randomly and independently assign each binary n -sequence to one of 2^{nR} subcodebooks $\mathcal{C}(m)$, $m \in [1 : 2^{nR}]$
 - To store message m , search in subcodebook $\mathcal{C}(m)$ for a sequence that matches the faulty cells and store it; otherwise declare an error
 - For large n , there are $\approx np$ stuck-at faults and so there are $\approx 2^{n(1-p)}$ sequences that match any given stuck-at pattern
 - Thus, if $R < (1 - p) - \delta$ and n sufficiently large, any given subcodebook has at least one matching sequence with high probability, and thus asymptotically $n(1 - p)$ bits can be reliably stored in an n -bit memory with $n(1 - p)$ faulty cells

Gelfand–Pinsker Theorem

- The Gelfand–Pinsker theorem generalizes the Kuznetsov–Tsybakov result to general DMCs with DM state using the same basic coding idea
- *Gelfand–Pinsker Theorem* [14]: The capacity of the DMC with DM state available noncausally only at the encoder is

$$C_{\text{SI-E}} = \max_{p(u|s), x(u,s)} (I(U;Y) - I(U;S)),$$

where $|\mathcal{U}| \leq \min\{|\mathcal{X}| \cdot |\mathcal{S}|, |\mathcal{Y}| + |\mathcal{S}| - 1\}$

- Example (Memory with defects):

Let $S = 2$ be the “no fault” state, $S = 1$ be the “stuck at 1” state, and $S = 0$ be the “stuck at 0” state

If $S = 2$, i.e., there is no fault, set $X = U \sim \text{Bern}(1/2)$

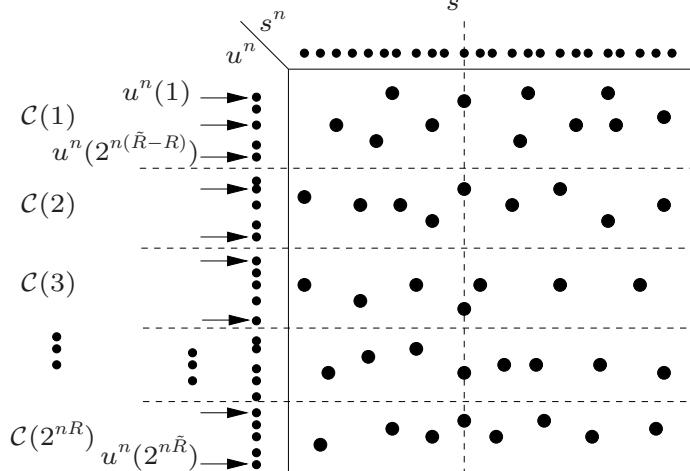
If $S = 1$ or 0 , set $U = X = S$

Since $Y = X$, we have

$$I(U;Y) - I(U;S) = H(U|S) - H(U|Y) = 1 - p$$

Outline of Achievability

- Fix $p(u|s)$ and $x(u,s)$ that achieve capacity and let $\tilde{R} \geq R$. For each message $m \in [1 : 2^{nR}]$, generate a *subcodebook* $\mathcal{C}(m)$ of $2^{n(\tilde{R}-R)}$ $u^n(l)$ sequences



- To send $m \in [1 : 2^{nR}]$ given s^n , find a $u^n(l) \in \mathcal{C}(m)$ that is jointly typical with s^n and transmit $x_i = x(u_i(l), s_i)$ for $i \in [1 : n]$
- Upon receiving y^n , the receiver finds a jointly typical $u^n(l)$ and declares the subcodebook index of $u^n(l)$ to be the message sent

Proof of Achievability [15]

- Codebook generation: Fix $p(u|s)$, $x(u, s)$ that achieve capacity
For each message $m \in [1 : 2^{nR}]$ generate a subcodebook $\mathcal{C}(m)$ consisting of $2^{n(\tilde{R}-R)}$ randomly and independently generated sequences $u^n(l)$,
 $l \in [(m-1)2^{n(\tilde{R}-R)} + 1 : m2^{n(\tilde{R}-R)}]$, each according to $\prod_{i=1}^n p_U(u_i)$
- Encoding: To send the message $m \in [1 : 2^{nR}]$ with the state sequence s^n observed, the encoder chooses a $u^n(l) \in \mathcal{C}(m)$ such that $(u^n(l), s^n) \in \mathcal{T}_{\epsilon'}^{(n)}$. If no such l exists, it picks an arbitrary sequence $u^n(l) \in \mathcal{C}(m)$
The encoder then transmits $x_i = x(u_i(l), s_i)$ at time $i \in [1 : n]$
- Decoding: Let $\epsilon > \epsilon'$. Upon receiving y^n , the decoder declares that $\hat{m} \in [1 : 2^{nR}]$ is sent if it is the unique message such that $(u^n(l), y^n) \in \mathcal{T}_{\epsilon}^{(n)}$ for some $u^n(l) \in \mathcal{C}(\hat{m})$; otherwise it declares an error

- Analysis of the probability of error: Assume without loss of generality that $M = 1$ and let L denote the index of the chosen U^n codeword for $M = 1$ and S^n

An error occurs only if

$$\begin{aligned}\mathcal{E}_1 &:= \{(U^n(l), S^n) \notin \mathcal{T}_{\epsilon'}^{(n)} \text{ for all } U^n(l) \in \mathcal{C}(1)\}, \text{ or} \\ \mathcal{E}_2 &:= \{(U^n(L), Y^n) \notin \mathcal{T}_{\epsilon}^{(n)}\}, \text{ or} \\ \mathcal{E}_3 &:= \{(U^n(l), Y^n) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } U^n(l) \notin \mathcal{C}(1)\}\end{aligned}$$

The probability of error is upper bounded as

$$P(\mathcal{E}) \leq P(\mathcal{E}_1) + P(\mathcal{E}_1^c \cap \mathcal{E}_2) + P(\mathcal{E}_3)$$

We now bound the probability of each event

1. By the covering lemma, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R} - R > I(U; S) + \delta(\epsilon')$
2. Since $\mathcal{E}_1^c = \{(U^n(L), S^n) \in \mathcal{T}_{\epsilon'}^{(n)}\} = \{(U^n(L), X^n, S^n) \in \mathcal{T}_{\epsilon'}^{(n)}\}$,
 $Y^n | \{U^n(L) = u^n, X^n = x^n, S^n = s^n\} \sim \prod_{i=1}^n p_{Y|U,X,S}(y_i | u_i, x_i, s_i) = \prod_{i=1}^n p_{Y|X,S}(y_i | x_i, s_i)$, and $\epsilon > \epsilon'$, by the conditional typicality lemma,
 $P(\mathcal{E}_1^c \cap \mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$

3. Since every $U^n(l) \notin \mathcal{C}(1)$ is distributed according to $\prod_{i=1}^n p_U(u_i)$ and is independent of Y^n , by the packing lemma, $P(\mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R} < I(U; Y) - \delta(\epsilon)$

Note that here Y^n is not generated i.i.d. However, we can still use the packing lemma

- Combining these results, we have shown $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(U; Y) - I(U; S) - \delta(\epsilon) - \delta(\epsilon')$

This completes the proof of achievability

Proof of Converse [16]

- Again the trick is to identify U_i such that $U_i \rightarrow (X_i, S_i) \rightarrow Y_i$ form a Markov chain
- By Fano's inequality, $H(M|Y^n) \leq n\epsilon_n$
- Now, consider

$$\begin{aligned}
 nR &\leq I(M; Y^n) + n\epsilon_n = \sum_{i=1}^n I(M; Y_i | Y^{i-1}) + n\epsilon_n \\
 &\leq \sum_{i=1}^n I(M, Y^{i-1}; Y_i) + n\epsilon_n \\
 &= \sum_{i=1}^n I(M, Y^{i-1}, S_{i+1}^n; Y_i) - \sum_{i=1}^n I(Y_i; S_{i+1}^n | M, Y^{i-1}) + n\epsilon_n \\
 &\stackrel{(a)}{=} \sum_{i=1}^n I(M, Y^{i-1}, S_{i+1}^n; Y_i) - \sum_{i=1}^n I(Y^{i-1}; S_i | M, S_{i+1}^n) + n\epsilon_n \\
 &\stackrel{(b)}{=} \sum_{i=1}^n I(M, Y^{i-1}, S_{i+1}^n; Y_i) - \sum_{i=1}^n I(M, Y^{i-1}, S_{i+1}^n; S_i) + n\epsilon_n
 \end{aligned}$$

Here (a) follows from the Csiszár sum identity and (b) follows from the fact that (M, S_{i+1}^n) is independent of S_i

- Now, define $U_i := (M, Y^{i-1}, S_{i+1}^n)$

Note that as desired $U_i \rightarrow (X_i, S_i) \rightarrow Y_i$, $i \in [1 : n]$, form a Markov chain, thus

$$\begin{aligned} nR &\leq \sum_{i=1}^n (I(U_i; Y_i) - I(U_i; S_i)) + n\epsilon_n \\ &\leq n \max_{p(u, x|s)} (I(U; Y) - I(U; S)) + n\epsilon_n, \end{aligned}$$

We now show that it suffices to maximize over $p(u|s)$ and functions $x(u, s)$. Fix $p(u|s)$. Note that

$$p(y|u) = \sum_{x,s} p(s|u)p(x|u,s)p(y|x,s)$$

is linear in $p(x|u, s)$

Since $p(u|s)$ is fixed, the maximization over the Gelfand–Pinsker formula is only over $I(U; Y)$, which is convex in $p(y|u)$ ($p(u)$ is fixed) and hence in $p(x|u, s)$

This implies that the maximum is achieved at an extreme point of the set of $p(x|u, s)$, that is, using one of the deterministic mappings $x(u, s)$

- This complete the proof of the converse

Comparison to the Causal Case

- Consider the Gelfand–Pinsker capacity expression

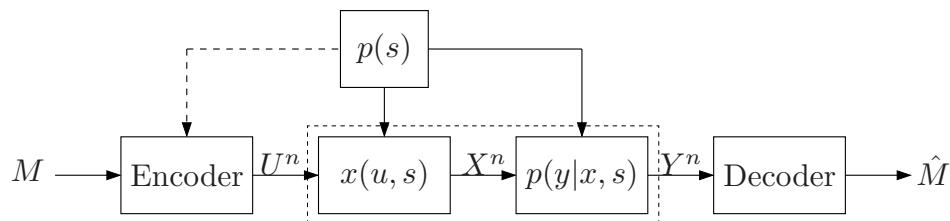
$$C_{\text{SI-E}} = \max_{p(u|s), x(u,s)} (I(U; Y) - I(U; S))$$

- On the other hand, the capacity when the state information is available *causally* at the encoder can expressed as

$$C_{\text{CSI-E}} = \max_{p(u), x(u,s)} (I(U; Y) - I(U; S)),$$

since $I(U; S) = 0$. This is the same formula as the noncausal case, except that here the maximum is over $p(u)$ instead of $p(u|s)$

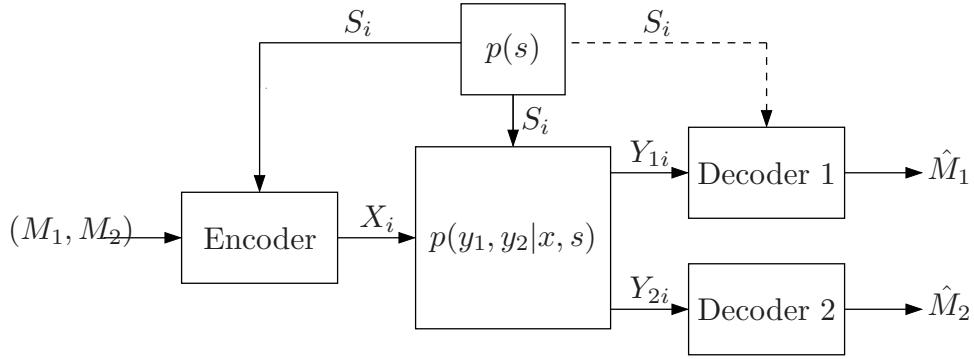
- Also, the coding schemes for both scenarios are the same except that in the noncausal case, the entire state sequence S^n is given to the encoder (and hence the encoder can choose a U^n sequence that is jointly typical with the given S^n)



- Therefore the cost of causality (i.e., the gap between the causal and the noncausal capacities) is captured only by the more restrictive independence condition between U and S

Extensions to Degraded BC With State Available At Encoder

- Using the Shannon strategy, any state information available causally at the encoders in a multiple user channel can be utilized by coding over function indices. Similarly, Gelfand–Pinsker coding can be generalized to multiple-user channels when the state sequence is available noncausally at encoders. The optimality of these extensions, however, is not known in most cases
- Here we consider an example of degraded DM-BC with DM state and discuss a few special cases for which the capacity region is known [17, 18]
- Consider a DM-BC with DM state $(\mathcal{X} \times \mathcal{S}, p(y_1, y_2|x, s)p(s), \mathcal{Y}_1 \times \mathcal{Y}_2)$. We assume that Y_2 is a degraded version of Y_1 , i.e.,
$$p(y_1, y_2|x, s) = p(y_1|x, s)p(y_2|y_1)$$



- The capacity region when the state information is available causally at the encoder only (i.e., the encoder is given by $x_i(s^i)$ and the decoders are given by $\hat{m}_1(y_1^n), \hat{m}_2(y_2^n)$) is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(U_1; Y_1 | U_2),$$

$$R_2 \leq I(U_2; Y_2)$$

for some $p(u_1, u_2), x(u_1, u_2, s)$, where U_1, U_2 are auxiliary random variables independent of S with $|\mathcal{U}_1| \leq |\mathcal{S}||\mathcal{X}|(|\mathcal{S}||\mathcal{X}| + 1)$ and $|\mathcal{U}_2| \leq |\mathcal{S}||\mathcal{X}| + 1$

- When the state information is available causally at the encoder and decoder 1 (but not decoder 2), the capacity region is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X; Y_1 | U, S),$$

$$R_2 \leq I(U; Y_2)$$

for some $p(u)p(x|u, s)$ with $|\mathcal{U}| \leq |\mathcal{S}||\mathcal{X}| + 1$

- When the state information is available noncausally at the encoder and decoder 1 (but not decoder 2), the capacity region is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X; Y_1 | U, S),$$

$$R_2 \leq I(U; Y_2) - I(U; S)$$

for some $p(u, x|s)$ with $|\mathcal{U}| \leq |\mathcal{S}||\mathcal{X}| + 1$

Costa's Writing on Dirty Paper

- First consider a BSC with additive Bernoulli state S : $Y_i = X_i \oplus S_i \oplus Z_i$, where the noise $\{Z_i\}$ is a $\text{Bern}(p)$ process and the state sequence $\{S_i\}$ is a $\text{Bern}(q)$ process and the two processes are independent

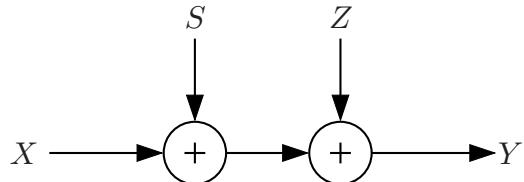
Clearly if the encoder knows the state in advance (or even only causally), the capacity is $C = 1 - H(p)$, and is achieved by setting $X = U \oplus S$ (to make the channel effectively $U \rightarrow U \oplus Z$) and taking $U \sim \text{Bern}(1/2)$

Note that this result generalizes to an arbitrary state sequence S^n , i.e., the state does not need to be i.i.d. (must be independent of the noise, however)

- Does a similar result hold for the AWGN channel with AWGN state?

We cannot use the same encoding scheme because of potential power constraint violation. Nevertheless, it turns out that the same result holds for the AWGN case!

- This result is referred to as *writing on dirty paper* and was established by Costa [19], who considered the AWGN channel with AWGN state: $Y_i = X_i + S_i + Z_i$, where the state sequence $\{S_i\}$ is a $\text{WGN}(Q)$ process and the noise $\{Z_i\}$ is a $\text{WGN}(1)$ process, and the two processes are independent. Assume an average power constraint P on the channel input X



- With no knowledge of the state at either the encoder or decoder, the capacity is simply

$$C = C\left(\frac{P}{1+Q}\right)$$

- If the decoder knows the state, the capacity is

$$C_{\text{SI-D}} = C(P)$$

The decoder simply subtracts off the state sequence and the channel reduces to a simple AWGN channel

- Now assume that only the encoder knows the state sequence S^n

We know the capacity expression, so we need to find the best distribution on U given S and function $x(u, s)$ subject to the power constraint

Let's try $U = X + \alpha S$, where $X \sim N(0, P)$ independent of S !!

With this choice, we have

$$\begin{aligned} I(U; Y) &= h(X + S + Z) - h(X + S + Z | X + \alpha S) \\ &= h(X + S + Z) + h(X + \alpha S) - h(X + S + Z, X + \alpha S) \\ &= \frac{1}{2} \log \left(\frac{(P + Q + 1)(P + \alpha^2 Q)}{PQ(1 - \alpha)^2 + (P + \alpha^2 Q)} \right), \text{ and} \\ I(U; S) &= \frac{1}{2} \log \left(\frac{P + \alpha^2 Q}{P} \right) \end{aligned}$$

Thus

$$\begin{aligned} R(\alpha) &= I(U; Y) - I(U; S) \\ &= \frac{1}{2} \log \left(\frac{P(P + Q + 1)}{PQ(1 - \alpha)^2 + (P + \alpha^2 Q)} \right) \end{aligned}$$

Maximizing w.r.t. α , we find that $\alpha^* = P/(P + 1)$, which gives

$$R \left(\frac{P}{P+1} \right) = C(P),$$

the best one can hope to obtain!

- Interestingly the optimal α corresponds to the weight of the minimum MSE linear estimate of X given $X + Z$. This is no accident and the following alternative derivation offers further insights

Alternative Proof of Achievability [20]

- As before let $U = X + \alpha S$, where $X \sim N(0, P)$ is independent of S , and $\alpha = P/(P + 1)$
- From the Gelfand–Pinsker theorem, we can achieve

$$I(U; Y) - I(U; S) = h(U|S) - h(U|Y)$$

We want to show that this is equal to

$$\begin{aligned} I(X; X + Z) &= h(X) - h(X|X + Z) \\ &= h(X) - h(X - \alpha(X + Z)|X + Z) \\ &= h(X) - h(X - \alpha(X + Z)), \end{aligned}$$

where the last step follows by the fact that $(X - \alpha(X + Z))$, which is the error of the best MSE estimate of X given $(X + Z)$, and $(X + Z)$ are orthogonal and thus independent because X and $(X + Z)$ are jointly Gaussian

First consider

$$h(U|S) = h(X + \alpha S|S) = h(X|S) = h(X)$$

Next we show that $h(U|Y) = h(X - \alpha(X + Z))$

Since $(X - \alpha(X + Z))$ is independent of $(X + Z, S)$, it is independent of $Y = X + S + Z$. Thus

$$\begin{aligned} h(U|Y) &= h(X + \alpha S|Y) \\ &= h(X + \alpha S - \alpha Y|Y) \\ &= h(X - \alpha(X + Z)|Y) \\ &= h(X - \alpha(X + Z)) \end{aligned}$$

This completes the proof

- Note that this derivation does not require S to be Gaussian. Hence we have $C_{\text{SI-E}} = C(P)$ for any non-Gaussian state S with finite power!
- A similar result can be also obtained for the case of nonstationary, nonergodic Gaussian noise and state [21]

Writing on Dirty Paper for AWGN-MAC

- The writing on dirty paper result can be extended to several multiple-user AWGN channels
- Consider the AWGN-MAC with AWGN state: $Y_i = X_{1i} + X_{2i} + S_i + Z_i$, where the state sequence $\{S_i\}$ is a WGN(Q) process, the noise $\{Z_i\}$ is a WGN(1) process, and the two processes are independent. Assume average power constraints P_1, P_2 on the channel inputs X_1, X_2 , respectively. We assume that the state sequence S^n is available noncausally at both encoders
- The capacity region [22, 23] of this channel is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq C(P_1), \\ R_2 &\leq C(P_2), \\ R_1 + R_2 &\leq C(P_1 + P_2) \end{aligned}$$

- This is the capacity region when the state sequence is available also at the decoder (so the interference S^n can be cancelled out). Thus the proof of the converse is trivial

- For the achievability, consider the “writing on dirty paper” channel $Y = X_1 + S + (X_2 + Z)$ with input X_1 , known state S , and unknown noise $(X_2 + Z)$ that will be shortly shown to be independent of S . Then by taking $U_1 = X_1 + \alpha_1 S$, where $X_1 \sim N(0, P_1)$ independent of S and $\alpha_1 = P_1/(P_1 + P_2 + 1)$, we can achieve $R_1 = I(U_1; Y) - I(U_1; S) = C(P_1/(P_2 + 1))$

Now as in the successive cancellation for the regular AWGN-MAC, once u_1^n is decoded correctly, the decoder can subtract it from y^n to get the effective channel

$$\tilde{y}^n = y^n - u_1^n = x_2^n + (1 - \alpha_1)s^n + z^n$$

Now for sender 2, the channel is another “writing on dirty paper” channel with input X_2 , known state $(1 - \alpha_1)S$, and unknown noise Z . Therefore, by taking $U_2 = X_2 + \alpha_2 S$, where $X_2 \sim N(0, P_2)$ is independent of S and $\alpha_2 = (1 - \alpha_1)P_2/(P_2 + 1) = P_2/(P_1 + P_2 + 1)$, we can achieve $R_2 = I(U_2; Y') - I(U_2; S) = C(P_2)$

Therefore, we can achieve a corner point of the capacity region $(R_1, R_2) = (C(P_1/(P_2 + 1)), C(P_2))$. The other corner point can be achieved by reversing the role of two encoders. The rest of the capacity region can then be achieved using time sharing

- Achievability can be proved alternatively by considering the inner bound to the capacity region of the DM-MAC with DM state $(\mathcal{X} \times \mathcal{S}, p(y|x_1, x_2, s)p(s), \mathcal{Y})$ with state available noncausally at the encoders that consists of the set of rate pairs (R_1, R_2) such that

$$R_1 < I(U_1; Y|U_2) - I(U_1; S|U_2),$$

$$R_2 < I(U_2; Y|U_1) - I(U_2; S|U_1),$$

$$R_1 + R_2 < I(U_1, U_2; Y) - I(U_1, U_2; S)$$

for some $p(u_1|s)p(u_2|s)x_1(u_1, s)x_2(u_2, s)$. By choosing (U_1, U_2, X_1, X_2) as above, we can show (check!) that this inner bound simplifies to the capacity region. It is not known if this inner bound is tight for a general DM-MAC with DM state

Writing on Dirty Paper for AWGN-BC

- Now consider the AWGN-BC:

$$Y_{1i} = X_i + S_{1i} + Z_{1i}, \quad Y_{2i} = X_i + S_{2i} + Z_{2i},$$

where the states $\{S_{1i}\}, \{S_{2i}\}$ are WGN(Q_1) and WGN(Q_2) processes, respectively, the noise $\{Z_{1i}\}, \{Z_{2i}\}$ are WGN(N_1) and WGN(N_2) processes, respectively, independent of $\{S_{1i}\}, \{S_{2i}\}$, and the input X has an average power constraint P . We assume that the state sequence S^n is available noncausally at the encoder

- The capacity region [22, 23, 17] of this channel is the set of rate pairs (R_1, R_2) satisfying

$$R_1 \leq C(\alpha P/N_1),$$

$$R_2 \leq C((1 - \alpha)P/(\alpha P + N_2))$$

for some $\alpha \in [0 : 1]$

- This is the same as the capacity region when the state sequences are available also at the respective decoders. Thus the proof of the converse is trivial
- The proof of achievability follows closely that of the MAC case. We split the input into two independent parts $X_1 \sim N(0, \alpha P)$ and $X_2 \sim N(0, \bar{\alpha}P)$ such

that $X = X_1 + X_2$. For the worse receiver, consider the “writing on dirty paper” channel $Y_{2i} = X_{2i} + S_{2i} + (X_{1i} + Z_{2i})$ with input X_{2i} , known state S_{2i} , and noise $(X_{1i} + Z_{2i})$. Then by taking $U_2 = X_2 + \beta_2 S_2$, where $X_2 \sim N(0, (1 - \alpha)P)$ independent of S_2 and $\beta_2 = (1 - \alpha)P/(P + N_2)$, we can achieve $R_2 = I(U_2; Y_2) - I(U_2; S_2) = C((1 - \alpha)P/(\alpha P + N_2))$

For the better receiver, consider another “writing on dirty paper” channel $Y_{1i} = X_{1i} + (X_{2i} + S_{1i}) + Z_{1i}$ with input X_{1i} , known interference $(X_{2i} + S_{1i})$, and noise Z_{1i} . Using the writing on dirty paper result with $U_1 = X_1 + \beta_1(X_2 + S_1)$ and $\beta_1 = \alpha P/(\alpha P + N_1)$, we can achieve $R_1 = C(\alpha P/N_1)$

- Achievability can be proved alternatively by considering the inner bound to the capacity region of the DM-BC $(\mathcal{X} \times \mathcal{S}, p(y_1, y_2|x, s)p(s), \mathcal{Y}_1 \times \mathcal{Y}_2)$ with state available noncausally at the encoder that consists of the set of rate pairs (R_1, R_2) such that

$$R_1 < I(U_1; Y_1) - I(U_1; S),$$

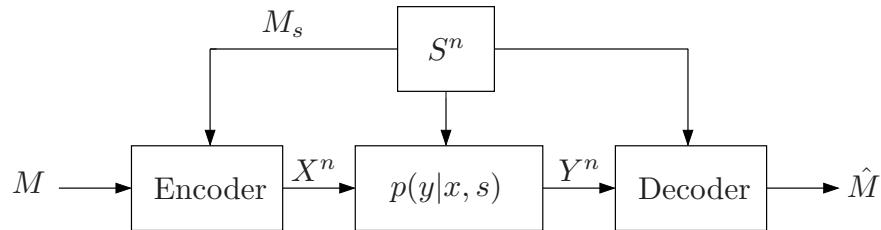
$$R_2 < I(U_2; Y_2) - I(U_2; S),$$

$$R_1 + R_2 < I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2) - I(U_1, U_2; S)$$

for some $p(u_1, u_2|s)$, $x(u_1, u_2, s)$. Taking $S = (S_1, S_2)$ and choosing (U_1, U_2, X) as above, this inner bound simplifies to the capacity region (check)

Coded State Information

- Now consider the scenario where coded state information $m_s(s^n) \in [1 : 2^{nR_s}]$ is available noncausally at the encoder and the complete state is available at the decoder



Here a code is specified by an encoder $x^n(m, m_s)$ and a decoder $\hat{m}(y^n, s^n)$. In this case there is a tradeoff between the transmission rate R and the state encoding rate R_s

It can be shown [15] that this tradeoff is characterized by the set of rate pairs (R, R_s) such that

$$R \leq I(X; Y|S, U),$$

$$R_s \geq I(U; S)$$

for some $p(u|s)p(x|u)$

- Achievability follows by joint typicality encoding to describe the state sequence S^n by U^n at rate R_s and using time-sharing on the “compressed state” sequence U^n as described earlier
- For the converse, recognize $U_i = (M_s, S^{i-1})$ and consider

$$\begin{aligned}
nR_s &\geq H(M_s) \\
&= I(M_s; S^n) \\
&= \sum_{i=1}^n I(M_s; S_i | S^{i-1}) \\
&= \sum_{i=1}^n I(M_s, S^{i-1}; S_i) \\
&= \sum_{i=1}^n I(U_i; S_i)
\end{aligned}$$

On the other hand, from Fano's inequality,

$$\begin{aligned}
nR &\leq I(M; Y^n, S^n) + n\epsilon_n \\
&= I(M; Y^n | S^n) + n\epsilon_n \\
&= \sum_{i=1}^n I(M; Y_i | Y^{i-1}, S^n) + n\epsilon_n \\
&\leq \sum_{i=1}^n H(Y_i | Y^{i-1}, S^n, M_s) - H(Y_i | Y^{i-1}, S^n, M_s, M, X_i) + n\epsilon_n \\
&\leq \sum_{i=1}^n H(Y_i | S_i, S^{i-1}, M_s) - H(Y_i | X_i, S_i, S^{i-1}, M_s) + n\epsilon_n \\
&\leq \sum_{i=1}^n I(X_i; Y_i | S_i, U_i)
\end{aligned}$$

Since $S_i \rightarrow U_i \rightarrow X_i$ and $U_i \rightarrow (X_i, S_i) \rightarrow Y_i$, $i \in [1 : n]$, form a Markov chain, we can complete the proof by introducing the usual time sharing random variable

Key New Ideas and Techniques

- State-dependent channel models
- Shannon strategy
- Multicoding (subcodebook generation)
- Gelfand–Pinsker coding
- Writing on dirty paper coding

References

- [1] D. Blackwell, L. Breiman, and A. J. Thomasian, “The capacity of a class of channels,” *Ann. Math. Statist.*, vol. 30, pp. 1229–1241, 1959.
- [2] I. Csiszár and J. Körner, *Information Theory*. Budapest: Akadémiai Kiadó, 1981.
- [3] A. Lapidoth and P. Narayan, “Reliable communication under channel uncertainty,” *IEEE Trans. Inf. Theory*, vol. 44, no. 6, pp. 2148–2177, 1998.
- [4] D. Blackwell, L. Breiman, and A. J. Thomasian, “The capacity of a certain channel classes under random coding,” *Ann. Math. Statist.*, vol. 31, pp. 558–567, 1960.
- [5] R. Ahlswede and J. Wolfowitz, “Correlated decoding for channels with arbitrarily varying channel probability functions,” *Inf. Control*, vol. 14, pp. 457–473, 1969.
- [6] ———, “The capacity of a channel with arbitrarily varying channel probability functions and binary output alphabet,” *Z. Wahrsch. Verw. Gebiete*, vol. 15, pp. 186–194, 1970.
- [7] R. Ahlswede, “Elimination of correlation in random codes for arbitrarily varying channels,” *Probab. Theory Related Fields*, vol. 44, no. 2, pp. 159–175, 1978.
- [8] J. Wolfowitz, *Coding Theorems of Information Theory*, 3rd ed. Berlin: Springer-Verlag, 1978.
- [9] I. Csiszár and P. Narayan, “The capacity of the arbitrarily varying channel revisited: Positivity, constraints,” *IEEE Trans. Inf. Theory*, vol. 34, no. 2, pp. 181–193, 1988.
- [10] I. Csiszár and J. Körner, “On the capacity of the arbitrarily varying channel for maximum probability of error,” *Z. Wahrsch. Verw. Gebiete*, vol. 57, no. 1, pp. 87–101, 1981.
- [11] A. J. Goldsmith and P. P. Varaiya, “Capacity of fading channels with channel side information,” *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1986–1992, 1997.

- [12] C. E. Shannon, "Channels with side information at the transmitter," *IBM J. Res. Develop.*, vol. 2, pp. 289–293, 1958.
- [13] A. V. Kuznetsov and B. S. Tsypakov, "Coding in a memory with defective cells," *Probl. Inf. Transm.*, vol. 10, no. 2, pp. 52–60, 1974.
- [14] S. I. Gelfand and M. S. Pinsker, "Coding for channel with random parameters," *Probl. Control Inf. Theory*, vol. 9, no. 1, pp. 19–31, 1980.
- [15] C. Heegard and A. El Gamal, "On the capacity of computer memories with defects," *IEEE Trans. Inf. Theory*, vol. 29, no. 5, pp. 731–739, 1983.
- [16] C. Heegard, "Capacity and coding for computer memory with defects," Ph.D. Thesis, Stanford University, Stanford, CA, Nov. 1981.
- [17] Y. Steinberg, "Coding for the degraded broadcast channel with random parameters, with causal and noncausal side information," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2867–2877, 2005.
- [18] S. Sigurjónsson and Y.-H. Kim, "On multiple user channels with causal state information at the transmitters," in *Proc. IEEE International Symposium on Information Theory*, Adelaide, Australia, September 2005, pp. 72–76.
- [19] M. H. M. Costa, "Writing on dirty paper," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 439–441, 1983.
- [20] A. S. Cohen and A. Lapidot, "The Gaussian watermarking game," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1639–1667, 2002.
- [21] W. Yu, A. Sutivong, D. J. Julian, T. M. Cover, and M. Chiang, "Writing on colored paper," in *Proc. IEEE International Symposium on Information Theory*, Washington D.C., 2001, p. 302.
- [22] S. I. Gelfand and M. S. Pinsker, "On Gaussian channels with random parameters," in *Proc. the Sixth International Symposium on Information Theory*, vol. Part 1, Tashkent, USSR, 1984, pp. 247–250, (in Russian).
- [23] Y.-H. Kim, A. Sutivong, and S. Sigurjónsson, "Multiple user writing on dirty paper," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, Illinois, June/July 2004, p. 534.

- Sixth International Symposium on Information Theory*, vol. Part 1, Tashkent, USSR, 1984, pp. 247–250, (in Russian).
- [23] Y.-H. Kim, A. Sutivong, and S. Sigurjónsson, "Multiple user writing on dirty paper," in *Proc. IEEE Int. Symp. Inf. Theory*, Chicago, Illinois, June/July 2004, p. 534.

Lecture Notes 8

Fading Channels

- Introduction
- Gaussian Fading Channel
- Gaussian Fading MAC
- Gaussian Fading BC
- Gaussian Fading IC
- Key New Ideas and Techniques

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Introduction

- Fading channels are models of wireless communication channels. They represent important examples of channels with random state available at the decoders and fully or partially at the encoders p
- The channel state (fading coefficient) typically varies much slower than transmission symbol duration. To simplify the model, we assume a *block fading model* [1] whereby the state is constant over *coherence time intervals* and stationary ergodic across these intervals
 - Fast fading: If the code block length spans a large number of coherence time intervals, then the channel becomes ergodic with a well-defined Shannon capacity (sometimes referred to as *ergodic capacity*) for both full and partial channel state information at the encoders. However, the main problem with coding over a large number of coherence times is excessive delay
 - Slow fading: If the code block length is in the order of the coherence time interval, then the channel is not ergodic and as such does not have a Shannon capacity in general. In this case, there have been various coding strategies and corresponding performance metrics proposed that depend on whether the encoders know the channel state or not
- We discuss several canonical fading channel models under both fast and slow fading assumptions using various coding strategies

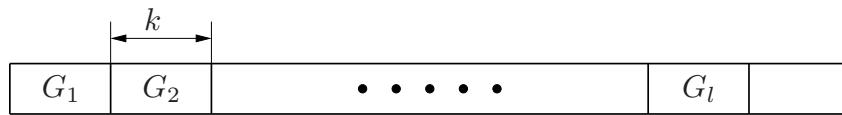
Gaussian Fading Channel

- Consider the Gaussian fading channel

$$Y_i = G_i X_i + Z_i,$$

where $\{G_i \in \mathcal{G} \subseteq \mathbb{R}^+\}$ is a *channel gain* process that models fading in wireless communication, and $\{Z_i\}$ is a WGN(1) process independent of $\{G_i\}$. Assume that every codeword $x^n(m)$ must satisfy the average power constraint
 $\frac{1}{n} \sum_{i=1}^n x_i^2(m) \leq P$ (if the channel gain is not available at the encoder) or
 $\frac{1}{n} \sum_{i=1}^n \mathbb{E}(x_i^2(G^i, m)) \leq P$ (if the channel gain is available at the encoder)

- Assume a block fading model [1] whereby the gain G_l over each coherence time interval $[(l-1)k+1 : lk]$ is constant for $l = 1, 2, \dots$ and $\{G_l\}$ is stationary ergodic



- We consider several cases: (1) fast or slow fading, and (2) whether the channel gain is available only at the decoder or at both the encoder and decoder

Fast Fading

- In fast fading, we code over many coherence time intervals (i.e., $n \gg k$) and the fading process is stationary ergodic, for example, i.i.d.
- Channel gain available only at the decoder: The ergodic capacity is

$$\begin{aligned} C_{\text{SI-D}} &= \max_{F(x): \mathbb{E}(X^2) \leq P} I(X; Y|G) \\ &= \max_{F(x): \mathbb{E}(X^2) \leq P} h(Y|G) - h(Y|G, X) \\ &= \max_{F(x): \mathbb{E}(X^2) \leq P} h(GX + Z|G) - h(Z) \\ &= \mathbb{E}_G [C(G^2P)], \end{aligned}$$

which is achieved by $X \sim N(0, P)$. This is same as the capacity for i.i.d. state with the same marginal distribution available at the decoder discussed in Lecture Notes 7

- Channel gain available at the encoder and decoder: The ergodic capacity [2] is

$$\begin{aligned}
C_{\text{SI-ED}} &= \max_{F(x|g): \mathbb{E}(X^2) \leq P} I(X; Y|G) \\
&= \max_{F(x|g): \mathbb{E}(X^2) \leq P} h(Y|G) - h(Y|G, X) \\
&= \max_{F(x|g): \mathbb{E}(X^2) \leq P} h(GX + Z|G) - h(Z) \\
&\stackrel{(a)}{=} \max_{\phi(g): \mathbb{E}(\phi(G)) \leq P} \mathbb{E}_G [\mathcal{C}(G^2\phi(G))] ,
\end{aligned}$$

where $F(x|g)$ is the conditional cdf of X given $\{G = g\}$, (a) is achieved by taking $X|\{G = g\} \sim N(0, \phi(g))$. This is same as the capacity for i.i.d. state available at the encoder and decoder in Lecture Notes 7

Using a Lagrange multiplier λ , we can show that the optimal solution $\phi^*(g)$ is

$$\phi^*(g) = \left(\lambda - \frac{1}{g^2} \right)^+,$$

where λ is chosen to satisfy

$$\mathbb{E}_G(\phi^*(G)) = \mathbb{E}_G \left[\left(\lambda - \frac{1}{G^2} \right)^+ \right] = P$$

This power allocation corresponds to “water-filling” in time

- Remarks:

- At high SNR, the capacity gain from power control vanishes and $C_{\text{SI-ED}} - C_{\text{SI-D}} \rightarrow 0$
- The main disadvantage of fast fading is excessive coding delay over a large number of coherence time intervals

Slow Fading

- In slow fading, we code over a single coherence time interval (i.e., $n = k$) and the notion of channel capacity is not well defined in general
- As before we consider the cases when the channel gain is available only at the decoder and when it is available at both the encoder and decoder. For each case, we discuss various coding strategies and corresponding performance metrics

Channel Gain Available at Decoder

- Compound channel approach: We code against the worst channel to guarantee reliable communication. The (Shannon) capacity under this coding strategy is well-defined and is

$$C_{CC} = \min_{g \in \mathcal{G}} C(g^2 P)$$

This compound channel approach becomes impractical when fading allows the channel gain to be close to zero. Hence, we consider alternative coding strategies that can be useful in practice

- Outage capacity approach [1]: Suppose the event that the channel gain is close to zero, referred to as an *outage*, has a low probability. Then we can send at a rate higher than C_{CC} most of the time and lose information only during an outage

Formally, suppose we can tolerate outage probability p_{out} , then we can send at any rate lower than the outage capacity

$$C_{out} := \max_{\{g: P\{G \leq g\} \leq p_{out}\}} C(g^2 P)$$

- Broadcasting approach [3, 4, 5]: For simplicity assume two fading states, i.e., $\mathcal{G} = \{g_1, g_2\}$, $g_1 > g_2$

We view the channel as an AWGN-BC with gains g_1 and g_2 and use superposition coding to send a common message to both receivers at rate $\tilde{R}_2 < C(g_2^2 \alpha P / (1 + \bar{\alpha} g_2^2 P))$, $\alpha \in [0, 1]$, and a private message to the stronger receiver at rate $\tilde{R}_1 < C(g_1^2 \bar{\alpha} P)$

If the gain is g_2 , the decoder of the fading channel can reliably decode the common message at rate $R_2 = \tilde{R}_2$, and if the gain is g_1 , it can reliably decode both messages and achieve a total rate of $R_1 = \tilde{R}_1 + \tilde{R}_2$

Assuming $P\{G = g_1\} = p$ and $P\{G = g_2\} = 1 - p$, we can compute the *broadcasting capacity* as

$$C_{\text{BC}} = \max_{\alpha \in [0,1]} pR_1 + (1-p)R_2 = \max_{\alpha \in [0,1]} p C(g_1^2 \bar{\alpha} P) + C(g_2^2 \alpha P / (1 + \bar{\alpha} g_2^2 P))$$

Remark: This approach is most suited to sending multi-media (video or music) over the fading channel using successive refinement (cf. Lecture Notes 14): If the channel gain is low, the receiver decodes only the low fidelity description and if the gain is high, it also decodes the refinement and obtains the high fidelity description

Channel Gain Available at Encoder and Decoder

- Compound channel approach: If the channel gain is available at the encoder, the compound channel capacity is

$$C_{\text{CC-E}} = \inf_{g \in \mathcal{G}} C(g^2 P) = C_{\text{CC}}$$

Thus, in this case capacity is the same as when the encoder does not know the state

- Adaptive coding: Instead of communicating at the capacity of the channel with the worst gain, we adapt the transmission rate to the channel gain and communicate at maximum rate $C_g := C(g^2 P)$ when the gain is g

We define the *adaptive capacity* as

$$C_A = E_G [C(G^2 P)]$$

Although it is same as the ergodic capacity when the channel gain is available only at the decoder, the adaptive capacity is just a convenient performance metric and is *not* a capacity in the Shannon sense

- Adaptive coding with power control: Since the encoder knows the channel gain, it can adapt the power as well as the transmission rate. In this case, we define the *power-control adaptive capacity* as

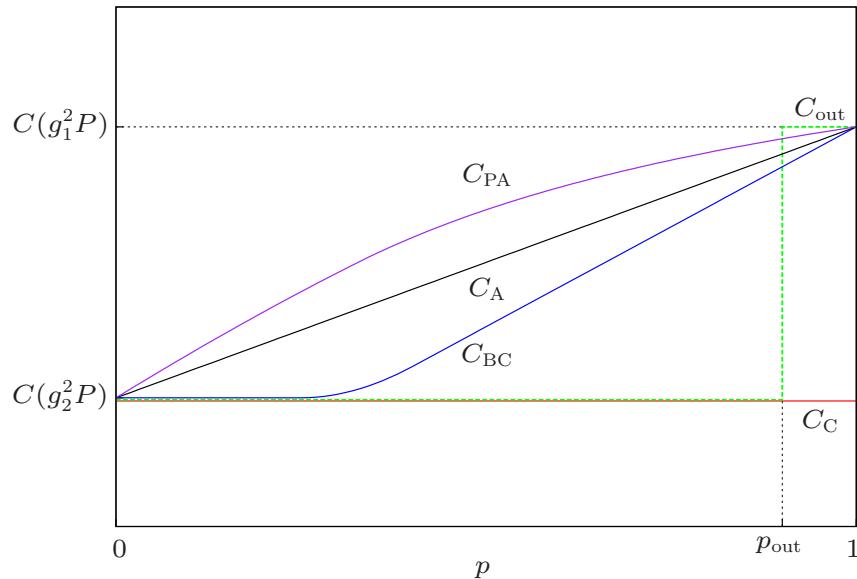
$$C_{PA} = \max_{\phi(g): E(\phi(G)) \leq P} E(C(G^2 \phi(G))),$$

where the maximum is achieved by the water-filling power allocation that satisfies the expected power constraint $E(\phi(G)) \leq P$

Note that the power-control adaptive capacity is identical to the ergodic capacity when the channel gain is available at both the encoder and decoder. Again it is not a capacity in the Shannon sense

Remark: Although using power control achieves a higher-rate on the average, in some practical situations such as under the FCC regulation the power constraint must be satisfied in each coding block

- Example: Assume two fading states $g_1 > g_2$ and $P\{G = g_1\} = p$. We compare C_C , C_{out} , C_{BC} , C_A , C_{PA} for different values of $p \in (0, 1)$



The broadcasting approach is useful when the good channel occurs often and power control is useful particularly when the channel varies frequently ($p = 1/2$)

Gaussian Fading MAC

- Consider the Gaussian fading MAC

$$Y_i = G_{1i}X_{1i} + G_{2i}X_{2i} + Z_i,$$

where $\{G_{1i} \in \mathcal{G}_1\}$ and $\{G_{2i} \in \mathcal{G}_2\}$ are jointly random channel gain processes, and the noise $\{Z_i\}$ is a WGN(1) process, independent of $\{G_{1i}\}$ and $\{G_{2i}\}$.

Assume average power constraint P on each of the inputs X_1 and X_2

As before, we assume block fading model where in block $l = 1, 2, \dots, L$, $G_{ji} = G_{jl}$ for $i \in [(l-1)n+1 : ln]$ and $j = 1, 2$, and consider fast and slow fading scenarios

Fast Fading

- Channel gains available only at the decoder: The ergodic capacity region [6] is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq E(C(G_1^2 P)),$$

$$R_2 \leq E(C(G_2^2 P)),$$

$$R_1 + R_2 \leq E(C((G_1^2 + G_2^2)P)) =: C_{SI-D}$$

- Channel gains available at both encoders and the decoder: The ergodic capacity region in this case [6] is the set of rate pairs (R_1, R_2) satisfying

$$R_1 \leq E(C(G_1^2 \phi_1(G_1, G_2))),$$

$$R_2 \leq E(C(G_2^2 \phi_2(G_1, G_2))),$$

$$R_1 + R_2 \leq E(C(G_1^2 \phi_1(G_1, G_2) + G_2^2 \phi_2(G_1, G_2)))$$

for some ϕ_1 and ϕ_2 such that $E_{G_1, G_2}(\phi_j(G_1, G_2)) \leq P$ for $j = 1, 2$

In particular, the ergodic sum-capacity C_{SI-ED} can be computed by solving the optimization problem [7]

$$\begin{aligned} & \text{maximize}_{G_1, G_2} E_{G_1, G_2}(C((G_1^2 \phi_1(G_1, G_2) + G_2^2 \phi_2(G_1, G_2)))) \\ & \text{subject to } E_{G_1, G_2}(\phi_j(G_1, G_2)) \leq P, \quad j = 1, 2 \end{aligned}$$

- Channel gains available at their respective encoder and the decoder: Consider a scenario where the receiver knows both channel gains but each sender knows only its own channel gain. This is motivated by the fact that in practical wireless communication systems, such as IEEE 802.11 wireless LAN, each sender can estimate its channel gain via electromagnetic reciprocity [] from a training signal globally transmitted by the receiver (access point). Complete knowledge of the state at the senders, however, is not always practical as it requires either communication between the senders or feedback control from the access point. Complete knowledge of the state at the receiver, on the other hand, is closer to reality since the access point can estimate the state of all senders from a training signal from each sender

The ergodic capacity region in this case [8, 9] is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq \mathbb{E}(C(G_1^2\phi_1(G_1))), \\ R_2 &\leq \mathbb{E}(C(G_2^2\phi_2(G_2))), \\ R_1 + R_2 &\leq \mathbb{E}(C(G_1^2\phi_1(G_1) + G_2^2\phi_2(G_2))) \end{aligned}$$

for some ϕ_1 and ϕ_2 such that $\mathbb{E}_{G_j}(\phi_j(G_j)) \leq P$ for $j = 1, 2$

In particular, the sum-capacity $C_{\text{DSI-ED}}$ can be computed by solving the optimization problem

$$\begin{aligned} \text{maximize } & \mathbb{E}_{G_1, G_2}(C(G_1^2\phi_1(G_1) + G_2^2\phi_2(G_2))) \\ \text{subject to } & \mathbb{E}_{G_j}(\phi_j(G_j)) \leq P, \quad j = 1, 2 \end{aligned}$$

Slow Fading

- If the channel gains are available only at the decoder or at both encoders and the decoder, the compound channel, outage capacity, and adaptive coding approaches and corresponding performance metrics can be analyzed as in the Gaussian fading channel case. Hence, we focus on the case when the channel gains are available at their respective encoders and at the decoder
- Compound channel approach: The capacity region using the compound approach is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq \min_{g_1} C(g_1^2 P),$$

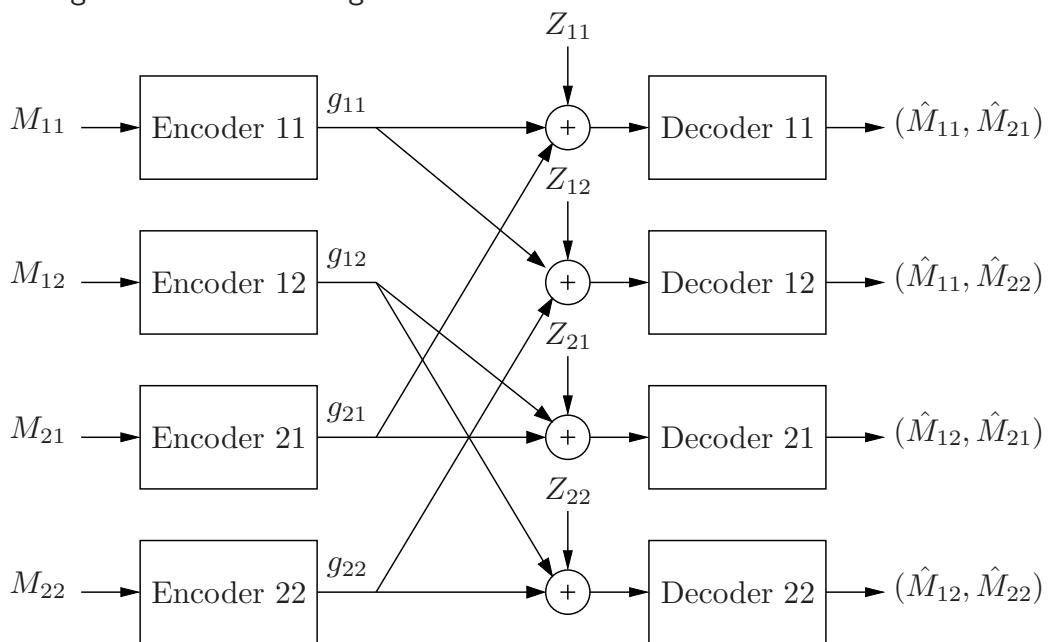
$$R_2 \leq \min_{g_2} C(g_2^2 P),$$

$$R_1 + R_2 \leq \min_{g_1, g_2} C((g_1^2 + g_2^2) P)$$

This is same as the case where the channel gains are available only at decoder

- Adaptive coding: When each encoder adapts its transmission rate according to its channel gain, the adaptive capacity region is the same as the ergodic capacity region when only the decoder knows the channel gains. The sum-capacity C_A is the same as the ergodic sum capacity $C_{\text{SI-D}}$

- Power-control adaptive coding [10, 11]: Here the channel is equivalent to multiple MACs with shared inputs as illustrated in the figure for $\mathcal{G}_j = \{g_{j1}, g_{j2}\}$, $j = 1, 2$. However, the receiver observes only the output corresponding to the channel gains in each block figure



If we let $M_{jk} \in [1 : 2^{nR_{jk}}]$ for $j = 1, 2$ and $k = 1, 2$, then we define the *power-control adaptive capacity region* to be the capacity region for the equivalent multiple MACs, which is the set of rate quadruples $(R_{11}, R_{12}, R_{21}, R_{22})$ such that

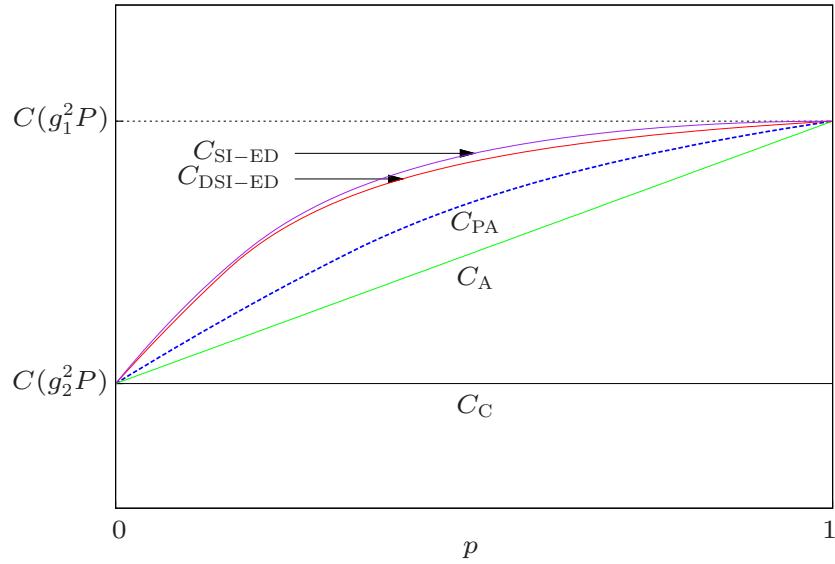
$$\begin{aligned} R_{11} &< C(g_{11}^2 P), \quad R_{12} < C(g_{12}^2 P), \quad R_{21} < C(g_{21}^2 P), \quad R_{22} < C(g_{22}^2 P), \\ R_{11} + R_{21} &< C((g_{11}^2 + g_{21}^2)P), \quad R_{11} + R_{22} < C((g_{11}^2 + g_{22}^2)P), \\ R_{12} + R_{21} &< C((g_{12}^2 + g_{21}^2)P), \quad R_{12} + R_{22} < C((g_{12}^2 + g_{22}^2)P) \end{aligned}$$

We can compute the power-control adaptive sum-capacity C_{PA} by solving the optimization problem

$$\begin{aligned} \text{maximize} \quad & E_{G_1}(R_1(G_1)) + E_{G_2}(R_2(G_2)) \\ \text{subject to} \quad & E_{G_j}(\phi_j(G_j)) \leq P, \quad j = 1, 2 \\ & R_1(g_1) \leq C(g_1^2 \phi_1(g_1)) \quad \text{for all } g_1 \in \mathcal{G}_1, \\ & R_2(g_2) \leq C(g_2^2 \phi_2(g_2)) \quad \text{for all } g_2 \in \mathcal{G}_2, \\ & R_1(g_1) + R_2(g_2) \leq C(g_1^2 \phi_1(g_1) + g_2^2 \phi_2(g_2)) \quad \text{for all } (g_1, g_2) \in \mathcal{G}_1 \times \mathcal{G}_2 \end{aligned}$$

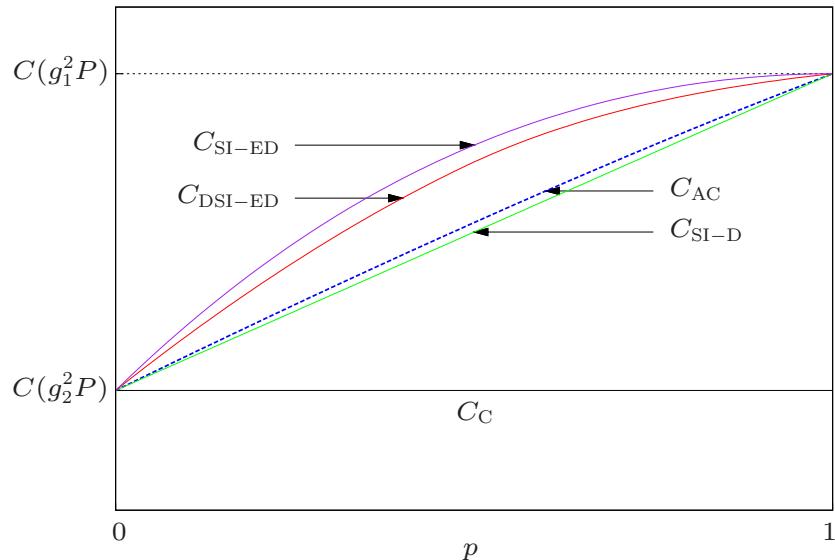
- Example: Assume G_1 and G_2 each assumes one of two fading states $g^{(1)} > g^{(2)}$ and $P\{G_j = g^{(1)}\} = p$, $j = 1, 2$. In the following figure, we compare for different values of $p \in (0, 1)$, the sum capacities C_C (compound channel approach), C_A (adaptive sum-capacity), C_{PA} (power-control adaptive sum-capacity), C_{DSI-ED} (ergodic sum-capacity), and C_{SI-ED} (ergodic sum-capacity with gains available at both encoders and the decoder)

- Low SNR



At low SNR, power control is useful for adaptive coding (C_{AC} vs. C_{SI-D})

- High SNR



At high SNR, complete knowledge of channel gains significantly improves upon distributed knowledge of channel gains

Gaussian Fading BC

- Consider the Gaussian fading BC

$$Y_{1i} = G_{1i}X_i + Z_{1i}, \quad Y_{2i} = G_{2i}X_i + Z_{2i},$$

where $\{G_{1i} \in \mathcal{G}_1\}$ and $\{G_{2i} \in \mathcal{G}_2\}$ are random channel gain processes, and the noise $\{Z_{1i}\}$ and $\{Z_{2i}\}$ are WGN(1) processes, independent of $\{G_{1i}\}$ and $\{G_{2i}\}$. Assume average power constraint P on X

As before assume the block fading model, whereby the channel gains are fixed in each coherence time interval, but stationary ergodic across the intervals

- Fast fading

- Channel gains available only at the decoders: The ergodic capacity region is not known in general
- Channel gains available at the encoder and decoders: Let $I(g_1, g_2) := 1$ if $g_2 \geq g_1$ and $I(g_1, g_2) := 0$, otherwise, and $\bar{I} := 1 - I$

The ergodic capacity [12] is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq \mathbb{E} \left(C \left(\frac{\alpha G_1^2 P}{1 + \bar{\alpha} G_1^2 P I(G_1, G_2)} \right) \right), \\ R_2 &\leq \mathbb{E} \left(C \left(\frac{\bar{\alpha} G_2^2 P}{1 + \alpha G_2^2 P \bar{I}(G_1, G_2)} \right) \right) \end{aligned}$$

for some $\alpha \in [0, 1]$

- Slow fading

- Compound channel approach: We code for the worst channel. Let g_1^* and g_2^* be the lowest gains for the channel to Y_1 and the channel to Y_2 , respectively, and assume without loss of generality that $g_1^* \geq g_2^*$. The compound capacity region is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq C(g_1^* \alpha P), \\ R_2 &\leq C \left(\frac{g_2^* \bar{\alpha} P}{1 + g_2^* \alpha P} \right) \text{ for some } \alpha \in [0, 1] \end{aligned}$$

- Outage capacity region is discussed in [12]
- Adaptive coding capacity regions are the same as the corresponding ergodic capacity regions

Gaussian Fading IC

- Consider a k -user Gaussian fading IC

$$\mathbf{Y}(i) = G(i)\mathbf{X}(i) + \mathbf{Z}(i),$$

where $\{G_{jj'}(i)\}_{i=1}^{\infty}$, $j, j' \in [1 : k]$, are the random channel gain processes from sender j' to receiver j , and $\{Z_{ji}\}_{i=1}^{\infty}$, $j \in [1 : k]$, are WGN(1) processes, independent of the channel gain processes. Assume average power constraint P on X_j , $j \in [1 : k]$

As before, assume the block fading model, whereby the channel gains are fixed in each coherence time interval, but stationary ergodic across the intervals

- We consider fast fading where the channel gains $\{G(i)\}$ are available at all k encoders and k decoders. Assuming that the channel gain processes $\{G_{jj'}(i)\}_{i=1}^n$ have marginals with symmetric distribution, that is, $P\{G_{jj'}(i) \leq g\} = P\{G_{jj'}(i) \geq -g\}$, we can apply the interference alignment technique introduced in Lecture Notes 6 to achieve higher rates than time division or treating interference as Gaussian noise
- We illustrate this with the following simple example
We assume that for each i , $G_{jj'}(i)$, $j, j' \in [1 : k]$, are i.i.d. with $G_{jj'}(i) \sim \text{Unif}\{-g, +g\}$

- Time division: Using time division with power control, we can easily show that the ergodic sum capacity is lower bounded as

$$C_{\text{SI-ED}} \geq C(g^2 k P),$$

thus the rate per user $\rightarrow 0$ as $k \rightarrow \infty$

- Treating interference as Gaussian noise: Using good point-to-point AWGN channel codes and treating interference as Gaussian noise, the ergodic sum capacity is lower bounded as

$$C_{\text{SI-ED}} \geq k C\left(\frac{g^2 P}{g^2(k-1)P + 1}\right),$$

thus again the rate per user $\rightarrow 0$ as $k \rightarrow \infty$

- Ergodic interference alignment [13]: Using interference alignment over time, we show that the ergodic sum capacity is

$$C_{\text{SI-ED}} = \frac{k}{2} C(2g^2 P)$$

- The proof of the converse follows by noting that the pairwise sum rate $R_j + R_{j'}$, $j \neq j'$, is upper bounded by the sum capacity of the following two 2-user AWGN-ICs with strong interference:

$$Y_j = gX_j + gX_{j'} + Z_j,$$

$$Y_{j'} = gX_j - gX_{j'} + Z_{j'}$$

and

$$Y_j = gX_j + gX_{j'} + Z_j,$$

$$Y_j = gX_j + gX_{j'} + Z_{j'}$$

(Note that these two AWGN-ICs have the same capacity region)

- Achievability can be proved by treating the channel gains G^n as a time-sharing sequence (cf. Lecture Notes 7) and repeating each codeword twice such that the interfering signals are aligned

For a channel gain matrix G , let \bar{G} be its *conjugate* channel gain matrix such that $G_{jj'} + \bar{G}_{jj'} = 0$ for $j \neq j'$ and $G_{jj} = \bar{G}_{jj}$. Under our channel model, there are $|\mathcal{G}| = 2^k$ channel gain matrices and $|\mathcal{G}|/2$ pairs of $\{G, \bar{G}\}$, and $p(G) = 1/|\mathcal{G}|$ for all G

Following the coding procedure for the DMC with DM state available at both the encoder and the decoder, we associate with each channel gain matrix G a FIFO buffer of length n . Divide the message M_j into $|\mathcal{G}|/2$ equal-rate messages $M_{j,G}$ of rate $2R_j/|\mathcal{G}|$ and generate codewords $x_j^n(m_{j,G}, G)$ for each pair $\{G, \bar{G}\}$. Store each codeword twice into FIFO buffers corresponding to each G and its conjugate. Then transmit the codewords by multiplexing over the buffers based on the channel gain matrix sequence

Now since the same codeword is repeated twice, the demultiplexed channel

outputs corresponding to each (G, \bar{G}) pair are

$$\mathbf{Y}(G) = G\mathbf{X} + \mathbf{Z}(G), \quad \mathbf{Y}(\bar{G}) = \bar{G}\mathbf{X} + \mathbf{Z}(\bar{G})$$

with the same \mathbf{X} . Here $\mathbf{Z}(G)$ and $\mathbf{Z}(\bar{G})$ are independent of each other (since they are from separate transmission times)

Thus, for each pair of (G, \bar{G}) , the effective channel is

$$\tilde{\mathbf{Y}} = (G + \bar{G})\mathbf{X} + \mathbf{Z}(G) + \mathbf{Z}(\bar{G}),$$

which has no interference since $G + \bar{G}$ is diagonal! Hence, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$, if the rate of $M_{j,G}$ satisfies

$$R_{j,G} < (1 - \epsilon)p(G) C(2g^2P) - \delta(\epsilon)$$

or equivalently

$$R_j < \frac{1}{2}((1 - \epsilon) C(2g^2P) - \delta(\epsilon))$$

- Remark: This ergodic interference alignment technique can be extended to symmetric fading distributions by quantizing channel gain matrices [13]

Key New Ideas and Techniques

- Fading channel models
- Different coding approaches:
 - Coding over coherence time intervals (ergodic capacity)
 - Compound channel
 - Outage
 - Broadcasting
 - Adaptive
- Ergodic interference alignment

References

- [1] L. H. Ozarow, S. Shamai, and A. D. Wyner, "Information theoretic considerations for cellular mobile radio," *IEEE Trans. Veh. Technol.*, vol. 43, no. 2, pp. 359–378, May 1994.
- [2] A. J. Goldsmith and P. P. Varaiya, "Capacity of fading channels with channel side information," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1986–1992, 1997.
- [3] T. M. Cover, "Broadcast channels," *IEEE Trans. Inf. Theory*, vol. 18, no. 1, pp. 2–14, Jan. 1972.
- [4] S. Shamai, "A broadcast strategy for the Gaussian slowly fading channel," in *Proc. IEEE International Symposium on Information Theory*, Ulm, Germany, June/July 1997, p. 150.
- [5] S. Shamai and A. Steiner, "A broadcast approach for a single-user slowly fading MIMO channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2617–2635, 2003.
- [6] D. N. C. Tse and S. V. Hanly, "Multiaccess fading channels—I. Polymatroid structure, optimal resource allocation and throughput capacities," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2796–2815, 1998.
- [7] R. Knopp and P. Humblet, "Information capacity and power control in single-cell multiuser communications," in *Proc. IEEE International Conference on Communications*, vol. 1, Seattle, WA, June 1995, pp. 331–335.
- [8] Y. Cemal and Y. Steinberg, "The multiple-access channel with partial state information at the encoders," *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 3992–4003, 2005.
- [9] S. A. Jafar, "Capacity with causal and noncausal side information: A unified view," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5468–5474, 2006.

- [10] S. Shamai and I. E. Telatar, "Some information theoretic aspects of decentralized power control in multiple access fading channels," in *Proc. IEEE Information Theory and Networking Workshop*, Metsovo, Greece, June/July 1999, p. 23.
- [11] C.-S. Hwang, M. Malkin, A. El Gamal, and J. M. Cioffi, "Multiple-access channels with distributed channel state information," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 1561–1565.
- [12] L. Li and A. J. Goldsmith, "Capacity and optimal resource allocation for fading broadcast channels—I. Ergodic capacity," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 1083–1102, 2001.
- [13] B. Nazer, M. Gastpar, S. A. Jafar, and S. Vishwanath, "Ergodic interference alignment," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 1769–1773.

Lecture Notes 9

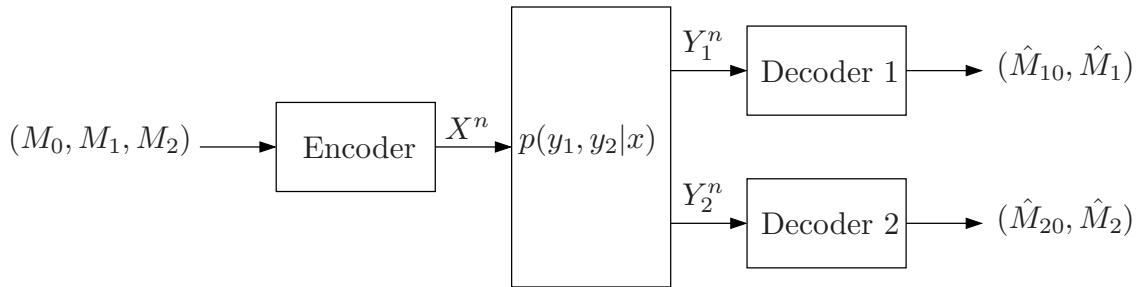
General Broadcast Channels

- Problem Setup
- DM-BC with Degraded Message Sets
- 3-Receiver Multilevel DM-BC with Degraded Message Sets
- Marton's Inner Bound
- Nair–El Gamal Outer Bound
- Inner Bound for More Than 2 Receivers
- Key New Ideas and Techniques
- Appendix: Proof of Mutual Covering Lemma
- Appendix: Proof of Nair–El Gamal Outer Bound

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- Again consider a 2-receiver DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$



- The definitions of a code, achievability, and capacity regions are as in Lecture Notes #5
- As we discussed, the capacity region of the DM-BC is not known in general. We first discuss the case of degraded message sets ($R_2 = 0$) for which the capacity region is completely characterized, and then present inner and outer bounds on the capacity region for private messages and for the general case

- As for the BC classes discussed in Lecture Notes #5, the capacity region of the 2-receiver DM-BC with degraded message sets is achieved using superposition coding, which requires that one of the receivers decodes both messages (cloud center and satellite codeword) and the other receiver decodes only the cloud center. As we will see, these decoding requirements can result in lower achievable rates for the 3-receiver DM-BC with degraded message sets and for the 2-receiver DM-BC with the general message requirement
- To overcome the limitation of superposition coding, we introduce two new coding techniques:
 - Indirect decoding: A receiver who only wishes to decode the common message uses satellite codewords to help it *indirectly* decode the correct cloud center
 - Marton coding: Codewords for independent messages can be jointly distributed according to any desired pmf without the use of a superposition structure

DM-BC with Degraded Message Sets

- Consider a general DM-BC with $M_2 = \emptyset$ (i.e., $R_2 = 0$). Since Y_2 wishes to decode the common message only while the receiver Y_1 wishes to decode both the common and private messages, this setup is referred to as the DM-BC *with degraded message sets*. The capacity region is known for this case
- Theorem 1 [1]:* The capacity region of the DM-BC with degraded message sets is the set of (R_0, R_1) such that

$$\begin{aligned} R_0 &\leq I(U; Y_2), \\ R_1 &\leq I(X; Y_1 | U), \\ R_0 + R_1 &\leq I(X; Y_1) \end{aligned}$$

for some $p(u, x)$, where $|\mathcal{U}| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1| \cdot |\mathcal{Y}_2|\} + 2$

- Achievability follows from the superposition coding inner bound in Lecture Notes #5 by noting that receiver Y_1 needs to reliably decode both M_0 and M_1

- As in the converse for the more capable BC, we consider the alternative characterization of the capacity region that consists of the set of rate pairs (R_0, R_1) such that

$$\begin{aligned} R_0 &\leq I(U; Y_2), \\ R_0 + R_1 &\leq I(X; Y_1), \\ R_0 + R_1 &\leq I(X; Y_1|U) + I(U; Y_2) \end{aligned}$$

for some $p(u, x)$. We then prove the converse for this region using the Csiszár sum identity and other standard techniques (check!)

- Can we show that the above region is achievable directly?

The answer is yes, and the proof involves (unnecessary) *rate splitting*:

- Divide M_1 into two independent message; M_{10} at rate R_{10} and M_{11} at rate R_{11} . Represent (M_0, M_{10}) by U and (M_0, M_{10}, M_{11}) by X

- Following similar steps to the proof of achievability of the superposition coding inner bound, we can show that (R_0, R_{10}, R_{11}) is achievable if

$$\begin{aligned} R_0 + R_{10} &< I(U; Y_2), \\ R_{11} &< I(X; Y_1|U), \\ R_0 + R_1 &< I(X; Y_1) \end{aligned}$$

for some $p(u, x)$

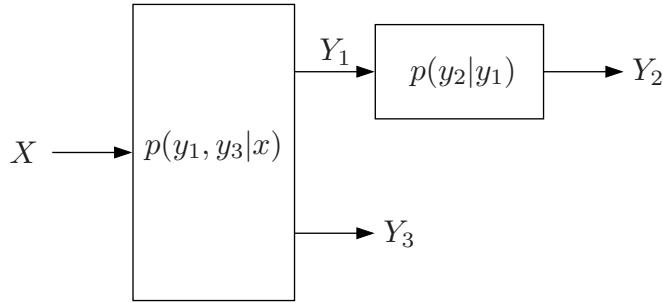
- Substituting $R_{11} = R_1 - R_{10}$, we have the conditions

$$\begin{aligned} R_{10} &\geq 0, \\ R_{10} &< I(U; Y_2) - R_0, \\ R_{10} &> R_1 - I(X; Y_1|U), \\ R_0 + R_1 &< I(X; Y_1), \\ R_{10} &\leq R_1 \end{aligned}$$

- Using the Fourier–Motzkin procedure (see Appendix D) to eliminate R_{10} gives the desired region
- Rate splitting turns out to be important when the DM-BC has more than 2 receivers

3-Receiver Multilevel DM-BC with Degraded Message Sets

- The capacity region of the DM-BC with two degraded message sets is not known in general for more than two receivers. We show that the straightforward extension of the superposition coding inner bound presented in Lecture Notes #5 to more than two receivers is not optimal for three receivers
- A 3-receiver *multilevel* DM-BC [2] $(\mathcal{X}, p(y_1, y_3|x)p(y_2|y_1), \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_3)$ is a 3-receiver DM-BC where receiver Y_2 is a degraded version of receiver Y_1



- Consider the two degraded message sets scenario in which a common message $M_0 \in [1 : 2^{nR_0}]$ is to be reliably sent to all receivers, and a private message $M_1 \in [1 : 2^{nR_1}]$ is to be sent only to receiver Y_1 . What is the capacity region?

- A straightforward extension of the superposition coding inner bound to the 3-receiver multilevel DM-BC, where Y_2 and Y_3 decode the cloud center and Y_1 decodes the satellite codeword, gives the set of rate pairs (R_0, R_1) such that

$$R_0 < \min\{I(U; Y_2), I(U; Y_3)\},$$

$$R_1 < I(X; Y_1|U)$$

for some $p(u, x)$

Note that the fourth bound $R_0 + R_1 < I(X; Y_1)$ drops out by the assumption that Y_2 is a degraded version of Y_1

- This region turns out not to be optimal in general

Theorem 5 [3]: The capacity region of the 3-receiver multilevel DM-BC is the set of rate pairs (R_0, R_1) such that

$$R_0 \leq \min\{I(U; Y_2), I(V; Y_3)\},$$

$$R_1 \leq I(X; Y_1|U),$$

$$R_0 + R_1 \leq I(V; Y_3) + I(X; Y_1|V)$$

for some $p(u)p(v|u)p(x|v)$, where $|\mathcal{U}| \leq |\mathcal{X}| + 4$ and $|\mathcal{V}| \leq |\mathcal{X}|^2 + 5|\mathcal{X}| + 4$

- The converse uses the converses for the degraded BC and 2-receiver degraded message sets [3]. The bound on cardinality uses the techniques in Appendix C

Proof of Achievability

- We use *rate splitting* and the new idea of *indirect decoding*
- Rate splitting: Split the private message M_1 into two independent parts M_{10}, M_{11} with rates R_{10}, R_{11} , respectively. Thus $R_1 = R_{10} + R_{11}$
- Codebook generation: Fix $p(u, v)p(x|v)$. Randomly and independently generate $u^n(m_0)$, $m_0 \in [1 : 2^{nR_0}]$, sequences each according to $\prod_{i=1}^n p_U(u_i)$
For each m_0 , randomly and conditionally independently generate $v^n(m_0, m_{10})$, $m_{10} \in [1 : 2^{nR_{10}}]$, sequences each according to $\prod_{i=1}^n p_{V|U}(v_i|u_i(m_0))$
For each (m_0, m_{10}) , randomly and conditionally independently generate $x^n(m_0, m_{10}, m_{11})$, $m_{11} \in [1 : 2^{nR_{11}}]$, sequences each according to $\prod_{i=1}^n p_{X|V}(x_i|v_i(m_0, m_{10}))$
- Encoding: To send $(m_0, m_1) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$, where m_1 is represented by $(m_{10}, m_{11}) \in [1 : 2^{nR_{10}}] \times [1 : 2^{nR_{11}}]$, the encoder transmits $x^n(m_0, m_{10}, m_{11})$

- Decoding and analysis of the probability of error for decoders 1 and 2:
 - Decoder 2 declares that $\hat{m}_{02} \in [1 : 2^{nR_0}]$ is sent if it is the unique message such that $(u^n(\hat{m}_{02}), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$. By the LLN and the packing lemma, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_0 < I(U; Y_2) - \delta(\epsilon)$$
 - Decoder 1 declares that $(\hat{m}_{01}, \hat{m}_{10}, \hat{m}_{11})$ is sent if it is the unique triple such that $(u^n(\hat{m}_{01}), v^n(\hat{m}_{01}, \hat{m}_{10}), x^n(\hat{m}_{01}, \hat{m}_{10}, \hat{m}_{11}), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$. By the LLN and the packing lemma, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_{11} < I(X; Y_1|V) - \delta(\epsilon),$$

$$R_{10} + R_{11} < I(X; Y_1|U) - \delta(\epsilon),$$

$$R_0 + R_{10} + R_{11} < I(X; Y_1) - \delta(\epsilon)$$
- Decoding and analysis of the probability of error for decoder 3:
 - If receiver Y_3 decodes m_0 directly by finding the unique \hat{m}_{03} such that $(u^n(\hat{m}_{03}), y_3^n) \in \mathcal{T}_\epsilon^{(n)}$, we obtain $R_0 < I(U; Y_3)$, which together with previous conditions gives the extended superposition coding inner bound

- To achieve the larger region, receiver Y_3 decodes m_0 *indirectly*:
It declares that \hat{m}_{03} is sent if it is the unique index such that
 $(u^n(\hat{m}_{03}), v^n(\hat{m}_{03}, m_{10}), y_3^n) \in \mathcal{T}_\epsilon^{(n)}$ for some $m_{10} \in [1 : 2^{nR_{10}}]$ Assume
 $(m_0, m_{10}) = (1, 1)$ is sent
- Consider the pmfs for the triple $(U^n(m_0), V^n(m_0, m_{10}), Y_3^n)$

m_0	m_{10}	Joint pmf
1	1	$p(u^n, v^n)p(y_3^n v^n)$
1	*	$p(u^n, v^n)p(y_3^n u^n)$
*	*	$p(u^n, v^n)p(y_3^n)$
*	1	$p(u^n, v^n)p(y_3^n)$

- The second case does not result in an error, and the last 2 cases have the same pmf
- Thus, we are left with only two error events

$$\mathcal{E}_{31} := \{(U^n(1), V^n(1, 1), Y_3^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$

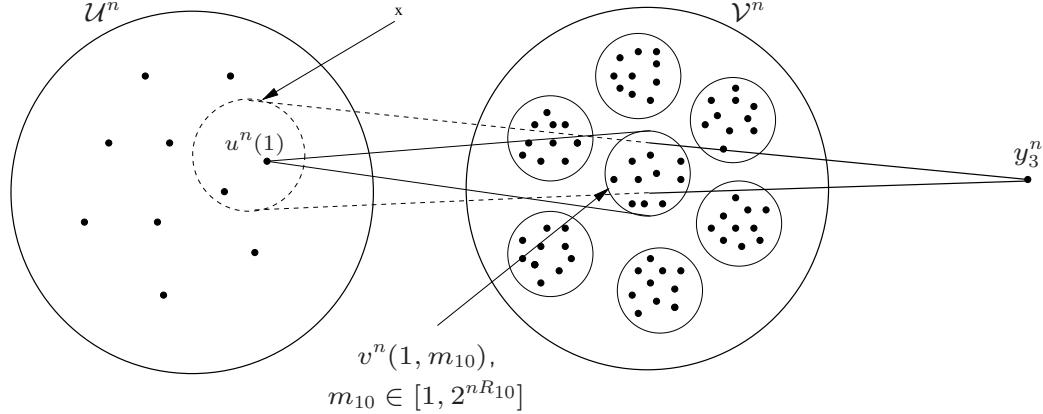
$$\mathcal{E}_{32} := \{(U^n(m_0), V^n(m_0, m_{10}), Y_3^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_0 \neq 1, m_{10}\}$$

Then, the probability of error for decoder 3 averaged over codebooks
 $P(\mathcal{E}_3) \leq P(\mathcal{E}_{31}) + P(\mathcal{E}_{32})$

- By the LLN, $P(\mathcal{E}_{31}) \rightarrow 0$ as $n \rightarrow \infty$
- By the packing lemma (with $|\mathcal{A}| = 2^{n(R_0+R_{10})} - 1$, $X \rightarrow (U, V)$, $U = \emptyset$),
 $P(\mathcal{E}_{32}) \rightarrow 0$ as $n \rightarrow \infty$ if $R_0 + R_{10} < I(U, V; Y_3) - \delta(\epsilon) = I(V; Y_3) - \delta(\epsilon)$
- Combining the bounds, substituting $R_{10} + R_{11} = R_1$, and using the Fourier–Motzkin procedure to eliminate R_{10} and R_{11} complete the proof of achievability

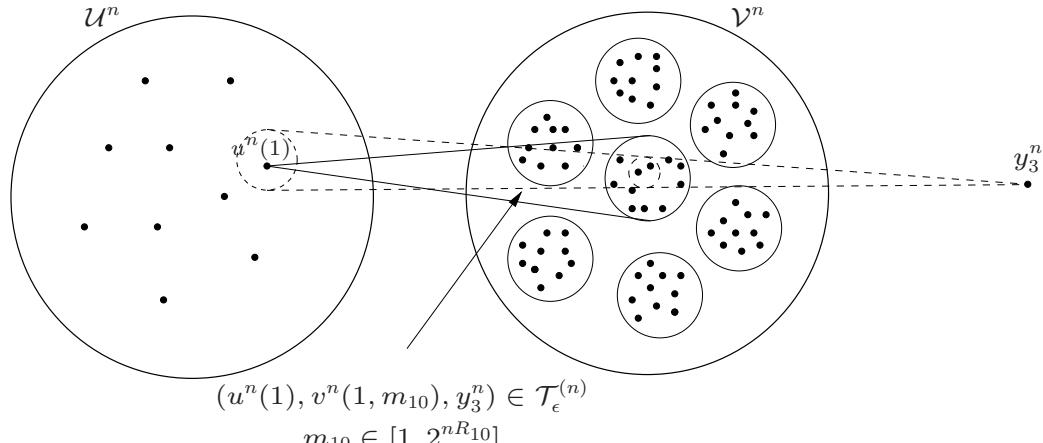
Indirect Decoding Interpretation

- Suppose that $R_0 > I(U; Y_3)$
- Y_3 cannot directly decode the cloud center $u^n(1)$



Indirect Decoding Interpretation

- Assume $R_0 > I(U; Y_3)$ but $R_0 + R_{10} < I(V; Y_3)$
- Y_3 decodes cloud center *indirectly*



- The above condition suffices in general (even when $R_0 < I(U; Y_3)$)

Multilevel Product BC

- We show that the extended superposition coding inner bound can be strictly smaller than the capacity region
- Consider the product of two 3-receiver BCs given by the Markov relationships

$$X_1 \rightarrow Y_{31} \rightarrow Y_{11} \rightarrow Y_{21},$$

$$X_2 \rightarrow Y_{12} \rightarrow Y_{22}.$$

- The extended superposition coding inner bound reduces to the set of rate pairs (R_0, R_1) such that

$$R_0 \leq I(U_1; Y_{21}) + I(U_2; Y_{22}),$$

$$R_0 \leq I(U_1; Y_{31}),$$

$$R_1 \leq I(X_1; Y_{11}|U_1) + I(X_2; Y_{12}|U_2)$$

for some $p(u_1, x_1)p(u_2, x_2)$

- Similarly, it can be shown that the capacity region reduces to the set of rate pairs (R_0, R_1) such that

$$R_0 \leq I(U_1; Y_{21}) + I(U_2; Y_{22}),$$

$$R_0 \leq I(V_1; Y_{31}),$$

$$R_1 \leq I(X_1; Y_{11}|U_1) + I(X_2; Y_{12}|U_2),$$

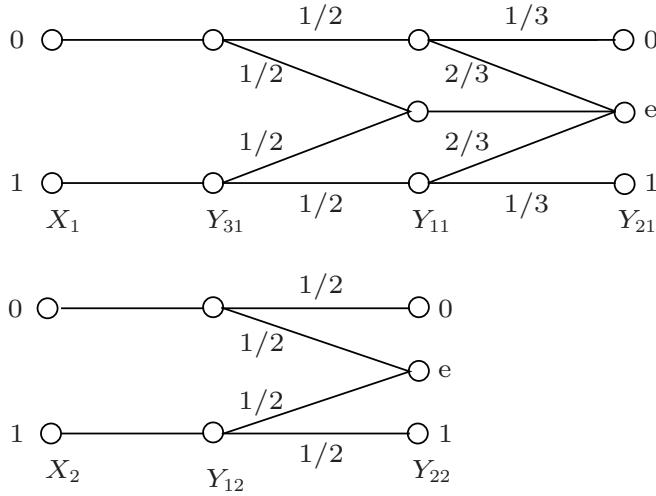
$$R_0 + R_1 \leq I(V_1; Y_{31}) + I(X_1; Y_{11}|V_1) + I(X_2; Y_{12}|U_2)$$

for some $p(u_1)p(v_1|u_1)p(x_1|v_1)p(u_2)p(x_2|u_2)$

- We now compare these two regions via the following example

Example

- Consider the multilevel product DM-BC example in the figure, where $\mathcal{X}_1 = \mathcal{X}_2 = \mathcal{Y}_{12} = \mathcal{Y}_{21} = \{0, 1\}$ and $\mathcal{Y}_{11} = \mathcal{Y}_{31} = \mathcal{Y}_{32} = \{0, 1\}$



- It can be shown that the extended superposition coding inner bound can be simplified to the set of rate pairs (R_0, R_1) such that

$$R_0 \leq \min \left\{ \frac{p}{6} + \frac{q}{2}, p \right\}, \quad R_1 \leq \frac{1-p}{2} + 1-q$$

for some $0 \leq p, q \leq 1$. It is straightforward to show that $(R_0, R_1) = (1/2, 5/12)$ lies on the boundary of this region

- The capacity region can be simplified to set of rate pairs (R_0, R_1) such that

$$R_0 \leq \min \left\{ \frac{r}{6} + \frac{s}{2}, t \right\},$$

$$R_1 \leq \frac{1-r}{2} + 1-s,$$

$$R_0 + R_1 \leq t + \frac{1-t}{2} + 1-s$$

for some $0 \leq r \leq t \leq 1, 0 \leq s \leq 1$

- Note that substituting $r = t$ yields the extended superposition coding inner bound. By setting $r = 0, s = 1, t = 1$ it can be shown that $(R_0, R_1) = (1/2, 1/2)$ lies on the boundary of the capacity region. On the other hand, for $R_0 = 1/2$, the maximum achievable R_1 in the extended superposition coding inner bound is $5/12$. Thus the capacity region is strictly larger than the extended superposition coding inner bound

Cover–van der Meulen Inner Bound

- We now turn attention to the 2-receiver DM-BC with private messages only, i.e., where $R_0 = 0$
- First consider the following special case of the inner bound in [4, 5]:

Theorem 1 (Cover–van der Meulen Inner Bound): A rate pair (R_1, R_2) is achievable for a DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$ if

$$R_1 < I(U_1; Y_1), \quad R_2 < I(U_2; Y_2)$$

for some $p(u_1)p(u_2)$ and function $x(u_1, u_2)$

- Achievability is straightforward
- Codebook generation: Fix $p(u_1)p(u_2)$ and $x(u_1, u_2)$. Randomly and independently generate 2^{nR_1} sequences $u_1^n(m_1)$, $m_1 \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{U_1}(u_{1i})$ and 2^{nR_2} sequences $u_2^n(m_2)$, $m_2 \in [1 : 2^{nR_2}]$ each according to $\prod_{i=1}^n p_{U_2}(u_{2i})$
- Encoding: To send (m_1, m_2) , transmit $x_i(u_{1i}(m_1), u_{2i}(m_2))$ at time $i \in [1 : n]$
- Decoding and analysis of the probability of error: Decoder $j = 1, 2$ declares that message \hat{m}_j is sent if it is the unique message such that $(U_j^n(\hat{m}_j), Y_j^n) \in \mathcal{T}_\epsilon^{(n)}$
By the LLN and packing lemma, the probability of decoding error $\rightarrow 0$ as $n \rightarrow \infty$ if $R_j < I(U_j; Y_j) - \delta(\epsilon)$ for $j = 1, 2$

Marton's Inner Bound

- Marton's inner bound allows U_1, U_2 in the Cover–van der Meulen bound to be correlated (even though the messages are independent). This comes at an apparent penalty term in the sum rate
- *Theorem 2* (Marton's Inner Bound) [6, 7]: A rate pair (R_1, R_2) is achievable for a DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$ if

$$R_1 < I(U_1; Y_1),$$

$$R_2 < I(U_2; Y_2),$$

$$R_1 + R_2 < I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2)$$

for some $p(u_1, u_2)$ and function $x(u_1, u_2)$

- Remarks:
 - Marton's inner bound reduces to the Cover–van der Meulen bound if the region is evaluated with independent U_1 and U_2 only
 - As in the Gelfand–Pinsker theorem, the region does not increase when evaluated with general conditional pmfs $p(x|u_1, u_2)$
 - This region is not convex in general

Semi-deterministic DM-BC

- Marton's inner bound is tight for *semi-deterministic* DM-BC [8], where $p(y_1|x)$ is a $(0, 1)$ matrix (i.e., $Y_1 = y_1(X)$). The capacity region is obtained by setting $U_1 = Y_1$ in Marton's inner bound (and relabeling U_2 as U), which gives the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq H(Y_1), \\ R_2 &\leq I(U; Y_2), \\ R_1 + R_2 &\leq H(Y_1|U) + I(U; Y_2) \end{aligned}$$

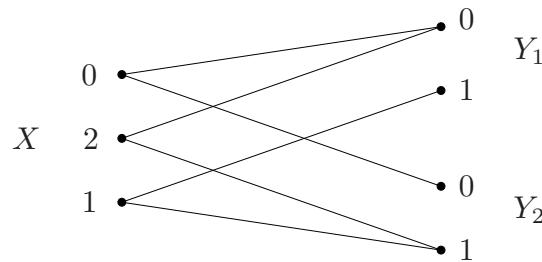
for some $p(u, x)$

- For the special case of fully deterministic DM-BC (i.e., $Y_1 = y_1(X)$ and $Y_2 = y_2(X)$), the capacity region reduces to the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq H(Y_1), \\ R_2 &\leq H(Y_2), \\ R_1 + R_2 &\leq H(Y_1, Y_2) \end{aligned}$$

for some $p(x)$

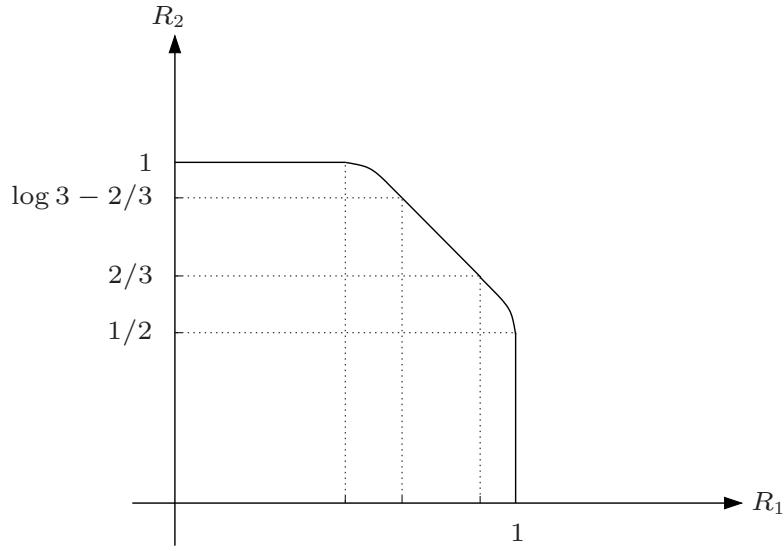
Example (*Blackwell channel* [9]): Consider the following deterministic BC



The capacity region [10] is the union of the two regions (see figure):

$$\begin{aligned} \{(R_1, R_2) : R_1 \leq H(\alpha), R_2 \leq H(\alpha/2), R_1 + R_2 \leq H(\alpha) + \bar{\alpha} \text{ for } \alpha \in [1/3, 1/2]\}, \\ \{(R_1, R_2) : R_1 \leq H(\alpha/2), R_2 \leq H(\alpha), R_1 + R_2 \leq H(\alpha) + \bar{\alpha} \text{ for } \alpha \in [1/3, 1/2]\} \end{aligned}$$

The first region is achieved using $p_X(0) = p_X(2) = \alpha/2$, $p_X(1) = \bar{\alpha}$

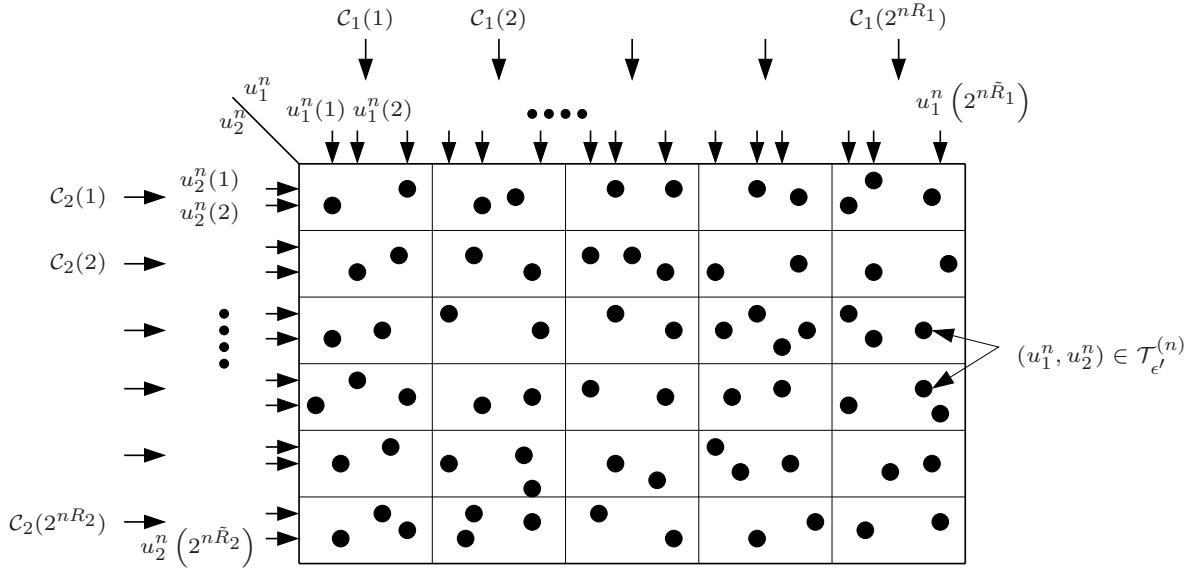


- Marton's inner bound is also tight for MIMO Gaussian broadcast channels [11, 12], which we discuss in Lecture Notes #10

Proof of Achievability

- Codebook generation: Fix $p(u_1, u_2)$ and $x(u_1, u_2)$ and let $\tilde{R}_1 \geq R_1, \tilde{R}_2 \geq R_2$
 For each message $m_1 \in [1 : 2^{nR_1}]$ generate a *subcodebook* $\mathcal{C}_1(m_1)$ consisting of $2^{n(\tilde{R}_1-R_1)}$ randomly and independently generated sequences $u_1^n(l_1)$,
 $l_1 \in [(m_1 - 1)2^{n(\tilde{R}_1-R_1)} + 1 : m_12^{n(\tilde{R}_1-R_1)}]$, each according to $\prod_{i=1}^n p_{U_1}(u_{1i})$
 Similarly, for each message $m_2 \in [1 : 2^{nR_2}]$ generate a subcodebook $\mathcal{C}_2(m_2)$
 consisting of $2^{n(\tilde{R}_2-R_2)}$ randomly and independently generated sequences
 $u_2^n(l_2)$, $l_2 \in [(m_2 - 1)2^{n(\tilde{R}_2-R_2)} + 1 : m_22^{n(\tilde{R}_2-R_2)}]$, each according to
 $\prod_{i=1}^n p_{U_2}(u_{2i})$
 For $m_1 \in [1 : 2^{nR_1}]$ and $m_2 \in [1 : 2^{nR_2}]$, define the set

$$\mathcal{C}(m_1, m_2) := \{(u_1^n(l_1), u_2^n(l_2)) \in \mathcal{C}_1(m_1) \times \mathcal{C}_2(m_2) : (u_1^n(l_1), u_2^n(l_2)) \in \mathcal{T}_{\epsilon'}^{(n)}\}$$



For each message pair $(m_1, m_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$, pick one sequence pair $(u_1^n(l_1), u_2^n(l_2)) \in \mathcal{C}(m_1, m_2)$. If no such pair exists, pick an arbitrary pair $(u_1^n(l_1), u_2^n(l_2)) \in \mathcal{C}_1(m_1) \times \mathcal{C}_2(m_2)$

- Encoding: To send a message pair (m_1, m_2) , transmit $x_i = x(u_{1i}(l_1), u_{2i}(l_2))$ at time $i \in [1 : n]$

- Decoding: Let $\epsilon > \epsilon'$. Decoder 1 declares that \hat{m}_1 is sent if it is the unique message such that $(u_1^n(l_1), y_1^n) \in \mathcal{T}_{\epsilon}^{(n)}$ for some $u_1^n(l_1) \in \mathcal{C}_1(\hat{m}_1)$; otherwise it declares an error
Similarly, Decoder 2 finds the unique message \hat{m}_2 such that $(u_2^n(l_2), y_2^n) \in \mathcal{T}_{\epsilon}^{(n)}$ for some $u_2^n(l_2) \in \mathcal{C}_2(\hat{m}_2)$

- A crucial requirement for this coding scheme to work is that we have at least one sequence pair $(u_1^n(l_1), u_2^n(l_2)) \in \mathcal{C}(m_1, m_2)$

The constraint on the subcodebook sizes to guarantee this is provided by the following lemma

Mutual Covering Lemma

- *Mutual Covering Lemma [7]:* Let $(U_1, U_2) \sim p(u_1, u_2)$ and $\epsilon > 0$. Let $U_1^n(m_1), m_1 \in [1 : 2^{nr_1}]$, be pairwise independent random sequences, each distributed according to $\prod_{i=1}^n p_{U_1}(u_{1i})$. Similarly, let $U_2^n(m_2), m_2 \in [1 : 2^{nr_2}]$, be pairwise independent random sequences, each distributed according to $\prod_{i=1}^n p_{U_2}(u_{2i})$. Assume that $\{U_1^n(m_1) : m_1 \in [1 : 2^{nr_1}]\}$ and $\{U_2^n(m_2) : m_2 \in [1 : 2^{nr_2}]\}$ are independent

Then, there exists $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$ such that

$$\mathbb{P}\{(U_1^n(m_1), U_2^n(m_2)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m_1 \in [1 : 2^{nr_1}], m_2 \in [1 : 2^{nr_2}]\} \rightarrow 0$$

as $n \rightarrow \infty$ if $r_1 + r_2 > I(U_1; U_2) + \delta(\epsilon)$

- The proof of the lemma is given in the Appendix
- This lemma extends the covering lemma (without conditioning) in two ways:
 - By considering a single U_1^n sequence ($r_1 = 0$), we get the same rate requirement $r_2 > I(U_1; U_2) + \delta(\epsilon)$ as in the covering lemma
 - The condition of pairwise independence among codewords implies that it suffices to use linear codes for certain lossy source coding setups (such as for a binary symmetric source with Hamming distortion)

Analysis of the Probability of Error

- Assume without loss of generality that $(M_1, M_2) = (1, 1)$ and let (L_1, L_2) denote the pair of chosen indices in $\mathcal{C}(1, 1)$
- For the average probability of error at decoder 1, define the error events

$$\mathcal{E}_0 := \{|\mathcal{C}(1, 1)| = 0\},$$

$$\mathcal{E}_{11} := \{(U_1^n(L_1), Y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\mathcal{E}_{12} := \{(U_1^n(l_1), Y_1^n) \in \mathcal{T}_\epsilon^{(n)}(U_1, Y_1) \text{ for some } u_1^n(l_1) \notin \mathcal{C}(1)\}$$

Then the probability of error for decoder 1 is bounded by

$$\mathbb{P}(\mathcal{E}_1) \leq \mathbb{P}(\mathcal{E}_0) + \mathbb{P}(\mathcal{E}_0^c \cap \mathcal{E}_{11}) + \mathbb{P}(\mathcal{E}_{12})$$

1. To bound $\mathbb{P}(\mathcal{E}_0)$, we note that the subcodebook $\mathcal{C}_1(1)$ consists of $2^{n(\tilde{R}_1 - R_1)}$ i.i.d. $U_1^n(l_1)$ sequences and subcodebook $\mathcal{C}_2(1)$ consists of $2^{n(\tilde{R}_2 - R_2)}$ i.i.d. $U_2^n(l_2)$ sequences. Hence, by the mutual covering lemma with $r_1 = \tilde{R}_1 - R_1$ and $r_2 = \tilde{R}_2 - R_2$, $\mathbb{P}\{|\mathcal{C}(1, 1)| = 0\} \rightarrow 0$ as $n \rightarrow \infty$ if $(\tilde{R}_1 - R_1) + (\tilde{R}_2 - R_2) > I(U_1; U_2) + \delta(\epsilon')$
2. By the conditional typicality lemma, since $(U_1^n(L_1), U_2^n(L_2)) \in \mathcal{T}_{\epsilon'}^{(n)}$ and $\epsilon' < \epsilon$, $\mathbb{P}\{(U_1^n(L_1), U_2^n(L_2), X^n, Y_1^n) \notin \mathcal{T}_\epsilon^{(n)}\} \rightarrow 0$ as $n \rightarrow \infty$. Hence, $\mathbb{P}(\mathcal{E}_0^c \cap \mathcal{E}_{11}) \rightarrow 0$ as $n \rightarrow \infty$

3. By the packing lemma, since Y_1^n is independent of every $U_1^n(l_1) \notin \mathcal{C}(1)$ and $U_1^n(l_1) \sim \prod_{i=1}^n p_{U_1}(u_{1i})$, $\mathbb{P}(\mathcal{E}_{12}) \rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R}_1 < I(U_1; Y_1) - \delta(\epsilon)$
- Similarly, the average probability of error $\mathbb{P}(\mathcal{E}_2)$ for Decoder 2 $\rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R}_2 < I(U_2; Y_2) + \delta(\epsilon)$ and $(\tilde{R}_1 - R_1) + (\tilde{R}_2 - R_2) > I(U_1; U_2) + \delta(\epsilon')$
 - Thus, we have the average probability of error $\mathbb{P}(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$ if the rate pair (R_1, R_2) satisfies

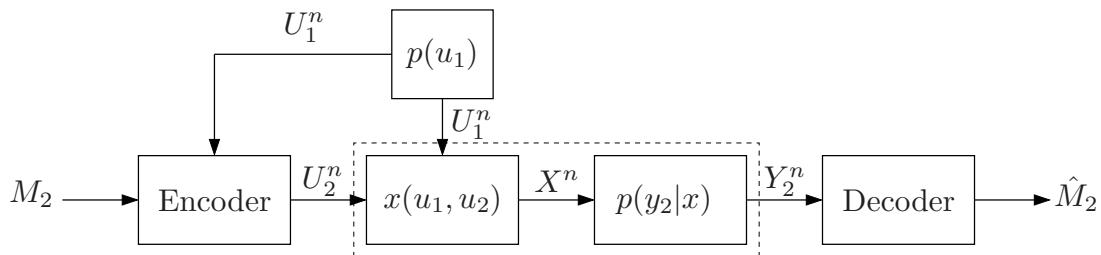
$$\begin{aligned} R_1 &\leq \tilde{R}_1, \\ R_2 &\leq \tilde{R}_2, \\ \tilde{R}_1 &< I(U_1; Y_1) - \delta(\epsilon), \\ \tilde{R}_2 &< I(U_2; Y_2) - \delta(\epsilon), \\ R_1 + R_2 &< \tilde{R}_1 + \tilde{R}_2 - I(U_1; U_2) - \delta(\epsilon') \end{aligned}$$

for some $(\tilde{R}_1, \tilde{R}_2)$, or equivalently, if

$$\begin{aligned} R_1 &< I(U_1; Y_1) - \delta(\epsilon), \\ R_2 &< I(U_2; Y_2) - \delta(\epsilon), \\ R_1 + R_2 &< I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2) - \delta(\epsilon') \end{aligned}$$

Relationship to Gelfand–Pinsker

- Fix $p(u_1, u_2)$, $x(u_1, u_2)$ and consider the achievable rate pair $R_1 < I(U_1; Y_1)$ and $R_2 < I(U_2; Y_2) - I(U_1; U_2)$



- So the coding scheme for sending M_2 to Y_2 is identical to that of sending M_2 over a channel $p(y_2|u_1, u_2) = p(y_2|x(u_1, u_2))$ with state U_1 available noncausally at the encoder
- Of course, since we do not know if Marton coding is optimal, it is not clear how fundamental this relationship is
- This relationship, however, turned out to be crucial in establishing the capacity region of MIMO Gaussian BCs (which are not in general degraded)

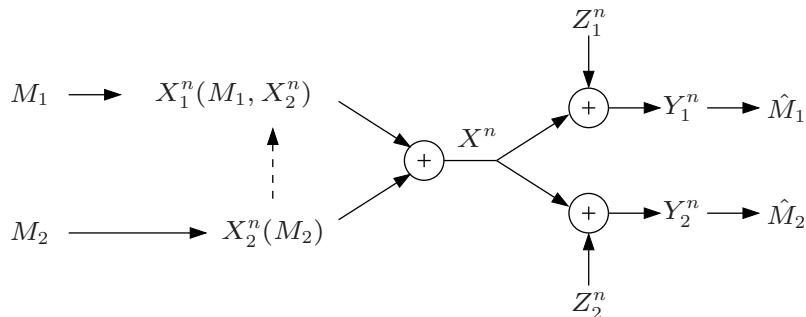
Application: AWGN Broadcast Channel

- We revisit the AWGN-BC studied in Lecture Notes #5. At time i , $Y_{1i} = X_i + Z_{1i}$, $Y_{2i} = X_i + Z_{2i}$, and $\{Z_{1i}\}$ and $\{Z_{2i}\}$ are WGN processes with average power N_1 and N_2 , respectively
- We show that for any $\alpha \in [0, 1]$ the rate pair

$$R_1 < C(\alpha S_1), \quad R_2 < C\left(\frac{\bar{\alpha}S_2}{\alpha S_2 + 1}\right),$$

where $S_j := P/N_j$, $j = 1, 2$, is achievable without successive cancellation and even when $N_1 > N_2$

- Decompose the channel input X into two independent parts $X_1 \sim N(0, \alpha P)$ and $X_2 \sim N(0, \bar{\alpha}P)$ such that $X = X_1 + X_2$



- To send M_2 to Y_2 , consider the channel $Y_{2i} = X_{2i} + X_{1i} + Z_{2i}$ with input X_{2i} , AWGN interference signal X_{1i} , and AWGN Z_{2i} . Treating the interference signal X_{1i} as noise, by the coding theorem for the AWGN channel, M_2 can be sent reliably to Y_2 provided $R_2 < C(\bar{\alpha}S_2/(\alpha S_2 + 1))$
- To send M_1 to Y_1 , consider the channel $Y_{1i} = X_{1i} + X_{2i} + Z_{1i}$, with input X_{1i} , AWGN state X_{2i} , and AWGN Z_{1i} , where the state $X_2^n(M_2)$ is known noncausally at the encoder. By the writing on dirty paper result, M_1 can be sent reliably to Y_1 provided $R_1 < C(\alpha S_1)$
- In the next lecture notes, we extend this result to vector Gaussian broadcast channels, in which the receiver outputs are no longer degraded, and show that a vector version of the dirty paper coding achieves the capacity region

Marton's Inner Bound with Common Message

- *Theorem 3 [6]:* Any rate triple (R_0, R_1, R_2) is achievable for a DM-BC if

$$R_0 + R_1 < I(U_0, U_1; Y_1),$$

$$R_0 + R_2 < I(U_0, U_2; Y_2),$$

$$R_0 + R_1 + R_2 < I(U_0, U_1; Y_1) + I(U_2; Y_2|U_0) - I(U_1; U_2|U_0),$$

$$R_0 + R_1 + R_2 < I(U_1; Y_1|U_0) + I(U_0, U_2; Y_2) - I(U_1; U_2|U_0),$$

$$2R_0 + R_1 + R_2 < I(U_0, U_1; Y_1) + I(U_0, U_2; Y_2) - I(U_1; U_2|U_0)$$

for some $p(u_0, u_1, u_2)$ and function $x(u_0, u_1, u_2)$, where $|\mathcal{U}_0| \leq |\mathcal{X}| + 4$, $|\mathcal{U}_1| \leq |\mathcal{X}|$, $|\mathcal{U}_2| \leq |\mathcal{X}|$

- Remark: The cardinality bounds on auxiliary random variables are proved via the perturbation technique by Gohari and Anantharam [13] discussed in Appendix C
- Outline of achievability: Divide M_j , $j = 1, 2$, into two independent messages M_{j0} and M_{jj} . Thus $R_j = R_{j0} + R_{jj}$ for $j = 1, 2$
Randomly and independently generate $2^{n(R_0+R_{10}+R_{20})}$ sequences $u_0^n(m_0, m_{10}, m_{20})$

For each (m_0, m_{10}, m_{20}) , use Marton coding to generate $2^{n(R_{11}+R_{22})}$ sequence pairs $(u_1^n(m_0, m_{10}, m_{20}, l_{11}), u_2^n(m_0, m_{10}, m_{20}, l_{22}))$, $l_{11} \in [1, 2^{n\bar{R}_{11}}]$, $l_{22} \in [1, 2^{n\bar{R}_{22}}]$

To send (m_0, m_1, m_2) , transmit $x_i = x(u_{0i}(m_0, m_{10}, m_{20}), u_{1i}(m_0, m_{10}, m_{20}, l_{11}), u_{2i}(m_0, m_{10}, m_{20}, l_{22}))$ for $i \in [1 : n]$

Receiver Y_j , $j = 1, 2$, uses joint typicality decoding to find (m_0, m_j)

Using standard analysis of the probability of error and Fourier–Motzkin procedure, it can be shown that the above inequalities are sufficient for the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ (check)

- An equivalent region [14]: Any rate triple (R_0, R_1, R_2) is achievable for a DM-BC if

$$R_0 < \min\{I(U_0; Y_1), I(U_0; Y_2)\},$$

$$R_0 + R_1 < I(U_0, U_1; Y_1),$$

$$R_0 + R_2 < I(U_0, U_2; Y_2),$$

$$R_0 + R_1 + R_2 < I(U_0, U_1; Y_1) + I(U_2; Y_2|U_0) - I(U_1; U_2|U_0),$$

$$R_0 + R_1 + R_2 < I(U_1; Y_1|U_0) + I(U_0, U_2; Y_2) - I(U_1; U_2|U_0)$$

for some $p(u_0, u_1, u_2)$ and function $x(u_0, u_1, u_2)$

It is straightforward to show that if (R_0, R_1, R_2) is in this region, it is also in the above region. The other direction is established in [14]

- The above inner bound is tight for all classes of DM-BCs with known capacity regions

In particular, the capacity region of the deterministic BC ($Y_1 = y_1(X)$, $Y_2 = y_2(X)$) with common message [8] is the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_0 &\leq \min\{I(U; Y_1), I(U; Y_2)\}, \\ R_0 + R_1 &< H(Y_1), \\ R_0 + R_2 &< H(Y_2), \\ R_0 + R_1 + R_2 &< H(Y_1) + H(Y_2|U, Y_1), \\ R_0 + R_1 + R_2 &< H(Y_1|U, Y_2) + H(Y_2) \end{aligned}$$

for some $p(u, x)$

- It is not known if this inner bound is tight in general

- If we set $R_0 = 0$, we obtain an inner bound for the private message sets case, which consists of the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &< I(U_0, U_1; Y_1), \\ R_2 &< I(U_0, U_2; Y_2), \\ R_1 + R_2 &< I(U_0, U_1; Y_1) + I(U_2; Y_2|U_0) - I(U_1; U_2|U_0), \\ R_1 + R_2 &< I(U_1; Y_1|U_0) + I(U_0, U_2; Y_2) - I(U_1; U_2|U_0) \end{aligned}$$

for some $p(u_0, u_1, u_2)$ and function $x(u_o, u_1, u_2)$

This inner bound is in general larger than Marton's inner bound discussed earlier, where $U_0 = \emptyset$, and is tight for all classes of broadcast channels with known private message capacity regions. For example, Marton's inner bound with $U_0 = \emptyset$ is not optimal in general for the degraded BC, while the above inner bound is tight for this class

Nair–El Gamal Outer Bound

- *Theorem 4* (Nair–El Gamal Outer Bound) [15]: If a rate triple (R_0, R_1, R_2) is achievable for a DM-BC, then it must satisfy

$$R_0 \leq \min\{I(U_0; Y_1), I(U_0; Y_2)\},$$

$$R_0 + R_1 \leq I(U_0, U_1; Y_1),$$

$$R_0 + R_2 \leq I(U_0, U_2; Y_2),$$

$$R_0 + R_1 + R_2 \leq I(U_0, U_1; Y_1) + I(U_2; Y_2 | U_0, U_1),$$

$$R_0 + R_1 + R_2 \leq I(U_1; Y_1 | U_0, U_2) + I(U_0, U_2; Y_2)$$

for some $p(u_0, u_1, u_2, x) = p(u_1)p(u_2)p(u_0|u_1, u_2)$ and function $x(u_0, u_1, u_2)$

- This bound is tight for *all* broadcast channel classes with known capacity regions. It is also strictly tighter than earlier outer bounds by Sato [?] and Körner–Marton [6]
- Note that the outer bound coincides with Marton's inner bound if $I(U_1; U_2 | U_0, Y_1) = I(U_1; U_2 | U_0, Y_2) = 0$ for each joint pmf $p(u_0, u_1, u_2, x)$ that defines a rate region with points on the boundary of the outer bound

To see this, consider the second description of Marton's inner bound with common message

If $I(U_1; U_2 | U_0, Y_1) = I(U_1; U_2 | U_0, Y_2) = 0$ for every joint pmf that defines a rate region with points on the boundary of the outer bound, then the outer bound coincides with this inner bound

- The proof of the outer bound is quite similar to the converse for the capacity region of the more capable DM-BC in Lecture Notes #5 (see Appendix)
- In [?], it is shown that the above outer bound with no common message, i.e., $R_0 = 0$, is equal to the simpler region consisting of all (R_1, R_2) such that

$$R_1 \leq I(U_1; Y_1),$$

$$R_2 \leq I(U_2; Y_2),$$

$$R_1 + R_2 \leq \min\{I(U_1; Y_1) + I(X; Y_2 | U_1), I(U_2; Y_2) + I(X; Y_1 | U_2)\}$$

for some $p(u_1, u_2, x)$

- Note that this region is tight for all classes of DM-BC with known private message capacity regions. In contrast and as noted earlier, Marton's inner bound with private messages with $U_0 = \emptyset$ can be strictly smaller than that with general U_0

Example (a BSC and a BEC) [16]: Consider the DM-BC example where the channel to Y_1 is a BSC(p) and the channel to Y_2 is a BEC(ϵ). As discussed earlier, if $H(p) < \epsilon \leq 1$, the channel does not belong to any class with known capacity region. It can be shown, however, that the private-message capacity region is achieved using superposition coding and is given by the set of rate pairs (R_1, R_2) such that

$$R_2 \leq I(U; Y_2), \\ R_1 + R_2 \leq I(U; Y_2) + I(X; Y_1|U)$$

for some $p(u, x)$ such that $X \sim \text{Bern}(1/2)$

- Proof: First note that for the BSC–BEC broadcast channel, given any $(U, X) \sim p(u, x)$, there exists $(\tilde{U}, \tilde{X}) \sim p(\tilde{u}, \tilde{x})$ such that $\tilde{X} \sim \text{Bern}(1/2)$ and

$$I(U; Y_2) \leq I(\tilde{U}; \tilde{Y}_2), \\ I(X; Y_1) \leq I(\tilde{X}; \tilde{Y}_1), \\ I(X; Y_1|U) \leq I(\tilde{X}; \tilde{Y}_1|\tilde{U}),$$

where \tilde{Y}_1, \tilde{Y}_2 are the broadcast channel output symbols corresponding to \tilde{X} . Further, if $H(p) < \epsilon \leq 1$, then $I(U; Y_2) \leq I(U; Y_1)$ for all $p(u, x)$ such that $X \sim \text{Bern}(1/2)$, i.e., Y_1 is “essentially” less noisy than Y_2

Achievability: Recall the superposition inner bound consisting of the set of rate pairs (R_1, R_2) such that

$$R_2 < I(U; Y_2), \\ R_1 + R_2 < I(U; Y_2) + I(X; Y_1|U), \\ R_1 + R_2 < I(X; Y_1)$$

for some $p(u, x)$

Since for $X \sim \text{Bern}(1/2)$, $I(U; Y_2) \leq I(U; Y_1)$, any rate pair in the capacity region is achievable

Converse: Consider the equivalent Nair–El Gamal outer bound for private messages in [?]. Setting $U_2 = U$, we obtain the outer bound consisting of the set rate pairs (R_1, R_2) such that

$$R_2 \leq I(U; Y_2), \\ R_1 + R_2 \leq I(U; Y_2) + I(X; Y_1|U), \\ R_1 \leq I(X; Y_1)$$

for some $p(u, x)$

We first show that it suffices to consider joint pmfs $p(u, x)$ with $X \sim \text{Bern}(1/2)$ only. Given $(U, X) \sim p(u, x)$, let $W' \sim \text{Bern}(1/2)$ and U', \tilde{X} be such that

$$\mathbb{P}\{U' = u, \tilde{X} = x | W' = w\} = p_{U,X}(u, x \oplus w)$$

Let \tilde{Y}_1, \tilde{Y}_2 be the channel outputs corresponding to the input \tilde{X} . Then, by the symmetries in the input construction and the channels, it is easy to check that $\tilde{X} \sim \text{Bern}(1/2)$ and

$$\begin{aligned} I(U; Y_2) &= I(U'; \tilde{Y}_2 | W') \leq I(U', W'; \tilde{Y}_2) = I(\tilde{U}; \tilde{Y}_2), \\ I(X; Y_1) &= I(\tilde{X}; \tilde{Y}_1 | W') \leq I(\tilde{X}; \tilde{Y}_1), \\ I(X; Y_1 | U) &= I(\tilde{X}; \tilde{Y}_1 | U', W') = I(\tilde{X}; \tilde{Y}_1 | \tilde{U}), \end{aligned}$$

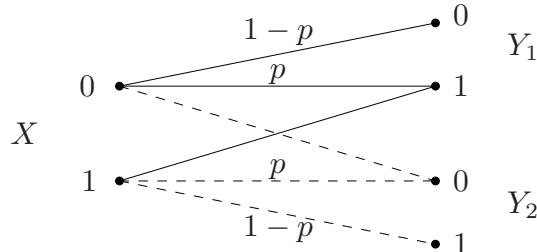
where $\tilde{U} := (U', W')$. This proves the sufficiency of $X \sim \text{Bern}(1/2)$

On the other hand, it can be also easily checked that $I(U; Y_2) \leq I(U; Y_1)$ for all $p(u, x)$ if $X \sim \text{Bern}(1/2)$. Therefore, the above outer bound reduces to the characterization of the capacity region (why?)

- In [17, 18], more general outer bounds are presented. It is not known, however, if they can be strictly larger than the Nair–El Gamal outer bound

Example: Binary Skew-Symmetric Broadcast Channel

- The binary skew-symmetric broadcast channel consists of two skew-symmetric Z-channels (assume $p = 1/2$)



- The private-message sum capacity $C_{\text{sum}} := \max\{R_1 + R_2 : (R_1, R_2) \in \mathcal{C}\}$ is bounded by

$$0.3616 \leq C_{\text{sum}} \leq 0.3726$$

- The lower bound is achieved by the following *randomized time sharing* technique [19]

- We split message M_j , $j = 1, 2$, into two independent message M_{j0} and M_{jj}
- Codebook generation: Randomly and independently generate $2^{n(R_{10}+R_{20})}$ $u^n(m_{10}, m_{20})$ sequences, each i.i.d. $\text{Bern}(1/2)$. For each $u^n(m_{10}, m_{20})$, let $k(m_{10}, m_{20})$ be the number of locations where $u_i(m_{10}, m_{20}) = 1$. Randomly

and conditionally independently generate $2^{nR_{11}} x^{k(m_{10}, m_{20})}(m_{10}, m_{20}, m_{11})$ sequences, each i.i.d. $\text{Bern}(\alpha)$. Similarly, randomly and conditionally independently generate $2^{nR_{22}} x^{n-k(m_{10}, m_{20})}(m_{10}, m_{20}, m_{22})$ sequences, each i.i.d. $\text{Bern}(1 - \alpha)$

- Encoding: To send message pair (m_1, m_2) , represent it by the quadruple $(m_{10}, m_{20}, m_{11}, m_{22})$. Transmit $x^{k(m_{10}, m_{20})}(m_{10}, m_{20}, m_{11})$ in the locations where $u_i(m_{10}, m_{20}) = 1$ and $x^{n-k(m_{10}, m_{20})}(m_{10}, m_{20}, m_{22})$ in the locations where $u_i(m_{10}, m_{20}) = 0$. Thus the private messages are transmitted by time sharing with respect to $u^n(m_{10}, m_{20})$
- Decoding: Each decoder first decodes $u^n(m_{10}, m_{20})$ and then proceeds to decode its own private message from the output subsequence that corresponds to the respective symbol locations in $u^n(m_{10}, m_{20})$
- It is straightforward to show that a rate pair (R_1, R_2) is achievable using this scheme if

$$R_1 < \min\{I(U; Y_1), I(U; Y_2)\} + \frac{1}{2}I(X; Y_1|U = 1),$$

$$R_2 < \min\{I(U; Y_1), I(U; Y_2)\} + \frac{1}{2}I(X; Y_2|U = 0),$$

$$R_1 + R_2 < \min\{I(U; Y_1), I(U; Y_2)\} + \frac{1}{2}(I(X; Y_1|U = 1) + I(X; Y_2|U = 0))$$

for some $\alpha \in [0, 1]$. Taking the maximum of the sum-rate bound over α gives the sum-capacity lower bound of 0.3616

- By taking $U_0 \sim \text{Bern}(1/2)$, $U_1 \sim \text{Bern}(\alpha)$, $U_2 \sim \text{Bern}(\alpha)$, independent of each other, and $X = U_0 U_1 + (1 - U_0)(1 - U_2)$, Marton's inner bound (or Cover–van der Meulen inner bound with U_0) reduces to the above rate region. In fact, it can be shown [13, ?, 20] that the lower bound 0.3616 is the best achievable sum rate from Marton's inner bound
- The upper bound follows from the Nair–El Gamal outer bound. The sum-capacity is upper bounded by

$$\begin{aligned} C_{\text{sum}} &\leq \max_{p(u_1, u_2, x)} \min\{I(U_1; Y_1) + I(U_2; Y_2|U_1), I(U_2; Y_2) + I(U_1; Y_1|U_2)\} \\ &\leq \max_{p(u_1, u_2, x)} \frac{1}{2}(I(U_1; Y_1) + I(U_2; Y_2|U_1) + I(U_2; Y_2) + I(U_1; Y_1|U_2)) \end{aligned}$$

The latter maximum can be shown to be achieved by $X \sim \text{Bern}(1/2)$ and U_1, U_2 binary, which gives the upper bound of 0.3726

Inner Bound for More Than 2 Receivers

- The mutual covering lemma can be extended to more than two random variables. This leads to a natural extension of Marton's inner bound to more than 2 receivers
- The above inner bound can be improved via superposition coding, rate splitting, and the use of indirect decoding. We show through an example how to obtain an inner bound for any given prescribed message set requirement using these techniques

Multivariate Covering Lemma

- Lemma: Let $(U_1, \dots, U_k) \sim p(u_1, \dots, u_k)$ and $\epsilon > 0$. For each $j \in [1 : k]$, let $U_j^n(m_j), m_j \in [1 : 2^{nr_j}]$, be pairwise independent random sequences, each distributed according to $\prod_{i=1}^n p_{U_j}(u_{ji})$. Assume that $\{U_1^n(m_1) : m_1 \in [1 : 2^{nr_1}]\}, \{U_2^n(m_2) : m_2 \in [1 : 2^{nr_2}]\}, \dots, \{U_k^n(m_k) : m_k \in [1 : 2^{nr_k}]\}$ are mutually independent

Then, there exists $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$ such that

$P\{(U_1^n(m_1), U_2^n(m_2), \dots, U_k^n(m_k)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } (m_1, m_2, \dots, m_k)\} \rightarrow 0$
as $n \rightarrow \infty$, if $\sum_{j \in \mathcal{J}} r_j > \sum_{j \in \mathcal{J}} H(U_j) - H(U(\mathcal{J})) + \delta(\epsilon)$ for all $\mathcal{J} \subseteq [1 : k]$ with $|\mathcal{J}| \geq 2$

- The proof is a straightforward extension of the case $k = 2$ in the appendix
- For example, let $k = 3$, the conditions for covering become

$$r_1 + r_2 > I(U_1; U_2) + \delta(\epsilon),$$

$$r_1 + r_3 > I(U_1; U_3) + \delta(\epsilon),$$

$$r_2 + r_3 > I(U_2; U_3) + \delta(\epsilon),$$

$$r_1 + r_2 + r_3 > I(U_1; U_2) + I(U_1, U_2; U_3) + \delta(\epsilon)$$

Extended Marton's Inner Bound

- We illustrate the inner bound construction for $k = 3$ receivers
- Consider a 3-receiver DM-BC $(\mathcal{X}, p(y_1, y_2, y_3|x), \mathcal{Y}_1, \mathcal{Y}_2, \mathcal{Y}_3)$ with three private messages $M_j \in [1 : 2^{nR_j}]$ for $j = 1, 2, 3$
- A rate triple (R_1, R_2, R_3) is achievable for a 3-receiver DM-BC if

$$R_j < I(U_j; Y_j) \text{ for } j = 1, 2, 3,$$

$$R_1 + R_2 < I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2),$$

$$R_1 + R_3 < I(U_1; Y_1) + I(U_3; Y_3) - I(U_1; U_3),$$

$$R_2 + R_3 < I(U_2; Y_2) + I(U_3; Y_3) - I(U_2; U_3),$$

$$R_1 + R_2 + R_3 < I(U_1; Y_1) + I(U_2; Y_2) + I(U_3; Y_3) - I(U_1; U_2) - I(U_1, U_2; U_3)$$

for some $p(u_1, u_2, u_3)$ and function $x(u_1, u_2, u_3)$

- Achievability follows similar lines to the case of 2 receivers
- This extended bound is tight for deterministic DM-BC with k receivers, where we substitute $U_j = Y_j$ for $j \in [1 : k]$

Inner Bound for $k > 2$ Receivers

- An inner bound for general DM-BC with more than 2 receivers for any given messaging requirement can be constructed by combining rate splitting, superposition coding, indirect decoding, and Marton coding []
- We illustrate this using an example of 3-receivers with degraded message sets. Consider a 3-receiver DM-BC with 2-degraded message sets, where a common message $M_0 \in [1 : 2^{nR_0}]$ to be sent to receivers Y_1, Y_2 , and Y_3 , and a private message $M_1 \in [1 : 2^{nR_1}]$ to be sent only to receiver Y_1
- *Proposition [3]:* A rate pair (R_0, R_1) is achievable for a general 3-receiver DM-BC with 2-degraded message sets if

$$R_0 < \min\{I(V_2; Y_2), I(V_3; Y_3)\},$$

$$2R_0 < I(V_2; Y_2) + I(V_3; Y_3) - I(V_2; V_3|U),$$

$$R_0 + R_1 < \min\{I(X; Y_1), I(V_2; Y_2) + I(X; Y_1|V_2), I(V_3; Y_3) + I(X; Y_1|V_3)\},$$

$$2R_0 + R_1 < I(V_2; Y_2) + I(V_3; Y_3) + I(X; Y_1|V_2, V_3) - I(V_2; V_3|U),$$

$$2R_0 + 2R_1 < I(V_2; Y_2) + I(V_3; Y_3) + I(X; Y_1|V_2) + I(X; Y_1|V_3) - I(V_2; V_3|U),$$

$$2R_0 + 2R_1 < I(V_2; Y_2) + I(V_3; Y_3) + I(X; Y_1|U) + I(X; Y_1|V_2, V_3) - I(V_2; V_3|U),$$

for some $p(u, v_2, v_3, x) = p(u)p(v_2|u)p(x, v_3|v_2) = p(u)p(v_3|u)p(x, v_2|v_3)$, i.e., both $U \rightarrow V_2 \rightarrow (V_3, X)$ and $U \rightarrow V_3 \rightarrow (V_2, X)$ form Markov chains

- This region is tight for the class of multilevel DM-BC discussed earlier and when Y_1 is less noisy than Y_2 (which is a generalization of the class of multilevel DM-BC) (check)
- Proof of achievability: The general idea is to split M_1 into four independent messages, M_{10}, M_{11}, M_{12} , and M_{13} . The message pair (M_0, M_{10}) is represented by U . Using superposition coding and Marton coding, the message triple (M_0, M_{10}, M_{12}) is represented by V_2 and the message triple (M_0, M_{10}, M_{13}) is represented by V_3 . Finally using superposition coding, the message pair (M_0, M_1) is represented by X . Receiver Y_1 decodes U, V_2, V_3, X , receivers Y_2 and Y_3 find M_0 via indirect decoding of V_2 and V_3 , respectively

We now provide a more detailed outline of the proof

- Codebook generation: Let $R_1 = R_{10} + R_{11} + R_{12} + R_{13}$, where $R_{1j} \geq 0$, $j \in [1 : 3]$ and $\tilde{R}_2 \geq R_{12}$, $\tilde{R}_3 \geq R_{13}$. Fix a pmf of the required form $p(u, v_2, v_3, x) = p(u)p(v_2|u)p(x, v_3|v_2) = p(u)p(v_3|u)p(x, v_2|v_3)$
Randomly and independently generate $2^{n(R_0+R_{10})}$ sequences $u^n(m_0, m_{10})$, $m_0 \in [1 : 2^{nR_0}]$, $m_{10} \in [1 : 2^{n\tilde{R}_{10}}]$, each according to $\prod_{i=1}^n p_U(u_i)$

For each $u^n(m_0, m_{10})$ randomly and conditionally independently generate $2^{n\tilde{R}_2}$ sequences $v_2^n(m_0, m_{10}, l_2)$, $l_2 \in [1 : 2^{n\tilde{R}_2}]$, each according to $\prod_{i=1}^n p_{V_2|U}(v_{2i}|u_i)$, and $2^{n\tilde{R}_3}$ sequences $v_3^n(m_0, m_{10}, l_3)$, $l_3 \in [1 : 2^{n\tilde{R}_3}]$, each according to $\prod_{i=1}^n p_{V_3|U}(v_{3i}|u_i)$

Partition the set of $2^{n\tilde{R}_2}$ sequences $v_2^n(m_0, m_{10}, l_2)$ into equal-size subcodebooks $\mathcal{C}_2(m_{12})$, $m_{12} \in [1 : 2^{nR_{12}}]$, and the set of $2^{n\tilde{R}_3}$ $v_3^n(m_0, m_{10}, l_3)$ sequences into equal-size subcodebooks $\mathcal{C}_3(m_{13})$, $m_{13} \in [1 : 2^{nR_{13}}]$. By the mutual covering lemma, each product subcodebook $\mathcal{C}_2(m_{12}) \times \mathcal{C}_3(m_{13})$ contains a jointly typical pair $(v_2^n(m_0, m_{10}, l_2), v_3^n(m_0, m_{10}, l_3))$ with probability of error $\rightarrow 0$ as $n \rightarrow \infty$, if

$$R_{12} + R_{13} < \tilde{R}_2 + \tilde{R}_3 - I(V_2; V_3|U) - \delta(\epsilon)$$

Finally for each chosen jointly typical pair

$(v_2^n(m_0, m_{10}, l_2), v_3^n(m_0, m_{10}, l_3)) \in \mathcal{C}_2(m_{12}) \times \mathcal{C}_3(m_{13})$, randomly and conditionally independently generate $2^{nR_{11}}$ sequences $x^n(m_0, m_{10}, l_2, l_3, m_{11})$, $m_{11} \in [1 : 2^{nR_{11}}]$, each according to $\prod_{i=1}^n p_{X|V_2, V_3}(x_i|v_{2i}, v_{3i})$

- Encoding: To send the message pair (m_0, m_1) , we express m_1 by the quadruple $(m_{10}, m_{11}, m_{12}, m_{13})$. Let $(v_2^n(m_0, m_{10}, l_2), v_3^n(m_0, m_{10}, l_3))$ be the chosen pair of sequences in the product subcodebook $\mathcal{C}_2(m_{12}) \times \mathcal{C}_3(m_{13})$. Transmit codeword $x^n(m_0, m_{10}, l_2, l_3, m_{11})$

- Decoding and analysis of the probability of error:
 - Decoder 1 declares that $(\hat{m}_{01}, \hat{m}_{101}, \hat{m}_{12}, \hat{m}_{13}, \hat{m}_{11})$ is sent if it is the unique message tuple such that
 $(u^n(\hat{m}_{01}, \hat{m}_{101}), v_2^n(\hat{m}_{01}, \hat{m}_{101}, \hat{l}_2), v_3^n(\hat{m}_{01}, \hat{m}_{101}, \hat{l}_3), x^n(\hat{m}_{01}, \hat{m}_{101}, \hat{l}_2, \hat{l}_3, \hat{m}_{11}), y_1^n) \in \mathcal{T}_\epsilon^{(n)}$ for some $v_2^n(\hat{m}_{01}, \hat{m}_{101}, \hat{l}_2) \in \mathcal{C}_2(m_{12})$ and $v_3^n(\hat{m}_{01}, \hat{m}_{101}, \hat{l}_3) \in \mathcal{C}_3(m_{13})$. Assuming $(m_0, m_1, m_{10}, m_{11}) = (1, 1, 1, 1)$ is sent and (L_2, L_3) are the chosen indices for (m_{12}, m_{13}) , we divide the error event as follows:
 - Error event corresponding to $(m_0, m_{10}) \neq (1, 1)$. By the packing lemma, the probability of this event $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_0 + R_{10} + R_{11} + R_{12} + R_{13} < I(X; Y_1) - \delta(\epsilon)$$
 - Error event corresponding to $m_0 = 1, m_{10} = 1, l_2 \neq L_2, l_3 \neq L_3$. By the packing lemma, the probability of this event $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_{11} + R_{12} + R_{13} < I(X; Y_1|U) - \delta(\epsilon)$$
 - Error event corresponding to $m_0 = 1, m_{10} = 1, l_2 = L_2, l_3 \neq L_3$ for some l_3 not in subcodebook $\mathcal{C}_3(m_{13})$. By the packing lemma, the probability of this event $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_{11} + R_{13} < I(X; Y_1|U, V_2) - \delta(\epsilon) = I(X; Y_1|V_2) - \delta(\epsilon),$$
 where the equality follows since $U \rightarrow V_2 \rightarrow (V_3, X)$ form a Markov chain

- 4. Error event corresponding to $m_0 = 1, m_{10} = 1, l_2 \neq L_2, l_3 = L_3$ for some l_2 not in subcodebook $\mathcal{C}_2(m_{12})$. By the packing lemma, the probability of this event $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_{11} + R_{12} < I(X; Y_1|U, V_3) - \delta(\epsilon) = I(X; Y_1|V_3) - \delta(\epsilon)$$
- 5. Error event corresponding to $m_0 = 1, m_{10} = 1, l_2 = L_2, l_3 = L_3, m_{11} \neq 1$. By the packing lemma, the probability of this event $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_{11} < I(X; Y_1|U, V_2, V_3) - \delta(\epsilon) = I(X; Y_1|V_2, V_3) - \delta(\epsilon),$$
 where equality uses the weaker Markov structure $U \rightarrow (V_2, V_3) \rightarrow X$
- Decoder 2 decodes m_0 via indirect decoding through v_2^n . It declares that the pair $(\hat{m}_{02}, \hat{m}_{102})$ is sent if it is the unique pair such that
 $(u^n(\hat{m}_{02}, \hat{m}_{102}), v_2^n(\hat{m}_{02}, \hat{m}_{102}, l_2), y_2^n) \in \mathcal{T}_\epsilon^{(n)}$ for some l_2 . By the packing lemma, the probability of this event $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_0 + R_{10} + \tilde{R}_2 < I(V_2; Y_2) - \delta(\epsilon)$$
- Similarly, decoder 3 finds m_0 via indirect decoding through v_3^n . By the packing lemma, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R_0 + R_{10} + \tilde{R}_3 < I(V_3; Y_3) - \delta(\epsilon)$$
- Combining the above conditions and using the Fourier–Motzkin procedure completes the proof of achievability

Key New Ideas and Techniques

- Indirect decoding
- Marton coding technique
- Mutual covering lemma
- Open problems:
 - What is the capacity region of the general 3-receiver DM-BC with degraded message sets (one common message for all three receivers and one private message for one receiver)?
 - Is Marton's inner bound tight in general?
 - Is the Nair–El Gamal outer bound tight in general?
 - What is the sum-capacity of the binary skew-symmetric broadcast channel?

References

- [1] J. Körner and K. Marton, "General broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 60–64, 1977.
- [2] S. Borade, L. Zheng, and M. Trott, "Multilevel broadcast networks," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 1151–1155.
- [3] C. Nair and A. El Gamal, "The capacity region of a class of three-receiver broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.
- [4] T. M. Cover, "An achievable rate region for the broadcast channel," *IEEE Trans. Inf. Theory*, vol. 21, pp. 399–404, 1975.
- [5] E. C. van der Meulen, "Random coding theorems for the general discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 21, pp. 180–190, 1975.
- [6] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 3, pp. 306–311, 1979.
- [7] A. El Gamal and E. C. van der Meulen, "A proof of Marton's coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 27, no. 1, pp. 120–122, Jan. 1981.
- [8] S. I. Gelfand and M. S. Pinsker, "Capacity of a broadcast channel with one deterministic component," *Probl. Inf. Transm.*, vol. 16, no. 1, pp. 24–34, 1980.
- [9] E. C. van der Meulen, "A survey of multi-way channels in information theory: 1961–1976," *IEEE Trans. Inf. Theory*, vol. 23, no. 1, pp. 1–37, 1977.

- [10] S. I. Gelfand, "Capacity of one broadcast channel," *Probl. Inf. Transm.*, vol. 13, no. 3, pp. 106–108, 1977.
- [11] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sept. 2006.
- [12] M. Mohseni and J. M. Cioffi, "A proof of the converse for the capacity of Gaussian MIMO broadcast channels," 2006, submitted to *IEEE Trans. Inf. Theory*, 2006.
- [13] A. A. Gohari and V. Anantharam, "Evaluation of Marton's inner bound for the general broadcast channel," 2009, submitted to *IEEE Trans. Inf. Theory*, 2009.
- [14] Y. Liang, G. Kramer, and H. V. Poor, "Equivalence of two inner bounds on the capacity region of the broadcast channel," in *Proc. 46th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, Sept. 2008.
- [15] C. Nair and A. El Gamal, "An outer bound to the capacity region of the broadcast channel," *IEEE Trans. Inf. Theory*, vol. 53, no. 1, pp. 350–355, Jan. 2007.
- [16] C. Nair, "Capacity regions of two new classes of 2-receiver broadcast channels," 2009. [Online]. Available: <http://arxiv.org/abs/0901.0595>
- [17] Y. Liang, G. Kramer, and S. Shamai, "Capacity outer bounds for broadcast channels," in *Proc. Information Theory Workshop*, Porto, Portugal, May 2008, pp. 2–4.
- [18] A. A. Gohari and V. Anantharam, "An outer bound to the admissible source region of broadcast channels with arbitrarily correlated sources and channel variations," in *Proc. 46th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, Sept. 2008.

- [19] B. E. Hajek and M. B. Pursley, "Evaluation of an achievable rate region for the broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 1, pp. 36–46, 1979.
- [20] V. Jog and C. Nair, "An information inequality for the BSSC channel," 2009. [Online]. Available: <http://arxiv.org/abs/0901.1492>

Appendix: Proof of Mutual Covering Lemma

- Let

$\mathcal{A} = \{(m_1, m_2) \in [1 : 2^{nr_1}] \times [1 : 2^{nr_2}] : (U_1^n(m_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}(U_1, U_2)\}$.
Then the probability of the event of interest can be bounded as

$$\begin{aligned}\mathbb{P}\{|\mathcal{A}| = 0\} &\leq \mathbb{P}\{(|\mathcal{A}| - \mathbb{E}|\mathcal{A}|)^2 \geq (\mathbb{E}|\mathcal{A}|)^2\} \\ &\leq \frac{\text{Var}(|\mathcal{A}|)}{(\mathbb{E}|\mathcal{A}|)^2}\end{aligned}$$

by Chebychev's inequality

- We now show that $\text{Var}(|\mathcal{A}|)/(\mathbb{E}|\mathcal{A}|)^2 \rightarrow 0$ as $n \rightarrow \infty$ if

$$r_1 > 3\delta(\epsilon),$$

$$r_2 > 3\delta(\epsilon),$$

$$r_1 + r_2 > I(U_1; U_2) + \delta(\epsilon)$$

Using indicator random variables, we can express $|\mathcal{A}|$ as

$$|\mathcal{A}| = \sum_{m_1=1}^{2^{nr_1}} \sum_{m_2=1}^{2^{nr_2}} E(m_1, m_2),$$

where

$$E(m_1, m_2) := \begin{cases} 1 & \text{if } (U_1^n(m_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}, \\ 0 & \text{otherwise} \end{cases}$$

for each $(m_1, m_2) \in [1 : 2^{nr_1}] \times [1 : 2^{nr_2}]$

Let

$$\begin{aligned}p_1 &:= \mathbb{P}\{(U_1^n(1), U_2^n(1)) \in \mathcal{T}_\epsilon^{(n)}\}, \\ p_2 &:= \mathbb{P}\{(U_1^n(1), U_2^n(1)) \in \mathcal{T}_\epsilon^{(n)}, (U_1^n(1), U_2^n(2)) \in \mathcal{T}_\epsilon^{(n)}\}, \\ p_3 &:= \mathbb{P}\{(U_1^n(1), U_2^n(1)) \in \mathcal{T}_\epsilon^{(n)}, (U_1^n(2), U_2^n(1)) \in \mathcal{T}_\epsilon^{(n)}\}, \\ p_4 &:= \mathbb{P}\{(U_1^n(1), U_2^n(1)) \in \mathcal{T}_\epsilon^{(n)}, (U_1^n(2), U_2^n(2)) \in \mathcal{T}_\epsilon^{(n)}\} = p_1^2\end{aligned}$$

Then

$$\mathbb{E}(|\mathcal{A}|) = \sum_{m_1, m_2} \mathbb{P}\{(U_1^n(m_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}\} = 2^{n(r_1+r_2)} p_1$$

and

$$\begin{aligned}
& \mathbb{E}(|\mathcal{A}|^2) \\
&= \sum_{m_1, m_2} \mathsf{P}\{(U_1^n(m_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}\} \\
&\quad + \sum_{m_1, m_2} \sum_{m'_2 \neq m_2} \mathsf{P}\{(U_1^n(m_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}, (U_1^n(m_1), U_2^n(m'_2)) \in \mathcal{T}_\epsilon^{(n)}\} \\
&\quad + \sum_{m_1, m_2} \sum_{m'_1 \neq m_1} \mathsf{P}\{(U_1^n(m_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}, (U_1^n(m'_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}\} \\
&\quad + \sum_{m_1, m_2} \sum_{m'_1 \neq m_1} \sum_{m'_2 \neq m_2} \mathsf{P}\{(U_1^n(m_1), U_2^n(m_2)) \in \mathcal{T}_\epsilon^{(n)}, (U_1^n(m'_1), U_2^n(m'_2)) \in \mathcal{T}_\epsilon^{(n)}\} \\
&\leq 2^{n(r_1+r_2)} p_1 + 2^{n(r_1+2r_2)} p_2 + 2^{n(2r_1+r_2)} p_3 + 2^{2n(r_1+r_2)} p_4
\end{aligned}$$

Hence

$$\text{Var}(|\mathcal{A}|) \leq 2^{n(r_1+r_2)} p_1 + 2^{n(r_1+2r_2)} p_2 + 2^{n(2r_1+r_2)} p_3$$

Now by the joint typicality lemma, we have

$$\begin{aligned}
p_1 &\geq 2^{-n(I(U_1; U_2) + \delta(\epsilon))}, \\
p_2 &\leq 2^{-n(2I(U_1; U_2) - \delta(\epsilon))}, \\
p_3 &\leq 2^{-n(2I(U_1; U_2) - \delta(\epsilon))},
\end{aligned}$$

hence

$$p_2/p_1^2 \leq 2^{3n\delta(\epsilon)}, \quad p_3/p_1^2 \leq 2^{3n\delta(\epsilon)}$$

Therefore,

$$\frac{\text{Var}(|\mathcal{A}|)}{(\mathbb{E}|\mathcal{A}|)^2} \leq 2^{-n(r_1+r_2-I(U_1; U_2)-\delta(\epsilon))} + 2^{-n(r_1-3\delta(\epsilon))} + 2^{-n(r_2-3\delta(\epsilon))},$$

which $\rightarrow 0$ as $n \rightarrow \infty$, provided that

$$r_1 > 3\delta(\epsilon),$$

$$r_2 > 3\delta(\epsilon),$$

$$r_1 + r_2 > I(U_1; U_2) + \delta(\epsilon)$$

- Similarly, $\mathsf{P}\{|\mathcal{A}| = 0\} \rightarrow 0$ as $n \rightarrow 0$ if $r_1 = 0$ and $r_2 > I(U_1; U_2) + \delta(\epsilon)$, or if $r_1 > I(U_1; U_2) + \delta(\epsilon)$ and $r_2 = 0$
- Combining three sets of inequalities, we have shown that $\mathsf{P}\{|\mathcal{A}| = 0\} \rightarrow 0$ as $n \rightarrow \infty$ if $r_1 + r_2 > I(U_1; U_2) + 4\delta(\epsilon)$

Appendix: Proof of Nair–El Gamal Outer Bound

- By Fano's inequality and following standard steps, we have

$$\begin{aligned}
 nR_0 &\leq \min\{I(M_0; Y_1^n), I(M_0; Y_2^n)\} + n\epsilon, \\
 n(R_0 + R_1) &\leq I(M_0, M_1; Y_1^n) + n\epsilon, \\
 n(R_0 + R_2) &\leq I(M_0, M_2; Y_2^n) + n\epsilon, \\
 n(R_0 + R_1 + R_2) &\leq I(M_0, M_1; Y_1^n) + I(M_2; Y_2^n | M_0, M_1) + n\epsilon, \\
 n(R_0 + R_1 + R_2) &\leq I(M_1; Y_1^n | M_0, M_2) + I(M_0, M_2; Y_2^n) + n\epsilon
 \end{aligned}$$

We bound the mutual information terms in the above bounds

- First consider the terms in the fourth inequality

$$\begin{aligned}
 I(M_0, M_1; Y_1^n) + I(M_2; Y_2^n | M_0, M_1) &= \sum_{i=1}^n I(M_0, M_1; Y_{1i} | Y_1^{i-1}) \\
 &\quad + \sum_{i=1}^n I(M_2; Y_{2i} | M_0, M_1, Y_{2,i+1}^n)
 \end{aligned}$$

- Now, consider

$$\begin{aligned}
 \sum_{i=1}^n I(M_0, M_1; Y_{1i} | Y_1^{i-1}) &\leq \sum_{i=1}^n I(M_0, M_1, Y_1^{i-1}; Y_{1i}) \\
 &= \sum_{i=1}^n I(M_0, M_1, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1i}) \\
 &\quad - \sum_{i=1}^n I(Y_{2,i+1}^n; Y_{1i} | M_0, M_1, Y_1^{i-1})
 \end{aligned}$$

- Also,

$$\begin{aligned}
 \sum_{i=1}^n I(M_2; Y_{2i} | M_0, M_1, Y_{2,i+1}^n) &\leq \sum_{i=1}^n I(M_2, Y_1^{i-1}; Y_{2i} | M_0, M_1, Y_{2,i+1}^n) \\
 &= \sum_{i=1}^n I(Y_1^{i-1}; Y_{2i} | M_0, M_1, Y_{2,i+1}^n) \\
 &\quad + \sum_{i=1}^n I(M_2; Y_{2i} | M_0, M_1, Y_{2,i+1}^n, Y_1^{i-1})
 \end{aligned}$$

- Combining the above results, and defining $U_{0i} := (M_0, Y_1^{i-1}, Y_{2,i+1}^n)$,

$U_{1i} := M_1$, and $U_{2i} := M_2$, we obtain

$$\begin{aligned}
& I(M_0, M_1; Y_1^n) + I(M_2; Y_2^n | M_0, M_1) \\
& \leq \sum_{i=1}^n I(M_0, M_1, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1i}) - \sum_{i=1}^n I(Y_{2,i+1}^n; Y_{1i} | M_0, M_1, Y_1^{i-1}) \\
& \quad + \sum_{i=1}^n I(Y_1^{i-1}; Y_{2i} | M_0, M_1, Y_{2,i+1}^n) + \sum_{i=1}^n I(M_2; Y_{2i} | M_0, M_1, Y_{2,i+1}^n, Y_1^{i-1}) \\
& \stackrel{(a)}{=} \sum_{i=1}^n I(M_0, M_1, Y_1^{i-1}, Y_{2,i+1}^n; Y_{1i}) + \sum_{i=1}^n I(M_2; Y_{2i} | M_0, M_1, Y_{2,i+1}^n, Y_1^{i-1}) \\
& = \sum_{i=1}^n I(U_{0i}, U_{1i}; Y_{1i}) + \sum_{i=1}^n I(U_{2i}; Y_{2i} | U_{0i}, U_{1i})
\end{aligned}$$

The equality (a) follows from the Csiszár sum identity

- We can similarly show that

$$I(M_1; Y_1^n | M_0, M_2) + I(M_0, M_2; Y_2^n) \leq \sum_{i=1}^n I(U_{1i}; Y_{1i} | U_{0i}, U_{2i}) + \sum_{i=1}^n I(U_{0i}, U_{2i}; Y_{2i})$$

- Now, it easy to show that

$$\begin{aligned}
\min\{I(M_0; Y_1^n), I(M_0; Y_2^n)\} & \leq \left\{ \sum_{i=1}^n I(U_{0i}; Y_{1i}), \sum_{i=1}^n I(U_{0i}; Y_{2i}) \right\} \\
I(M_0, M_1; Y_1^n) & \leq \sum_{i=1}^n I(U_{0i}, U_{1i}; Y_{1i}) \\
I(M_0, M_2; Y_2^n) & \leq \sum_{i=1}^n I(U_{0i}, U_{2i}; Y_{2i})
\end{aligned}$$

The rest of the proof follows by introducing a time-sharing random variable Q independent of $M_0, M_1, M_2, X^n, Y_1^n, Y_2^n$, and uniformly distributed over $[1 : n]$, and defining

$$U_0 = (Q, U_{0Q}), U_1 = U_{1Q}, U_2 = V_{2Q}, X = X_Q, Y_1 = Y_{1Q}, Y_2 = Y_{2Q}$$

- Showing that a function $x(u_0, u_1, u_2)$ suffices, we use similar arguments to the proof of the converse for the Gelfand–Pinsker theorem
- Note that the independence of the messages M_1 and M_2 implies the independence of the auxiliary random variables U_1 and U_2 as specified

Lecture Notes 10

Gaussian Vector Channels

- Gaussian Vector Channels
- Gaussian Vector Fading Channels
- Gaussian Vector Multiple Access Channels
- Spectral Gaussian Broadcast Channels
- Vector Writing on Dirty Paper
- Gaussian Vector Broadcast Channels
- Key New Ideas and Techniques
- Appendix: Proof of the BC-MAC Duality
- Appendix: Uniqueness of the Supporting Hyperplane

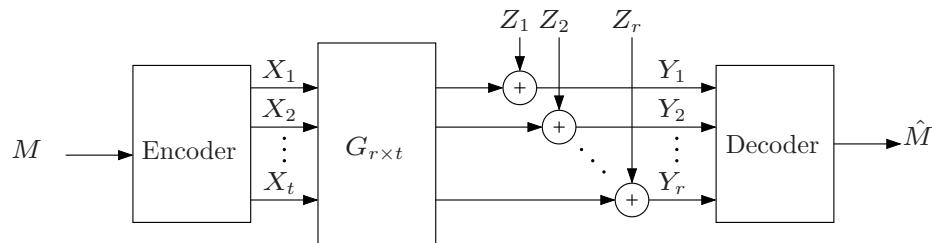
© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Gaussian Vector Channels

- The Gaussian vector channel is a model for a multi-antenna (multiple-input multiple-output/MIMO) wireless communication channel
- Consider the discrete-time Gaussian vector channel

$$\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{Z}(i),$$

where the channel output $\mathbf{Y}(i)$ is an r -vector, the channel input $\mathbf{X}(i)$ is a t -vector, $\{\mathbf{Z}(i)\}$ is an r -dimensional vector WGN(K_Z) process with $K_Z > 0$, and G is an $r \times t$ constant channel gain matrix with the element G_{jk} representing the gain of the channel from the transmitter antenna j to the receiver antenna k



- Remark: Note that we can assume without loss of generality that $K_{\mathbf{Z}} = I_r$, i.e., $\{\mathbf{Z}(i)\}$ is an r -dimensional vector WGN(I_r) process. Indeed, the channel $\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{Z}(i)$ with a general $K_{\mathbf{Z}} \succ 0$ can be transformed into the channel

$$\tilde{\mathbf{Y}}(i) = K_{\mathbf{Z}}^{-1/2}\mathbf{Y}(i) = K_{\mathbf{Z}}^{-1/2}G\mathbf{X}(i) + \tilde{\mathbf{Z}}(i),$$

where $\tilde{\mathbf{Z}}(i) = K_{\mathbf{Z}}^{-1/2}\mathbf{Z}(i) \sim \mathcal{N}(\mathbf{0}, I_r)$, and vice versa

- Average power constraint: For every codeword $\mathbf{x}^n(m) = (\mathbf{x}(m, 1), \dots, \mathbf{x}(m, n))$

$$\sum_{i=1}^n \mathbf{x}^T(m, i)\mathbf{x}(m, i) \leq nP$$

- Note that the vector channel reduces to the Gaussian product channel (cf. Lecture Notes 3) when $r = t = d$ and $G = \text{diag}(g_1, g_2, \dots, g_d)$
- *Theorem 1:* The capacity of the Gaussian vector channel is

$$C = \max_{K_{\mathbf{X}} \succeq 0: \text{tr}(K_{\mathbf{X}}) \leq P} \frac{1}{2} \log |GK_{\mathbf{X}}G^T + I_r|$$

This can be easily shown by considering

$$\begin{aligned} C &\leq \max_{F(\mathbf{x}): E(\mathbf{x}^T \mathbf{x}) \leq P} I(\mathbf{X}; \mathbf{Y}) = \max_{F(\mathbf{x}): E(\mathbf{x}^T \mathbf{x}) \leq P} h(\mathbf{Y}) - h(\mathbf{Z}) \\ &= \max_{K_{\mathbf{X}} \succeq 0: \text{tr}(K_{\mathbf{X}}) \leq P} \frac{1}{2} \log |GK_{\mathbf{X}}G^T + I_r|, \end{aligned}$$

where the last equality follows since the output differential entropy is maximized by some Gaussian input \mathbf{X} with zero mean and covariance matrix $K_{\mathbf{X}}$

Achievability is proved using a similar procedure to extending the achievability proof for the DMC with input cost to the AWGN channel

- Suppose G has rank d and singular value decomposition $G = \Phi\Gamma\Psi^T$ with $\Gamma = \text{diag}(\gamma_1, \gamma_2, \dots, \gamma_d)$. Then

$$\begin{aligned} C &= \max_{\text{tr}(K_{\mathbf{X}}) \leq P} \frac{1}{2} \log \frac{|GK_{\mathbf{X}}G^T + I_r|}{|I_r|} \\ &= \max_{\text{tr}(K_{\mathbf{X}}) \leq P} \frac{1}{2} \log |I_r + GK_{\mathbf{X}}G^T| \\ &= \max_{\text{tr}(K_{\mathbf{X}}) \leq P} \frac{1}{2} \log |I_r + \Phi\Gamma\Psi^T K_{\mathbf{X}} \Psi\Gamma\Phi^T| \\ &\stackrel{(a)}{=} \max_{\text{tr}(K_{\mathbf{X}}) \leq P} \frac{1}{2} \log_2 |I_d + \Phi^T \Phi\Gamma\Psi^T K_{\mathbf{X}} \Psi\Gamma| \\ &\stackrel{(b)}{=} \max_{\text{tr}(K_{\mathbf{X}}) \leq P} \frac{1}{2} \log_2 |I_d + \Gamma\Psi^T K_{\mathbf{X}} \Psi\Gamma| \\ &\stackrel{(c)}{=} \max_{\text{tr}(\tilde{K}_{\mathbf{X}}) \leq P} \frac{1}{2} \log_2 |I_d + \Gamma\tilde{K}_{\mathbf{X}}\Gamma|, \end{aligned}$$

where (a) follows from the fact that if $A = \Phi\Gamma\Psi^T K_X \Psi\Gamma$ and $B = \Phi^T$, then $|I_r + AB| = |I_d + BA|$ and (b) follows since $\Phi^T\Phi = I_d$ (recall the definition of singular value decomposition in Lecture Notes 1), and (c) follows since the two maximization problems can be shown to be equivalent via the transformations $\tilde{K}_X = \Psi^T K_X \Psi$ and $K_X = \Psi \tilde{K}_X \Psi^T$

By Hadamard's inequality, the optimal \tilde{K}_X^* is a diagonal matrix $\text{diag}(P_1, P_2, \dots, P_d)$ such that the water-filling condition is satisfied:

$$P_j = \left(\lambda - \frac{1}{\gamma_i^2} \right)^+,$$

where λ is chosen such that $\sum_{j=1}^d P_j = P$

Finally, from the transformation between K_X and \tilde{K}_X , the optimal K_X^* is given by $K_X^* = \Psi \tilde{K}_X^* \Psi^T$. Thus the transmitter should align its signal *direction* with the singular vectors of the effective channel and allocate an appropriate amount of power in each direction to *water-fill* the singular values

Equivalent Gaussian Product Channel

- The role of singular values for Gaussian vector channels can be seen more directly as follows
- Let $\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{Z}(i)$ and suppose $G = \Phi\Gamma\Psi^T$ has rank d . We show that this channel is *equivalent* to the Gaussian product channel

$$\tilde{Y}_{ji} = \gamma_j \tilde{X}_{ji} + \tilde{Z}_{ji}, \quad j \in [1 : d]$$

where $\{\tilde{Z}_{ji}\}$ are i.i.d. WGN(1) processes

- First consider the channel $\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{Z}(i)$ with the input transformation $\mathbf{X}(i) = \Psi \tilde{\mathbf{X}}(i)$ and the output transformation $\tilde{\mathbf{Y}}(i) = \Phi^T \mathbf{Y}(i)$. This gives the new channel

$$\begin{aligned} \tilde{\mathbf{Y}}(i) &= \Phi^T G \mathbf{X}(i) + \Phi^T \mathbf{Z}(i) \\ &= \Phi^T (\Phi\Gamma\Psi^T) \Psi \tilde{\mathbf{X}}(i) + \Phi^T \mathbf{Z}(i) \\ &= \Gamma \tilde{\mathbf{X}}(i) + \tilde{\mathbf{Z}}(i), \end{aligned}$$

where the new d -dimensional vector WGN process $\tilde{\mathbf{Z}}(i) := \Phi^T \mathbf{Z}(i)$ has the covariance matrix $\Phi^T \Phi = I_d$

Let $\tilde{K}_X := E(\tilde{\mathbf{X}}\tilde{\mathbf{X}}^T)$ and $K_X := E(\mathbf{X}\mathbf{X}^T)$. Then

$$\text{tr}(K_X) = \text{tr}(\Psi\tilde{K}_X\Psi^T) = \text{tr}(\Psi^T\Psi\tilde{K}_X) = \text{tr}(\tilde{K}_X)$$

Hence a code for the Gaussian product channel $\tilde{\mathbf{Y}}(i) = \Gamma\tilde{\mathbf{X}}(i) + \tilde{\mathbf{Z}}(i)$ can be transformed into a code for the Gaussian vector channel $\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{Z}(i)$ without violating the power constraint

- Conversely, given the channel $\tilde{\mathbf{Y}}(i) = \Gamma\tilde{\mathbf{X}}(i) + \tilde{\mathbf{Z}}(i)$, we can perform the input transformation $\tilde{\mathbf{X}}(i) = \Psi^T\mathbf{X}(i)$ and the output transformation $\mathbf{Y}'(i) = \Phi\tilde{\mathbf{Y}}(i)$ to obtain

$$\begin{aligned}\mathbf{Y}'(i) &= \Phi\Gamma\Psi^T\mathbf{X}(i) + \Phi\tilde{\mathbf{Z}}(i) \\ &= G\mathbf{X}(i) + \Phi\tilde{\mathbf{Z}}(i)\end{aligned}$$

Since $\Phi\Phi^T \preceq I_r$ (why?), we can further add to $\mathbf{Y}'(i)$ an independent r -dimensional vector WGN($I_r - \Phi\Phi^T$) process $\mathbf{Z}'(i)$. This gives

$$\mathbf{Y}(i) = \mathbf{Y}'(i) + \mathbf{Z}'(i) = G\mathbf{X}(i) + \Phi\tilde{\mathbf{Z}}(i) + \mathbf{Z}'(i) = G\mathbf{X}(i) + \mathbf{Z}(i),$$

where $\mathbf{Z}(i) := \Phi\tilde{\mathbf{Z}}(i) + \mathbf{Z}'(i)$ has the covariance matrix $\Phi\Phi^T + (I_r - \Phi\Phi^T) = I_r$

Also, since $\Psi\Psi^T \preceq I_t$, $\text{tr}(\tilde{K}_X) = \text{tr}(\Psi^T K_X \Psi) = \text{tr}(\Psi\Psi^T K_X) \leq \text{tr}(K_X)$

Hence a code for the Gaussian vector channel $\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{Z}(i)$ can be transformed into a code for the Gaussian product channel $\tilde{\mathbf{Y}}(i) = \Gamma\tilde{\mathbf{X}}(i) + \tilde{\mathbf{Z}}(i)$ without violating the power constraint

- Note that the above equivalence implies that the minimum probabilities of error for both channels are the same. Hence both channels have the same capacity

Reciprocity

- Since the channel gain matrices G and G^T have the same set of (nonzero) singular values, the channels corresponding to G and G^T have the same capacity
In fact, these two channels are equivalent to the same Gaussian product channel, and hence are equivalent to each other
The following result is an immediate consequence of this equivalence, and will be useful later in proving the MAC–BC duality
- *Reciprocity Lemma:* For any $r \times t$ channel matrix G and any $t \times t$ matrix $K \succeq 0$, there exists an $r \times r$ matrix $\bar{K} \succeq 0$ such that

$$\mathrm{tr}(\bar{K}) \leq \mathrm{tr}(K)$$

and

$$|G^T \bar{K} G + I_t| = |G K G^T + I_r|$$

To show this, given a singular value decomposition $G = \Phi \Gamma \Psi^T$, we take $\bar{K} = \Phi \Psi^T K \Psi \Phi^T$ and check that \bar{K} satisfies both properties

Indeed, since $\Psi \Psi^T \preceq I_t$,

$$\mathrm{tr}(\bar{K}) = \mathrm{tr}(\Phi^T \Psi \Psi^T K \Phi) = \mathrm{tr}(\Psi \Psi^T K) \leq \mathrm{tr}(K)$$

To check the second property, let $d = \mathrm{rank}(G)$ and consider

$$\begin{aligned} |G^T \bar{K} G + I_t| &= |\Psi \Gamma \Phi^T (\Phi \Psi^T K \Psi \Phi^T) \Phi \Gamma \Psi^T + I_t| \\ &\stackrel{(a)}{=} |(\Psi^T \Psi) \Gamma \Psi^T K \Psi \Gamma + I_d| \\ &= |\Gamma \Psi^T K \Psi \Gamma + I_d| \\ &= |(\Phi^T \Phi) \Gamma \Psi^T K \Psi \Gamma + I_d| \\ &\stackrel{(b)}{=} |\Phi \Gamma \Psi^T K \Psi \Gamma \Phi^T + I_r| \\ &= |G K G^T + I_r|, \end{aligned}$$

where (a) follows from the fact that if $A = \Psi \Gamma \Psi^T K \Psi \Gamma$ and $B = \Psi^T$, then $|AB + I| = |BA + I|$, and (b) follows similarly (check!)

Alternative Characterization of K_X^*

- Consider the Gaussian vector channel $\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{Z}(i)$, where $\mathbf{Z}(i)$ has a general covariance matrix $K_Z \succ 0$. We have already characterized the optimal input covariance matrix K_X^* for the effective channel gain matrix $K_Z^{-1/2}G$ via singular value decomposition and water-filling
- Here we give an alternative characterization via Lagrange duality

First note that the optimal input covariance matrix K_X^* is the solution to the following convex optimization problem:

$$\begin{aligned} & \text{maximize} && \frac{1}{2} \log |GK_X G^T + K_Z| \\ & \text{subject to} && K_X \succeq 0 \\ & && \text{tr}(K_X) \leq P \end{aligned}$$

- Recall that if a convex optimization problem satisfies *Slater's condition* (i.e., the feasible region has an interior point), then the *KKT condition* provides necessary and sufficient condition for the optimal solution [1] (see Appendix E). Here Slater's condition is satisfied for any $P > 0$

- With dual variables

$$\text{tr}(K_X) \leq P \Leftrightarrow \lambda \geq 0,$$

$$K_X \succeq 0 \Leftrightarrow \Upsilon \succeq 0,$$

we can form the Lagrangian

$$L(K_X, \Upsilon, \lambda) = \frac{1}{2} \log |GK_X G^T + K_Z| + \text{tr}(\Upsilon K_X) - \lambda(\text{tr}(K_X) - P)$$

- A solution K_X^* is primal optimal iff there exists a dual optimal solution $\lambda^* > 0$ and $\Upsilon^* \succeq 0$ that satisfies the KKT condition:

- the Lagrangian is stationary (zero differentials with respect to K_X):

$$\frac{1}{2} G^T (GK_X^* G^T + K_Z)^{-1} G + \Upsilon^* - \lambda^* I_r = 0$$

- the complementary slackness conditions are satisfied:

$$\lambda^* (\text{tr}(K_X^*) - P) = 0, \quad \text{tr}(\Upsilon^* K_X^*) = 0$$

- In particular, fixing $\Upsilon^* = 0$, any solution K_X^* with $\text{tr}(K_X^*) = P$ is optimal if

$$\frac{1}{2} G^T (GK_X^* G^T + K_Z)^{-1} G = \lambda^* I_r$$

for some $\lambda^* > 0$. Such a covariance matrix K_X^* corresponds to water-filling with all subchannels under water (which happens at sufficiently high SNR)

Gaussian Vector Fading Channels

- A Gaussian vector channel with fading is defined as follows: At time i , $\mathbf{Y}(i) = G(i)\mathbf{X}(i) + \mathbf{Z}(i)$, where the noise $\{\mathbf{Z}(i)\}$ is an r -dimensional vector WGN(I_r) process and the channel gain matrix $G(i)$ is a *random* matrix that models random multipath fading. The matrix elements $\{G_{jk}(i)\}$, $j \in [1 : t]$, $k \in [1 : r]$, are assumed to be independent random processes
Two important special cases:
 - Slow fading: $G_{jk}(i) = G_{jk}$ for $i \in [1 : n]$, i.e., the channel gains do not change over the transmission block
 - Fast fading: $G_{jk}(i)$ are i.i.d. over the time index i
- In rich scattering environments, Rayleigh fading is assumed, i.e., $G_{jk}(i) \sim N(0, 1)$
- In the framework of channels with state, the fast fading matrix G represents the channel state. As such one can investigate various channel state information scenarios—state is known to both the encoder and decoder, state known only to the decoder—and various coding approaches—compound channel, outage capacity, superposition coding, adaptive coding, coding over blocks (cf. Lecture Notes 8)

Gain Matrix Known at the Decoder

- Consider the case of fast fading, where the sequence of fading matrices $G(1), G(2), \dots, G(n)$ is independently distributed according to the same joint pdf f_G , and is available only at the decoder
- The (ergodic) capacity in this case (see Lecture Notes 7) is

$$C = \max_{F(\mathbf{x}): E(\mathbf{x}^T \mathbf{x}) \leq P} I(\mathbf{X}; \mathbf{Y}|G)$$

- It is not difficult to show that a Gaussian input pdf achieves the capacity. Thus

$$C = \max_{\text{tr}(K_X) \leq P} E_G \left[\frac{1}{2} \log |I_r + GK_XG^T| \right]$$

- The maximization can be further simplified if G is isotropic, i.e., the joint pdf of matrix elements G_{jk} is invariant under orthogonal transformations

Theorem 2: [2]: If the channel gain matrix G is isotropic, then the capacity is

$$C = E \left[\frac{1}{2} \log \left| I_r + \frac{P}{t} GG^T \right| \right] = \frac{1}{2} \sum_{j=1}^{\min(t,r)} E \left[\log \left(1 + \frac{P}{t} \Lambda_j \right) \right],$$

where Λ_j are (random) eigenvalues of GG^T , and is achieved by $K_X^* = (P/t)I_t$

- At small P (low SNR), assuming Rayleigh fading with $E(|G_{jk}|^2) = 1$

$$\begin{aligned}
C &= \frac{1}{2} \sum_{j=1}^{\min(t,r)} E \left[\log \left(1 + \frac{P}{t} \Lambda_j \right) \right] \approx \frac{P}{2t \log 2} \sum_{j=1}^{\min(t,r)} E(\Lambda_j) \\
&= \frac{P}{2t \log 2} E[\text{tr}(GG^T)] \\
&= \frac{P}{2t \log 2} E \left[\sum_{j,k} |G_{jk}|^2 \right] = \frac{rP}{2 \log 2}
\end{aligned}$$

This is an r -fold SNR gain compared to the single antenna case

- At large P (high SNR),

$$\begin{aligned}
C &= \frac{1}{2} \sum_{j=1}^{\min(t,r)} E \left[\log \left(1 + \frac{P}{t} \Lambda_j \right) \right] \approx \frac{1}{2} \sum_{j=1}^{\min(t,r)} E \left[\log \left(\frac{P}{t} \Lambda_j \right) \right] \\
&= \frac{\min(t,r)}{2} \log \left(\frac{P}{t} \right) + \frac{1}{2} \sum_{j=1}^{\min(t,r)} E(\log \Lambda_j)
\end{aligned}$$

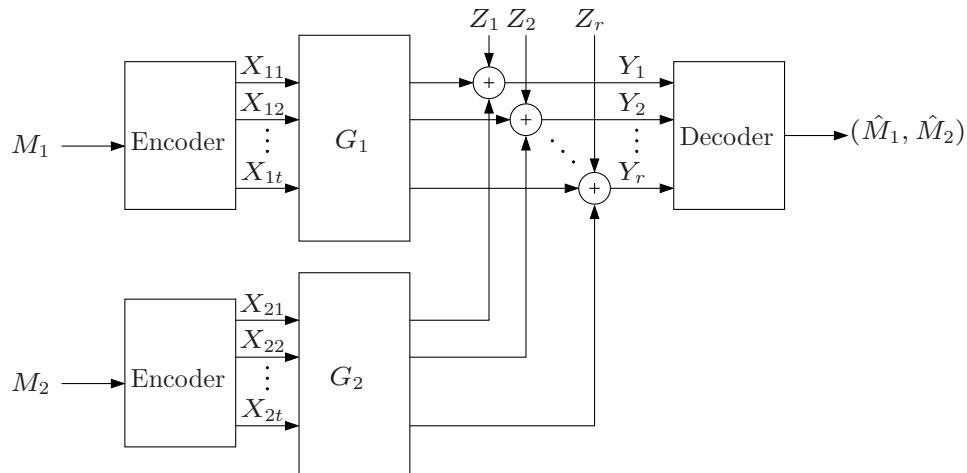
This is a $\min(t,r)$ -fold increase in capacity over the single antenna case

Gaussian Vector Multiple Access Channels

- Consider the Gaussian vector multiple-access channel (GV-MAC)

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

where G_1 and G_2 are $r \times t$ constant channel gain matrices and $\{\mathbf{Z}(i)\}$ is an r -dimensional vector WGN(K_Z) process. Without loss of generality, we assume that $K_Z = I_r$



- Average power constraints: For every codeword, $\frac{1}{n} \sum_{i=1}^n \mathbf{x}_j^T(i) \mathbf{x}_j(i) \leq P$, $j = 1, 2$
- Remark: Unlike the point-to-point Gaussian vector channel, where the channel is always equivalent to a product of AWGN channels, the GV-MAC cannot be factorized into a product of AWGN-MACs in general
- *Theorem 3:* The capacity region of the GV-MAC is the set of rate pairs (R_1, R_2) such that

$$R_1 \leq \frac{1}{2} \log |G_1 K_1 G_1^T + I_r|,$$

$$R_2 \leq \frac{1}{2} \log |G_2 K_2 G_2^T + I_r|,$$

$$R_1 + R_2 \leq \frac{1}{2} \log |G_1 K_1 G_1^T + G_2 K_2 G_2^T + I_r|$$

for some $K_1, K_2 \succeq 0$ with $\text{tr}(K_j) \leq P$, $j = 1, 2$

To show this, note that the capacity region is the set of rate pairs (R_1, R_2) such

that

$$R_1 \leq I(\mathbf{X}_1; \mathbf{Y} | \mathbf{X}_2, Q),$$

$$R_2 \leq I(\mathbf{X}_2; \mathbf{Y} | \mathbf{X}_1, Q),$$

$$R_1 + R_2 \leq I(\mathbf{X}_1, \mathbf{X}_2; \mathbf{Y} | Q)$$

for some conditionally independent \mathbf{X}_1 and \mathbf{X}_2 given Q satisfying $E(\mathbf{X}_j^T \mathbf{X}_j) \leq P$, $j = 1, 2$

Furthermore, it is easy to show that $|\mathcal{Q}| = 1$ suffices and that among all input distributions with given correlation matrices $K_1 = \mathbb{E}(\mathbf{X}_1\mathbf{X}_1^T)$ and $K_2 = \mathbb{E}(\mathbf{X}_2\mathbf{X}_2^T)$, Gaussian input vectors $\mathbf{X}_1 \sim \mathcal{N}(0, K_1)$ and $\mathbf{X}_2 \sim \mathcal{N}(0, K_2)$ simultaneously maximize all three mutual information bounds

- Sum-rate maximization problem:

$$\begin{aligned} & \text{maximize} && \log |G_1 K_1 G_1^T + G_2 K_2 G_2^T + I_r| \\ & \text{subject to} && \text{tr}(K_j) \leq P, \\ & && K_j \succeq 0, \quad j = 1, 2 \end{aligned}$$

- The above problem is convex and the optimal solution is attained when K_1 is the single-user water-filling covariance matrix for the channel G_1 with noise covariance matrix $G_2 K_2 G_2^T + I_r$ and K_2 is the single-user water-filling covariance matrix for the channel G_2 with noise covariance matrix $G_1 K_1 G_1^T + I_r$

- The following *iterative water-filling* algorithm [3] finds the optimal K_1, K_2

repeat

$$\Sigma_1 = G_2 K_2 G_2^T + I_r$$

$$K_1 = \arg \max_K \log |G_1 K G_1^T + \Sigma_1|, \text{ subject to } \text{tr}(K) \leq P_1$$

$$\Sigma_2 = G_1 K_1 G_1^T + I_r$$

$$K_2 = \arg \max_K \log |G_2 K G_2^T + \Sigma_2|, \text{ subject to } \text{tr}(K) \leq P_2$$

until the desired accuracy is reached

- It can be shown that this algorithm converges to the optimal solution from any initial assignment of K_1 and K_2

GV-MAC with More Than Two Senders

- Consider a k -sender GV-MAC

$$\mathbf{Y}(i) = G_1 \mathbf{X}_1(i) + \cdots + G_k \mathbf{X}_k(i) + \mathbf{Z}(i)$$

with $\{\mathbf{Z}(i)\}$ is an r -dimensional vector $\text{WGN}(I_r)$ process. Assume an average power constraint P on each sender

- The capacity region is the set of rate tuples (R_1, R_2, \dots, R_k) such that

$$\sum_{j \in \mathcal{J}} R_j \leq \frac{1}{2} \log \left| \sum_{j \in \mathcal{J}} G_j K_j G_j^T + I_r \right|, \quad \mathcal{J} \subseteq [1 : k]$$

for some positive semidefinite matrices K_1, \dots, K_k with $\text{tr}(K_j) \leq P$, $j \in [1 : k]$

- The iterative water-filling algorithm can be easily extended to find the optimal K_1, \dots, K_k

Spectral Gaussian Broadcast Channels

- Consider a product of AWGN-BCs: At time i

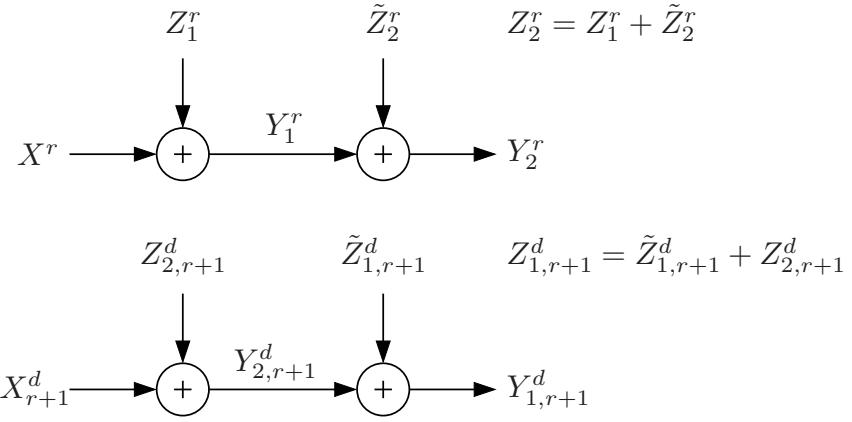
$$\begin{aligned}\mathbf{Y}_1(i) &= \mathbf{X}(i) + \mathbf{Z}_1(i), \\ \mathbf{Y}_2(i) &= \mathbf{X}(i) + \mathbf{Z}_2(i),\end{aligned}$$

where $\{Z_{jk}(i)\}$, $j = 1, 2$, $k \in [1 : d]$, are independent $\text{WGN}(N_{jk})$ processes

- We assume that $N_{1k} \leq N_{2k}$ for $k \in [1 : r]$ and $N_{1k} > N_{2k}$ for $[r + 1 : d]$

If $r = d$, then the channel is degraded and it can be easily shown (check!) that the capacity region is the Minkowski sum of the capacity regions for each component AWGN-BC (up to power allocation) [4]

In general, however, the channel is not degraded, but instead a product of *reversely* (or *inconsistently*) degraded broadcast channels



- Average power constraint: For every codeword, $\frac{1}{n} \sum_{i=1}^n \mathbf{x}^T(i) \mathbf{x}(i) \leq P$
- The product of AWGN-BCs models the spectral Gaussian broadcast channel in which the noise spectrum for each receiver varies over frequency or time and so does relative orderings among the receivers

- *Theorem 4 [5]:* The capacity region of the product of AWGN-BCs is the set of rate triples (R_0, R_1, R_2) such that

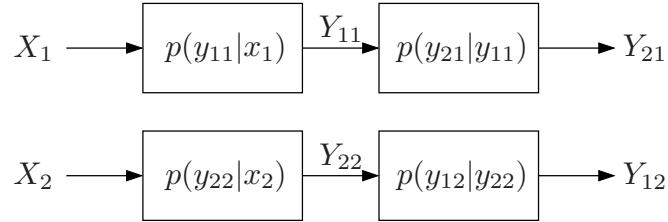
$$\begin{aligned}
 R_0 + R_1 &\leq \sum_{k=1}^r C\left(\frac{\beta_k P}{N_{1k}}\right) + \sum_{k=r+1}^d C\left(\frac{\alpha_k \beta_k P}{\bar{\alpha}_k \beta_k P + N_{1k}}\right) \\
 R_0 + R_2 &\leq \sum_{k=1}^r C\left(\frac{\alpha_k \beta_k P}{\bar{\alpha}_k \beta_k P + N_{2k}}\right) + \sum_{k=r+1}^d C\left(\frac{\beta_k P}{N_{2k}}\right) \\
 R_0 + R_1 + R_2 &\leq \sum_{k=1}^r C\left(\frac{\beta_k P}{N_{1k}}\right) + \sum_{k=r+1}^d \left(C\left(\frac{\alpha_k \beta_k P}{\bar{\alpha}_k \beta_k P + N_{1k}}\right) + C\left(\frac{\bar{\alpha}_k \beta_k P}{N_{2k}}\right) \right) \\
 R_0 + R_1 + R_2 &\leq \sum_{k=1}^r \left(C\left(\frac{\alpha_k \beta_k P}{\bar{\alpha}_k \beta_k P + N_{2k}}\right) + C\left(\frac{\bar{\alpha}_k \beta_k P}{N_{1k}}\right) \right) + \sum_{k=r+1}^d C\left(\frac{\beta_k P}{N_{2k}}\right)
 \end{aligned}$$

for some $\alpha_k, \beta_k \in [0 : 1]$, $k \in [1 : d]$, satisfying $\sum_{k=1}^d \beta_k = 1$

- Converse follows (check!) from similar steps to the converse for the AWGN-BC by using the conditional EPI for each component channel

Proof of Achievability

- To prove the achievability, we first consider two *reversely degraded* DM-BCs $(\mathcal{X}_1, p(y_{11}|x_1)p(y_{21}|y_{11}), \mathcal{Y}_{11} \times \mathcal{Y}_{21})$ and $(\mathcal{X}_2, p(y_{22}|x_2)p(y_{12}|y_{22}), \mathcal{Y}_{12} \times \mathcal{Y}_{22})$. The product of these two reversely degraded DM-BC is a DM-BC with $\mathcal{X} := \mathcal{X}_1 \times \mathcal{X}_2$, $\mathcal{Y}_1 := \mathcal{Y}_{11} \times \mathcal{Y}_{12}$, $\mathcal{Y}_2 := \mathcal{Y}_{21} \times \mathcal{Y}_{22}$, and $p(y_1, y_2|x) = p(y_{11}|x_1)p(y_{21}|y_{11})p(y_{22}|x_2)p(y_{12}|y_{22})$



Proposition: The capacity region for this DM-BC [5] is the set of rate triples (R_0, R_1, R_2) such that

$$R_0 + R_1 \leq I(X_1; Y_{11}) + I(U_2; Y_{12}),$$

$$R_0 + R_2 \leq I(X_2; Y_{22}) + I(U_1; Y_{21}),$$

$$R_0 + R_1 + R_2 \leq I(X_1; Y_{11}) + I(U_2; Y_{12}) + I(X_2; Y_{22}|U_2),$$

$$R_0 + R_1 + R_2 \leq I(X_2; Y_{22}) + I(U_1; Y_{21}) + I(X_1; Y_{11}|U_1)$$

for some $p(u_1, x_1)p(u_2, x_2)$

The proof of converse for the proposition follows easily from the standard converse steps (or from the Nair–El Gamal outer bound in Lecture Notes 9)

The proof of achievability uses rate splitting and superposition coding

- Rate splitting: Split M_j , $j = 1, 2$, into two independent messages: M_{j0} at rate R_{j0} and M_{jj} at rate R_{jj}
- Codebook generation: Fix $p(u_1, x_1)p(u_2, x_2)$. Randomly and independently generate 2^{nR_0} sequence pairs $(u_1^n, u_2^n)(m_0, m_{10}, m_{20})$, $(m_0, m_{10}, m_{20}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_{10}}] \times [1 : 2^{nR_{20}}]$, each according to $\prod_{i=1}^n p_{U_i}(u_{1i})p_{U_i}(u_{2i})$

For $j = 1, 2$ and each $u_j^n(m_0, m_{10}, m_{20})$, randomly and conditionally independently generate $2^{nR_{jj}}$ sequences $x_j^n(m_0, m_{10}, m_{20}, m_{jj})$, $m_{jj} \in [1 : 2^{nR_{jj}}]$, each according to $\prod_{i=1}^n p_{X_j|U_j}(x_{ji}|u_{ji}(m_0, m_{10}, m_{20}))$

- Encoding: To send (m_0, m_1, m_2) , transmit $(x_1^n(m_0, m_{10}, m_{20}, m_{11}), x_2^n(m_0, m_{10}, m_{20}, m_{22}))$
- Decoding and analysis of the probability of error: Decoder 1 declares that $(\hat{m}_{01}, \hat{m}_1)$ is sent if it is the unique pair such that $((u_1^n, u_2^n)(\hat{m}_{01}, \hat{m}_{10}, m_{20}), x_1^n(\hat{m}_{01}, \hat{m}_1, m_2), y_{11}^n, y_{12}^n) \in \mathcal{T}_\epsilon^{(n)}$ for some m_2 . Similarly, decoder 2 declares that $(\hat{m}_{02}, \hat{m}_2)$ is sent if it is the unique pair such that $((u_1^n, u_2^n)(\hat{m}_{02}, m_{10}, \hat{m}_{20}), x_2^n(\hat{m}_{02}, m_1, \hat{m}_2), y_{21}^n, y_{22}^n) \in \mathcal{T}_\epsilon^{(n)}$ for some m_1

Following standard arguments, it can be shown that the probability of error for decoder 1 $\rightarrow 0$ as $n \rightarrow \infty$ if

$$\begin{aligned} R_0 + R_1 + R_{20} &< I(U_1, U_2, X_1; Y_{11}, Y_{12}) - \delta(\epsilon) \\ &= I(X_1; Y_{11}) + I(U_2; Y_{12}) - \delta(\epsilon), \\ R_{11} &< I(X_1; Y_{11}|U_1) - \delta(\epsilon) \end{aligned}$$

Similarly, the probability of error for decoder 2 $\rightarrow 0$ as $n \rightarrow \infty$ if

$$\begin{aligned} R_0 + R_{10} + R_2 &< I(X_2; Y_{22}) + I(U_1; Y_{21}) - \delta(\epsilon), \\ R_{22} &< I(X_2; Y_{22}|U_2) - \delta(\epsilon) \end{aligned}$$

Substituting $R_{jj} = R_j - R_{j0}$, $j = 1, 2$, combining with the condition $R_{10}, R_{20} \geq 0$, and eliminating R_{10}, R_{20} by the Fourier–Motzkin procedure, we obtain the desired region

- Remarks:
 - It is interesting to note that even though U_1 and U_2 are statistically independent, each decoder jointly decodes them to find the common message
 - In general, this region can be much larger than the sum of the capacity regions of two component degraded BCs. For example, consider the special case of reversely degraded BC with $Y_{21} = Y_{12} = \emptyset$. The common-message capacities of the component BCs are $C_{01} = C_{02} = 0$, while the common-message capacity of the product BC is $C_0 = \min\{\max_{p(x_1)} I(X_1; Y_{11}), \max_{p(x_2)} I(X_2; Y_{22})\}$. This illustrates that simultaneous decoding can be much more powerful than separate decoding

- The above result can be extended to the product of any number of channels. Suppose $X_k \rightarrow Y_{1k} \rightarrow Y_{2k}$ for $k \in [1 : r]$ and $X_k \rightarrow Y_{2k} \rightarrow Y_{1k}$ for $k \in [r + 1 : d]$. Then the capacity region of the product of these d reversely degraded DM-BCs is

$$\begin{aligned} R_0 + R_1 &\leq \sum_{k=1}^d I(X_k; Y_{1k}) + \sum_{k=r+1}^d I(U_k; Y_{1k}), \\ R_0 + R_2 &\leq \sum_{k=1}^d I(U_k; Y_{2k}) + \sum_{k=r+1}^d I(X_k; Y_{2k}), \\ R_0 + R_1 + R_2 &\leq \sum_{k=1}^d I(X_k; Y_{1k}) + \sum_{k=r+1}^d (I(U_k; Y_{1k}) + I(X_k; Y_{2k}|U_k)), \\ R_0 + R_1 + R_2 &\leq \sum_{k=1}^d (I(U_k; Y_{2k}) + I(X_k; Y_{1k}|U_k)) + \sum_{k=r+1}^d I(X_k; Y_{2k}) \end{aligned}$$

for some $p(u_1, x_1)p(u_2, x_2)$

- Now the achievability for the product of AWGN-BCs follows immediately (check!) by taking $U_k \sim N(0, \alpha_k \beta_k P)$, $V_k \sim N(0, \bar{\alpha}_k \beta_k P)$, $k \in [1 : d]$, independent of each other, and $X_k = U_k + V_k$, $k \in [1 : d]$

- A similar coding scheme, however, does not generalize easily to more than 2 receivers. In fact, the capacity region of the product of reversely degraded DM-BCs for more than 2 receivers is not known in general
- In addition, it does not handle the case where component channels are dependent
- Specializing the result to private messages only gives the private-message capacity region, which consists of the set of rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y_{11}) + I(U_2; Y_{12}),$$

$$R_2 \leq I(X_2; Y_{22}) + I(U_1; Y_{21}),$$

$$R_1 + R_2 \leq I(X_1; Y_{11}) + I(U_2; Y_{12}) + I(X_2; Y_{22}|U_2),$$

$$R_1 + R_2 \leq I(X_2; Y_{22}) + I(U_1; Y_{21}) + I(X_1; Y_{11}|U_1)$$

for some $p(u_1, x_1)p(u_2, x_2)$. This can be further optimized as follows [6]. Let $C_{11} := \max_{p(x_1)} I(X_1; Y_{11})$ and $C_{22} := \max_{p(x_2)} I(X_2; Y_{22})$, then we have

$$R_1 \leq C_{11} + I(U_2; Y_{12}),$$

$$R_2 \leq C_{22} + I(U_1; Y_{21}),$$

$$R_1 + R_2 \leq C_{11} + I(U_2; Y_{12}) + I(X_2; Y_{22}|U_2),$$

$$R_1 + R_2 \leq C_{22} + I(U_1; Y_{21}) + I(X_1; Y_{11}|U_1)$$

for some $p(u_1, x_1)p(u_2, x_2)$

Note that the capacity region \mathcal{C} in this case can be expressed as the intersection of the two regions

- o \mathcal{C}_1 consisting of the set of rate pairs (R_1, R_2) such that

$$R_1 \leq C_{11} + I(U_2; Y_{12}),$$

$$R_1 + R_2 \leq C_{11} + I(U_2; Y_{12}) + I(X_2; Y_{22}|U_2)$$

for some $p(u_2, x_2)$, and

- o \mathcal{C}_2 consisting of the set of rate pairs (R_1, R_2) such that

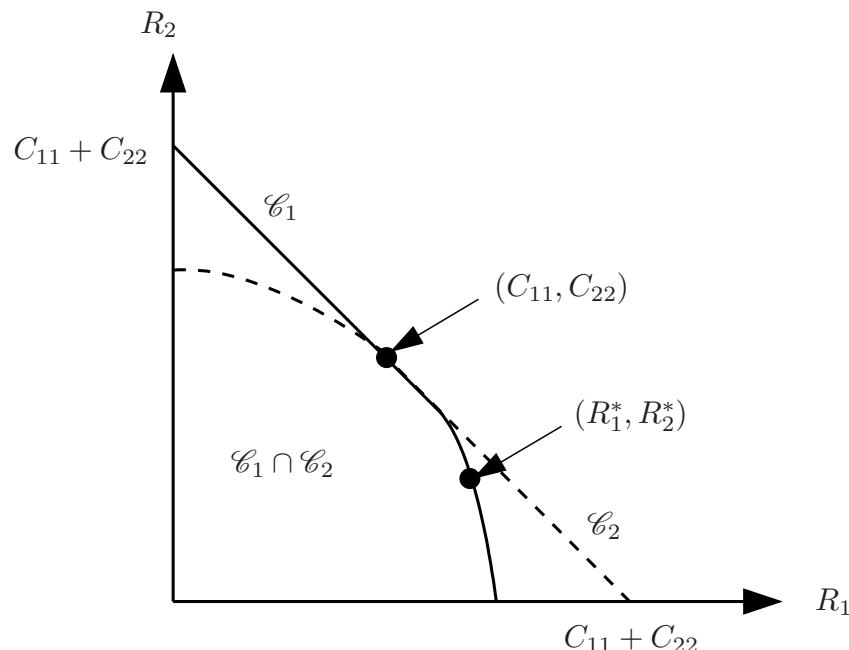
$$R_2 \leq C_{22} + I(U_1; Y_{21}),$$

$$R_1 + R_2 \leq C_{22} + I(U_1; Y_{21}) + I(X_1; Y_{11}|U_1)$$

for some $p(u_1, x_1)$

Note that \mathcal{C}_1 is the capacity region of the *enhanced* degraded product BC [7] with $Y_{21} = Y_{11}$, which is in general larger than the capacity region of the original product BC. Similarly \mathcal{C}_2 is the capacity region of the enhanced degraded product BC with $Y_{12} = Y_{22}$. Thus $\mathcal{C} \subseteq \mathcal{C}_1 \cap \mathcal{C}_2$

On the other hand, each boundary point of $\mathcal{C}_1 \cap \mathcal{C}_2$ lies on the boundary of the capacity region \mathcal{C} , i.e., $\mathcal{C} \supseteq \mathcal{C}_1 \cap \mathcal{C}_2$. To show this, note first that $(C_{11}, C_{22}) \in \mathcal{C}$ is on the boundary of $\mathcal{C}_1 \cap \mathcal{C}_2$ (see Figure)



Moreover, each boundary point (R_1^*, R_2^*) with $R_1^* \geq C_{11}$ is on the boundary of \mathcal{C}_1 and satisfies $R_1^* = C_{11} + I(U_2; Y_{12})$, $R_2^* = I(X_2; Y_{22}|U_2)$ for some $p(u_2, x_2)$

By evaluating \mathcal{C} with the same $p(u_2, x_2)$, $U_1 = \emptyset$, and $p(x_1)$ that achieves C_{11} , it follows that (R_1^*, R_2^*) lies on the boundary of \mathcal{C} . We can similarly show that boundary points (R_1^*, R_2^*) with $R_1^* \leq C_{11}$ also lies on the boundary of \mathcal{C} .

This completes the proof of $\mathcal{C} = \mathcal{C}_1 \cap \mathcal{C}_2$

- Remarks

- This argument provides the proof of converse immediately since the capacity region of the original BC is contained in the capacity regions of each enhanced degraded BC
- The above private-message capacity result generalizes to any number of receivers
- The approach of proving the converse by considering each point on the boundary of the capacity region of the original BC and constructing an enhanced degraded BC whose capacity region is in general larger than the capacity region of the original BC but coincides with it at this point turns out to be very useful for the general Gaussian vector BC as we will see later

Vector Writing on Dirty Paper

- Here we generalize Costa's writing on dirty paper coding to Gaussian vector channels, which will be subsequently applied to the Gaussian vector BC
- Consider a vector Gaussian channel with additive Gaussian state $\mathbf{Y}(i) = G\mathbf{X}(i) + \mathbf{S}(i) + \mathbf{Z}(i)$, where $\mathbf{S}(i)$ and $\mathbf{Z}(i)$ are independent vector WGN(K_S) and WGN(I_r) processes, respectively. Assume that the *interference* vector $(\mathbf{S}(1), \mathbf{S}(2), \dots, \mathbf{S}(n))$ is available noncausally at the encoder. Further assume average power constraint P on \mathbf{X}
- The capacity of this channel is the same as if \mathbf{S} were not present, that is,

$$C = \max_{\text{tr}(K_X) \leq P} \frac{1}{2} \log |I_r + GK_XG^T|$$

- This follows by optimizing the Gelfand–Pinsker capacity expression

$$C = \sup_{F(\mathbf{u}, \mathbf{x}|\mathbf{s})} (I(\mathbf{U}; \mathbf{Y}) - I(\mathbf{U}; \mathbf{S})),$$

subject to the power constraint $E(\mathbf{X}^T \mathbf{X}) \leq P$

Similar to the scalar case, this expression is maximized by choosing

$\mathbf{U} = \mathbf{X} + A\mathbf{S}$, where $\mathbf{X} \sim N(\mathbf{0}, K_X)$ is independent of \mathbf{S} and

$$A = K_X G^T (G K_X G^T + I_r)^{-1}$$

We can easily check that this A is chosen such that $A(G\mathbf{X} + \mathbf{Z})$ is the MMSE estimate of \mathbf{X} . Thus, $\mathbf{X} - A(G\mathbf{X} + \mathbf{Z})$ is independent of $G\mathbf{X} + \mathbf{Z}$, \mathbf{S} , and hence $\mathbf{Y} = G\mathbf{X} + \mathbf{Z} + \mathbf{S}$. Finally consider

$$h(\mathbf{U}|\mathbf{S}) = h(\mathbf{X} + A\mathbf{S}|\mathbf{S}) = h(\mathbf{X})$$

and

$$\begin{aligned} h(\mathbf{U}|\mathbf{Y}) &= h(\mathbf{X} + A\mathbf{S}|\mathbf{Y}) \\ &= h(\mathbf{X} + A\mathbf{S} - A\mathbf{Y}|\mathbf{Y}) \\ &= h(\mathbf{X} - A(G\mathbf{X} + \mathbf{Z})|\mathbf{Y}) \\ &= h(\mathbf{X} - A(G\mathbf{X} + \mathbf{Z})) \\ &= h(\mathbf{X} - A(G\mathbf{X} + \mathbf{Z})|G\mathbf{X} + \mathbf{Z}) \\ &= h(\mathbf{X}|G\mathbf{X} + \mathbf{Z}), \end{aligned}$$

which implies that we can achieve

$$h(\mathbf{X}) - h(\mathbf{X}|G\mathbf{X} + \mathbf{Z}) = I(\mathbf{X}; G\mathbf{X} + \mathbf{Z}) = \frac{1}{2} \log |I_r + GK_{\mathbf{X}}G^T|$$

for any $K_{\mathbf{X}}$ with $\text{tr}(K_{\mathbf{X}}) \leq P$

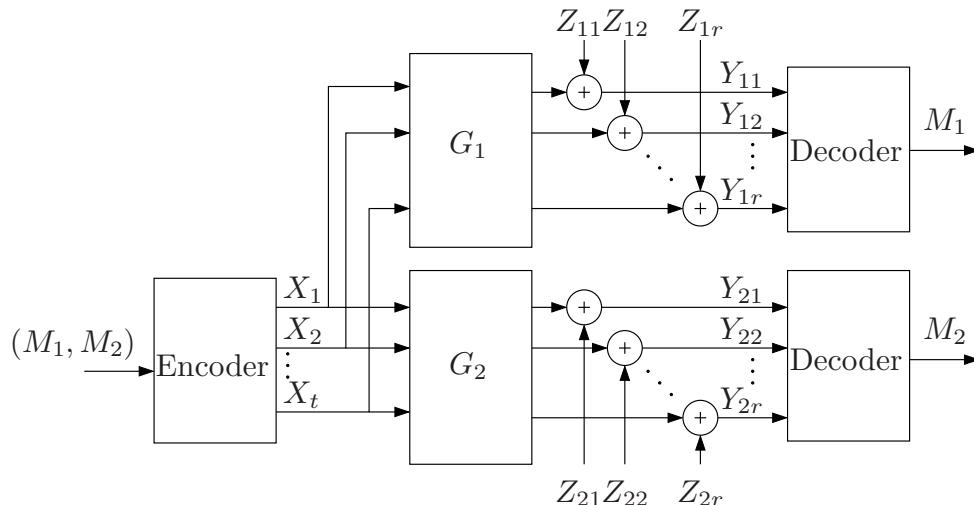
- Note that the same result holds for any non-Gaussian state \mathbf{S}

Gaussian Vector Broadcast Channels

- Consider the Gaussian vector broadcast channel (GV-BC)

$$\mathbf{Y}_1(i) = G_1\mathbf{X}(i) + \mathbf{Z}_1(i), \quad \mathbf{Y}_2(i) = G_2\mathbf{X}(i) + \mathbf{Z}_2(i),$$

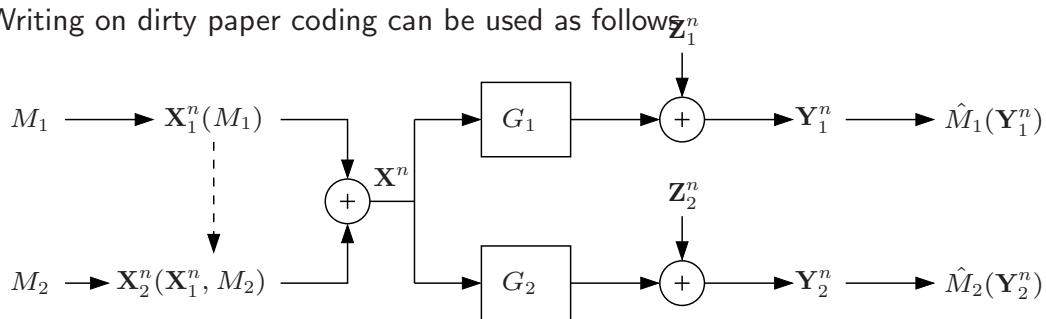
G_1, G_2 are $r \times t$ matrices and $\{\mathbf{Z}_1(i)\}, \{\mathbf{Z}_2(i)\}$ are vector WGN(K_{Z_1}) and WGN(K_{Z_2}) processes, respectively. Without loss of generality, we assume that $K_{Z_1} = K_{Z_2} = I_r$



- Average power constraint: For every codeword, $(1/n) \sum_{i=1}^n \mathbf{x}^T(i)\mathbf{x}(i) \leq P$
- If $G_1^T G_1$ and $G_2^T G_2$ have the same set of eigenvectors, then it can be easily shown that the channel is a product of AWGN-BCs and superposition coding achieves the capacity region.
- Note that this condition is a special case of degraded GV-BC. In general even if the channel is degraded, the converse is does not follow simply by using the EPI (why?)

Dirty Paper Coding Region

- Writing on dirty paper coding can be used as follows



- Encoding: Messages are encoded successively and the corresponding Gaussian random codewords are added to form the transmitted codeword. In the figure, M_1 is encoded first using a zero-mean Gaussian $\mathbf{X}_1^n(M_1)$ sequence with covariance matrix K_1 . The codeword $\mathbf{X}_1^n(M_1)$ is then viewed as independent Gaussian interference for receiver 2 that is available noncausally at the encoder. By the writing on dirty paper result, the encoder can *effectively* pre-subtract this interference without increasing its power. As stated earlier, $\mathbf{X}_2^n(\mathbf{X}_1^n, M_2)$ is also a zero-mean Gaussian and independent of $\mathbf{X}_1^n(M_1)$. Denote its covariance matrix by K_2

- Decoding: Decoder 1 treats $\mathbf{X}_2^n(\mathbf{X}_1^n, M_2)$ as noise, while decoder 2 decodes its message in the absence of any effect of interference from $\mathbf{X}_1^n(M_1)$. Thus any rate pair (R_1, R_2) such that

$$R_1 < \frac{1}{2} \log \frac{|G_1 K_1 G_1^T + G_1 K_2 G_1^T + I_r|}{|G_1 K_2 G_1^T + I_r|},$$

$$R_2 < \frac{1}{2} \log |G_2 K_2 G_2^T + I_r|,$$

and $\text{tr}(K_1 + K_2) \leq P$ is achievable. Denote the rate region consisting of all such rate pairs as \mathcal{R}_1

Now, by considering the other message encoding order, we can similarly find an achievable rate region \mathcal{R}_2 consisting of all rate pair (R_1, R_2) such that

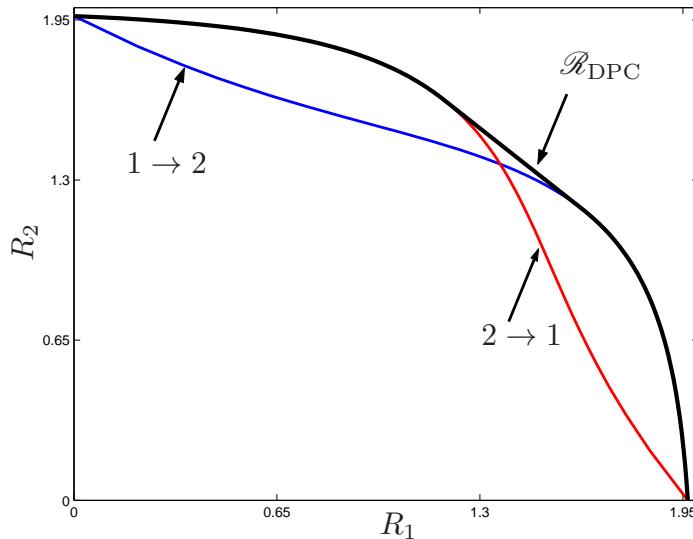
$$R_1 < \frac{1}{2} \log |G_1 K_1 G_1^T + I_r|$$

$$R_2 < \frac{1}{2} \log \frac{|G_2 K_2 G_2^T + G_2 K_1 G_2^T + I_t|}{|G_2 K_1 G_2^T + I_r|}$$

for some $K_1, K_2 \succeq 0$ with $\text{tr}(K_1 + K_2) \leq P$

- The dirty paper rate region \mathcal{R}_{DPC} is the convex closure of $\mathcal{R}_1 \cup \mathcal{R}_2$

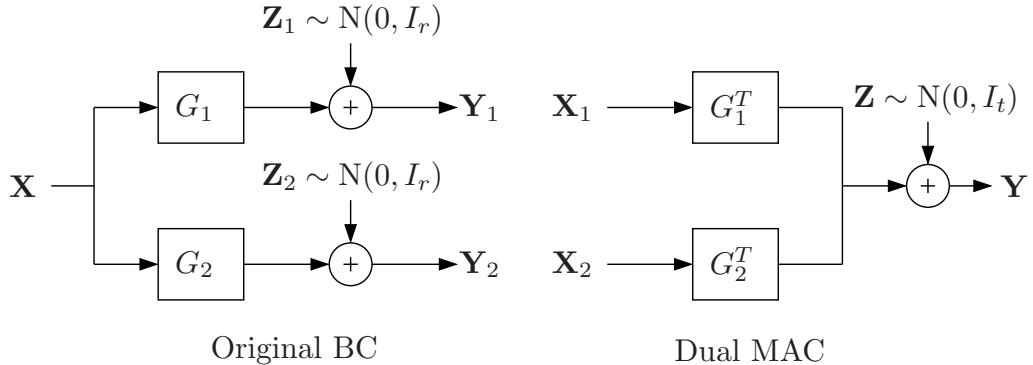
- Example: $t = 2$ and $r = 1$



- Computing the dirty paper coding (DPC) region is difficult because the rate terms for R_j , $j = 1, 2$, in the DPC region are not concave functions of K_1 and K_2 . This difficulty can be overcome by the duality between the Gaussian vector BC and the Gaussian vector MAC with sum power constraint

Gaussian Vector BC-MAC Duality

- This generalizes the scalar Gaussian BC–MAC duality discussed in the homework
 - Given the GV-BC (referred to as the *original BC*) with channel gain matrices G_1, G_2 and power constraint P , consider a GV-MAC with channel matrices G_1^T, G_2^T (referred to as the *dual MAC*)



- *MAC-BC Duality Lemma* [8, 9]: Let $\mathcal{C}_{\text{DMAC}}$ denote the capacity of the dual MAC under sum power constraint $\frac{1}{n} \sum_{i=1}^n (\mathbf{x}_1^T(i)\mathbf{x}_1(i) + \mathbf{x}_2^T(i)\mathbf{x}_2(i)) \leq P$. Then

$$\mathcal{R}_{\text{DPC}} = \mathcal{C}_{\text{DMAC}}$$

- It is easy to characterize $\mathcal{C}_{\text{DMAC}}$:

- Let K_1 and K_2 be the covariance matrices for each sender. Then any rate pair in the interior of the following set is achievable for the dual MAC:

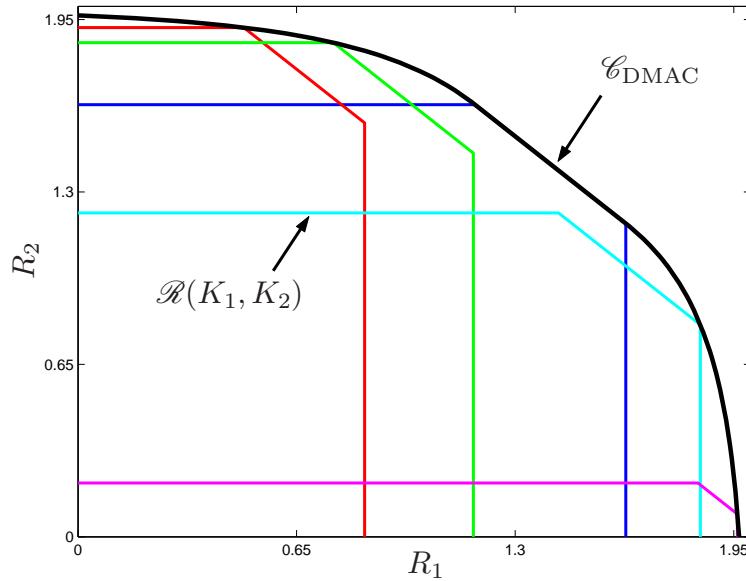
$$\begin{aligned}\mathcal{R}(K_1, K_2) = & \left\{ (R_1, R_2) : R_1 \leq \frac{1}{2} \log |G_1^T K_1 G_1 + I_t|, \right. \\ & R_2 \leq \frac{1}{2} \log |G_2^T K_2 G_2 + I_t|, \\ & \left. R_1 + R_2 \leq \frac{1}{2} \log |G_1^T K_1 G_1 + G_2^T K_2 G_2 + I_t| \right\}\end{aligned}$$

- The capacity region of the dual MAC under sum power constraint:

$$\mathcal{C}_{\text{DMAC}} = \bigcup_{K_1, K_2 \succeq 0 : \text{tr}(K_1) + \text{tr}(K_2) \leq P} \mathcal{R}(K_1, K_2)$$

The converse proof follows the same steps of that from the GV-MAC with individual power constraint

- Example: Dual GV-MAC with $t = 1$ and $r = 2$



Properties of the Dual MAC Capacity Region

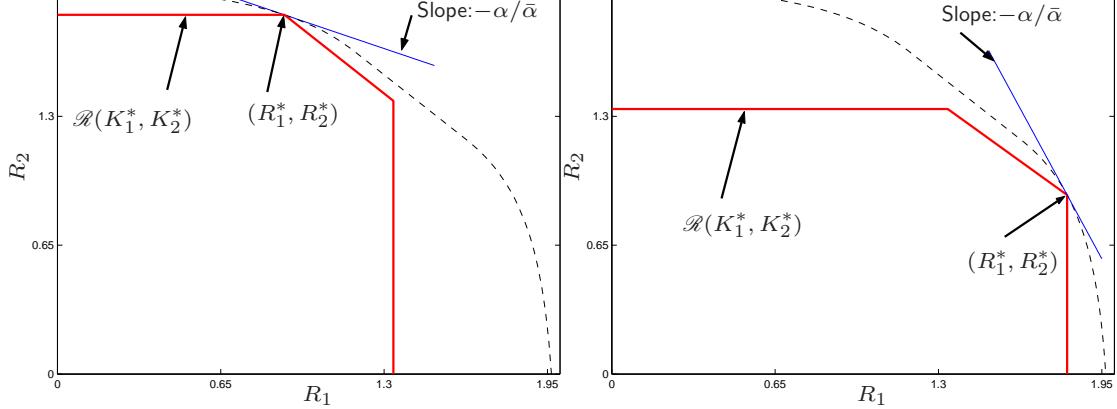
- The dual representation $\mathcal{R}_{\text{DPC}} = \mathcal{C}_{\text{DMAC}} = \bigcup_{K_1, K_2} \mathcal{R}(K_1, K_2)$ exhibits the following useful properties (check!):
 - Rate terms for $\mathcal{R}(K_1, K_2)$ are concave functions of K_1, K_2 (so we can use tools from convex optimization)
 - The region $\bigcup \mathcal{R}(K_1, K_2)$ is closed and convex
- Consequently, each boundary point (R_1^*, R_2^*) of $\mathcal{C}_{\text{DMAC}}$ lies on the boundary of $\mathcal{R}(K_1, K_2)$ for some K_1, K_2 , and is a solution to the (convex) optimization problem

$$\begin{aligned} & \text{maximize } \alpha R_1 + \bar{\alpha} R_2 \\ & \text{subject to } (R_1, R_2) \in \mathcal{C}_{\text{DMAC}} \end{aligned}$$

for some $\alpha \in [0, 1]$. That is, (R_1^*, R_2^*) is tangent to a supporting hyperplane (line) with slope $-\alpha/\bar{\alpha}$

- It can be easily seen that each boundary point (R_1^*, R_2^*) of $\mathcal{C}_{\text{DMAC}}$ is either
 - a corner point of $\mathcal{R}(K_1, K_2)$ for some K_1, K_2 (we refer to such a corner point (R_1^*, R_2^*) as an *boundary corner point*) or
 - a convex combination of boundary corner points (or both)

- If a boundary corner point (R_1^*, R_2^*) is inside the positive orthant (quadrant), i.e., if $R_1^*, R_2^* > 0$, then it has a *unique* supporting hyperplane (see the Appendix for the proof). In other words, $\mathcal{C}_{\text{DMAC}}$ does not have a kink inside the positive orthant
- Example: the dual MAC with $t = 1$ and $r = 2$



Optimality of the DPC Region

- *Theorem 4 [7]:* The capacity region of the GV-BC is $\mathcal{C} = \mathcal{R}_{\text{DPC}}$
- *Proof outline [10]:* From the MAC–BC duality, it suffices to show that $\mathcal{C} = \mathcal{C}_{\text{DMAC}}$

The corner points of $\mathcal{C}_{\text{DMAC}}$ are $(C_1, 0)$ and $(0, C_2)$, where

$$C_j = \max_{K_j \succeq 0: \text{tr}(K_j) \leq P} \frac{1}{2} \log |G_j^T K_j G_j + I_r|, \quad j = 1, 2,$$

is the capacity of the single-user channel to each receiver. By the reciprocity lemma, these corner points correspond to the individual capacity bounds for the GV-BC and hence are on the boundary of its capacity region \mathcal{C} .

We now focus on proving the optimality of $\mathcal{C}_{\text{DMAC}}$ inside the positive orthant

- We first characterize the boundary corner point $(R_1^*(\alpha), R_2^*(\alpha))$ associated with the supporting hyperplane of slope $-\alpha/\bar{\alpha}$ via Lagrange duality
- Next, we construct an *enhanced* degraded Gaussian vector BC for each boundary corner point $(R_1^*(\alpha), R_2^*(\alpha))$ such that the capacity region \mathcal{C} of the original BC is contained in the capacity region $\mathcal{C}_{\text{DBC}(\alpha)}$ of the enhanced BC (Lemma 3)

- We then show that the boundary corner point $(R_1^*(\alpha), R_2^*(\alpha))$ is on the boundary of $\mathcal{C}_{\text{DBC}(\alpha)}$ (Lemma 4). Since $\mathcal{C}_{\text{DMAC}} = \mathcal{R}_{\text{DPC}} \subseteq \mathcal{C} \subseteq \mathcal{C}_{\text{DBC}(\alpha)}$, we can conclude that each boundary corner point $(R_1^*(\alpha), R_2^*(\alpha))$ is on the boundary of \mathcal{C}
- Finally because every boundary corner point $(R_1^*(\alpha), R_2^*(\alpha))$ of $\mathcal{C}_{\text{DMAC}}$ inside the positive orthant has a unique supporting hyperplane, the boundary of $\mathcal{C}_{\text{DMAC}}$ must coincide with that of \mathcal{C} by Lemma A.2 in Appendix A

Boundary Corner Points of $\mathcal{C}_{\text{DMAC}}$ via Lagrange Duality

- Recall that every boundary corner point (R_1^*, R_2^*) inside the positive orthant maximizes $\alpha R_1 + \bar{\alpha} R_2$ for some $\alpha \in [0, 1]$. Without loss of generality, suppose $\bar{\alpha} \geq 1/2 \geq \alpha$. Then the rate pair

$$R_1^* = \frac{1}{2} \log \frac{|G_1^T K_1^* G_1 + G_2^T K_2^* G_2 + I_t|}{|G_2^T K_2^* G_2 + I_t|}, \quad R_2^* = \frac{1}{2} \log |G_2^T K_2^* G_2 + I_t|,$$

uniquely corresponds to an optimal solution to the following convex optimization problem in K_1, K_2 :

$$\text{maximize} \quad \frac{\alpha}{2} \log |G_1^T K_1 G_1 + G_2^T K_2 G_2 + I_t| + \frac{\bar{\alpha} - \alpha}{2} \log |G_2^T K_2 G_2 + I_t|$$

$$\text{subject to} \quad \text{tr}(K_1) + \text{tr}(K_2) \leq P, \quad K_1, K_2 \succeq 0$$

- Since Slater's condition is satisfied for $P > 0$, the KKT condition characterizes the optimal K_1^*, K_2^*
 - With dual variables

$$\text{tr}(K_1) + \text{tr}(K_2) \leq P \Leftrightarrow \lambda \geq 0,$$

$$K_1, K_2 \succeq 0 \Leftrightarrow \Upsilon_1, \Upsilon_2 \succeq 0,$$

we form the Lagrangian

$$\begin{aligned} L(K_1, K_2, \Upsilon_1, \Upsilon_2, \lambda) = & \frac{\alpha}{2} \log |G_1^T K_1 G_1 + G_2^T K_2 G_2 + I_t| \\ & + \frac{\bar{\alpha} - \alpha}{2} \log |G_2^T K_2 G_2 + I_t| \\ & + \text{tr}(\Upsilon_1 K_1) + \text{tr}(\Upsilon_1 K_2) - \lambda(\text{tr}(K_1) + \text{tr}(K_2) - P) \end{aligned}$$

- KKT condition: a primal solution (K_1^*, K_2^*) is optimal iff there exists a dual optimal solution $(\lambda^*, \Upsilon_1^*, \Upsilon_2^*)$ satisfying

$$\begin{aligned} G_1 \Sigma_1 G_1^T + \frac{1}{\lambda^*} \Upsilon_1^* - I_r &= 0, \quad G_2 \Sigma_2 G_2^T + \frac{1}{\lambda^*} \Upsilon_2^* - I_r = 0, \\ \lambda^* (\text{tr}(K_1^*) + \text{tr}(K_2^*) - P) &= 0, \quad \text{tr}(\Upsilon_1^* K_1^*) = \text{tr}(\Upsilon_2^* K_2^*) = 0, \end{aligned}$$

where

$$\begin{aligned} \Sigma_1 &= \frac{\alpha}{2\lambda^*} (G_1^T K_1^* G_1 + G_2^T K_2^* G_2 + I_t)^{-1}, \\ \Sigma_2 &= \frac{\alpha}{2\lambda^*} (G_1^T K_1^* G_1 + G_2^T K_2^* G_2 + I_t)^{-1} + \frac{\bar{\alpha} - \alpha}{2\lambda^*} (G_2^T K_2^* G_2 + I_t)^{-1} \end{aligned}$$

Note that $\Sigma_2 \succeq \Sigma_1 \succ 0$ and $\lambda^* > 0$ since we use full power at transmitter

- Further define

$$\begin{aligned} K_1^{**} &= \frac{\alpha}{2\lambda^*} (G_2^T K_2^* G_2 + I_t)^{-1} - \Sigma_1, \\ K_2^{**} &= \frac{\bar{\alpha}}{2\lambda^*} I_t - K_1^{**} - \Sigma_2 \end{aligned}$$

It can be easily seen (check!) that

1. $K_1^{**}, K_2^{**} \succeq 0$ and $\text{tr}(K_1^{**}) + \text{tr}(K_2^{**}) = P$
2. The boundary corner point (R_1^*, R_2^*) can be written as

$$R_1^* = \frac{1}{2} \log \frac{|K_1^{**} + \Sigma_1|}{|\Sigma_1|}, \quad R_2^* = \frac{1}{2} \log \frac{|K_1^{**} + K_2^{**} + \Sigma_2|}{|K_1^{**} + \Sigma_2|}$$

Construction of the Enhanced Degraded GV-BC

- For each boundary corner point $(R_1^*(\alpha), R_2^*(\alpha))$ corresponding to supporting hyperplane $(\alpha, \bar{\alpha})$, we define the GV-BC DBC(α) as

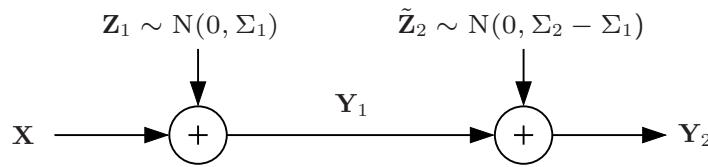
$$\mathbf{Y}_1 = \mathbf{X} + \mathbf{Z}_1,$$

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

where $\mathbf{Z}_1 \sim N(0, \Sigma_1)$ and $\mathbf{Z}_2 \sim N(0, \Sigma_2)$ are additive Gaussian noise

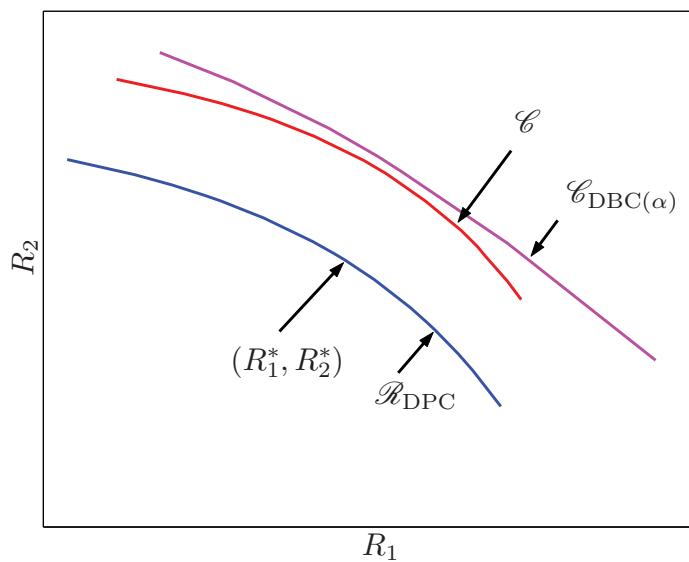
As in the original BC, we assume the input power constraint P

- Since $\Sigma_2 \succeq \Sigma_1$, the enhanced channel DBC(α) is a degraded BC. Without loss of generality, we assume it is *physically* degraded



Lemma 3: $\mathcal{C} \subseteq \mathcal{C}_{DBC(\alpha)}$

- Lemma 3:* The capacity region $\mathcal{C}_{DBC(\alpha)}$ of DBC(α) is an outer bound on the capacity region \mathcal{C} of the original BC



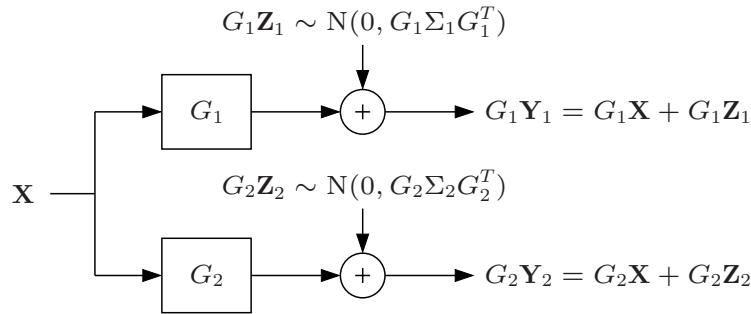
- To show this, we prove that the original BC is a degraded version of the enhanced DBC(α). This clearly implies that any code originally designed for the original BC can be used in DBC(α) with same or smaller probability of error, and thus that each rate pair in \mathcal{C} is also in $\mathcal{C}_{DBC(\alpha)}$

- From the KKT optimality conditions for K_1^*, K_2^*

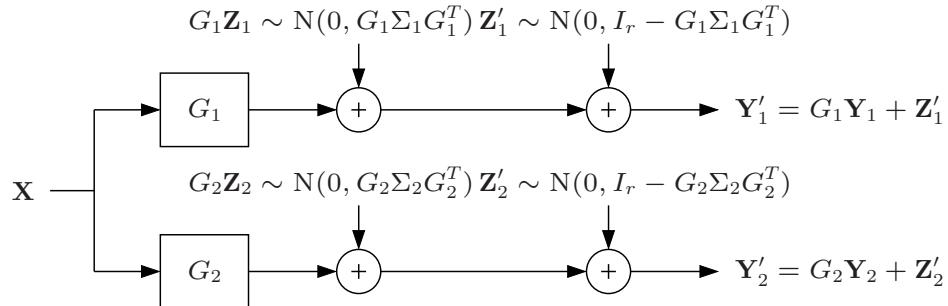
$$I_r - G_j \Sigma_j G_j^T \succeq 0, j = 1, 2$$

- Each receiver of DBC(α) can

- Multiply the received signal $\mathbf{Y}_j(i)$ by G_j



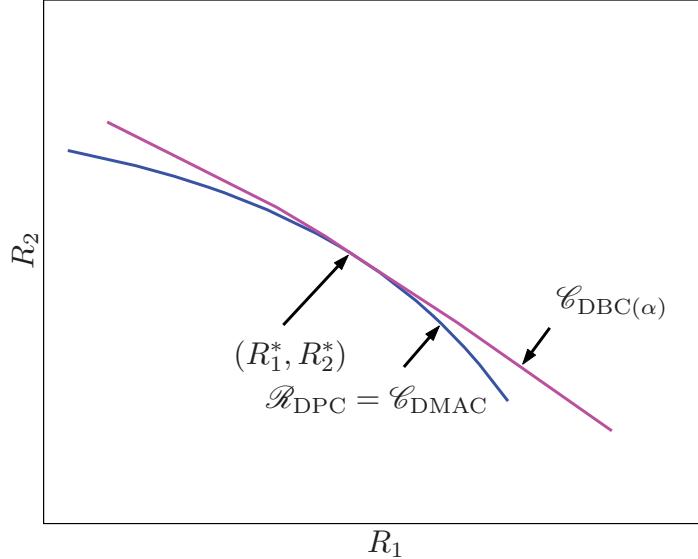
- Add to each $G\mathbf{Y}_j(i)$ an independent WGN vector $\mathbf{Z}'_j(i)$ with covariance matrix $I_r - G_j \Sigma_j G_j^T$



- Thus the transformed received signal $\mathbf{Y}'_j(i)$ for DBC(α) has the same distribution as the received signal $\mathbf{Y}_j(i)$ for the original BC with channel matrix G_j and noise covariance matrix I_r

Lemma 4: Optimality of $(R_1^*(\alpha), R_2^*(\alpha))$

- *Lemma 4:* Every boundary corner point $(R_1^*(\alpha), R_2^*(\alpha))$ of the dual MAC region to the original BC in the positive orthant, corresponding to the supporting hyperplane of slope $-\alpha/\bar{\alpha}$, is on the boundary of the capacity region of $\mathcal{C}_{\text{DBC}(\alpha)}$



- Proof: We follow the similar lines as the converse proof for the scalar AWGN-BC

- We first recall the representation of the boundary corner point (R_1^*, R_2^*) from the KKT condition:

$$R_1^* = \frac{1}{2} \log \frac{|K_1^{**} + \Sigma_1|}{|\Sigma_1|}, \quad R_2^* = \frac{1}{2} \log \frac{|K_1^{**} + K_2^{**} + \Sigma_2|}{|K_1^{**} + \Sigma_2|},$$

where

$$K_1^{**} = \frac{\alpha}{2\lambda^*} (G_2^T K_2^* G_2 + I_t)^{-1} - \Sigma_1, \quad K_2^{**} = \frac{\bar{\alpha}}{2\lambda^*} I_t - K_1^{**} - \Sigma_2$$

- Consider a $(2^{nR_1}, 2^{nR_2}, n)$ code for $\mathcal{C}_{\text{DBC}(\alpha)}$ with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
To prove the optimality of (R_1^*, R_2^*) , we show that if $R_1 > R_1^*$, then $R_2 \leq R_2^*$
 - By Fano's inequality, we have

$$nR_2 \leq I(M_2; \mathbf{Y}_2^n) + n\epsilon_n = h(\mathbf{Y}_2^n) - h(\mathbf{Y}_2^n | M_2) + n\epsilon_n$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$

- First note that $h(\mathbf{Y}_2^n) = h(\mathbf{X}^n + \mathbf{Z}_2^n)$ is upper bounded by

$$\max_{K_X} \frac{n}{2} \log(2\pi e)^t |K_X + \Sigma_2|$$

under the constraint $\text{tr}(K_X) \leq P$

But recalling the properties $\text{tr}(K_1^{**} + K_2^{**}) = P$ and

$$K_1^{**} + K_2^{**} + \Sigma_2 = \frac{\bar{\alpha}}{\lambda^*} I_t,$$

we see that the covariance matrix $K_1^{**} + K_2^{**}$ satisfies the KKT condition for the single-user channel $\mathbf{Y}_2 = \mathbf{X} + \mathbf{Z}_2$. Therefore,

$$h(\mathbf{Y}_2^n) \leq \frac{n}{2} \log(2\pi e)^t |K_1^{**} + K_2^{**} + \Sigma_2|$$

- As in the scalar AWGN-GC converse proof, we use the EPI to lower bound $h(\mathbf{Y}_2^n|M_2)$. By Fano's inequality and the assumption $R_1^* < R_1$,

$$\begin{aligned} \frac{n}{2} \log \frac{|K_1^{**} + \Sigma_1|}{|\Sigma_1|} &= nR_1^* \\ &< I(M_1; \mathbf{Y}_1^n|M_2) + n\epsilon_n \\ &= h(\mathbf{Y}_1^n|M_2) - h(\mathbf{Y}_1^n|M_1, M_2) + n\epsilon_n \\ &\leq h(\mathbf{Y}_1^n|M_2) - \frac{n}{2} \log(2\pi e)^t |\Sigma_1| + n\epsilon_n, \end{aligned}$$

or equivalently,

$$h(\mathbf{Y}_1^n|M_2) \geq \frac{n}{2} \log(2\pi e)^t |K_1^{**} + \Sigma_1| - n\epsilon_n$$

Since $\mathbf{Y}_2^n = \mathbf{Y}_1^n + \tilde{\mathbf{Z}}_2^n$, and \mathbf{Y}_1^n and $\tilde{\mathbf{Z}}_2^n$ are independent and have densities, by the conditional EPI

$$\begin{aligned} h(\mathbf{Y}_2^n|M_2) &\geq \frac{nt}{2} \log \left(2^{\frac{2}{nt} h(\mathbf{Y}_1^n|M_2)} + 2^{\frac{2}{nt} h(\tilde{\mathbf{Z}}_2^n|M_2)} \right) \\ &\geq \frac{nt}{2} \log \left((2\pi e) |K_1^{**} + \Sigma_1|^{1/t} + (2\pi e) |\Sigma_2 - \Sigma_1|^{1/t} \right) - n\epsilon'_n \end{aligned}$$

But from the definitions of $\Sigma_1, \Sigma_2, K_1^{**}, K_2^{**}$, the matrices

$$K_1^{**} + \Sigma_1 = \frac{\alpha}{2\lambda^*} (G_2^T K_2^* G_2 + I_t)^{-1},$$

$$\Sigma_2 - \Sigma_1 = \frac{(\bar{\alpha} - \alpha)}{2\lambda^*} (G_2^T K_2^* G_2 + I_t)^{-1}$$

are scaled versions of each other. Hence

$$\begin{aligned} |K_1^{**} + \Sigma_1|^{1/t} + |\Sigma_2 - \Sigma_1|^{1/t} &= |(K_1^{**} + \Sigma_1) + (\Sigma_2 - \Sigma_1)|^{1/t} \\ &= |K_1^{**} + \Sigma_2|^{1/t} \end{aligned}$$

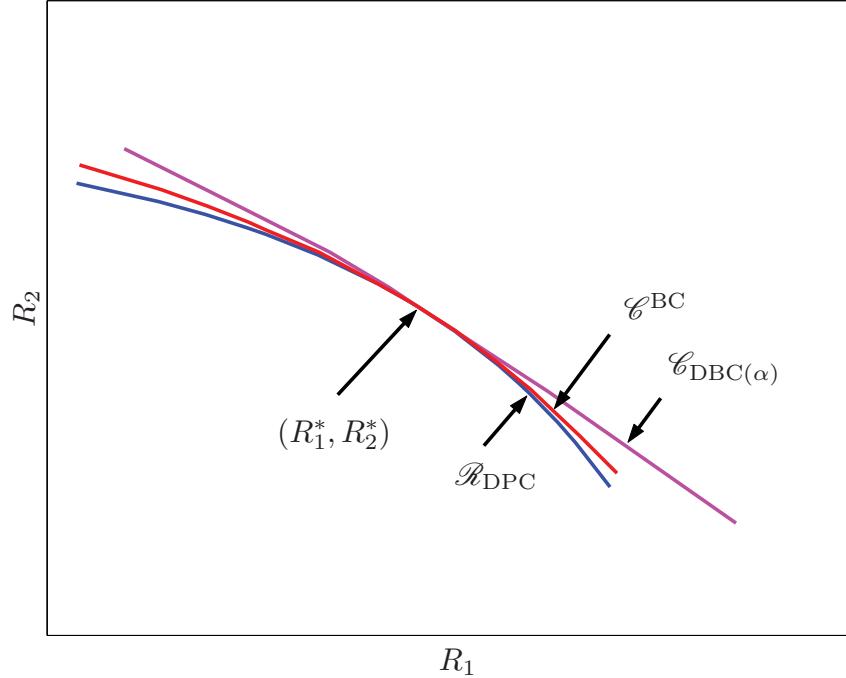
Therefore

$$h(\mathbf{Y}_2^n|M_2) \geq \frac{n}{2} \log(2\pi e)^t |K_1^{**} + \Sigma_2| - n\epsilon_n,$$

- Combining bounds and taking $n \rightarrow \infty$, we finally obtain

$$R_2 \leq \frac{1}{2} \log \frac{|K_1^{**} + K_2^{**} + \Sigma_2|}{|K_1^{**} + \Sigma_2|} = R_2^*$$

- Optimality of (R_1^*, R_2^*) :



GV-BC with More Than Two Receivers

- Consider a k -receiver Gaussian vector broadcast channel

$$\mathbf{Y}_j(i) = G_j \mathbf{X}(i) + \mathbf{Z}_j(i), \quad j \in [1 : k],$$

where $\{\mathbf{Z}_j\}$ is a vector WGN(I_r) process, $j \in [1 : k]$, and assume average power constraint P

- The capacity region is the convex hull of the set of rate tuples such that

$$R_{\sigma(j)} \leq \frac{1}{2} \log \frac{|\sum_{j' \geq j} G_{\sigma(j')} K_{\sigma(j')} G_{\sigma(j')}^T + I_r|}{|\sum_{j' > j} G_{\sigma(j')} K_{\sigma(j')} G_{\sigma(j')}^T + I_r|}$$

for some permutation σ on $[1 : k]$ and positive semidefinite matrices K_1, \dots, K_k with $\sum_j \text{tr}(K_j) \leq P$

- Given σ , the corresponding rate region is achievable by dirty paper coding with decoding order $\sigma(1) \rightarrow \dots \rightarrow \sigma(k)$

- As in the 2-receiver case, the converse hinges on the MAC–BC duality (which can be easily extended to more than 2 receivers)
 - The corresponding dual MAC capacity region $\mathcal{C}_{\text{DMAC}}$ is the set of rate tuples satisfying

$$\sum_{j \in \mathcal{J}} R_j \leq \frac{1}{2} \log \left| \sum_{j \in \mathcal{J}} G_j^T K_j G_j + I_r \right|, \quad \mathcal{J} \subseteq [1 : k]$$

for some positive semidefinite matrices K_1, \dots, K_k with $\sum_j \text{tr}(K_j) \leq P$

- The optimality of $\mathcal{C}_{\text{DMAC}}$ can be proved by induction on k . For the case $R_j = 0$ for some $j \in [1 : k]$, the problem reduces to proving the optimality of $\mathcal{C}_{\text{DMAC}}$ for $k - 1$ receivers. Therefore we can consider (R_1, \dots, R_k) in the positive orthant only

Now as in the 2-receiver case, each boundary corner point can be shown to be optimal by constructing a corresponding degraded GV-BC (check!), and establishing that the boundary corner point is on the boundary of the capacity region of the degraded GV-BC and hence on the boundary of the capacity region of the original GV-BC. It can be also shown that $\mathcal{C}_{\text{DMAC}}$ does not have a kink, i.e., every boundary corner point has a unique supporting hyperplane. Therefore the boundary of $\mathcal{C}_{\text{DMAC}}$ must coincide with the capacity region, which proves the optimality of the dirty paper coding

Key New Ideas and Techniques

- Singular value decomposition
- Water-filling and iterative water-filling
- Enhanced channel for the converse proof
- Vector DPC
- MAC–BC duality
- Convex optimization
- Dirty paper coding (Marton's inner bound) is optimal for vector Gaussian broadcast channels
- Open problems
 - Simple characterization of the spectral Gaussian BC for more than 2 receivers
 - Capacity region of the Gaussian vector BC with common message

References

- [1] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge: Cambridge University Press, 2004.
- [2] I. E. Telatar, "Capacity of multi-antenna Gaussian channels," Bell Laboratories, Murray Hill, NJ, Technical memorandum, 1995.
- [3] W. Yu, W. Rhee, S. Boyd, and J. M. Cioffi, "Iterative water-filling for Gaussian vector multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 50, no. 1, pp. 145–152, 2004.
- [4] D. Hughes-Hartogs, "The capacity of the degraded spectral Gaussian broadcast channel," Ph.D. Thesis, Stanford University, Stanford, CA, Aug. 1975.
- [5] A. El Gamal, "Capacity of the product and sum of two unmatched broadcast channels," *Probl. Inf. Transm.*, vol. 16, no. 1, pp. 3–23, 1980.
- [6] G. S. Poltyrev, "The capacity of parallel broadcast channels with degraded components," *Probl. Inf. Transm.*, vol. 13, no. 2, pp. 23–35, 1977.
- [7] H. Weingarten, Y. Steinberg, and S. Shamai, "The capacity region of the Gaussian multiple-input multiple-output broadcast channel," *IEEE Trans. Inf. Theory*, vol. 52, no. 9, pp. 3936–3964, Sept. 2006.
- [8] S. Vishwanath, N. Jindal, and A. Goldsmith, "Duality, achievable rates, and sum-rate capacity of Gaussian MIMO broadcast channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 10, pp. 2658–2668, 2003.
- [9] P. Viswanath and D. N. C. Tse, "Sum capacity of the vector Gaussian broadcast channel and uplink-downlink duality," *IEEE Trans. Inf. Theory*, vol. 49, no. 8, pp. 1912–1921, 2003.

- [10] M. Mohseni, "Capacity of Gaussian vector broadcast channels," Ph.D. Thesis, Stanford University, Stanford, CA, Sept. 2006.

Appendix: Proof of the BC–MAC Duality

- We show that $\mathcal{R}_{\text{DPC}} \subseteq \mathcal{C}_{\text{DMAC}}$. The other direction of inclusion can be proved similarly
 - Consider the DPC scheme in which the message M_1 is encoded before M_2
 - Denote by K_1 and K_2 the covariance matrices for $\mathbf{X}_{11}^n(M_1)$ and $\mathbf{X}_{21}^n(\mathbf{X}_{11}^n(M_1), M_2)$, respectively. We know that the following rates are achievable:

$$R_1 = \frac{1}{2} \log \frac{|G_1(K_1 + K_2)G_1^T + I_r|}{|G_1K_2G_1^T + I_r|},$$

$$R_2 = \frac{1}{2} \log |G_2K_2G_2^T + I_r|$$

We show that (R_1, R_2) is achievable in the dual MAC with the sum-power constraint $P = \text{tr}(K_1) + \text{tr}(K_2)$ using successive cancellation decoding with M_2 is decoded before M_1

- Let $K'_1, K'_2 \succeq 0$ be defined as
 1. $K'_1 := \Sigma_1^{-1/2} \bar{K}_1 \Sigma_1^{-1/2}$,
where $\Sigma_1^{-1/2}$ is the symmetric square root inverse of $\Sigma_1 := G_1 K_2 G_1^T + I_r$ and \bar{K}_1 is obtained by the reciprocity lemma for the covariance matrix K_1 and the channel matrix $\Sigma_1^{-1/2} G_1$ such that $\text{tr}(\bar{K}_1) \leq \text{tr}(K_1)$ and

$$|\Sigma_1^{-1/2} G_1 K_1 G_1^T \Sigma_1^{-1/2} + I_r| = |G_1^T \Sigma_1^{-1/2} \bar{K}_1 \Sigma_1^{-1/2} G_1 + I_t|$$

2. $K'_2 := \overline{\Sigma_2^{1/2} K_2 \Sigma_2^{1/2}}$,
where $\Sigma_2^{1/2}$ is the symmetric square root of $\Sigma_2 := G_1^T K'_1 G_1 + I_t$ and the bar over $\Sigma_2^{1/2} K_2 \Sigma_2^{1/2}$ means K'_2 is obtained by the reciprocity lemma for the covariance matrix $\Sigma_2^{1/2} K_2 \Sigma_2^{1/2}$ and the channel matrix $G_2 \Sigma_2^{-1/2}$ such that

$$\text{tr}(K'_2) \leq \text{tr}(\Sigma_2^{1/2} K_2 \Sigma_2^{1/2})$$

and

$$|G_2 \Sigma_2^{-1/2} (\Sigma_2^{1/2} K_2 \Sigma_2^{1/2}) \Sigma_2^{-1/2} G_2^T + I_r| = |\Sigma_2^{-1/2} G_2^T K'_2 G_2 \Sigma_2^{-1/2} + I_t|$$

- Using the covariance matrices K'_1, K'_2 for senders 1 and 2, respectively, the following rates are achievable in the dual MAC when M_2 is decoded before M_1 (reverse the encoding order for the BC):

$$R'_1 = \frac{1}{2} \log |G_1^T K'_1 G_1 + I_t|,$$

$$R'_2 = \frac{1}{2} \log \frac{|G_1^T K'_1 G_1 + G_2^T K'_2 G_2 + I_t|}{|G_1^T K'_1 G_1 + I_t|}$$

- From the definitions of $K'_1, K'_2, \Sigma_1, \Sigma_2$, we have

$$\begin{aligned} R_1 &= \frac{1}{2} \log \frac{|G_1(K_1 + K_2)G_1^T + I_r|}{|G_1 K_2 G_1^T + I_r|} \\ &= \frac{1}{2} \log \frac{|G_1 K_1 G_1^T + \Sigma_1|}{|\Sigma_1|} \\ &= \frac{1}{2} \log |\Sigma_1^{-1/2} G_1 K_1 G_1^T P^{-1/2} + I_r| \\ &= \frac{1}{2} \log |G_1^T \Sigma^{-1/2} \bar{K}_1 \Sigma^{-1/2} G_1 + I_t| \\ &= R'_1 \end{aligned}$$

and similarly we can show that $R_2 = R'_2$

Furthermore,

$$\begin{aligned} \text{tr}(K'_2) &= \text{tr} \left(\overline{\Sigma_2^{1/2} K_2 \Sigma_2^{1/2}} \right) \\ &\leq \text{tr}(\Sigma_2^{1/2} K_2 \Sigma_2^{1/2}) \\ &= \text{tr}(\Sigma_2 K_2) \\ &= \text{tr}((G_1^T K'_1 G_1 + I_t) K_2) \\ &= \text{tr}(K_2) + \text{tr}(K'_1 G_1 K_2 G_1^T) \\ &= \text{tr}(K_2) + \text{tr}(K'_1 (\Sigma_1 - I_r)) \\ &= \text{tr}(K_2) + \text{tr}(\Sigma_1^{1/2} K'_1 \Sigma_1^{1/2}) - \text{tr}(K'_1) \\ &= \text{tr}(K_2) + \text{tr}(\bar{K}_1) - \text{tr}(K'_1) \\ &\leq \text{tr}(K_2) + \text{tr}(K_1) - \text{tr}(K'_1) \end{aligned}$$

Therefore, any point in the DPC region of the BC is also achievable in the dual MAC under the sum-power constraint

- The proof for the case where M_2 is encoded before M_1 follows similarly

Appendix: Uniqueness of the Supporting Hyperplane

- We show that every boundary corner point (R_1^*, R_2^*) with $R_1^*, R_2^* > 0$ has a unique supporting hyperplane $(\alpha, \bar{\alpha})$
- Consider a boundary corner point (R_1^*, R_2^*) in the positive orthant. Without loss of generality assume that $0 \leq \alpha \leq 1/2$ and (R_1^*, R_2^*) is given by

$$R_1^* = \frac{1}{2} \log \frac{|G_1^T K_1^* G_1 + G_2^T K_2^* G_2 + I_t|}{|G_2^T K_2^* G_2 + I_t|}, \quad R_2^* = \frac{1}{2} \log |G_2^T K_2^* G_2 + I_t|,$$

where (K_1^*, K_2^*) is an optimal solution to the convex optimization problem

$$\begin{aligned} \text{maximize } & \frac{\alpha}{2} \log |G_1^T K_1 G_1 + G_2^T K_2 G_2 + I_t| + \frac{\bar{\alpha} - \alpha}{2} \log |G_2^T K_2 G_2 + I_t| \\ \text{subject to } & \text{tr}(K_1) + \text{tr}(K_2) \leq P \\ & K_1, K_2 \succeq 0 \end{aligned}$$

- We will prove the uniqueness by contradiction. Suppose (R_1^*, R_2^*) has another supporting hyperplane $(\beta, \bar{\beta}) \neq (\alpha, \bar{\alpha})$
 - First note that α and β must be nonzero. Otherwise, $K_1^* = 0$, which contradicts the assumption that $R_1^* > 0$. Also by the assumption that $R_1^* > 0$, we must have $G_1^T K_1^* G_1 \neq 0$ as well as $K_1^* \neq 0$

- Now consider a feasible solution of the optimization problem at $((1 - \epsilon)K_1^*, \epsilon K_1^* + K_2^*)$, given by

$$\begin{aligned} & \frac{\alpha}{2} \log |G_1^T (1 - \epsilon) K_1^* G_1 + G_2^T (\epsilon K_1^* + K_2^*) G_2 + I_t| \\ & + \frac{\bar{\alpha} - \alpha}{2} \log |G_2^T (\epsilon K_1^* + K_2^*) G_2 + I_t| \end{aligned}$$

Taking derivative [1] at $\epsilon = 0$ and using optimality of (K_1^*, K_2^*) , we obtain

$$\begin{aligned} & \alpha \text{tr} [(G_1^T K_1^* G_1 + G_2^T K_2^* G_2 + I_t)^{-1} (G_2^T K_2^* G_2 - G_1^T K_1^* G_1)] \\ & + (\bar{\alpha} - \alpha) \text{tr} [(G_2^T K_2^* G_2 + I_t)^{-1} (G_2^T K_2^* G_2)] = 0 \end{aligned}$$

and similarly

$$\begin{aligned} & \beta \text{tr} [(G_1^T K_1^* G_1 + G_2^T K_2^* G_2 + I_t)^{-1} (G_2^T K_2^* G_2 - G_1^T K_1^* G_1)] \\ & + (\bar{\beta} - \beta) \text{tr} [(G_2^T K_2^* G_2 + I_t)^{-1} (G_2^T K_2^* G_2)] = 0 \end{aligned}$$

- But since $\alpha \neq \beta$, this implies that

$$\begin{aligned} & \text{tr} [(G_1^T K_1^* G_1 + G_2^T K_2^* G_2 + I_t)^{-1} (G_2^T K_2^* G_2 - G_1^T K_1^* G_1)] \\ & = \text{tr} [(G_2^T K_2^* G_2 + I_t)^{-1} (G_2^T K_2^* G_2)] = 0, \end{aligned}$$

which in turn implies that $G_1^T K_1^* G_1 = 0$ and that $R_1^* = 0$. But this contradicts the hypothesis that $R_1^* > 0$, which completes the proof

Lecture Notes 11

Distributed Lossless Source Coding

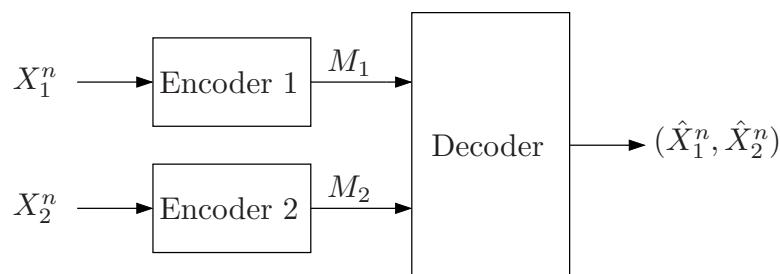
- Problem Setup
- The Slepian–Wolf Theorem
- Achievability via Cover’s Random Binning
- Lossless Source Coding with a Helper
- Extension to More Than Two Sources
- Key New Ideas and Techniques

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- The sources X_1 and X_2 are separately encoded (described) and the descriptions are sent over noiseless links to a decoder who wishes to reconstruct both sources (X_1, X_2) losslessly
- Consider the distributed source coding problem for a 2-component DMS (2-DMS) $(\mathcal{X}_1 \times \mathcal{X}_2, p(x_1, x_2))$, informally referred to as *correlated sources* (X_1, X_2) , that consists of two finite alphabets $\mathcal{X}_1, \mathcal{X}_2$ and a joint pmf $p(x_1, x_2)$ over $\mathcal{X}_1 \times \mathcal{X}_2$

The 2-DMS $(\mathcal{X}_1 \times \mathcal{X}_2, p(x_1, x_2))$ generates a jointly i.i.d. random process $\{(X_{1i}, X_{2i})\}$ with $(X_{1i}, X_{2i}) \sim p_{X_1, X_2}(x_{1i}, x_{2i})$



- Formally, a $(2^{nR_1}, 2^{nR_2}, n)$ distributed source code for the 2-DMS (X_1, X_2) consists of:
 1. Two encoders: Encoder 1 assigns an index $m_1(x_1^n) \in [1 : 2^{nR_1}]$ to each sequence $x_1^n \in \mathcal{X}_1^n$, and encoder 2 assigns to each sequence $x_2^n \in \mathcal{X}_2^n$ an index $m_2(x_2^n) \in [1 : 2^{nR_2}]$
 2. A decoder that assigns an estimate $(\hat{x}_1^n, \hat{x}_2^n) \in \mathcal{X}_1^n \times \mathcal{X}_2^n$ or an error message e to each index pair $(m_1, m_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$
- The probability of error for a distributed source code is defined as

$$P_e^{(n)} = P\{(\hat{X}_1^n, \hat{X}_2^n) \neq (X_1^n, X_2^n)\}$$

- A rate pair (R_1, R_2) is said to be *achievable* if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ distributed source codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The *optimal rate region* \mathcal{R} is the closure of the set of all achievable rates

Inner and Outer Bounds on the Optimal Rate Region

- Inner bound on \mathcal{R} : By the lossless source coding theorem, clearly a rate pair (R_1, R_2) is achievable if $R_1 > H(X_1)$, $R_2 > H(X_2)$
- Outer bound on \mathcal{R} :
 - By the lossless source coding theorem, a rate $R \geq H(X_1, X_2)$ is necessary and sufficient to send a pair of sources (X_1, X_2) together to a receiver. Thus, $R_1 + R_2 \geq H(X_1, X_2)$ is necessary for the distributed source coding problem
 - Also, it seems plausible that $R_1 \geq H(X_1|X_2)$ is necessary. Let's prove this
Given a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^{(n)} \rightarrow 0$, consider the induced empirical pmf

$$(X_1^n, X_2^n, M_1, M_2) \sim p(x_1^n, x_2^n)p(m_1|x_1^n)p(m_2|x_2^n),$$

where $M_1 = m_1(X_1^n)$ and $M_2 = m_2(X_2^n)$ are the indices assigned by the encoders of the $(2^{nR_1}, 2^{nR_2}, n)$ code

By Fano's inequality $H(X_1^n, X_2^n|M_1, M_2) \leq n\epsilon_n$

Thus also

$$H(X_1^n|M_1, M_2, X_2^n) = H(X_1^n|M_1, X_2^n) \leq H(X_1^n, X_2^n|M_1, M_2) \leq n\epsilon_n$$

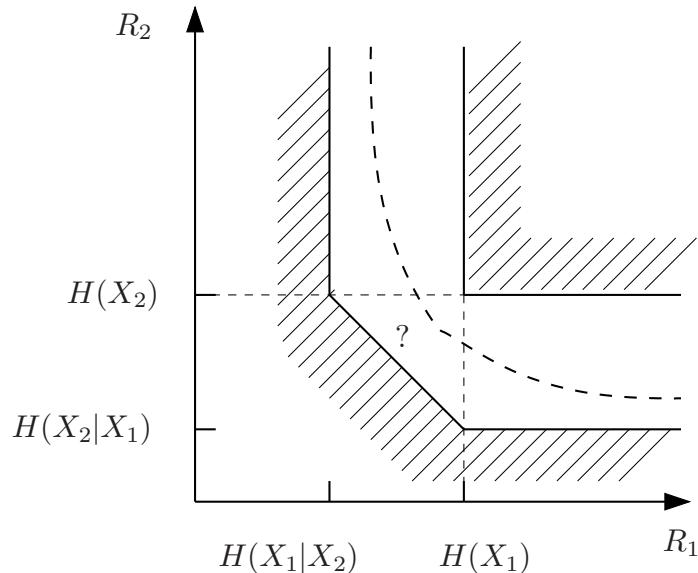
Now, consider

$$\begin{aligned}
 nR_1 &\geq H(M_1) \\
 &\geq H(M_1|X_2^n) \\
 &= I(X_1^n; M_1|X_2^n) + H(M_1|X_1^n, X_2^n) \\
 &= I(X_1^n; M_1|X_2^n) \\
 &= H(X_1^n|X_2^n) - H(X_1^n|M_1, X_2^n) \\
 &\geq H(X_1^n|X_2^n) - n\epsilon_n \\
 &= nH(X_1|X_2) - n\epsilon_n
 \end{aligned}$$

Therefore by taking $n \rightarrow \infty$, $R_1 \geq H(X_1|X_2)$

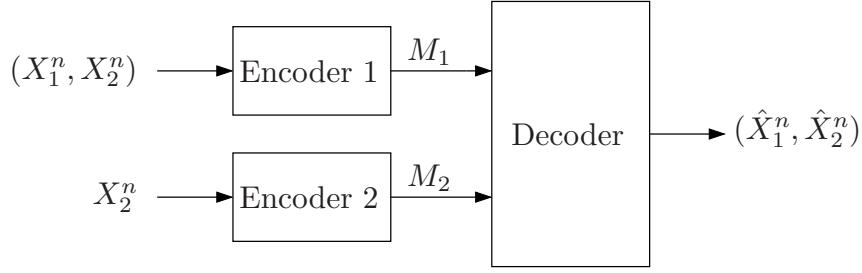
- o Similarly, $R_2 \geq H(X_2|X_1)$
- o Combining the above inequalities shows that if (R_1, R_2) is achievable, then $R_1 \geq H(X_1|X_2)$, $R_2 \geq H(X_2|X_1)$, and $R_1 + R_2 \geq H(X_1, X_2)$

- Here is a plot of the inner and outer bounds on \mathcal{R}



The boundary of the optimal rate region is somewhere in between the boundaries of these regions

- Now, suppose sender 1 knows both X_1 and X_2



Consider the corner point ($R_1 = H(X_1|X_2)$, $R_2 = H(X_2)$) on the boundary of the outer bound

By a conditional version of the lossless source coding theorem, this corner point is achievable as follows:

Let $\epsilon > 0$. We show the rate pair ($R_1 = H(X_1|X_2) + \delta(\epsilon)$, $R_2 = H(X_2) + \delta(\epsilon)$) with $\delta(\epsilon) = \epsilon \cdot \max\{H(X_1|X_2), H(X_2)\}$ is achievable

Encoder 2 uses the encoding procedure of the lossless source coding theorem

For each typical x_2^n , encoder 1 assigns a unique index $m_1 \in [1 : 2^{nR_1}]$ to each $x_1^n \in \mathcal{T}_\epsilon^{(n)}(X_1|x_2^n)$, and assigns the index $m_1 = 1$ to all atypical (x_1^n, x_2^n) sequences

Upon receiving (m_1, m_2) , the decoder first declares $\hat{x}_2^n = x_2^n(m_2)$ for the unique sequence $x_2^n(m_2) \in \mathcal{T}_\epsilon^{(n)}(X_2)$. It then declares $\hat{x}_1^n = x_1^n(m_1, m_2)$ for the unique sequence $x_1^n(m_1, m_2) \in \mathcal{T}_\epsilon^{(n)}(X_1|x_2^n(m_2))$

By the choice of the rate pair, the decoder makes an error only if $(X_1^n, X_2^n) \notin \mathcal{T}_\epsilon^{(n)}(X_1, X_2)$. By the LLN, the probability of this event $\rightarrow 0$ as $n \rightarrow \infty$

- Slepian and Wolf showed that this corner point is achievable even when sender 1 does *not* know X_2 . Thus the sum rate $R_1 + R_2 = H(X_1, X_2) + \delta(\epsilon)$ is achievable even though the sources are separately encoded, and the outer bound is tight!

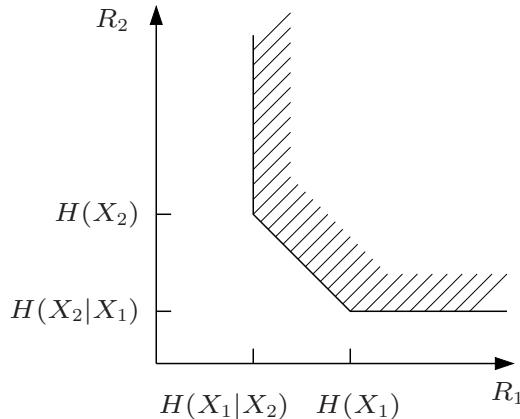
The Slepian–Wolf Theorem

- *Slepian–Wolf Theorem [1]:* The optimal rate region \mathcal{R} for distributed coding of a 2-DMS $(\mathcal{X}_1 \times \mathcal{X}_2, p(x_1, x_2))$ is the set of (R_1, R_2) pairs such that

$$R_1 \geq H(X_1|X_2),$$

$$R_2 \geq H(X_2|X_1),$$

$$R_1 + R_2 \geq H(X_1, X_2)$$



- This result can significantly reduce the total transmission rate as illustrated in the following examples

- Example: Consider a *doubly symmetric binary source* (DSBS(p)) (X_1, X_2) , where X_1 and X_2 are binary with $p_{X_1, X_2}(0, 0) = p_{X_1, X_2}(1, 1) = (1 - p)/2$ and $p_{X_1, X_2}(0, 1) = p_{X_1, X_2}(1, 0) = p/2$, i.e., $X_1 \sim \text{Bern}(1/2)$ and $X_2 \sim \text{Bern}(1/2)$ are connected through a BSC(p) with noise $Z := X_1 \oplus X_2 \sim \text{Bern}(p)$
 - Suppose $p = 0.055$. Then the joint pmf of the DSBS is $p_{X_1, X_2}(0, 0) = 0.445$, $p_{X_1, X_2}(0, 1) = 0.055$, $p_{X_1, X_2}(1, 0) = 0.055$, and $p_{X_1, X_2}(1, 1) = 0.445$, and the sources X_1, X_2 are highly dependent

Assume we wish to send 100 bits of each source

 - We could send all the 100 bits from each source, making 200 bits in all
 - If we decided to compress the information independently, then we would still need $100H(0.5) = 100$ bits of information for each source for a total of 200 bits
 - If instead we use Slepian–Wolf coding, we need to send only a total of $H(X_1) + H(X_2|X_1) = 100H(0.5) + 100H(0.11) = 100 + 50 = 150$ bits

- In general, with Slepian–Wolf coding, we can encode DSBS(p) with

$$R_1 \geq H(p),$$

$$R_2 \geq H(p),$$

$$R_1 + R_2 \geq 1 + H(p)$$

- Example: Suppose X_1 and X_2 are binary with $p_{X_1, X_2}(0, 0) = p_{X_1, X_2}(1, 0) = p_{X_1, X_2}(1, 1) = 1/3$. If we compress each source independently, then we need $R_1 \geq H(1/3)$, $R_2 \geq H(1/3)$ bits per symbol. On the other hand, with the Slepian–Wolf coding, we need only

$$R_1 \geq \log 3 - H(1/3) = 2/3,$$

$$R_2 \geq 2/3,$$

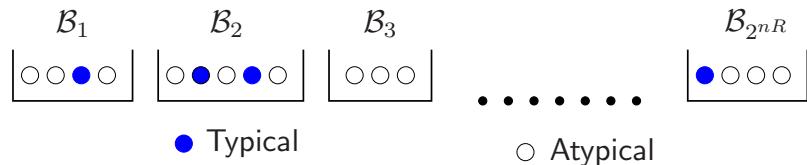
$$R_1 + R_2 \geq \log 3$$

- We already proved the converse to the Slepian–Wolf theorem. Achievability involves the new idea of *random binning*

Lossless Source Coding Revisited: Cover's Random Binning

- Consider the following *random binning* achievability proof for the single source lossless source coding problem
- Codebook generation: Randomly and independently assign an index $m(x^n) \in [1 : 2^{nR}]$ to each sequence $x^n \in \mathcal{X}^n$ according to a uniform pmf over $[1 : 2^{nR}]$. We will refer to each subset of sequences with the same index m as a *bin* $\mathcal{B}(m)$, $m \in [1 : 2^{nR}]$

The chosen bin assignments is revealed to the encoder and decoder



- Encoding: Upon observing $x^n \in \mathcal{B}(m)$, the encoder sends the bin index m
- Decoding: Upon receiving m , the decoder declares that \hat{x}^n to be the estimate of the source sequence if it is the unique typical sequence in $\mathcal{B}(m)$; otherwise it declares an error

- A decoding error occurs if x^n is not typical, or if there is more than one typical sequence in $\mathcal{B}(m)$
- Now we show that if $R > H(X)$, the probability of error averaged over random binnings $\rightarrow 0$ as $n \rightarrow \infty$
- Analysis of the probability of error: We bound the probability of error averaged over X^n and random binnings. Let M denote the random bin index of X^n , i.e., $X^n \in \mathcal{B}(M)$. Note that $M \sim \text{Unif}[1 : 2^{nR}]$, independent of X^n

An error occurs iff

$$\begin{aligned}\mathcal{E}_1 &:= \{X^n \notin \mathcal{T}_\epsilon^{(n)}\}, \text{ or} \\ \mathcal{E}_2 &:= \{\tilde{x}^n \in \mathcal{B}(M) \text{ for some } \tilde{x}^n \neq X^n, \tilde{x}^n \in \mathcal{T}_\epsilon^{(n)}\}\end{aligned}$$

Then, by symmetry of codebook construction, the average probability of error is

$$\begin{aligned}\mathsf{P}(\mathcal{E}) &= \mathsf{P}(\mathcal{E}_1 \cup \mathcal{E}_2) \\ &\leq \mathsf{P}(\mathcal{E}_1) + \mathsf{P}(\mathcal{E}_2) \\ &= \mathsf{P}(\mathcal{E}_1) + \mathsf{P}(\mathcal{E}_2 | X^n \in \mathcal{B}(1))\end{aligned}$$

We now bound each probability of error term

- By the LLN, $\mathsf{P}(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$

- For the second probability of error term, consider

$$\begin{aligned}\mathsf{P}(\mathcal{E}_2 | X^n \in \mathcal{B}(1)) &= \sum_{x^n} \mathsf{P}\{X^n = x^n | X^n \in \mathcal{B}(1)\} \mathsf{P}\{\tilde{x}^n \in \mathcal{B}(1) \text{ for some } \tilde{x}^n \neq x^n, \\ &\quad \tilde{x}^n \in \mathcal{T}_\epsilon^{(n)} | x^n \in \mathcal{B}(1), X^n = x^n\} \\ &\stackrel{(a)}{\leq} \sum_{x^n} p(x^n) \sum_{\substack{\tilde{x}^n \in \mathcal{T}_\epsilon^{(n)} \\ \tilde{x}^n \neq x^n}} \mathsf{P}\{\tilde{x}^n \in \mathcal{B}(1) | x^n \in \mathcal{B}(1), X^n = x^n\} \\ &\stackrel{(b)}{=} \sum_{x^n} p(x^n) \sum_{\substack{\tilde{x}^n \in \mathcal{T}_\epsilon^{(n)} \\ \tilde{x}^n \neq x^n}} \mathsf{P}\{\tilde{x}^n \in \mathcal{B}(1)\} \\ &\leq |\mathcal{T}_\epsilon^{(n)}| \cdot 2^{-nR} \\ &\leq 2^{n(H(X) + \delta(\epsilon))} 2^{-nR},\end{aligned}$$

where (a) and (b) follow because for $\tilde{x}^n \neq x^n$, the events $\{x^n \in \mathcal{B}(1)\}$, $\{\tilde{x}^n \in \mathcal{B}(1)\}$, and $\{X^n = x^n\}$ are mutually independent

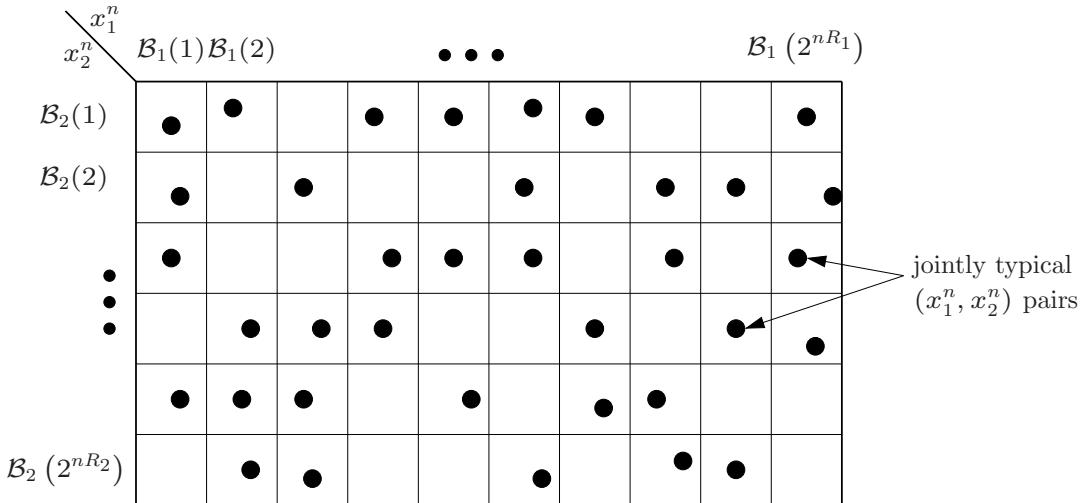
- Thus if $R > H(X) + \delta(\epsilon)$, the probability of error averaged over random binnings $\rightarrow 0$ as $n \rightarrow \infty$. Hence, there must exist at least one sequence of binnings with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$

- Remark: Note that in this proof, we have used only *pairwise* independence of bin assignments

Hence if X is binary, we can use a random *linear* binning (hashing), i.e., $m(x^n) = H x^n$, where $m \in [1 : 2^{nR}]$ is represented by a vector of nR bits, and elements of the $nR \times n$ “parity-check” random binary matrix H are generated i.i.d. $\text{Bern}(1/2)$ (cf. Lecture Notes 3). This result can be extended to the more general case in which $|\mathcal{X}|$ is equal to the cardinality of a finite field

Achievability of the Slepian-Wolf Region [2]

- Codebook generation: Randomly and independently assign an index $m_1(x_1^n)$ to each sequence $x_1^n \in \mathcal{X}_1^n$ according to a uniform pmf over $[1 : 2^{nR_1}]$. The sequences with the same index m_1 form a bin $\mathcal{B}_1(m_1)$. Similarly assign an index $m_2(x_2^n) \in [1 : 2^{nR_2}]$ to each sequence $x_2^n \in \mathcal{X}_2^n$. The sequences with the same index m_2 form a bin $\mathcal{B}_2(m_2)$



The bin assignments are revealed to the encoders and decoder

- Encoding: Observing $x_1^n \in \mathcal{B}_1(m_1)$, encoder 1 sends m_1 . Similarly, observing $x_2^n \in \mathcal{B}_2(m_2)$, encoder 2 sends m_2
- Decoding: Given the received index pair (m_1, m_2) , the decoder declares that $(\hat{x}_1^n, \hat{x}_2^n)$ to be the estimate of the source pair if it is the unique jointly typical pair in the product bin $\mathcal{B}_1(m_1) \times \mathcal{B}_2(m_2)$; otherwise it declares an error
- An error occurs iff $(x_1^n, x_2^n) \notin \mathcal{T}_\epsilon^{(n)}$ or there exists a jointly typical pair $(\tilde{x}_1^n, \tilde{x}_2^n) \neq (x_1^n, x_2^n)$ such that $(\tilde{x}_1^n, \tilde{x}_2^n) \in \mathcal{B}_1(m_1) \times \mathcal{B}_2(m_2)$
- Analysis of the probability of error: We bound the probability of error averaged over (X_1^n, X_2^n) and random binnings. Let M_1 and M_2 denote the random bin indices for X_1^n and X_2^n , respectively

An error occurs iff

$$\mathcal{E}_1 := \{(X_1^n, X_2^n) \notin \mathcal{T}_\epsilon^{(n)}\}, \text{ or}$$

$$\mathcal{E}_2 := \{\tilde{x}_1^n \in \mathcal{B}_1(M_1) \text{ for some } \tilde{x}_1^n \neq X_1^n, (\tilde{x}_1^n, X_2^n) \in \mathcal{T}_\epsilon^{(n)}\}, \text{ or}$$

$$\mathcal{E}_3 := \{\tilde{x}_2^n \in \mathcal{B}_2(M_2) \text{ for some } \tilde{x}_2^n \neq X_2^n, (X_1^n, \tilde{x}_2^n) \in \mathcal{T}_\epsilon^{(n)}\}, \text{ or}$$

$$\mathcal{E}_4 := \{\tilde{x}_1^n \in \mathcal{B}_1(M_1), \tilde{x}_2^n \in \mathcal{B}_2(M_2) \text{ for some } \tilde{x}_1^n \neq X_1^n, \tilde{x}_2^n \neq X_2^n, (\tilde{x}_1^n, \tilde{x}_2^n) \in \mathcal{T}_\epsilon^{(n)}\}$$

Then, by the symmetry of codebook construction, the average probability of error is upper bounded by

$$\begin{aligned} P(\mathcal{E}) &\leq P(\mathcal{E}_1) + P(\mathcal{E}_2) + P(\mathcal{E}_3) + P(\mathcal{E}_4) \\ &= P(\mathcal{E}_1) + P(\mathcal{E}_2 | X_1^n \in \mathcal{B}_1(1)) + P(\mathcal{E}_3 | X_2^n \in \mathcal{B}_2(1)) \\ &\quad + P(\mathcal{E}_4 | (X_1^n, X_2^n) \in \mathcal{B}_1(1) \times \mathcal{B}_2(1)) \end{aligned}$$

Now we bound each probability of error term

- By the LLN, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$
- Now consider the second probability of error term. Following similar steps to the single-source lossless source coding problem discussed before, we have

$$\begin{aligned} P(\mathcal{E}_2 | X_1^n \in \mathcal{B}_1(1)) &= \sum_{(x_1^n, x_2^n)} p(x_1^n, x_2^n) P\{\tilde{x}_1^n \in \mathcal{B}_1(1) \text{ for some } \tilde{x}_1^n \neq x_1^n, \\ &\quad (\tilde{x}_1^n, x_2^n) \in \mathcal{T}_\epsilon^{(n)} | x_1^n \in \mathcal{B}_1(1), (X_1^n, X_2^n) = (x_1^n, x_2^n)\} \\ &\leq \sum_{(x_1^n, x_2^n)} p(x_1^n, x_2^n) \sum_{\substack{(\tilde{x}_1^n, x_2^n) \in \mathcal{T}_\epsilon^{(n)}, \\ \tilde{x}_1^n \neq x_1^n}} P\{\tilde{x}_1^n \in \mathcal{B}(1)\} \\ &\leq 2^{-nR_1} \cdot 2^{n(H(X_1|X_2)+\delta(\epsilon))}, \end{aligned}$$

which $\rightarrow 0$ as $n \rightarrow \infty$ if $R_1 > H(X_1|X_2) + \delta(\epsilon)$

- Similarly, $P(\mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$ if $R_2 > H(X_2|X_1) + \delta(\epsilon)$ and $P(\mathcal{E}_4) \rightarrow 0$ if $R_1 + R_2 > H(X_1, X_2) + \delta(\epsilon)$

Thus the probability of error averaged over all random binnings $\rightarrow 0$ as $n \rightarrow \infty$, if (R_1, R_2) is in the interior of \mathcal{R} . Hence there exists a sequence of binnings with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$

- Remarks:

- Slepian–Wolf theorem *does not* in general hold for zero-error coding (using variable-length codes). In fact, for many sources, the optimal rate region is [3]:

$$\begin{aligned} R_1 &\geq H(X_1), \\ R_2 &\geq H(X_2) \end{aligned}$$

An example is the doubly symmetric binary symmetric sources X_1 and X_2 with joint pmf $p(0,0) = p(1,1) = 0.445$ and $p(0,1) = p(1,0) = 0.055$.

Error-free distributed encoding of these sources requires $R_1 = R_2 = 1$, i.e., no compression is possible

- The above achievability proof can be extended to any pair of stationary and ergodic sources X_1 and X_2 with joint entropy rates $\bar{H}(X_1, X_2)$ [2]. Since the converse can also be easily extended, the Slepian–Wolf theorem for this larger class of correlated sources is given by the set of (R_1, R_2) rate pairs such that

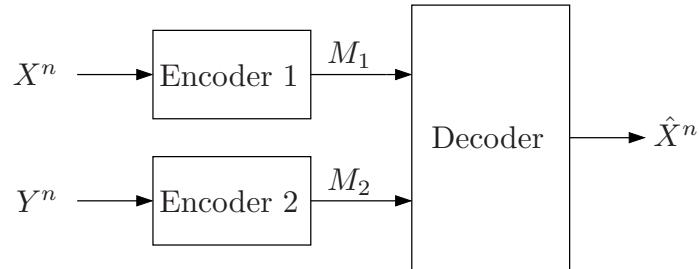
$$\begin{aligned} R_1 &\geq \bar{H}(X_1|X_2) := \bar{H}(X_1, X_2) - \bar{H}(X_2), \\ R_2 &\geq \bar{H}(X_2|X_1) := \bar{H}(X_1, X_2) - \bar{H}(X_1), \\ R_1 + R_2 &\geq \bar{H}(X_1, X_2) \end{aligned}$$

- If X_1 and X_2 are binary, we can use random *linear* binnings $m_1(x_1^n) = H_1 x_1^n$, $m_2(x_2^n) = H_2 x_2^n$, where H_1 and H_2 are independent and their entries are generated i.i.d. $\text{Bern}(1/2)$. If X_1 and X_2 are doubly symmetric as well (i.e., $Z = X_1 \oplus X_2 \sim \text{Bern}(p)$), then the following simpler coding scheme based on single-source linear binning is possible

Consider the corner point $(R_1, R_2) = (1, H(p))$ of the optimal rate region. Suppose X_1^n is sent uncoded while X_2^n is encoded as $H X_2^n$ with a randomly generated $n(H(p) + \delta(\epsilon)) \times n$ parity check matrix H . The decoder can calculate $H X_1^n \oplus H X_2^n = H Z^n$, from which \hat{Z}^n can be recovered as in the single-source lossless source coding via linear binning. Since $\hat{Z}^n = Z^n$ with high probability, $\hat{Y}_2^n = X_2^n \oplus \hat{Z}^n = X_2^n$ with high probability

Lossless Source Coding with a Helper

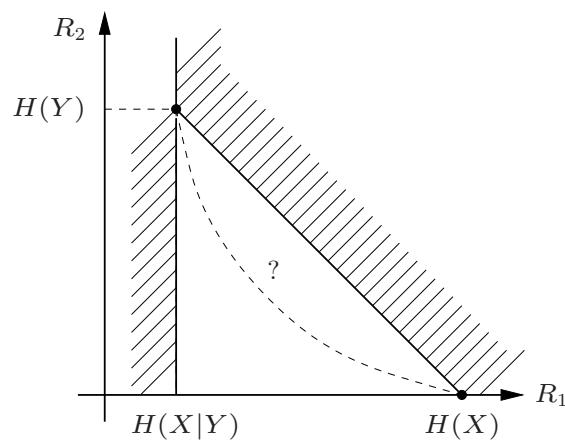
- Consider the distributed lossless source coding setup, where only one of the two sources is to be recovered losslessly and the encoder for the other source (helper) provides *side information* to the decoder to help reduce the first encoder's rate



- The definition of a code, achievability, and optimal rate region \mathcal{R} are similar to the distributed lossless source coding setup we discussed earlier

Simple Inner and Outer Bounds on \mathcal{R}

- At $R_2 = 0$ (no helper), $R_1 \geq H(X)$ is necessary and sufficient
- At $R_2 \geq H(Y)$ (lossless helper), by the Slepian–Wold theorem $R_1 \geq H(X|Y)$ is necessary and sufficient
- These two extreme points lead to a time-sharing inner bound and a trivial outer bound



- Neither bound is tight in general

Optimal Rate Region

- *Theorem 2* [4, 5]: Let (X, Y) be a 2-DMS. The optimal rate region \mathcal{R} for lossless source coding with a helper is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\geq H(X|U), \\ R_2 &\geq I(Y; U) \end{aligned}$$

for some $p(u|y)$, where $|\mathcal{U}| \leq |\mathcal{Y}| + 1$

- The above region is convex
- Example: Let (X, Y) be DSBS(p), $p \in [0, 1/2]$

The optimal region reduces to the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\geq H(\alpha * p), \\ R_2 &\geq 1 - H(\alpha) \end{aligned}$$

for some $\alpha \in [0, 1/2]$

It is straightforward to show that the above region is achieved by taking $p(u|y)$ to be a BSC(α) from Y to U

The proof of optimality uses Mrs. Gerber's lemma as in the converse for the binary symmetric BC in Lecture Notes 5

First, note that $H(p) \leq H(X|U) \leq 1$. Thus there exists an $\alpha \in [0, 1/2]$ such that $H(X|U) = H(\alpha * p)$

By the scalar Mrs. Gerber's lemma,

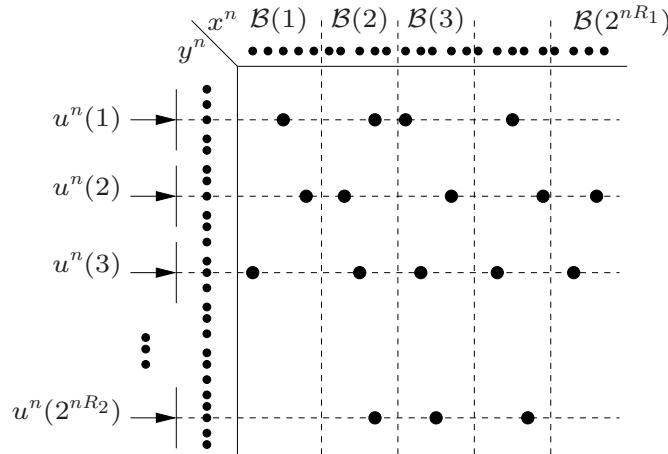
$H(X|U) = H(Y \oplus Z|U) \geq H(H^{-1}(H(Y|U)) * p)$, since given U , Z and Y remain independent

Thus, $H^{-1}(H(Y|U)) \leq \alpha$, which implies that

$$\begin{aligned} I(Y; U) &= H(Y) - H(Y|U) \\ &= 1 - H(Y|U) \\ &\geq 1 - H(\alpha) \end{aligned}$$

Proof of Achievability

- Encoder 2 uses jointly typicality encoding to describe Y^n with U^n , and encoder 1 uses random binning to help the decoder recover X^n given that it knows U^n . Fix $p(u|y)$. Randomly generate 2^{nR_2} u^n sequences. Encoder 2 sends the index m_2 of a jointly typical u^n with y^n
- Randomly partition the set of x^n sequences into 2^{nR_1} bins. Encoder 1 sends the bin index of x^n



- The decoder finds a unique $\hat{x}^n \in \mathcal{B}(m_1)$ that is jointly typical with $u^n(m_2)$
Now, for the details
- Codebook generation: Fix $p(u|y)$; then $p(u) = \sum_y p(y)p(u|y)$
Randomly and independently assign an index $m_1(x^n) \in [1 : 2^{nR_1}]$ to each sequence $x^n \in \mathcal{X}^n$. The set of sequences with the same index m_1 form a bin $\mathcal{B}(m_1)$
Randomly and independently generate 2^{nR_2} sequences $u^n(m_2)$, $m_2 \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_U(u_i)$
- Encoding: If $x^n \in \mathcal{B}(m_1)$, encoder 1 sends m_1
Encoder 2 finds an index m_2 such that $(u^n(m_2), y^n) \in \mathcal{T}_{\epsilon'}^{(n)}$
If there is more than one such m_2 , it sends the smallest index
If there is no such $u^n(m_2)$, it sends $m_2 = 1$
- Decoding: The receiver finds the unique $\hat{x}^n \in \mathcal{B}(m_1)$ such that $(\hat{x}^n, u^n(m_2)) \in \mathcal{T}_{\epsilon}^{(n)}$
If there is none or more than one, it declares an error

- Analysis of the probability of error: Assume that M_1 and M_2 are the chosen indices for encoding X^n and Y^n , respectively. Define the error events

$$\begin{aligned}\mathcal{E}_1 &:= \{(U^n(m_2), Y^n) \notin \mathcal{T}_{\epsilon'}^{(n)} \text{ for all } m_2 \in [1 : 2^{nR_2})\}, \\ \mathcal{E}_2 &:= \{(U^n(M_2), X^n) \notin \mathcal{T}_{\epsilon}^{(n)}\}, \\ \mathcal{E}_3 &:= \{\tilde{x}^n \in \mathcal{B}(M_1), (\tilde{x}^n, U^n(M_2)) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } \tilde{x}^n \neq X^n\}\end{aligned}$$

Then the probability of error is bounded by

$$P(\mathcal{E}) \leq P(\mathcal{E}_1) + P(\mathcal{E}_1^c \cap \mathcal{E}_2) + P(\mathcal{E}_3 | X^n \in \mathcal{B}(1))$$

We now bound each term

1. By the covering lemma, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ if $R_2 > I(Y; U) - \delta(\epsilon')$
2. By the conditional typicality lemma, $P(\mathcal{E}_1^c \cap \mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$

3. Finally consider

$$\begin{aligned}P(\mathcal{E}_3 | X^n \in \mathcal{B}(1)) &= \sum_{(x^n, u^n)} P\{(X^n, U^n) = (x^n, u^n) \mid X^n \in \mathcal{B}(1)\} \\ &\quad \cdot P\{\tilde{x}^n \in \mathcal{B}(1) \text{ for some } \tilde{x}^n \neq x^n, \\ &\quad \quad (\tilde{x}^n, u^n) \in \mathcal{T}_{\epsilon}^{(n)} \mid X^n \in \mathcal{B}(1), (X^n, U^n) = (x^n, u^n)\} \\ &\leq \sum_{(x^n, u^n)} p(x^n, u^n) \sum_{\substack{\tilde{x}^n \in \mathcal{T}_{\epsilon}^{(n)}(X|u^n) \\ \tilde{x}^n \neq x^n}} P\{\tilde{x}^n \in \mathcal{B}(1)\} \\ &\leq 2^{n(H(X|U)+\delta(\epsilon))} 2^{-nR_1},\end{aligned}$$

which $\rightarrow 0$ as $n \rightarrow \infty$ if $R_1 > H(X|U) + \delta(\epsilon)$

This completes the proof of achievability

Proof of Converse

- Let M_1 and M_2 denote the indices from encoders 1 and 2, respectively

By Fano's inequality, $H(X^n|M_1, M_2) \leq n\epsilon_n$

- First consider

$$\begin{aligned}
 nR_2 &\geq H(M_2) \\
 &\geq I(Y^n; M_2) \\
 &= \sum_{i=1}^n I(Y_i; M_2 | Y^{i-1}) \\
 &= \sum_{i=1}^n I(Y_i; M_2, Y^{i-1}) \\
 &\stackrel{(a)}{=} \sum_{i=1}^n I(Y_i; M_2, Y^{i-1}, X^{i-1}),
 \end{aligned}$$

where (a) follows because $X^{i-1} \rightarrow (M_2, Y^{i-1}) \rightarrow Y_i$ form a Markov chain

Define $U_i := (M_2, Y^{i-1}, X^{i-1})$. Note that $U_i \rightarrow Y_i \rightarrow X_i$ form a Markov chain

Thus we have shown that

$$nR_2 \geq \sum_{i=1}^n I(U_i; Y_i)$$

- Next consider

$$\begin{aligned}
 nR_1 &\geq H(M_1) \\
 &\geq H(M_1 | M_2) \\
 &= H(M_1 | M_2) + H(X^n | M_1, M_2) - H(X^n | M_1, M_2) \\
 &\geq H(X^n, M_1 | M_2) - n\epsilon_n \\
 &= H(X^n | M_2) - n\epsilon_n \\
 &= \sum_{i=1}^n H(X_i | M_2, X^{i-1}) - n\epsilon_n \\
 &\geq \sum_{i=1}^n H(X_i | M_2, X^{i-1}, Y^{i-1}) - n\epsilon_n \\
 &= \sum_{i=1}^n H(X_i | U_i) - n\epsilon_n
 \end{aligned}$$

- Using a time-sharing random variable $Q \sim \text{Unif}[1 : n]$ and independent of (X^n, Y^n, U^n) , we obtain

$$R_1 \geq \frac{1}{n} \sum_{i=1}^n H(X_i | U_i, Q = i) = H(X_Q | U_Q, Q),$$

$$R_2 \geq \frac{1}{n} \sum_{i=1}^n I(Y_i; U_i | Q = i) = I(Y_Q; U_Q | Q)$$

Since Q is independent of Y_Q (why?)

$$I(Y_Q; U_Q | Q) = I(Y_Q; U_Q, Q)$$

Defining $X := U_Q$ $Y := Y_Q$, $U := (U_Q, Q)$, we have shown the existence of U such that

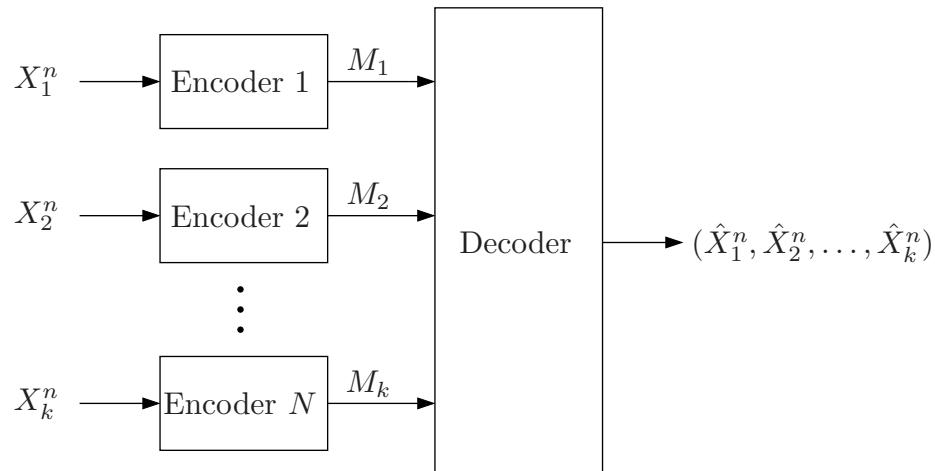
$$\begin{aligned} R_1 &\geq H(X | U), \\ R_2 &\geq I(Y; U) \end{aligned}$$

for some $p(u|y)$, where $U \rightarrow Y \rightarrow X$ form a Markov chain

- Remark: The bound on the cardinality of U can be proved using the technique described in Appendix C

Extension to More Than Two Sources

- The Slepian–Wolf theorem can be extended to k -DMS (X_1, \dots, X_k)



- Theorem 3:* The optimal rate region $\mathcal{R}(X_1, X_2, \dots, X_k)$ for k -DMS (X_1, \dots, X_k) is the set of rate tuples (R_1, R_2, \dots, R_k) such that

$$\sum_{j \in \mathcal{S}} R_j \geq H(X(\mathcal{S}) | X(\mathcal{S}^c)) \text{ for all } \mathcal{S} \subseteq [1 : k]$$

- For example, $\mathcal{R}(X_1, X_2, X_3)$ is the set of rate triples (R_1, R_2, R_3) such that

$$\begin{aligned} R_1 &\geq H(X_1 | X_2, X_3), \\ R_2 &\geq H(X_2 | X_1, X_3), \\ R_3 &\geq H(X_3 | X_1, X_2), \\ R_1 + R_2 &\geq H(X_1, X_2 | X_3), \\ R_1 + R_3 &\geq H(X_1, X_3 | X_2), \\ R_2 + R_3 &\geq H(X_2, X_3 | X_1), \\ R_1 + R_2 + R_3 &\geq H(X_1, X_2, X_3) \end{aligned}$$

- Theorem 2 can be generalized to k sources (X_1, X_2, \dots, X_k) and a helper Y

Theorem 4: Consider a $(k+1)$ -DMS $(X_1, X_2, \dots, X_k, Y)$. The optimal rate region for the lossless source coding of (X_1, X_2, \dots, X_k) with helper Y is the set of rate tuples $(R_1, R_2, \dots, R_k, R_{k+1})$ such that

$$\begin{aligned} \sum_{j \in \mathcal{S}} R_j &\geq H(X(\mathcal{S}) | U, X(\mathcal{S})) \quad \text{for all } \mathcal{S} \in [1 : k], \\ R_{k+1} &\geq I(Y; U) \end{aligned}$$

for some $p(u|y)$ with $|\mathcal{U}| \leq |\mathcal{Y}| + 2^k - 1$.

- The optimal rate region is not known in general for the lossless source coding with more than one helper even when there is only one source to be recovered

Key New Ideas and Techniques

- Optimal rate region
- Random binning
- Source coding via random linear code
- Limit for lossless distributed source coding can be smaller than that for zero-error coding

References

- [1] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, pp. 471–480, July 1973.
- [2] T. M. Cover, "A proof of the data compression theorem of Slepian and Wolf for ergodic sources," *IEEE Trans. Inf. Theory*, vol. 21, no. 2, pp. 226–228, Mar. 1975.
- [3] A. El Gamal and A. Orlitsky, "Interactive data compression," in *Proceedings of the 25th Annual Symposium on Foundations of Computer Science*, Washington, DC, Oct. 1984, pp. 100–108.
- [4] R. F. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, 1975.
- [5] A. D. Wyner, "On source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 21, pp. 294–300, 1975.

Lecture Notes 12

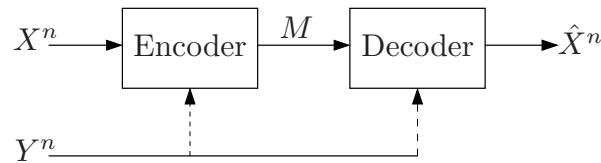
Source Coding with Side Information

- Problem Setup
- Simple Special Cases
- Causal Side information Available at Decoder
- Noncausal Side Information Available at the Decoder
- Source Coding when Side Information May Be Absent
- Key New Ideas and Techniques
- Appendix: Proof of Lemma 1

© Copyright 2002–2010 Abbas El Gamal and Young-Han Kim

Problem Setup

- Let (X, Y) be a 2-DMS and $d(x, \hat{x})$ be a distortion measure. The encoder generates a description of the source X and sends it to a decoder who has *side information* Y and wishes to reproduce X with distortion D (e.g., X is the Mona Lisa and Y is Leonardo da Vinci). What is the optimal tradeoff between the description rate and the distortion?



- As in the channel with state, there are many possible scenarios of side information availability
 - Side information may be available at the encoder, the decoder, or both
 - Side information may be available fully or encoded
 - At the decoder, side information may be available noncausally (the entire side information sequence is available for reconstruction) or causally (the side information sequence is available on the fly for each reconstruction symbol)
- For each set of assumptions, a $(2^{nR}, n)$ code, achievability, and rate-distortion function are defined as for the point-to-point lossy source coding setup

Simple Special Cases

- With no side information, the rate–distortion function is

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

In the lossless case, the optimal compression rate, which corresponds to $R(0)$ under the Hamming distortion measure (cf. Lecture Notes 3), is $R^* = H(X)$

- Side information available only at the encoder does not help (why?) and the rate–distortion function remains the same, that is,

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

For the lossless case, $R_{\text{SI-E}}^* = R^* = H(X)$

- Side information available at both the encoder and decoder: It is easy to show that the rate–distortion function in this case is

$$R_{\text{SI-ED}}(D) = \min_{p(\hat{x}|x,y): E(d(X, \hat{X})) \leq D} I(X; \hat{X}|Y)$$

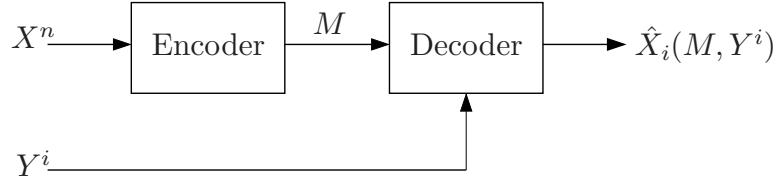
For the lossless case, this reduces to $R_{\text{SI-ED}}^* = H(X|Y)$, which follows by the lossless source coding theorem

Side information Available Only at the Decoder

- We consider yet another special case of side information availability. Suppose the side information sequence is available only at the decoder
- This is the most interesting special case. Here the rate–distortion function depends on whether the side information is available causally or noncausally
- This problem is in a sense dual to channel coding for DMC with DM state available only at the encoder in Lecture Notes 7. As we will see, the expressions for the rate–distortion functions $R_{\text{CSI-D}}$ and $R_{\text{SI-D}}$ for the causal and noncausal cases are dual to the capacity expressions for $C_{\text{CSI-E}}$ and $C_{\text{SI-E}}$, respectively

Causal Side information Available at Decoder

- We first consider the case in which side information is available *causally* at the decoder



- Formally, a $(2^{nR}, n)$ rate–distortion code with side information available causally at the decoder consists of
 1. An encoder that assigns an index $m(x^n) \in [1 : 2^{nR}]$ to each $x^n \in \mathcal{X}^n$, and
 2. A decoder that assigns an estimate $\hat{x}_i(m, y^i)$ to each received index m and side information sequence y^i for $i \in [1 : n]$
- The *rate–distortion function with causal side information* available only at the decoder $R_{\text{CSI-D}}(D)$ is the infimum of rates R such that there exists a sequence of $(2^{nR}, n)$ codes with $\limsup_{n \rightarrow \infty} E(d(X^n, \hat{X}^n)) \leq D$

- *Theorem 1* [1]: Let (X, Y) be a 2-DMS and $d(x, \hat{x})$ be a distortion measure. The rate–distortion function for X with causal side information Y available at the decoder is

$$R_{\text{CSI-D}}(D) = \min I(X; U),$$

where the minimum is over all $p(u|x)$ and all functions $\hat{x}(u, y)$ with $|\mathcal{U}| \leq |\mathcal{X}| + 1$, such that $E(d(X, \hat{X})) \leq D$

- Remark: $R_{\text{CSI-D}}(D)$ is nonincreasing, convex, and thus continuous in D

Doubly Symmetric Binary Sources

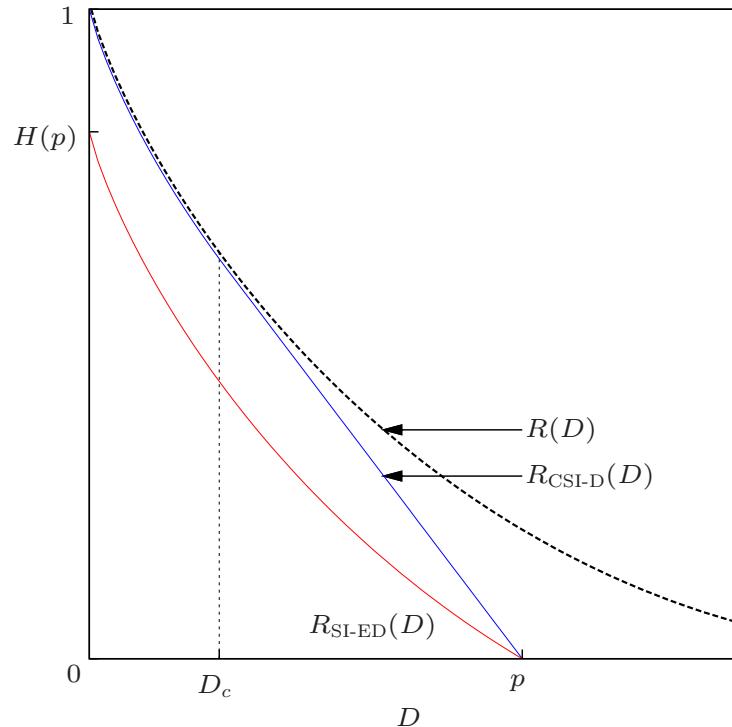
- Let (X, Y) be DSBS(p), $p \in [0, 1/2]$, and assume Hamming distortion measure:
 - No side information: $R(D) = 1 - H(D)$ for $0 \leq D \leq 1/2$, and 0 for $D > 1/2$
 - Side information at both encoder and decoder: $R_{\text{SI-ED}}(D) = H(p) - H(D)$ for $0 \leq D \leq p$, and 0 for $D > p$
 - Side information only at decoder: The rate-distortion function in this case is

$$R_{\text{CSI-D}}(D) = \begin{cases} 1 - H(D), & 0 \leq D \leq D_c \\ (p - D)H'(D_c) & D_c < D \leq p, \end{cases}$$

where H' is the derivative of the binary entropy function, and D_c is the solution to the equation $(1 - H(D_c))/(p - D_c) = H'(D_c)$

Thus $R_{\text{CSI-D}}(D)$ coincides with $R(D)$ for $0 \leq D \leq D_c$, and is otherwise given by the tangent to the graph of $R(D)$ that passes through the point $(p, 0)$ for $D_c \leq D \leq p$. In other words, optimum performance is achieved by time sharing between rate-distortion coding with no side information and zero-rate decoding that uses only the side information. For small enough distortion, this performance is attained by simply ignoring the side information

- Comparison of $R(D)$, $R_{\text{CSI-D}}(D)$, and $R_{\text{SI-ED}}(D)$ for $p = 1/4$:



Proof of Achievability

- As in the achievability of the lossy source coding theorem, we use joint typicality encoding to describe X^n by U^n . The description \hat{X}_i , $i \in [1 : n]$, at the decoder is a function of U_i and the side information Y_i
- Codebook generation: Fix $p(u|x)$ and $\hat{x}(u,y)$ that achieve $R_{\text{CSI-D}}(D/(1+\epsilon))$, where D is the desired distortion
Randomly and independently generate 2^{nR} sequences $u^n(m)$, $m \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_U(u_i)$
- Encoding: Given a source sequence x^n , the encoder finds an index m such that $(u^n(m), x^n) \in \mathcal{T}_{\epsilon'}^{(n)}$. If there is more than one such index, it selects the smallest one. If there is no such index, it selects $m = 1$
The encoder sends the index m to the decoder
- Decoding: The decoder finds the reconstruction $\hat{x}^n(m, y^n)$ by setting $\hat{x}_i = \hat{x}(u_i(m), y_i)$
- Analysis of the expected distortion: Let M denote the chosen index and $\epsilon > \epsilon'$.

Consider the following “error” events

$$\begin{aligned}\mathcal{E}_1 &:= \{(U^n(m), X^n) \notin \mathcal{T}_{\epsilon'}^{(n)} \text{ for all } m \in [1 : 2^{nR}]\}, \\ \mathcal{E}_2 &:= \{(U^n(M), Y^n) \notin \mathcal{T}_{\epsilon}^{(n)}\}\end{aligned}$$

The total probability of “error” $P(\mathcal{E}) = P(\mathcal{E}_1) + P(\mathcal{E}_1^c \cap \mathcal{E}_2)$

We now bound each term:

- By the covering lemma, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ if $R > I(X; U) + \delta(\epsilon')$
- Since $\mathcal{E}_1^c = \{(U^n(M), X^n) \in \mathcal{T}_{\epsilon'}^{(n)}\}$,
 $Y^n | \{U^n(M) = u^n, X^n = x^n\} \sim \prod_{i=1}^n p_{Y|U,X}(y_i | u_i, x_i) = \prod_{i=1}^n p_{Y|X}(y_i | x_i)$,
and $\epsilon > \epsilon'$, by the conditional typicality lemma, $P(\mathcal{E}_1^c \cap \mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$
- Thus, when there is no “error”, $(U^n(M), X^n, Y^n) \in \mathcal{T}_{\epsilon}^{(n)}$ and thus $(X^n, \hat{X}^n) \in \mathcal{T}_{\epsilon}^{(n)}$. By the typical average lemma, the asymptotic distortion averaged over the random codebook and over (X^n, Y^n) is bounded as

$$\limsup_{n \rightarrow \infty} E(d(X^n; \hat{X}^n)) \leq \limsup_{n \rightarrow \infty} (d_{\max} P(\mathcal{E}) + (1 + \epsilon) E(d(X, \hat{X})) P(\mathcal{E}^c)) \leq D$$
if $R > I(X; U) + \delta(\epsilon') = R_{\text{CSI-D}}(D/(1+\epsilon)) + \delta(\epsilon')$
- Finally by the continuity of $R_{\text{CSI-D}}(D)$ in D , taking $\epsilon \rightarrow 0$ shows that any rate $R > R_{\text{CSI-D}}(D)$ is achievable, which completes the proof

Proof of Converse

- Let M denote the index sent by the encoder. In general \hat{X}_i is a function of (M, Y^i) , so we set $U_i := (M, Y^{i-1})$. Note that $U_i \rightarrow X_i \rightarrow Y_i$ form a Markov chain as desired

- Consider

$$\begin{aligned}
nR &\geq H(M) \geq I(X^n; M) \\
&= \sum_{i=1}^n I(X_i; M | X^{i-1}) \\
&= \sum_{i=1}^n I(X_i; M, X^{i-1}) \\
&\stackrel{(a)}{=} \sum_{i=1}^n I(X_i; M, X^{i-1}, Y^{i-1}) \\
&\geq \sum_{i=1}^n I(X_i; U_i)
\end{aligned}$$

$$\begin{aligned}
&\geq \sum_{i=1}^n R_{\text{CSI-D}}(\mathbb{E}(d(X_i, \hat{X}_i))) \\
&\stackrel{(b)}{\geq} nR_{\text{CSI-D}}\left(\frac{1}{n} \sum_{i=1}^n \mathbb{E}(d(X_i, \hat{X}_i))\right),
\end{aligned}$$

where (a) follows by the Markov relation $X_i \rightarrow (M, X^{i-1}) \rightarrow Y^{i-1}$, and (b) follows by convexity of $R_{\text{CSI-D}}(D)$

Since $\limsup_{n \rightarrow \infty} \left((1/n) \sum_{i=1}^n \mathbb{E}(d(X_i, \hat{X}_i)) \right) \leq D$ (by assumption) and $R_{\text{CSI-D}}(D)$ is nonincreasing, $R \geq R_{\text{CSI-D}}(D)$. The cardinality bound on U can be proved using the technique described in Appendix C

Lossless Source Coding with Causal Side Information

- Consider the above source coding problem with causal side information when the decoder wishes to reconstruct X losslessly (i.e., the probability of error $P\{X^n \neq \hat{X}^n\} \rightarrow 0$ as $n \rightarrow \infty$). Denote the optimal compression rate by $R_{\text{CSI-D}}^*$
- Clearly $H(X|Y) \leq R_{\text{CSI-D}}^* \leq H(X)$. Consider some examples:
 1. $X = Y$: $R_{\text{CSI-D}}^* = H(X|Y)(= 0)$
 2. X and Y independent: $R_{\text{CSI}}^* = H(X|Y)(= H(X))$
 3. $X = (Y, Z)$, where Y and Z are independent: $R_{\text{CSI}}^* = H(X|Y)(= H(Z))$
- Theorem 2 [1]:* Let (X, Y) be a 2-DMS. The optimal compression rate for lossless source coding of X with causal side information Y available at the decoder is

$$R_{\text{CSI-D}}^* = \min_{p(u|x)} I(X; U),$$

where the minimum is over $p(u|x)$ with $|\mathcal{U}| \leq |\mathcal{X}| + 1$ such that $H(X|U, Y) = 0$

- Proof of Theorem 2: As in the alternative proof of the lossless source coding theorem (without side information) using random coding and joint typicality encoding in Lecture Notes 3, $R_{\text{CSI-D}}^* = R_{\text{CSI}}(0)$ under Hamming distortion measure. Details of the proof are as follows
 - Proof of converse: Consider the lossy source coding setting with $\mathcal{X} = \hat{\mathcal{X}}$ and d being the Hamming distortion measure, where the minimum in the theorem is evaluated at $D = 0$. Since block error probability $P\{X^n \rightarrow \hat{X}^n\} \rightarrow 0$ is a stronger requirement than average bit-error $E(d(X, \hat{X})) \rightarrow 0$, then by the converse proof of the lossy coding case, it follows that $R_{\text{CSI}}^* \geq R_{\text{CSI}}(0) = \min I(X; U)$, where the minimization is over $p(u|x)$ such that $E(d(X, \hat{x}(U, Y))) = 0$, or equivalently, $\hat{x}(u, y) = x$ for all (x, y, u) with $p(x, y, u) > 0$, $p(x|u, y) = 1$, or equivalently $H(X|U, Y) = 0$
 - Proof of achievability: Consider the proof of achievability for the lossy case. If $(x^n, y^n, u^n(l)) \in \mathcal{T}_\epsilon^{(n)}$ for some $l \in [1 : 2^{nR}]$, then $p_{X,Y,U}(x_i, y_i, u_i(l)) > 0$ for all $i \in [1 : n]$ and hence $\hat{x}(u_i(l), y_i) = x_i$ for all $i \in [1 : n]$. Thus

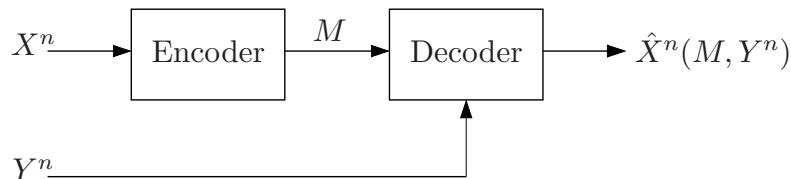
$$P\{\hat{X}^n = X^n | (U^n(l), X^n, Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } l \in [1 : 2^{nR}]\} = 1$$

But, since $P\{(U^n(l), X^n, Y^n) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } l \in [1 : 2^{nR}]\} \rightarrow 0$ as $n \rightarrow \infty$, $P\{\hat{X}^n \neq X^n\} \rightarrow 0$ as $n \rightarrow \infty$

- Now consider the special case, where $p(x, y) > 0$ for all (x, y) . Then the condition in the theorem reduces to $H(X|U) = 0$, or equivalently, $R_{\text{CSI-D}}^* = H(X)$. Thus in this case, side information does not help at all! We show this by contradiction. Suppose $H(X|U) > 0$, then $p(u) > 0$ and $0 < p(x|u) < 1$ for some (x, u) . Note that this also implies that $0 < p(x'|u) < 1$ for some $x' \neq x$. Since we cannot have both $d(x, \hat{x}(u, y)) = 0$ and $d(x', \hat{x}(u, y)) = 0$ hold simultaneously, and by assumption $p_{U,X,Y}(u, x, y) > 0$ and $p_{U,X,Y}(u, x', y) > 0$, then $E(d(X, \hat{x}(U, Y))) > 0$. This is a contradiction since $E(d(X, \hat{x}(U, Y))) = 0$. Thus, $H(X|U) = 0$ and $R_{\text{CSI-D}}^* = H(X)$. Compared to the Slepian–Wolf theorem, Theorem 2 shows that causality of side information can severely limit how encoders can leverage correlation among sources.

Noncausal Side Information Available at the Decoder

- We now consider the case in which side information is available *noncausally* at the decoder. In other words, $(2^{nR}, n)$ code is defined by an encoder $m(x^n)$ and a decoder $\hat{x}^n(m, y^n)$.



- In the lossless case, we know from the Slepian–Wolf theorem that the optimal compression rate is $R_{\text{SI-D}}^* = H(X|Y)$, which is the same rate as when side information is available at both the encoder and decoder.
- In general, can we do as well as if the side information is available at both the encoder and decoder as in the lossless case?

Wyner–Ziv Theorem

- *Wyner–Ziv Theorem* [2]: Let (X, Y) be a 2-DMS and $d(x, \hat{x})$ be a distortion measure. The rate–distortion function for X with side information Y available only at the decoder is

$$R_{\text{SI-D}}(D) = \min (I(X; U) - I(Y; U)) = \min I(X; U|Y),$$

where the minimum is over all conditional pmfs $p(u|x)$ and functions $\hat{x} : \mathcal{Y} \times \mathcal{U} \rightarrow \hat{\mathcal{X}}$ with $|\mathcal{U}| \leq |\mathcal{X}| + 1$ such that $E_{X,Y,U}(d(X, \hat{X})) \leq D$

- Note that $R_{\text{SI-D}}(D)$ is nonincreasing, convex, and thus continuous in D
- Clearly, $R_{\text{SI-ED}}(D) \leq R_{\text{SI-D}}(D) \leq R_{\text{CSI-D}}(D) \leq R(D)$
- The difference between $R_{\text{SI-D}}(D)$ and $R_{\text{CSI-D}}(D)$ is the subtracted term $I(Y; U)$
- Recall that with side information at both the encoder and decoder,

$$R_{\text{SI-ED}}(D) = \min_{p(u|x,y), \hat{x}(u,y)} I(X; U|Y)$$

Hence the difference between $R_{\text{SI-D}}$ and $R_{\text{SI-ED}}$ is in taking the minimum over $p(u|x)$ versus $p(u|x, y)$

Quadratic Gaussian Source Coding with Side Information

- We show that $R_{\text{SI-D}}(D) = R_{\text{SI-ED}}(D)$ for a 2-WGN source (X, Y) and squared error distortion
- Without loss of generality let $X \sim N(0, P)$ and the side information $Y = X + Z$, where $Z \sim N(0, N)$ is independent of X (why?)
- It is easy to show that the rate–distortion function when the side information Y is available at both the encoder and decoder is

$$R_{\text{SI-ED}}(D) = R\left(\frac{P'}{D}\right),$$

where $P' := \text{Var}(X|Y) = PN/(P + N)$

- Now, consider the Wyner-Ziv setup: Clearly, $R(D) = 0$ if $D \geq P'$. Consider $0 < D \leq P'$. Choose the auxiliary random variable $U = X + V$, where $V \sim N(0, Q)$ is independent of X and Y

Selecting $Q = P'D/(P' - D)$, it is easy to verify that

$$I(X; U|Y) = R\left(\frac{P'}{D}\right)$$

Now, let the reconstruction \hat{X} be the minimum MSE estimate of X given U and Y

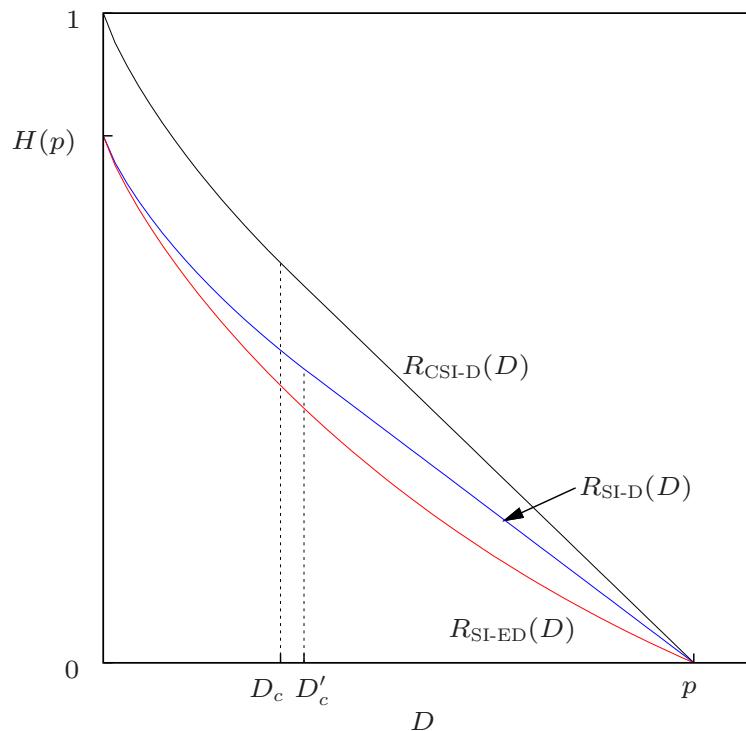
Thus $E[(X - \hat{X})^2] = \text{Var}(X|U, Y)$. Verify that it is equal to D

- Thus for Gaussian sources and squared error distortion, $R_{\text{SI-ED}}(D) = R_{\text{SI-ED}}(D)$
- This surprising result does not hold in general, however. For example, consider the case of DSBS(p), $p \in [0, 1/2]$, and Hamming distortion measure. The rate distortion function for this case is

$$R_{\text{SI-D}}(D) = \begin{cases} g(D), & 0 \leq D \leq D'_c \\ (p - D)g'(D'_c), & D_c < D \leq p, \end{cases}$$

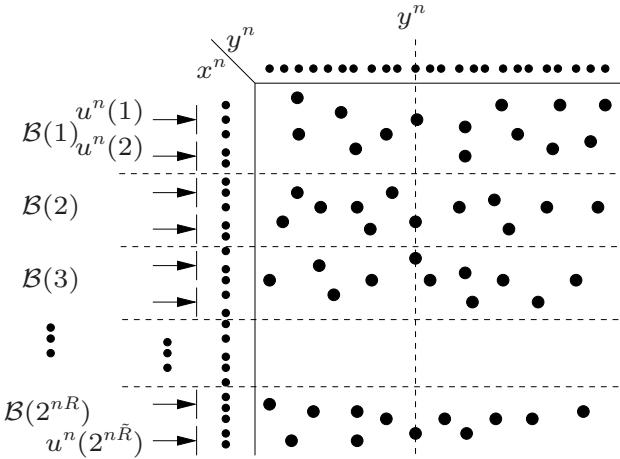
where $g(D) = H(p * D) - H(D)$, g' is the derivative of g , and D'_c is the solution to the equation $g(D'_c)/(p - D'_c) = g'(D'_c)$. It can be easily shown that $R_{\text{SI-D}}(D) < R_{\text{SI-ED}}(D) = H(p) - H(D)$ for all $D \in (0, p)$; thus there is a nonzero cost for the lack of side information at the encoder

Comparison of $R_{\text{CSI-D}}(D)$, $R_{\text{SI-D}}(D)$, and $R_{\text{SI-ED}}(D)$ for $p = 1/4$:



Outline of Achievability

- Again we use joint typicality encoding to describe X^n by U^n . Since U^n is correlated with Y^n , we use binning to reduce the encoding rate. Fix $p(u|x)$, $\hat{x}(u,y)$. Generate $2^{nI(X;U)}$ $u^n(l)$ sequences and partition them into 2^{nR} bins
- Given x^n find a jointly typical u^n sequence. Send the bin index of u^n



- The decoder finds unique $u^n(l) \in \mathcal{B}(m)$ that is jointly typical with y^n and constructs the description $\hat{x}_i = \hat{x}(u_i, y_i)$ for $i \in [1 : n]$

Proof of Achievability

- Codebook generation: Fix $p(u|x)$ and $\hat{x}(u,y)$ that achieve the rate–distortion function $R_{\text{SI-D}}(D/(1+\epsilon))$ where D is the desired distortion
Randomly and independently generate $2^{n\tilde{R}}$ sequences $u^n(l)$, $l \in [1 : 2^{n\tilde{R}}]$, each according to $\prod_{i=1}^n p_U(u_i)$
Partition the set of indices $l \in [1 : 2^{n\tilde{R}}]$ into equal-size subsets referred to as bins $\mathcal{B}(m) := [(m-1)2^{n(\tilde{R}-R)} + 1 : m2^{n(\tilde{R}-R)}]$, $m \in [1 : 2^{nR}]$
The codebook is revealed to the encoder and decoder
- Encoding: Given x^n , the encoder finds an l such that $(x^n, u^n(l)) \in \mathcal{T}_{\epsilon'}^{(n)}$. If there is more than one such index, it selects the smallest one. If there is no such index, it selects $l = 1$
The encoder sends the bin index m such that $l \in \mathcal{B}(m)$
- Decoding: Let $\epsilon > \epsilon'$. The decoder finds the unique $\hat{l} \in \mathcal{B}(m)$ such that $(u^n(\hat{l}), y^n) \in \mathcal{T}_{\epsilon}^{(n)}$
If there is such a unique index \hat{l} , the reproduction sequence is computed as $\hat{x}_i = \hat{x}(u_i(\hat{l}), y_i)$ for $i \in [1 : n]$; otherwise \hat{x}^n is set to an arbitrary sequence in $\hat{\mathcal{X}}^n$

- Analysis of the expected distortion: Let (L, M) denote the chosen indices. Define the “error” events:

$$\mathcal{E}_1 := \{(U^n(l), X^n) \notin \mathcal{T}_{\epsilon'}^{(n)} \text{ for all } l \in [1 : 2^{n\tilde{R}}]\},$$

$$\mathcal{E}_2 := \{(U^n(L), Y^n) \notin \mathcal{T}_{\epsilon}^{(n)}\},$$

$$\mathcal{E}_3 := \{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(M), \tilde{l} \neq L\}$$

The total probability of “error” is upper bounded as

$$P(\mathcal{E}) \leq P(\mathcal{E}_1) + P(\mathcal{E}_1^c \cap \mathcal{E}_2) + P(\mathcal{E}_3)$$

We now bound each term:

1. By the covering lemma, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R} > I(X; U) + \delta(\epsilon')$
2. Since $\mathcal{E}_1^c = \{(U^n(L), X^n) \in \mathcal{T}_{\epsilon'}^{(n)}\}$,
 $Y^n | \{U^n(L) = u^n, X^n = x^n\} \sim \prod_{i=1}^n p_{Y|U,X}(y_i | u_i, x_i) = \prod_{i=1}^n p_{Y|X}(y_i | x_i)$,
and $\epsilon > \epsilon'$, by the conditional typicality lemma, $P(\mathcal{E}_1^c \cap \mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$
3. To bound $P(\mathcal{E}_3)$, we first prove the following bound

Lemma 1: The probability of the error event

$$\begin{aligned} P(\mathcal{E}_3) &= P\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(M), \tilde{l} \neq L\} \\ &\leq P\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(1)\} \end{aligned}$$

The proof is given in the Appendix

Since each $U^n(\hat{l}) \sim \prod_{i=1}^n p_U(u_i)$ and is independent of Y^n , by the packing lemma, $P(\mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R} - R < I(Y; U) - \delta(\epsilon)$

4. Combining the bounds, we have shown that $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$ if
 $R > I(X; U) - I(Y; U) + \delta(\epsilon) + \delta(\epsilon')$

- When there is no “error”, $(U^n(L), X^n, Y^n) \in \mathcal{T}_{\epsilon}^{(n)}$. Thus by the law of total expectation and the typical average lemma, the asymptotic distortion averaged over the random code and over (X^n, Y^n) is bounded as

$$\limsup_{n \rightarrow \infty} E(d(X^n, \hat{X}^n)) \leq \limsup_{n \rightarrow \infty} (d_{\max} P(\mathcal{E}) + (1 + \epsilon) E(d(X, \hat{X})) P(\mathcal{E}^c)) \leq D$$

$$\text{if } R > I(X; U) - I(Y; U) + \delta(\epsilon) + \delta(\epsilon') = R_{\text{SI-D}}(D/(1 + \epsilon)) + \delta(\epsilon) + \delta(\epsilon')$$

- Finally from the continuity of $R_{\text{SI-D}}(D)$ in D , taking $\epsilon \rightarrow 0$ shows that any rate-distortion pair (R, D) with $R > R_{\text{SI-D}}(D)$ is achievable, which completes the proof

- Remark: Note that in this proof we used *deterministic* instead of random binning. This is because here we are dealing with a set of randomly generated sequences instead of a set of deterministic sequences, and therefore, there is no need to also randomize the binning. Following similar arguments to lossless source coding with causal side information, we can show that the Slepian–Wolf theorem is a special case of the Wyner–Ziv theorem. As such, random binning is not required for either
- Binning is the “dual” of multicoding:
 - The multicoding technique we used in the achievability proofs of the Gelfand–Pinsker theorem and Marton’s inner bound is a *channel coding* technique—we are given a set of messages and we generate a set of codewords for each message, which increases the rate. To send a message, we send one of the codewords in its subcodebook that satisfies a desired property
 - By comparison, binning is a *source coding* technique—we have many indices/sequences and we map them into a smaller number of bin indices, which reduces the rate. To send an index/sequence, we send its bin index

Proof of Converse

-
- Let M denote the encoded index of X^n . The key is to identify U_i . In general \hat{X}_i is a function of (M, Y^n) . We want \hat{X}_i to be a function of (U_i, Y_i) , so we define $U_i := (M, Y^{i-1}, Y_{i+1}^n)$. Note that this is a valid choice because $U_i \rightarrow X_i \rightarrow Y_i$ form a Markov chain. We first prove the theorem without the cardinality bound on U . Consider

$$\begin{aligned}
 nR &\geq H(M) \geq H(M|Y^n) \\
 &= I(X^n; M|Y^n) \\
 &= \sum_{i=1}^n I(X_i; M|Y^n, X^{i-1}) \\
 &\stackrel{(a)}{=} \sum_{i=1}^n I(X_i; M, Y^{i-1}, Y_{i+1}^n, X^{i-1}|Y_i) \\
 &\geq \sum_{i=1}^n I(X_i; U_i|Y_i) \geq \sum_{i=1}^n R_{\text{SI-D}}(\mathbb{E}(d(X_i, \hat{X}_i))),
 \end{aligned}$$

where (a) follows by the fact that (X_i, Y_i) is independent of $(Y^{i-1}, Y_{i+1}^n, X^{i-1})$

- Since $R_{\text{SI-D}}(D)$ is convex, $nR \geq nR_{\text{SI-D}}\left(\left(1/n\right)\sum_{i=1}^n \mathbb{E}(d(X_i, \hat{X}_i))\right)$
 Since by assumption $\limsup_{n \rightarrow \infty} \left(\left(1/n\right)\sum_{i=1}^n \mathbb{E}(d(X_i, \hat{X}_i))\right) \leq D$ and $R_{\text{SI-D}}(D)$ is nonincreasing, $R \geq R_{\text{SI-D}}(D)$. This completes the converse proof
- Remark: The bound on the cardinality of U can be proved using the technique described in Appendix C

Wyner–Ziv versus Gelfand–Pinsker

- First recall two fundamental limits of point-to-point communication: the rate–distortion function for DMS $R(D) = \min_{p(\hat{x}|x)} I(\hat{X}; X)$ and the capacity for DMC $C = \max_{p(x)} I(X; Y)$. In these two expressions, we can easily observe interesting dualities between the given source $X \sim p(x)$ and channel $p(y|x)$; the optimized reconstruction $p(\hat{x}|x)$ and channel input $X \sim p(x)$; and the minimum and maximum

Thus, roughly speaking, these two solutions (and underlying problems) are dual to each other. This duality can be made more precise [3, 4]

- As mentioned earlier, the channel coding problem for DMC with DM state available at the encoder and the source coding problem with side information at the decoder are dual to each other in a similar sense [5, 3]

Compare the rate–distortion functions with side information at the decoder

$$R_{\text{CSI-D}} = \min I(X; U), \quad R_{\text{SI-D}} = \min(I(X; U) - I(Y; U))$$

with the capacity expressions for DMC with DM state in Lecture Notes 7

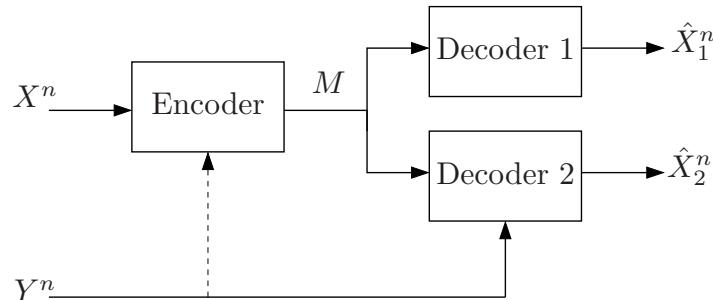
$$C_{\text{CSI-E}} = \max I(U; Y), \quad R_{\text{SI-E}} = \max(I(U; Y) - I(U; S))$$

There are dualities between the maximum and minimum and between multicoding and binning. But perhaps the most intriguing duality is that $R_{\text{SI-D}}$ is the difference between the “covering rate” $I(U; X)$ and the “packing rate” $I(U; Y)$, while $C_{\text{SI-E}}$ is the difference between the “packing rate” $I(U; Y)$ and the “covering rate” $I(U; S)$

- These types of dualities are abundant in network information theory. For example, we can make a similar observation between the Slepian–Wolf problem and the deterministic broadcast channel. While not mathematically precise (cf. the Lagrange duality in convex analysis or the MAC–BC duality in Lecture Notes 10), this covering–packing duality (or the source coding–channel coding duality in general) often leads to a unified understanding of the underlying coding techniques

Source Coding when Side Information May Be Absent

- Let (X, Y) be a 2-DMS and $d_j(x, \hat{x}_j)$, $j = 1, 2$, be two distortion measures. The encoder generates a description of X so that decoder 1 who does not have any side information can reconstruct X with distortion D_1 and decoder 2 who has side information Y can reconstruct X with distortion D_2



- This models the scenario, in which side information may be absent and thus the encoder should send a robust description of X with respect to this uncertainty (cf. the broadcast channel approach to compound channels in Lecture Notes 7)
- A $(2^{nR}, n)$ code, achievability at distortion pair (D_1, D_2) , and the rate–distortion function are defined as before

- Noncausal side information available only at decoder 2 [6, 7]
 - If the side information is available noncausally at decoder 2, then

$$R_{\text{SI-D2}} = \min_{p(u, \hat{x}_1|x) \hat{x}_2(u, \hat{x}_1, y)} (I(X; \hat{X}_1) + I(X; U|\hat{X}_1, Y)),$$
 where the minimum is over all $p(u, \hat{x}_1|x)$ and $\hat{x}_2(u, \hat{x}_1, y)$ with $|\mathcal{U}| \leq |\mathcal{X}||\hat{\mathcal{X}}_1| + 2$ such that $E(d_j(X, \hat{X}_j)) \leq D_j$, $j = 1, 2$
 Achievability follows by randomly generating a lossy source code for the source X and estimate \hat{X}_1 at rate $I(X; \hat{X}_1)$ and then using Wyner–Ziv coding with encoder side information \hat{X}_1 and decoder side information (\hat{X}_1, Y)
 Proof of converse: Let M be the encoded index of X^n . We identify the auxiliary random variable $U_i = (M, Y^{i-1}, Y_{i+1}^n, X^{i-1})$. Now, consider

$$\begin{aligned} nR &= H(M) = I(M; X^n, Y^n) \\ &= I(M; X^n|Y^n) + I(M; Y^n) \\ &= \sum_{i=1}^n (I(X_i; M|Y^n, X^{i-1}) + I(Y_i; M|Y^{i-1})) \\ &= \sum_{i=1}^n (I(X_i; M, X^{i-1}, Y^{i-1}, Y_{i+1}^n|Y_i) + I(Y_i; M, Y^{i-1})) \end{aligned}$$

$$\begin{aligned} &\geq \sum_{i=1}^n (I(X_i; U_i, \hat{X}_{1i}|Y_i) + I(Y_i; \hat{X}_{1i})) \\ &\geq \sum_{i=1}^n (I(X_i; U_i|\hat{X}_{1i}, Y_i) + I(X_i; \hat{X}_{1i})) \end{aligned}$$

The rest of the proof follows similar steps to the proof of the Wyner–Ziv theorem

- If side information is available *causally* only at decoder 2, then

$$R_{\text{CSI-D2}} = \min_{p(u|x), \hat{x}_1(u), \hat{x}_2(u, \hat{x}_1, y)} I(X; U)$$

where the minimum is over all $p(u|x)$, $\hat{x}_1(u)$, and $\hat{x}_2(u, \hat{x}_1, y)$ with $|\mathcal{U}| \leq |\mathcal{X}| + 2$ such that $E(d_j(X, \hat{X}_j)) \leq D_j$, $j = 1, 2$

- Side information available at both the encoder and decoder 2 [6]:

If side information is available (causally or noncausally) at both the encoder and decoder 2, then

$$R_{\text{SI-ED2}} = \min_{p(\hat{x}_1, \hat{x}_2|x, y)} (I(X, Y; \hat{X}_1) + I(X; \hat{X}_2|\hat{X}_1, Y)),$$

where the minimum is over all $p(\hat{x}_1, \hat{x}_2|x, y)$ such that $E(d_j(X, \hat{X}_j)) \leq D_j$, $j = 1, 2$

- Achievability follows by generating a lossy source code for (X^n, Y^n) with description \hat{X}_1^n at rate $I(X, Y; \hat{X}_1)$ and then using the lossy source coding with side information (\hat{X}_1^n, Y^n) at both the encoder and decoder 2
- Proof of converse: First observe that $I(X, Y; \hat{X}_1) + I(X; \hat{X}_2 | \hat{X}_1, Y) = I(\hat{X}_1; Y) + I(X; \hat{X}_1, \hat{X}_2 | Y)$. Using the same first steps as in the proof of the case of side information only at decoder 2, we have

$$\begin{aligned} nR &\geq \sum_{i=1}^n (I(X_i; M, X^{i-1}, Y^{i-1}, Y_{i+1}^n | Y_i) + I(Y_i; M, Y^{i-1})) \\ &\geq \sum_{i=1}^n (I(X_i; \hat{X}_{1i}, \hat{X}_{2i} | Y_i) + I(Y_i; \hat{X}_{1i})) \end{aligned}$$

The rest of the proof follows as before

Key New Ideas and Techniques

- Causal side information at decoder does not reduce lossless encoding rate when $p(x, y) > 0$ for all (x, y)
- Deterministic binning
- Slepian–Wolf is a special case of Wyner–Ziv

References

- [1] T. Weissman and A. El Gamal, "Source coding with limited-look-ahead side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 52, no. 12, pp. 5218–5239, Dec. 2006.
- [2] A. D. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 22, no. 1, pp. 1–10, 1976.
- [3] S. S. Pradhan, J. Chou, and K. Ramchandran, "Duality between source and channel coding and its extension to the side information case," *IEEE Trans. Inf. Theory*, vol. 49, no. 5, pp. 1181–1203, May 2003.
- [4] A. Gupta and S. Verdú, "Operational duality between lossy compression and channel coding: Channel decoders as lossy compressors," in *Proc. ITA Workshop*, La Jolla, CA, 2009.
- [5] T. M. Cover and M. Chiang, "Duality between channel capacity and rate distortion with two-sided state information," *IEEE Trans. Inf. Theory*, vol. 48, no. 6, pp. 1629–1638, 2002.
- [6] A. H. Kaspi, "Rate-distortion function when side-information may be present at the decoder," *IEEE Trans. Inf. Theory*, vol. 40, no. 6, pp. 2031–2034, Nov. 1994.
- [7] C. Heegard and T. Berger, "Rate distortion when side information may be absent," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 727–734, 1985.

Appendix: Proof of Lemma 1

- First we show that

$$\begin{aligned} & \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(m), \tilde{l} \neq L | M = m\} \\ & \leq \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(1) | M = m\} \end{aligned}$$

- This holds trivially for $m = 1$
- For $m \neq 1$, consider

$$\begin{aligned} & \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(m), \tilde{l} \neq L | M = m\} \\ & = \sum_{l \in \mathcal{B}(m)} p(l|m) \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(m), \tilde{l} \neq l | L = l, M = m\} \\ & \stackrel{(a)}{=} \sum_{l \in \mathcal{B}(m)} p(l|m) \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(m), \tilde{l} \neq l | L = l\} \\ & \stackrel{(b)}{=} \sum_{l \in \mathcal{B}(m)} p(l|m) \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in [1 : 2^{n(\tilde{R}-R)} - 1] | L = l\} \\ & \leq \sum_{l \in \mathcal{B}(m)} p(l|m) \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(1) | L = l\} \end{aligned}$$

$$\stackrel{(c)}{=} \sum_{l \in \mathcal{B}(m)} p(l|m) \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(1) | L = l, M = m\}$$

$$= \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{l} \in \mathcal{B}(1) | M = m\}$$

where (a) and (c) follow since M is a function of L and (b) follows since given $L = l$, any collection of $2^{n(\tilde{R}-R)} - 1$ $U^n(\tilde{l})$ codewords with $\tilde{l} \neq l$ has the same distribution

- Hence

$$\begin{aligned} & \mathbb{P}(\mathcal{E}_3) \\ &= \sum_m p(m) \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } U^n(\tilde{l}) \in \mathcal{B}(m), \tilde{l} \neq l | M = m\} \\ &\leq \sum_m p(m) \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } U^n(\tilde{l}) \in \mathcal{B}(1) | M = m\} \\ &= \mathbb{P}\{(U^n(\tilde{l}), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } U^n(\tilde{l}) \in \mathcal{B}(1)\} \end{aligned}$$

Lecture Notes 13

Distributed Lossy Source Coding

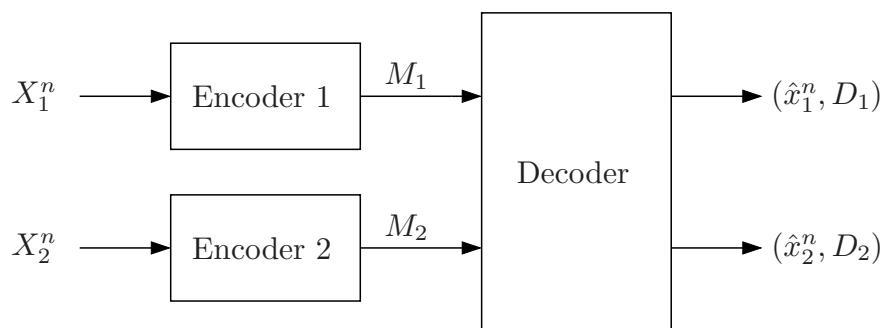
- Problem Setup
- Berger–Tung Inner Bound
- Berger–Tung Outer Bound
- Quadratic Gaussian Distributed Source Coding
- Gaussian CEO Problem
- Counterexample: Doubly Symmetric Binary Sources
- Extensions to More Than 2 Sources
- Key New Ideas and Techniques
- Appendix: Proof of Markov Lemma
- Appendix: Proof of Lemma 2
- Appendix: Proof of Lemma 3
- Appendix: Proof of Lemma 5

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- Consider the problem of distributed lossy source coding for 2-DMS (X_1, X_2) and two distortion measures $d_1(x_1, \hat{x}_1)$ and $d_2(x_2, \hat{x}_2)$

The sources X_1 and X_2 are separately encoded and the descriptions are sent over noiseless communication links to a decoder that wishes to reconstruct the two sources with distortions D_1 and D_2 , respectively. What are the minimum description rates required?



- A $(2^{nR_1}, 2^{nR_2}, n)$ distributed lossy source code consists of:
 1. Two encoders: Encoder 1 assigns an index $m_1(x_1^n) \in [1 : 2^{nR_1}]$ to each sequence $x_1^n \in \mathcal{X}_1^n$ and encoder 2 assigns an index $m_2(x_2^n) \in [1 : 2^{nR_2}]$ to each sequence $x_2^n \in \mathcal{X}_2^n$
 2. A decoder that assigns a pair of estimates $(\hat{x}_1^n, \hat{x}_2^n)$ to each index pair $(m_1, m_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$
- A rate pair (R_1, R_2) is said to be achievable with distortion pair (D_1, D_2) if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ distributed lossy codes with $\limsup_{n \rightarrow \infty} E(d_j(X_j, \hat{X}_j)) \leq D_j, j = 1, 2$
- The rate-distortion region $\mathcal{R}(D_1, D_2)$ for the distributed lossy source coding problem is the closure of the set of all rate pairs (R_1, R_2) such that (R_1, R_2, D_1, D_2) is achievable
- The rate-distortion region is not known in general

Berger–Tung Inner Bound

- *Theorem 1* (Berger–Tung Inner Bound) [1]: Let (X_1, X_2) be a 2-DMS and $d_1(x_1, \hat{x}_1)$ and $d_2(x_2, \hat{x}_2)$ be two distortion measures. A rate pair (R_1, R_2) is achievable with distortion (D_1, D_2) for distributed lossy source coding if

$$R_1 > I(X_1; U_1 | U_2, Q),$$

$$R_2 > I(X_2; U_2 | U_1, Q),$$

$$R_1 + R_2 > I(X_1, X_2; U_1, U_2 | Q)$$

for some $p(q)p(u_1|x_1, q)p(u_2|x_2, q)$ with $|\mathcal{U}_1| \leq |\mathcal{X}_1| + 4$, $|\mathcal{U}_2| \leq |\mathcal{X}_2| + 4$ and functions $\hat{x}_1(u_1, u_2, q)$, $\hat{x}_2(u_1, u_2, q)$ such that

$$D_1 \geq E(d_1(X_1, \hat{X}_1)),$$

$$D_2 \geq E(d_2(X_2, \hat{X}_2))$$

- There are several special cases where the Berger–Tung inner bound is optimal:
 - The inner bound reduces to the Slepian–Wolf region when d_1 and d_2 are Hamming distortion measures and $D_1 = D_2 = 0$ (set $U_1 = X_1$ and $U_2 = X_2$)
 - The inner bound reduces to the Wyner–Ziv rate–distortion function when there is no rate limit for X_2 ($R_2 \geq H(X_2)$). In this case, the only active constraint $I(X_1; U_1|U_2, Q)$ is minimized by $U_2 = X_2$ and $Q = \emptyset$
 - More generally, when d_2 is Hamming distortion and $D_2 = 0$, the inner bound reduces to

$$R_1 \geq I(X_1; U_1|X_2),$$

$$R_2 \geq H(X_2|U_1),$$

$$R_1 + R_2 \geq I(X_1; U_1|X_2) + H(X_2) = I(X_1; U_1) + H(X_2|U_1)$$

for some $p(u_1|x_1)$ and $\hat{x}_1(u_1, x_2)$ such that $E(d_1(X_1, \hat{X}_1)) \leq D_1$. It can be shown [2] that this region is the rate–distortion region

- The inner bound is optimal for in the quadratic Gaussian case, i.e., WGN sources and squared error distortion [3]. We will discuss this result in detail
- However, the Berger–Tung inner bound is not tight in general as we will see later via a counterexample

Markov Lemma

- To prove the achievability of the inner bound, we will need a stronger version of the conditional typicality lemma
- *Markov Lemma* [1]: Suppose $X \rightarrow Y \rightarrow Z$ form a Markov chain. Let $(x^n, y^n) \in \mathcal{T}_{\epsilon'}^{(n)}(X, Y)$ and $Z^n \sim p(z^n|y^n)$, where the conditional pmf $p(z^n|y^n)$ satisfies the following conditions:

1. $P\{(y^n, Z^n) \in \mathcal{T}_{\epsilon'}^{(n)}(Y, Z)\} \rightarrow 1$ as $n \rightarrow \infty$, and

2. for every $z^n \in \mathcal{T}_{\epsilon'}^{(n)}(Z|y^n)$ and n sufficiently large

$$2^{-n(H(Z|Y)+\delta(\epsilon'))} \leq p(z^n|y^n) \leq 2^{-n(H(Z|Y)-\delta(\epsilon'))}$$

for some $\delta(\epsilon') \rightarrow 0$ as $\epsilon' \rightarrow 0$

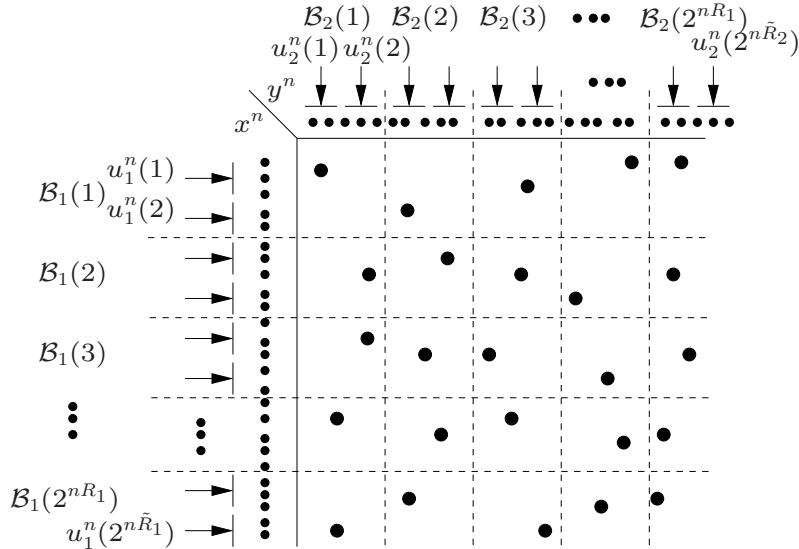
If ϵ' is sufficiently small compared to ϵ , then

$$P\{(x^n, y^n, Z^n) \in \mathcal{T}_{\epsilon}^{(n)}(X, Y, Z)\} \rightarrow 1 \quad \text{as } n \rightarrow \infty$$

- The proof of the lemma is given in the Appendix

Outline of Achievability

- Fix $p(u_1|x_1)p(u_2|x_2)$. Randomly generate $2^{n\tilde{R}_1}$ u_1^n sequences and partition them into 2^{nR_1} bins. Randomly generate $2^{n\tilde{R}_2}$ u_2^n sequences and partition them into 2^{nR_2} bins



- Encoder 1 finds a jointly typical u_1^n with x_1^n and sends its bin index m_1 . Encoder 2 finds a jointly typical u_2^n with x_2^n and sends its bin index m_2
- The decoder finds the unique jointly typical pair $(u_1^n, u_2^n) \in \mathcal{B}_1(m_1) \times \mathcal{B}_2(m_2)$ and construct descriptions $\hat{x}_{1i} = x_1(u_{1i}, u_{2i})$ and $\hat{x}_{2i} = x_2(u_{1i}, u_{2i})$ for $i \in [1 : n]$

Proof of Achievability

- We show achievability for $|\mathcal{Q}| = 1$; the rest of the proof follows using time sharing
- Codebook generation: Let $\epsilon > \epsilon' > \epsilon''$. Fix $p(u_1|x_1)p(u_2|x_2)$, $\hat{x}_1(u_1, u_2)$, and $\hat{x}_2(u_1, u_2)$ that achieve the rate region for some prescribed distortions D_1 and D_2 . Let $\tilde{R}_1 \geq R_1$, $\tilde{R}_2 \geq R_2$

For $j \in \{1, 2\}$, randomly and independently generate sequences $u_j^n(l_j)$, $l_j \in [1 : 2^{n\tilde{R}_j}]$, each according to $\prod_{i=1}^n p_{U_j}(u_{ji})$

Partition the indices $l_j \in [1 : 2^{n\tilde{R}_j}]$ into 2^{nR_j} equal-size bins $\mathcal{B}_j(m_j)$, $m_j \in [1 : 2^{nR_j}]$

The codebook and bin assignments are revealed to the encoders and decoder

- Encoding: Upon observing x_j^n , encoder $j = 1, 2$ finds an index $l_j \in [1 : 2^{n\tilde{R}_j}]$ such that $(x_j^n, u_j^n(l_j)) \in \mathcal{T}_{\epsilon'}^{(n)}$. If there is more than one such l_j index, encoder j selects the smallest index. If there is no such l_j , encoder j selects an arbitrary index $l_j \in [1 : 2^{n\tilde{R}_j}]$

Encoder $j \in \{1, 2\}$ sends the index m_j such that $l_j \in \mathcal{B}_j(m_j)$

- Decoding: The decoder finds the unique index pair $(\hat{l}_1, \hat{l}_2) \in \mathcal{B}_1(m_1) \times \mathcal{B}_2(m_2)$ such that $(u_1^n(\hat{l}_1), u_2^n(\hat{l}_2)) \in \mathcal{T}_{\epsilon}^{(n)}$
If there is such a unique index pair (\hat{l}_1, \hat{l}_2) , the reproductions \hat{x}_1^n and \hat{x}_2^n are computed as $\hat{x}_{1i}(u_{1i}(\hat{l}_1), u_{2i}(\hat{l}_2))$ and $\hat{x}_{2i}(u_{1i}(\hat{l}_1), u_{2i}(\hat{l}_2))$ for $i = 1, 2, \dots, n$; otherwise \hat{x}_1^n and \hat{x}_2^n are set to arbitrary sequences in $\hat{\mathcal{X}}_1^n$ and $\hat{\mathcal{X}}_2^n$, respectively
- Analysis of the expected distortion: Let (L_1, L_2) denote the pair of indices for the chosen (U_1^n, U_2^n) pair and (M_1, M_2) be the pair of corresponding bin indices. Define the “error” events as follows:

$$\mathcal{E}_1 := \{(U_1^n(l_1), X_1^n) \notin \mathcal{T}_{\epsilon''}^{(n)} \text{ for all } l_1 \in [1 : 2^{n\tilde{R}_1}]\},$$

$$\mathcal{E}_2 := \{(U_1^n(L_1), X_1^n, X_2^n) \notin \mathcal{T}_{\epsilon'}^{(n)}\},$$

$$\mathcal{E}_3 := \{(U_1^n(L_1), U_2^n(L_2)) \notin \mathcal{T}_{\epsilon}^{(n)}\},$$

$$\mathcal{E}_4 := \{(U_1^n(\tilde{l}_1), U_2^n(\tilde{l}_2)) \in \mathcal{T}_{\epsilon}^{(n)}$$

for some $(\tilde{l}_1, \tilde{l}_2) \in \mathcal{B}_1(M_1) \times \mathcal{B}_2(M_2), (\tilde{l}_1, \tilde{l}_2) \neq (L_1, L_2)\}$

The total probability of “error” is upper bounded as

$$P(\mathcal{E}) \leq P(\mathcal{E}_1) + P(\mathcal{E}_1^c \cap \mathcal{E}_2) + P(\mathcal{E}_2^c \cap \mathcal{E}_3) + P(\mathcal{E}_4)$$

We bound each term:

1. By the covering lemma, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R}_1 > I(U_1; X_1) + \delta(\epsilon'')$
2. Since $X_2^n | \{U_1^n(L_1) = u_1^n, X_1^n = x_1^n\} \sim \prod_{i=1}^n p_{X_2|U_1, X_1}(x_{2i} | u_{1i}, x_{1i}) = \prod_{i=1}^n p_{X_2|X_1}(x_{2i} | x_{1i})$ and $\epsilon' > \epsilon''$, by the conditional typicality lemma, $P(\mathcal{E}_1^c \cap \mathcal{E}_2) \rightarrow 0$
3. To bound $P(\mathcal{E}_2^c \cap \mathcal{E}_3)$, let $(u_1^n, x_1^n, x_2^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, X_1, X_2)$ and consider $P\{U_2^n(L_2) = u_2^n | X_2^n = x_2^n, X_1^n = x_1^n, U_1^n(L_1) = u_1^n\} = P\{U_2^n(L_2) = u_2^n | X_2^n = x_2^n\} =: p(u_2^n | x_2^n)$. First note that by the covering lemma, $P\{U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2 | x_2^n) | X_2^n = x_2^n\} \rightarrow 1$ as $n \rightarrow \infty$, that is, $p(u_2^n | x_2^n)$ satisfies the first condition in the Markov lemma. In the Appendix we show that it also satisfies the second condition

Lemma 2: For every $u_2^n \in \mathcal{T}_{\epsilon'}^{(n)}(U_2 | x_2^n)$ and n sufficiently large,

$$p(u_2^n | x_2^n) \doteq 2^{-nH(U_2 | X_2)}$$

Hence, by the Markov lemma (with $Z \leftarrow U_2$, $Y \leftarrow X_2$, and $X \leftarrow (U_1, X_1)$)

$P\{(u_1^n, x_1^n, x_2^n, U_2^n(L_2)) \in \mathcal{T}_{\epsilon'}^{(n)} | U_1^n(L_1) = u_1^n, X_1^n = x_1^n, X_2^n = x_2^n\} \rightarrow 1$ as $n \rightarrow \infty$, provided that $(u_1^n, x_1^n, x_2^n) \in \mathcal{T}_{\epsilon'}^{(n)}(U_1, X_1, X_2)$ and ϵ' is sufficiently small compared to ϵ . Therefore, $P(\mathcal{E}_2^c \cap \mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$, if ϵ' is sufficiently small compared to ϵ

4. Following a similar argument to Lemma 1 in the proof of the Wyner–Ziv theorem, we have

$$P(\mathcal{E}_4) \leq P\{(U_1^n(\tilde{l}_1), U_2^n(\tilde{l}_2)) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } (\tilde{l}_1, \tilde{l}_2) \in \mathcal{B}_1(1) \times \mathcal{B}_2(1)\}$$

Now we bound this probability using the following lemma, which is a straightforward generalization of the packing lemma:

Mutual Packing Lemma: Let $(U_1, U_2) \sim p(u_1, u_2)$ and $\epsilon > 0$. Let $U_1^n(l_1)$, $l_1 \in [1 : 2^{nr_1}]$, be random sequences, each distributed according to $\prod_{i=1}^n p_{U_1}(u_{1i})$ with arbitrary dependence on the rest of the $U_1^n(l_1)$ sequences. Similarly, let $U_2^n(l_2)$, $l_2 \in [1 : 2^{nr_2}]$, be random sequences, each distributed according to $\prod_{i=1}^n p_{U_2}(u_{2i})$ with arbitrary dependence on the rest of the $U_2^n(l_2)$ sequences. Assume that $\{U_1^n(l_1) : l_1 \in [1 : 2^{nr_1}]\}$ and $\{U_2^n(l_2) : l_2 \in [1 : 2^{nr_2}]\}$ are independent

Then there exists $\delta(\epsilon) \rightarrow 0$ as $\epsilon \rightarrow 0$ such that

$$P\{(U_1^n(l_1), U_2^n(l_2)) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } (l_1, l_2) \in [1 : 2^{nr_1}] \times [1 : 2^{nr_2}]\} \rightarrow 0$$

as $n \rightarrow \infty$ if $r_1 + r_2 < I(U_1; U_2) - \delta(\epsilon)$,

Hence, by the mutual packing lemma, $P(\mathcal{E}_4) \rightarrow 0$ as $n \rightarrow \infty$, if $(\tilde{R}_1 - R_1) + (\tilde{R}_2 - R_2) < I(U_1; U_2) - \delta(\epsilon)$

Combining the bounds and eliminating \tilde{R}_1 and \tilde{R}_2 , we have shown that $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$ if

$$\begin{aligned} R_1 &> I(U_1; X_1) - I(U_1; U_2) + \delta(\epsilon'') + \delta(\epsilon) \\ &= I(U_1; X_1|U_2) + \delta'(\epsilon), \\ R_2 &> I(U_2; X_2|U_1) + \delta'(\epsilon), \\ R_1 + R_2 &> I(U_1; X_1) + I(U_2; X_2) - I(U_1; U_2) + \delta'(\epsilon) \\ &= I(U_1, U_2; X_1, X_2) + \delta'(\epsilon) \end{aligned}$$

The rest of the proof follows by the same arguments used to complete previous lossy coding achievability proofs

Berger–Tung Outer Bound

- *Theorem 2* (Berger–Tung Outer Bound) [1]: Let (X_1, X_2) be a 2-DMS and $d_1(x, \hat{x}_1)$ and $d_2(x, \hat{x}_2)$ be two distortion measures. If a rate pair (R_1, R_2) is achievable with distortion (D_1, D_2) for distributed lossy source coding, then it must satisfy

$$\begin{aligned} R_1 &\geq I(X_1, X_2; U_1|U_2), \\ R_2 &\geq I(X_1, X_2; U_2|U_1), \\ R_1 + R_2 &\geq I(X_1, X_2; U_1, U_2) \end{aligned}$$

for some $p(u_1, u_2|x_1, x_2)$ with $U_1 \rightarrow X_1 \rightarrow X_2$ and $X_1 \rightarrow X_2 \rightarrow U_2$ forming Markov chains and functions $\hat{x}_1(u_1, u_2)$, $\hat{x}_2(u_1, u_2)$ such that

$$\begin{aligned} D_1 &\geq E(d_1(X_1, \hat{X}_1)), \\ D_2 &\geq E(d_2(X_2, \hat{X}_2)) \end{aligned}$$

- The Berger–Tung outer bound resembles the Berger–Tung inner bound except that the outer bound is convex without time-sharing and that Markov conditions for the outer bound are weaker than the Markov condition $U_1 \rightarrow X_1 \rightarrow X_2 \rightarrow U_2$ for the inner bound

- The proof follows by the standard argument with identifying $U_{1i} := (M_1, X_1^{i-1}, X_2^{i-1})$ and $U_{2i} := (M_2, X_1^{i-1}, X_2^{i-1})$
- There are several special cases where the Berger–Tung outer bound is tight:
 - Slepian–Wolf distributed lossless compression
 - Wyner–Ziv lossy source coding with side information
 - More generally, when d_2 is Hamming distortion and $D_2 = 0$
 - The outer bound is also tight when X_2 is a function of X_1 [4]. In this case, the inner bound is not tight in general [5]
- The outer bound is not tight in general [1], for example, it is not tight for the quadratic Gaussian case that will be discussed next. A strictly improved outer bound is given by Wagner and Anantharam [6]

Quadratic Gaussian Distributed Source Coding

- Consider the distributed lossy source coding problem for a 2-WGN($1, \rho$) source (X_1, X_2) and squared error distortion $d_j(x_j, \hat{x}_j) = (x_j - \hat{x}_j)^2$, $j = 1, 2$. Without loss of generality, we assume that $\rho = E(X_1 X_2) \geq 0$
- The Berger–Tung inner bound is tight for this case

Theorem 3 [3]: The rate–distortion region $\mathcal{R}(D_1, D_2)$ for the quadratic Gaussian distributed source coding problem of the 2-WGN source (X_1, X_2) and squared error distortion is the intersection of the following three regions:

$$\mathcal{R}_1(D_1) = \left\{ (R_1, R_2) : R_1 \geq R \left(\frac{1 - \rho^2 + \rho^2 2^{-2R_2}}{D_1} \right) =: g_1(R_2, D_1) \right\},$$

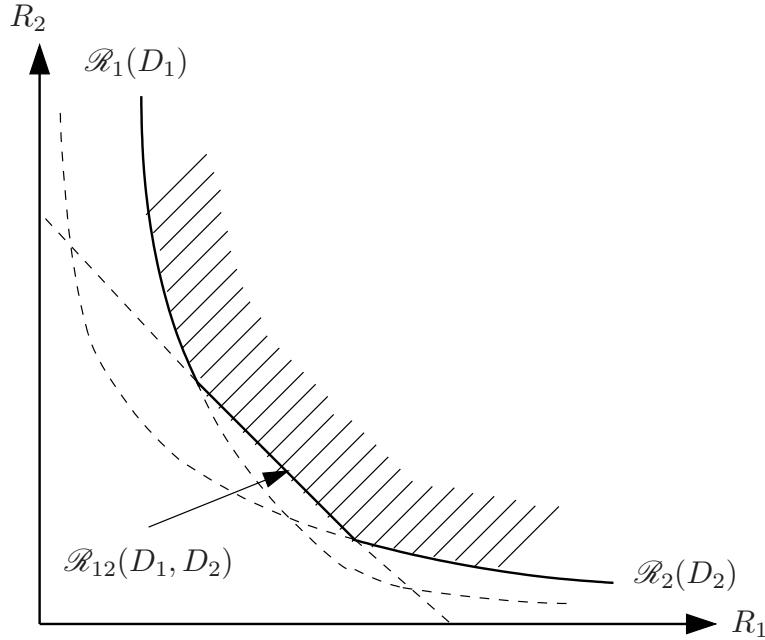
$$\mathcal{R}_2(D_2) = \left\{ (R_1, R_2) : R_2 \geq R \left(\frac{1 - \rho^2 + \rho^2 2^{-2R_1}}{D_2} \right) =: g_2(R_1, D_2) \right\},$$

$$\mathcal{R}_{12}(D_1, D_2) = \left\{ (R_1, R_2) : R_1 + R_2 \geq R \left(\frac{(1 - \rho^2)\phi(D_1, D_2)}{2D_1 D_2} \right) \right\},$$

where $\phi(D_1, D_2) := 1 + \sqrt{1 + 4\rho^2 D_1 D_2 / (1 - \rho^2)^2}$

- Remark: In [7], it is shown that the rate–distortion regions when only one source is to be estimated are $\mathcal{R}(D_1, 1) = \mathcal{R}_1(D_1)$ and $\mathcal{R}(1, D_2) = \mathcal{R}_2(D_2)$

- The $\mathcal{R}(D_1, D_2)$ region is plotted below



Proof of Achievability

- Without loss of generality, we assume throughout that $D_1 \leq D_2$
- Set the auxiliary random variables in the Berger–Tung bound to $U_1 = X_1 + V_1$ and $U_2 = X_2 + V_2$, where $V_1 \sim N(0, N_1)$ and $V_2 \sim N(0, N_2)$, $N_2 \geq N_1$, are independent of each other and of (X_1, X_2)
- Let the reconstructions \hat{X}_1 and \hat{X}_2 be the MMSE estimates $\hat{X}_1 = E(X_1|U_1, U_2)$ and $\hat{X}_2 = E(X_2|U_1, U_2)$
We refer to such choice of U_1, U_2 as a *distributed Gaussian test channel* characterized by N_1 and N_2
- Each distributed Gaussian test channel corresponds to the distortion pair

$$D_1 = E((X_1 - \hat{X}_1)^2) = \frac{N_1(1 + N_2 - \rho^2)}{(1 + N_1)(1 + N_2) - \rho^2},$$

$$D_2 = E((X_2 - \hat{X}_2)^2) = \frac{N_2(1 + N_1 - \rho^2)}{(1 + N_1)(1 + N_2) - \rho^2} \geq D_1$$

The achievable rate-distortion region is the set of rate pairs (R_1, R_2) such that

$$R_1 \geq I(X_1; U_1 | U_2) = R \left(\frac{(1+N_1)(1+N_2) - \rho^2}{N_1(1+N_2)} \right),$$

$$R_2 \geq I(X_2; U_2 | U_1) = R \left(\frac{(1+N_1)(1+N_2) - \rho^2}{N_2(1+N_1)} \right),$$

$$R_1 + R_2 \geq I(X_1, X_2; U_1, U_2) = R \left(\frac{(1+N_1)(1+N_2) - \rho^2}{N_1 N_2} \right)$$

- Since $U_1 \rightarrow X_1 \rightarrow X_2 \rightarrow U_2$, we have

$$\begin{aligned} I(X_1, X_2; U_1, U_2) &= I(X_1, X_2; U_1 | U_2) + I(X_1, X_2; U_2) \\ &= I(X_1; U_1 | U_2) + I(X_2; U_2) \\ &= I(X_1; U_1) + I(X_2; U_2 | U_1) \end{aligned}$$

Thus, in general, this region has two corner points $(I(X_1; U_1 | U_2), I(X_2; U_2))$ and $(I(X_1; U_1), I(X_2; U_2 | U_1))$. The first (left) corner point can be written as

$$R_2^l := I(X_2; U_2) = R((1+N_2)/N_2),$$

$$R_1^l := I(X_1; U_1 | U_2) = R \left(\frac{(1+N_1)(1+N_2) - \rho^2}{N_1(1+N_2)} \right) = g_1(R_2^l, D_1)$$

The other corner point (R_1^r, R_2^r) has a similar representation

- We now consider two cases

Case 1: $(1 - D_2) \leq \rho^2(1 - D_1)$

- For this case, the intersection for $\mathcal{R}(D_1, D_2)$ can be simplified as follows

Lemma 3: If $(1 - D_2) \leq \rho^2(1 - D_1)$, then $\mathcal{R}_1(D_1) \subseteq \mathcal{R}_2(D_2) \cap \mathcal{R}_{12}(D_1, D_2)$

The proof is in the Appendix

- Consider a distributed Gaussian test channel with $N_1 = D_1/(1 - D_1)$ and $N_2 = \infty$ (i.e., $U_2 = \emptyset$)

The (left) corner point (R_1^l, R_2^l) of the achievable rate region is $R_2^l = 0$ and

$$R_1^l = I(X_1; U_1) = \frac{1}{2} \log \left(\frac{1+N_1}{N_1} \right) = \frac{1}{2} \log \frac{1}{D_1} = g_1(R_2^l, D_1)$$

Also it can be easily verified that the distortion constraints are satisfied as

$$\begin{aligned} \mathbb{E}[(X_1 - \hat{X}_1)^2] &= 1 - \frac{1}{1+N_1} = D_1, \\ \mathbb{E}[(X_2 - \hat{X}_2)^2] &= 1 - \frac{\rho^2}{1+N_1} = 1 - \rho^2 + \rho^2 D_1 \leq D_2 \end{aligned}$$

- Now consider a test channel with $(\tilde{N}_1, \tilde{N}_2)$, where $\tilde{N}_2 < \infty$ and $\tilde{N}_1 \geq N_1$ such

that

$$\frac{\tilde{N}_1(1 + \tilde{N}_2 - \rho^2)}{(1 + \tilde{N}_1)(1 + \tilde{N}_2) - \rho^2} = \frac{N_1}{1 + N_1} = D_1$$

Then, the corresponding distortion pair $(\tilde{D}_1, \tilde{D}_2)$ satisfies $\tilde{D}_1 = D_1$ and

$$\frac{\tilde{D}_2}{\tilde{D}_1} = \frac{1/\tilde{N}_1 + 1/(1 - \rho^2)}{1/\tilde{N}_2 + 1/(1 - \rho^2)} \leq \frac{1/N_1 + 1/(1 - \rho^2)}{1/(1 - \rho^2)} = \frac{D_2}{D_1},$$

that is, $\tilde{D}_2 \leq D_2$

Furthermore, as shown before, the left corner point of the corresponding rate region is

$$\begin{aligned}\tilde{R}_2 &= I(X_2; U_2) = R((1 + \tilde{N}_2)/\tilde{N}_2), \\ \tilde{R}_1 &= g_1(\tilde{R}_2, \tilde{D}_1)\end{aligned}$$

Hence, by varying $0 < \tilde{N}_2 < \infty$, we can achieve the entire region $\mathcal{R}_1(D_1)$

Case 2: $(1 - D_2) > \rho^2(1 - D_1)$

- In this case, there exists a test channel (N_1, N_2) such that both distortion constraints are tight. To show this, we use the following result that is an easy consequence of the matrix inversion formula in Appendix B

Lemma 4: Let $U_j = X_j + V_j$, $j = 1, 2$, where $\mathbf{X} = (X_1, X_2)$ and $\mathbf{V} = (V_1, V_2)$ are independent zero mean Gaussian random vectors with respective covariance matrices $K_{\mathbf{X}}, K_{\mathbf{V}} \succ 0$. Let $K_{\mathbf{X}|\mathbf{U}} = K_{\mathbf{X}} - K_{\mathbf{XU}}K_{\mathbf{U}}^{-1}K_{\mathbf{XU}}^T$ be the error covariance matrix of the (linear) MMSE estimate of \mathbf{X} given \mathbf{U} . Then,

$$K_{\mathbf{X}|\mathbf{U}}^{-1} = K_{\mathbf{X}}^{-1} + K_{\mathbf{X}}^{-1}K_{\mathbf{XU}}^T(K_{\mathbf{U}} - K_{\mathbf{XU}}K_{\mathbf{X}}^{-1}K_{\mathbf{XU}}^T)^{-1}K_{\mathbf{XU}}K_{\mathbf{X}}^{-1} = K_{\mathbf{X}}^{-1} + K_{\mathbf{V}}^{-1}$$

Hence, V_1 and V_2 are independent iff $K_{\mathbf{V}}^{-1} = K_{\mathbf{X}|\mathbf{U}}^{-1} - K_{\mathbf{X}}^{-1}$ is diagonal

- Now let

$$K = \begin{bmatrix} D_1 & \theta\sqrt{D_1 D_2} \\ \theta\sqrt{D_1 D_2} & D_2 \end{bmatrix},$$

where $\theta \in [0, 1]$ is chosen such that $K^{-1} - K_X^{-1} = \text{diag}(N_1, N_2)$ for some $N_1, N_2 > 0$. It can be shown by simple algebra that θ can be chosen as

$$\theta = \frac{\sqrt{(1 - \rho^2)^2 + 4\rho^2 D_1 D_2} - (1 - \rho^2)}{2\rho\sqrt{D_1 D_2}}$$

if $(1 - D_2) > \rho^2(1 - D_1)$

Hence, by Lemma 4, we have the covariance matrix $K = K_{X-\hat{X}} = K_{X|U}$ with $U_j = X_j + V_j$, $j = 1, 2$, and $V_j \sim N(0, N_j)$, $j = 1, 2$, independent of each other and of (X_1, X_2) . In other words, there exists a distributed Gaussian test channel characterized by (N_1, N_2) with corresponding distortion pair (D_1, D_2)

- With such choice of the test channel, it can be readily verified that the left corner point (R_1^l, R_2^l) of the rate region satisfies the conditions

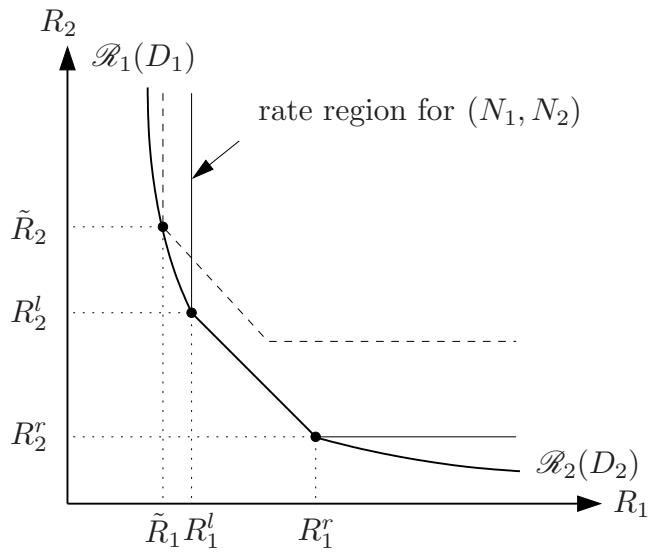
$$R_1^l + R_2^l = R\left(\frac{(1 - \rho^2)\phi(D_1, D_2)}{2D_1D_2}\right),$$

$$R_2^l = R\left(\frac{1 + N_2}{N_2}\right),$$

$$R_1^l = g_1(R_2^l, D_1)$$

Therefore it is on the boundary of both $\mathcal{R}_{12}(D_1, D_2)$ and $\mathcal{R}_1(D_1)$

- Following similar steps to case 1, we can show that any $(\tilde{R}_1, \tilde{R}_2)$ satisfying $\tilde{R}_1 = g_2(\tilde{R}_2, D_1)$ and $\tilde{R}_2 \geq R_2^l$ is achievable (see the figure)



- Similarly, the right corner point (R_1^r, R_2^r) is on the boundary of $\mathcal{R}_{12}(D_1, D_2)$ and $\mathcal{R}_2(D_2)$, and any rate pair $(\tilde{R}_1, \tilde{R}_2)$ satisfying $\tilde{R}_2 = g_2(\tilde{R}_1, D_2)$ and $\tilde{R}_1 \geq R_1^r$ is achievable
- Using time sharing between two corner points completes the proof for case 2

Proof of Converse: $\mathcal{R}(D_1, D_2) \subseteq \mathcal{R}_1(D_1) \cap \mathcal{R}_2(D_2)$ [7]

- We first show that the capacity region $\mathcal{R}(D_1, D_2) \subseteq \mathcal{R}_1(D_1) \cap \mathcal{R}_2(D_2)$
- Consider

$$\begin{aligned}
nR_1 &\geq H(M_1) \geq H(M_1|M_2) = I(M_1; X_1^n|M_2) \\
&= h(X_1^n|M_2) - h(X_1^n|M_1, M_2) \\
&\geq h(X_1^n|M_2) - h(X_1^n|\hat{X}_1^n) \\
&\geq h(X_1^n|M_2) - \sum_{i=1}^n h(X_{1i}|\hat{X}_{1i}) \\
&\geq \boxed{h(X_1^n|M_2)} - \frac{n}{2} \log(2\pi e D_1)
\end{aligned}$$

The last step follows by Jensen's inequality and the distortion constraint

- Next consider

$$\begin{aligned}
nR_2 &\geq I(M_2; X_2^n) \\
&= h(X_2^n) - h(X_2^n|M_2) \\
&= \frac{n}{2} \log(2\pi e) - \boxed{h(X_2^n|M_2)}
\end{aligned}$$

- Since X_1^n and X_2^n are each i.i.d. and they are jointly Gaussian, we can express $X_{1i} = \rho X_{2i} + W_i$, where $\{W_i\}$ is a WGN process with average power $(1 - \rho^2)$ and is independent of $\{X_{2i}\}$ and hence of M_2

By the conditional EPI,

$$\begin{aligned}
2^{\frac{2}{n}h(X_1^n|M_2)} &\geq 2^{\frac{2}{n}h(\rho X_2^n|M_2)} + 2^{\frac{2}{n}h(W^n|M_2)} \\
&= \rho^2 2^{\frac{2}{n}h(X_2^n|M_2)} + 2\pi e(1 - \rho^2) \\
&\geq 2\pi e (\rho^2 2^{-2R_2} + (1 - \rho^2))
\end{aligned}$$

Thus,

$$nR_1 \geq \frac{n}{2} \log (2\pi e (1 - \rho^2 + \rho^2 2^{-2R_2})) - \frac{n}{2} \log(2\pi e D_1) = n g_1(R_2, D_1),$$

and $(R_1, R_2) \in \mathcal{R}_1(D_1)$

- Similarly, $\mathcal{R}(D_1, D_2) \subseteq \mathcal{R}_2(D_2)$

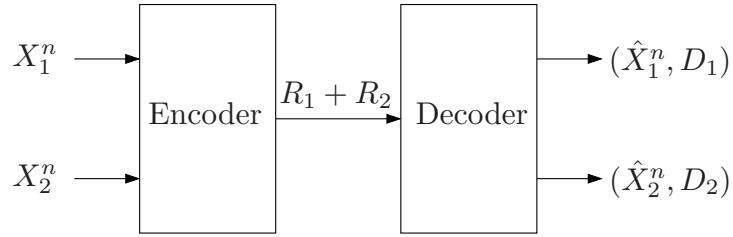
Proof of Converse: $\mathcal{R}(D_1, D_2) \subseteq \mathcal{R}_{12}(D_1, D_2)$ [3, 8]

- By assumption and in light of Lemma 3, we assume without loss of generality that $(1 - D_1) \geq (1 - D_2) \geq \rho^2(1 - D_1)$. In this case the sum rate bound is *active*

We establish the following two lower bounds $R_1(\theta)$ and $R_2(\theta)$ on the sum rate parameterized by $\theta \in [-1, 1]$ and show that

$\min_{\theta} \max\{R_1(\theta), R_2(\theta)\} = R((1 - \rho^2)\phi(D_1, D_2)/(2D_1D_2))$. This implies that $\mathcal{R}(D_1, D_2) \subseteq \mathcal{R}_{12}(D_1, D_2)$

- Cooperative lower bound: The sum rate is lower bounded by the sum rate for the following scenario



Consider

$$\begin{aligned}
 n(R_1 + R_2) &\geq H(M_1, M_2) = I(X_1^n, X_2^n; M_1, M_2) \\
 &= h(X_1^n, X_2^n) - h(X_1^n, X_2^n | M_1, M_2) \\
 &\geq \frac{n}{2} \log ((2\pi e)^2 |K_X|) - \sum_{i=1}^n h(X_{1i}, X_{2i} | M_1, M_2) \\
 &\geq \frac{n}{2} \log ((2\pi e)^2 |K_X|) - \sum_{i=1}^n h(X_{1i} - \hat{X}_{1i}, X_{2i} - \hat{X}_{2i}) \\
 &\geq \frac{n}{2} \log ((2\pi e)^2 |K_X|) - \sum_{i=1}^n \frac{1}{2} \log ((2\pi e)^2 |\tilde{K}_i|) \\
 &\geq \frac{n}{2} \log ((2\pi e)^2 |K_X|) - \frac{n}{2} \log ((2\pi e)^2 |\tilde{K}|) \\
 &= \frac{n}{2} \log \frac{|K_X|}{|\tilde{K}|},
 \end{aligned}$$

where $\tilde{K}_i = K_{X(i)-\hat{X}(i)}$ and $\tilde{K} = (1/n) \sum_{i=1}^n \tilde{K}_i$

Since $\tilde{K}(j,j) \leq D_j$, $j = 1, 2$,

$$\tilde{K} \preceq K(\theta) := \begin{bmatrix} D_1 & \theta\sqrt{D_1 D_2} \\ \theta\sqrt{D_1 D_2} & D_2 \end{bmatrix}$$

for some $\theta \in [-1, 1]$. Hence,

$$R_1 + R_2 \geq R_1(\theta) := R \left(\frac{|K_{\mathbf{x}}|}{|K(\theta)|} \right)$$

- **μ -sum lower bound:** Let $Y_i = \mu_1 X_{1i} + \mu_2 X_{2i} + Z_i = \mu^T \mathbf{X}(i) + Z_i$, where $\{Z_i\}$ is a WGN(N) process independent of $\{(X_{1i}, X_{2i})\}$. Then for any (μ, N) ,

$$\begin{aligned} n(R_1 + R_2) &\geq H(M_1, M_2) = I(\mathbf{X}^n, Y^n; M_1, M_2) \\ &\geq h(\mathbf{X}^n, Y^n) - h(Y^n | M_1, M_2) - h(\mathbf{X}^n | M_1, M_2, Y^n) \\ &\geq \sum_{i=1}^n (h(\mathbf{X}(i), Y_i) - h(Y_i | M_1, M_2) - h(\mathbf{X}(i) | M_1, M_2, Y^n)) \\ &\geq \sum_{i=1}^n \frac{1}{2} \log \frac{|K_{\mathbf{x}}| \cdot N}{|\hat{K}_i| \cdot (\mu^T \tilde{K}_i \mu + N)} \\ &\geq \frac{n}{2} \log \frac{|K_{\mathbf{x}}| \cdot N}{|\hat{K}| \cdot (\mu^T \tilde{K} \mu + N)} \end{aligned}$$

$$\geq \frac{n}{2} \log \frac{|K_{\mathbf{x}}| \cdot N}{|\hat{K}| \cdot (\mu^T K(\theta) \mu + N)},$$

where $\hat{K}_i = K_{\mathbf{X}(i) | M_1, M_2, Y^n}$, $\hat{K} = (1/n) \sum_{i=1}^n \hat{K}_i$, and $K(\theta)$ is defined as in the cooperative bound

From this point on, we take $\mu = (1/\sqrt{D_1}, 1/\sqrt{D_2})$ and $N = (1 - \rho^2)/(\rho\sqrt{D_1 D_2})$. Then $\mu^T K(\theta) \mu = 2(1 + \theta)$ and it can be readily shown that $X_{1i} \rightarrow Y_i \rightarrow X_{2i}$ form a Markov chain

Furthermore, we can bound $|\hat{K}|$ as follows:

Lemma 5: $|\hat{K}| \leq D_1 D_2 N^2 (1 + \theta)^2 / (2(1 + \theta) + N)^2$

This can be shown by noting that \hat{K} is diagonal (which follows from the Markovity $X_{1i} \rightarrow Y_i \rightarrow X_{2i}$) and proving the matrix inequality

$\hat{K} \preceq \left(\tilde{K}^{-1} + (1/N) \mu \mu^T \right)^{-1}$ via estimation theory. Details are given in the Appendix

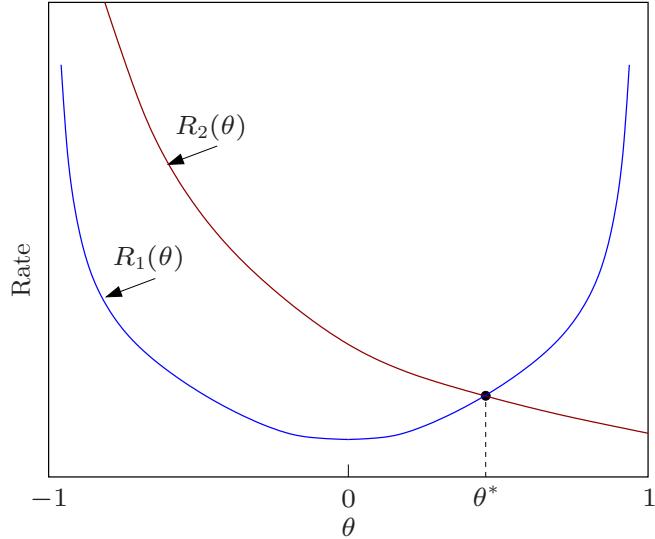
Thus, we have the following lower bound on the sum rate:

$$R_1 + R_2 \geq R_2(\theta) := R \left(\frac{|K_{\mathbf{x}}|(2(1 + \theta) + N)^2}{N D_1 D_2 (1 + \theta)^2} \right)$$

- Combining the two bounds, we have

$$R_1 + R_2 \geq \min_{\theta} \max \{R_1(\theta), R_2(\theta)\}$$

These two bounds are plotted in the following figure



It can be easily checked that $R_1(\theta) = R_2(\theta)$ at a unique point

$$\theta = \theta^* = \frac{\sqrt{(1-\rho^2)^2 + 4\rho^2 D_1 D_2} - (1-\rho^2)}{2\rho\sqrt{D_1 D_2}},$$

which is exactly what we chose in the proof of achievability

Finally, since $R_1(\theta)$ is increasing on $[\theta^*, 1]$ and $R_2(\theta)$ is decreasing on $(-1, 1)$, we can conclude that

$$\min_{\theta} \max\{R_1(\theta), R_2(\theta)\} = R_1(\theta^*) = R_2(\theta^*),$$

which implies that

$$R_1 + R_2 \geq R\left(\frac{(1-\rho^2)\phi(D_1, D_2)}{2D_1 D_2}\right)$$

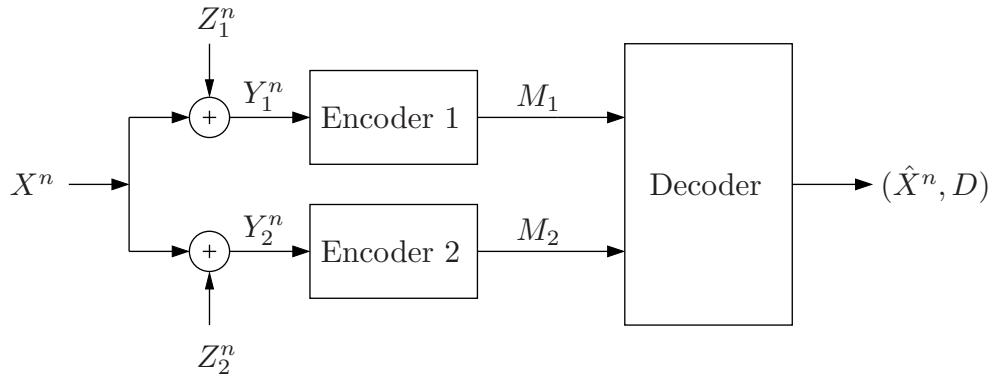
This completes the proof of converse.

- Remark: Our choice of Y such that $X_1 \rightarrow Y \rightarrow X_2$ form a Markov chain can be interpreted as capturing common information between two random variables X_1 and X_2 . We will encounter similar situations in Lecture Notes 14 and 15

Gaussian CEO Problem

- Consider the following distributed lossy source coding setup known as the Gaussian *CEO problem*, which is highly related to the quadratic Gaussian distributed source coding problem. Let X be a $\text{WGN}(P)$ source. Encoder $j = 1, 2$ observes a noisy version of X through an AWGN channel $Y_{ji} = X_i + Z_{ji}$, where $\{Z_{1i}\}$ and $\{Z_{2i}\}$ are independent WGN processes with average powers N_1 and N_2 , independent of $\{X_i\}$

The goal is to find an estimate \hat{X} of X with a prescribed average squared error distortion



- A $(2^{nR_1}, 2^{nR_2}, n)$ for the CEO problem code consists of:
 - Two encoders: Encoder 1 assigns an index $m_1(y_1^n) \in [1 : 2^{nR_1}]$ to each sequence $y_1^n \in \mathbb{R}^n$ and encoder 2 assigns an index $m_2(y_2^n) \in [1 : 2^{nR_2}]$ to each sequence $y_2^n \in \mathbb{R}^n$
 - A decoder that assigns an estimate \hat{x}^n to each index pair $(m_1, m_2) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$
- A rate-distortion triple (R_1, R_2, D) is said to be *achievable* if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with
$$\limsup_{n \rightarrow \infty} E \left(\frac{1}{n} \sum_{i=1}^n (X_i - \hat{X}_i)^2 \right) \leq D$$
- The rate-distortion region $\mathcal{R}_{\text{CEO}}(D)$ for the Gaussian CEO problem is the closure of the set of all rate pairs (R_1, R_2) such that (R_1, R_2, D) is achievable

Rate–Distortion Region of the Gaussian CEO Problem

- *Theorem [9, 10]:* The rate–distortion region $\mathcal{R}_{\text{CEO}}(D)$ for the Gaussian CEO problem is the set of (R_1, R_2) rate pairs such that

$$R_1 \geq r_1 + \frac{1}{2} \log \frac{1}{D} - \frac{1}{2} \log \left(\frac{1}{P} + \frac{1 - 2^{-2r_2}}{N_2} \right),$$

$$R_2 \geq r_2 + \frac{1}{2} \log \frac{1}{D} - \frac{1}{2} \log \left(\frac{1}{P} + \frac{1 - 2^{-2r_1}}{N_1} \right),$$

$$R_1 + R_2 \geq r_1 + r_2 + \frac{1}{2} \log \frac{P}{D}$$

for some $r_1 \geq 0$ and $r_2 \geq 0$ satisfying

$$\frac{1}{D} \leq \frac{1}{P} + \frac{1 - 2^{-2r_1}}{N_1} + \frac{1 - 2^{-2r_2}}{N_2}$$

- Achievability is proved using Berger–Tung coding with distributed Gaussian test channels as in the Gaussian distributed lossy source coding problem

Proof of Converse

- We need to show that for any sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with $\limsup_{n \rightarrow \infty} E \left(\frac{1}{n} \sum_{i=1}^n (X_i - \hat{X}_i)^2 \right) \leq D$, the rate pair $(R_1, R_2) \in \mathcal{R}_{\text{CEO}}(D)$
- Let \mathcal{J} be a subset of $\{1, 2\}$ and \mathcal{J}^c be its complement. Consider

$$\begin{aligned} \sum_{j \in \mathcal{J}} nR_j &\geq H(M(\mathcal{J})) \geq H(M(\mathcal{J})|M(\mathcal{J}^c)) \\ &\geq I(Y^n(\mathcal{J}); M(\mathcal{J})|M(\mathcal{J}^c)) \\ &= I(Y^n(\mathcal{J}), X^n; M(\mathcal{J})|M(\mathcal{J}^c)) \\ &= I(X^n; M(\mathcal{J})|M(\mathcal{J}^c)) + I(Y^n(\mathcal{J}); M(\mathcal{J})|X^n) \\ &= I(X^n; M(\mathcal{J}), M(\mathcal{J}^c)) - I(X^n; M(\mathcal{J}^c)) + \sum_{j \in \mathcal{J}} I(Y_j^n; M_j|X^n) \\ &\geq \frac{n}{2} \log \left(\frac{P}{D} \right) - I(X^n; M(\mathcal{J}^c)) + \sum_{j \in \mathcal{J}} nr_j, \end{aligned}$$

where $r_j := \frac{1}{n} I(Y_j^n; M_j|X^n)$ for $j = 1, 2$

- Let \tilde{X}_i be the MMSE estimate of X_i given $Y_i(\mathcal{J}^c)$. Then

$$\tilde{X}_i = \sum_{j \in \mathcal{J}^c} \frac{\tilde{N}}{N_j} Y_{ji} = \sum_{j \in \mathcal{J}^c} \frac{\tilde{N}}{N_j} (X_i + Z_{ji}), \quad X_i = \tilde{X}_i + \tilde{Z}_i,$$

where $\{\tilde{Z}_i\}$ is a WGN process with average power

$$\tilde{N} = 1 / \left(1/P + \sum_{j \in \mathcal{J}^c} 1/N_j \right), \text{ independent of } Y_i(\mathcal{J}^c)$$

- Using the conditional EPI, we have

$$\begin{aligned} 2^{\frac{2}{n}h(X^n|M(\mathcal{J}^c))} &\geq 2^{\frac{2}{n}h(\tilde{X}^n|M(\mathcal{J}^c))} + 2^{\frac{2}{n}h(\tilde{Z}^n|M(\mathcal{J}^c))} \\ &= 2^{\frac{2}{n}(h(\tilde{X}^n|X^n, M(\mathcal{J}^c)) + I(\tilde{X}^n; X^n|M(\mathcal{J}^c)))} + 2\pi e \tilde{N}, \text{ and} \end{aligned}$$

$$\begin{aligned} 2^{\frac{2}{n}h(\tilde{X}^n|X^n, M(\mathcal{J}^c))} &\geq \sum_{j \in \mathcal{J}^c} \frac{\tilde{N}^2}{N_j^2} 2^{\frac{2}{n}h(Y_j^n|X^n, M(\mathcal{J}^c))} = \sum_{j \in \mathcal{J}^c} \frac{\tilde{N}^2}{N_j^2} 2^{\frac{2}{n}h(Y_j^n|X^n, M_j)} \\ &= \sum_{j \in \mathcal{J}^c} \frac{\tilde{N}^2}{N_j^2} 2^{\frac{2}{n}(h(Y_j^n|X^n) + I(Y_j^n; M_j|X^n))} = \sum_{j \in \mathcal{J}^c} \frac{\tilde{N}^2}{N_j} 2\pi e 2^{-2r_j} \end{aligned}$$

Now,

$$2^{\frac{2}{n}I(X^n; \tilde{X}^n|M(\mathcal{J}^c))} = 2^{\frac{2}{n}(h(X^n|M(\mathcal{J}^c)) - h(X^n|\tilde{X}^n, M(\mathcal{J}^c)))} = \frac{1}{2\pi e \tilde{N}} \cdot 2^{\frac{2}{n}h(X^n|M(\mathcal{J}^c))}$$

We have

$$\begin{aligned} 2^{\frac{2}{n}h(X^n|M(\mathcal{J}^c))} &\geq \left(\sum_{j \in \mathcal{J}^c} \frac{\tilde{N}^2}{N_j} 2\pi e 2^{-2r_j} \right) \left(\frac{1}{2\pi e \tilde{N}} 2^{\frac{2}{n}h(X^n|M(\mathcal{J}^c))} \right) + 2\pi e \tilde{N} \\ &= \sum_{j \in \mathcal{J}^c} \frac{\tilde{N}}{N_j} 2^{-2r_j} 2^{\frac{2}{n}h(X^n|M(\mathcal{J}^c))} + 2\pi e \tilde{N}, \\ 2^{\frac{2}{n}I(X^n; M(\mathcal{J}^c))} &= 2^{\frac{2}{n}(h(X^n) - h(X^n|M(\mathcal{J}^c)))} = (2\pi e P) 2^{-\frac{2}{n}h(X^n|M(\mathcal{J}^c))} \\ &\leq \frac{P}{\tilde{N}} - \sum_{j \in \mathcal{J}^c} \frac{P}{N_j} 2^{-2r_j} = 1 + \sum_{j \in \mathcal{J}^c} \frac{P}{N_j} (1 - 2^{-2r_j}) \end{aligned}$$

Thus,

$$\begin{aligned} \sum_{j \in \mathcal{J}} R_j &\geq \frac{1}{2} \log \left(\frac{P}{D} \right) - \frac{1}{2} \log \left(1 + \sum_{j \in \mathcal{J}^c} \frac{P}{N_j} (1 - 2^{-2r_j}) \right) + \sum_{j \in \mathcal{J}} r_j \\ &= \frac{1}{2} \log \left(\frac{1}{D} \right) - \frac{1}{2} \log \left(\frac{1}{P} + \sum_{j \in \mathcal{J}^c} \frac{1}{N_j} (1 - 2^{-2r_j}) \right) + \sum_{j \in \mathcal{J}} r_j \end{aligned}$$

Substituting $\mathcal{J} = \{1, 2\}$, $\{1\}$, $\{2\}$, and \emptyset establishes the three inequalities of the rate-distortion region

Counterexample: Doubly Symmetric Binary Sources

- The Berger–Tung inner bound is not tight in general. We show this via the following counterexample [5]
- Let (\tilde{X}, \tilde{Y}) be DSBS(p) with $p \in (0, 1/2)$, $X_1 = (\tilde{X}, \tilde{Y})$, $X_2 = \tilde{Y}$, $d_1(x_1, \hat{x}_1) = d(\tilde{x}, \hat{x}_1)$ be the Hamming distortion measure on \tilde{X} , and $d_2(x_2, \hat{x}_2) \equiv 0$ (i.e., the decoder is interested in recovering X_1 only). We consider the minimum sum-rate achievable for distortion D_1
- Since both encoders have access to \tilde{Y} , encoder 2 can describe \tilde{Y} by V and then encoder 1 can describe \tilde{X} conditioned on V . Hence it can be easily shown that the rate pair (R_1, R_2) is achievable for distortion D_1 if

$$R_1 > I(\tilde{X}; \hat{X}_1 | V), \quad R_2 > I(\tilde{Y}; V)$$

for some $p(v|\tilde{y})p(\hat{x}_1|\tilde{x}, v)$ such that $E(d(\tilde{X}, \hat{X}_1)) \leq D_1$. By taking $p(v|\tilde{y})$ to be a BSC(α), this region can be further simplified (check!) as the set of rate pairs (R_1, R_2) such that

$$R_1 > H(\alpha * p) - H(D_1), \quad R_2 > 1 - H(\alpha)$$

for some $\alpha \in [0, 1/2]$ satisfying $H(\alpha * p) - H(D_1) \geq 0$

- It can be easily shown that the Berger–Tung inner bound is contained in the above region. In fact, noting that $R_{\text{SI-ED}}(D_1) < R_{\text{SI-D}}(D_1)$ for DSBS($\alpha * p$) and using Mrs. Gerber's lemma, we can prove that some boundary point of the above region lies strictly outside the rate region of Theorem 5
- Berger–Tung coding does not handle well the case in which encoders can cooperate using their knowledge about the other source
- Remarks
 - The above rate region is optimal and characterizes the rate–distortion region
 - More generally, if X_2 is a function of X_1 and $d_2 \equiv 0$, the rate–distortion region [4] is the set of rate–distortion triples (R_1, R_2, D_1) such that

$$R_1 \geq I(X_1; \hat{X}_1 | V), \quad R_2 \geq I(X_2; V), \quad D_1 \geq E(d_1(X_1, \hat{X}_1))$$

for some $p(v|x_2)p(\hat{x}_1|x_1, v)$ with $|\mathcal{V}| \leq |\mathcal{X}_2| + 2$

The converse follows from the Berger–Tung outer bound. The achievability follows similar lines to the one for the above example. This coding scheme can be generalized [5] to include the Berger–Tung inner bound and cooperation between encoders based on common part between X_1 and X_2 (cf. Lecture Notes 15)

Extensions to More Than 2 Sources

- The rate–distortion region of the quadratic Gaussian distributed source coding problem with more than two sources is known only for sources satisfying a certain tree-structure Markovity condition [11].
- In addition, the optimal sum rate of the quadratic Gaussian distributed lossy source coding problem with more than two sources is known when the prescribed distortions are identical
- The rate–distortion region for the Gaussian CEO problem can be extended to more than two encoders [9, 10]

Key New Ideas and Techniques

- Mutual packing lemma
- Estimation theoretic techniques
- CEO problem

References

- [1] S.-Y. Tung, "Multiterminal source coding," Ph.D. Thesis, Cornell University, Ithaca, NY, 1978.
- [2] T. Berger and R. W. Yeung, "Multiterminal source encoding with one distortion criterion," *IEEE Trans. Inf. Theory*, vol. 35, no. 2, pp. 228–236, 1989.
- [3] A. B. Wagner, S. Tavildar, and P. Viswanath, "Rate region of the quadratic Gaussian two-encoder source-coding problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1938–1961, May 2008.
- [4] A. H. Kaspi and T. Berger, "Rate-distortion for correlated sources with partially separated encoders," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 828–840, 1982.
- [5] A. B. Wagner, B. G. Kelly, and Y. Altuğ, "The lossy one-helper conjecture is false," in *Proc. 47th Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, Sept. 2009.
- [6] A. B. Wagner and V. Anantharam, "An improved outer bound for multiterminal source coding," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1919–1937, 2008.
- [7] Y. Oohama, "Gaussian multiterminal source coding," *IEEE Trans. Inf. Theory*, vol. 43, no. 6, pp. 1912–1923, Nov. 1997.
- [8] J. Wang, J. Chen, and X. Wu, "On the minimum sum rate of gaussian multiterminal source coding: New proofs," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 1463–1467.
- [9] Y. Oohama, "Rate-distortion theory for Gaussian multiterminal source coding systems with several side informations at the decoder," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2577–2593, July 2005.

- [10] V. Prabhakaran, D. N. C. Tse, and K. Ramchandran, "Rate region of the quadratic Gaussian CEO problem," in *Proc. IEEE International Symposium on Information Theory*, Chicago, IL, June/July 2004, p. 117.
- [11] S. Tavildar, P. Viswanath, and A. B. Wagner, "The Gaussian many-help-one distributed source coding problem," in *Proc. IEEE Information Theory Workshop*, Chengdu, China, Oct. 2006, pp. 596–600.
- [12] W. Uhlmann, "Vergleich der hypergeometrischen mit der Binomial-Verteilung," *Metrika*, vol. 10, pp. 145–158, 1966.
- [13] A. Orlitsky and A. El Gamal, "Average and randomized communication complexity," *IEEE Trans. Inf. Theory*, vol. 36, no. 1, pp. 3–16, 1990.

Appendix: Proof of Markov Lemma

- By the union of events bound,

$$\begin{aligned} \mathsf{P}\{(x^n, y^n, Z^n) \notin \mathcal{T}_\epsilon^{(n)}\} \\ \leq \sum_{x, y, z} \mathsf{P}\{|\pi(x, y, z | x^n, y^n, Z^n) - p(x, y, z)| \geq \epsilon p(x, y, z)\} \end{aligned}$$

Hence it suffices to show that

$$\begin{aligned} \mathsf{P}(\mathcal{E}(x, y, z)) := \mathsf{P}\{|\pi(x, y, z | x^n, y^n, Z^n) - p(x, y, z)| \geq \epsilon p(x, y, z)\} \rightarrow 0 \\ \text{as } n \rightarrow \infty \text{ for each } (x, y, z) \in \mathcal{X} \times \mathcal{Y} \times \mathcal{Z} \end{aligned}$$

- Given (x, y, z) , define the sets

$$\begin{aligned} \mathcal{A}(n_{yz}) &:= \{z^n : \pi(y, z | y^n, z^n) = n_{yz}/n\}, \quad \text{for } n_{yz} \in [0 : n] \\ \mathcal{A}_1 &:= \{z^n : (y^n, z^n) \in \mathcal{T}_{\epsilon'}^{(n)}(Y, Z)\}, \\ \mathcal{A}_2 &:= \{z^n : |\pi(x, y, z | x^n, y^n, z^n) - p(x, y, z)| \geq \epsilon p(x, y, z)\} \end{aligned}$$

Then,

$$\mathsf{P}(\mathcal{E}(x, y, z)) = \mathsf{P}\{Z^n \in \mathcal{A}_2\} \leq \mathsf{P}\{Z^n \in \mathcal{A}_1^c\} + \mathsf{P}\{Z^n \in \mathcal{A}_1 \cap \mathcal{A}_2\}$$

We bound each term:

- By the assumption on $p(z^n | y^n)$, the first term $\rightarrow 0$ as $n \rightarrow \infty$
- For the second term, consider

$$\begin{aligned} \mathsf{P}\{Z^n \in \mathcal{A}_1 \cap \mathcal{A}_2\} &= \sum_{z^n \in \mathcal{A}_1 \cap \mathcal{A}_2} p(z^n | y^n) \\ &\leq \sum_{n_{yz}} |\mathcal{A}(n_{yz}) \cap \mathcal{A}_2| \cdot 2^{-n(H(Z|Y) - \delta(\epsilon'))} \end{aligned}$$

where the last summation is over all n_{yz} such that

$$|n_{yz} - np(y, z)| \leq \epsilon' np(y, z)$$

and the inequality follows from the first condition of the lemma

Let $n_{xy} := n\pi(x, y | x^n, y^n)$ and $n_y := n\pi(y | y^n)$. Let K be a hypergeometric random variable that represents the number of red balls in a sequence of n_{yz} draws without replacement from a bag of n_{xy} red balls and $n_y - n_{xy}$ blue balls. Then

$$\mathsf{P}\{K = k\} = \frac{\binom{n_{xy}}{k} \binom{n_y - n_{xy}}{n_{yz} - k}}{\binom{n_y}{n_{yz}}}$$

for $k \in [0 : n_{xy}]$

Consider

$$\begin{aligned}
|\mathcal{A}(n_{yz}) \cap \mathcal{A}_2| &= \sum_{k:|k-np(x,y,z)| \geq \epsilon np(x,y,z)} \binom{n_{xy}}{k} \binom{n_y - n_{xy}}{n_{yz} - k} \\
&= \sum_{k:|k-np(x,y,z)| \geq \epsilon np(x,y,z)} \binom{n_y}{n_{yz}} \mathbb{P}\{K = k\} \\
&\stackrel{(a)}{\leq} 2^{n_y H(n_{yz}/n_y)} \mathbb{P}\{|K - np(x, y, z)| \geq \epsilon np(x, y, z)\} \\
&\stackrel{(b)}{\leq} 2^{np(y)(H(p(z|y)) + \delta(\epsilon'))} \mathbb{P}\{|K - np(x, y, z)| \geq \epsilon np(x, y, z)\} \\
&\stackrel{(c)}{\leq} 2^{n(H(Z|Y) + \delta(\epsilon'))} \mathbb{P}\{|K - np(x, y, z)| \geq \epsilon np(x, y, z)\}
\end{aligned}$$

where (a) follows since $\binom{n_y}{n_{yz}} \leq 2^{n_y H(n_{yz}/n_y)}$, (b) follows since $|n_y - np(y)| \leq \epsilon' p(y)$, $|n_{yz} - np(y, z)| \leq \epsilon' p(y, z)$, and (c) follows since $p(y)H(p(z|y)) \leq \sum_y p(y)H(p(z|y)) = H(I_{\{Z=z\}}|Y) \leq H(Z|Y)$

Note that $E(K) = n_{xy}n_{yz}/n_y$ satisfies

$$(1 - \delta(\epsilon'))p(x, y, z) \leq E(K) \leq (1 + \delta(\epsilon'))p(x, y, z)$$

from the conditions on n_{xy}, n_{yz}, n_y

Now let $K' \sim \text{Binom}(n_{xy}, n_{yz}/n_y)$ be a binomial random variable with the

same mean $E(K') = E(K) = n_{xy}n_{yz}/n_y$. It can be shown [12, 13] that if $n(1 - \epsilon)p(x, y, z) \leq E(K) \leq n(1 + \epsilon)p(x, y, z)$ (which holds if ϵ' is sufficiently small), then

$$\begin{aligned}
\mathbb{P}\{|K - np(x, y, z)| \geq \epsilon np(x, y, z)\} &\leq \mathbb{P}\{|K' - np(x, y, z)| \geq \epsilon np(x, y, z)\} \\
&\leq 2e^{-(\epsilon - \delta(\epsilon'))^2 p(x, y, z)/4},
\end{aligned}$$

where the inequality follows by the Chernoff bound

Combining the above inequalities, we have

$$\begin{aligned}
\mathbb{P}\{Z^n \in \mathcal{A}_1 \cap \mathcal{A}_2\} &\leq \sum_{n_{yz}} 2^{n\delta(\epsilon')} \cdot 2e^{-(\epsilon - \delta(\epsilon'))^2 p(x, y, z)/4} \\
&\leq (n+1)2^{n\delta(\epsilon')} \cdot 2e^{-(\epsilon - \delta(\epsilon'))^2 p(x, y, z)/4},
\end{aligned}$$

which tends to zero as $n \rightarrow \infty$ if ϵ' is sufficiently small

Appendix: Proof of Lemma 2

- For every $u_2^n \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)$,

$$\begin{aligned}
& \mathsf{P}\{U_2^n(L_2) = u_2^n \mid X_2^n = x_2^n\} \\
&= \mathsf{P}\{U_2^n(L_2) = u_2^n, U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n) \mid X_2^n = x_2^n\} \\
&= \mathsf{P}\{U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n) \mid X_2^n = x_2^n\} \\
&\quad \cdot \mathsf{P}\{U_2^n(L_2) = u_2^n \mid X_2^n = x_2^n, U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\} \\
&\leq \mathsf{P}\{U_2^n(L_2) = u_2^n \mid X_2^n = x_2^n, U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\} \\
&= \sum_{l_2} \mathsf{P}\{U_2^n(L_2) = u_2^n, L_2 = l_2 \mid X_2^n = x_2^n, U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\} \\
&= \sum_{l_2} \mathsf{P}\{L_2 = l_2 \mid X_2^n = x_2^n, U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\} \\
&\quad \cdot \mathsf{P}\{U_2^n(l_2) = u_2^n \mid X_2^n = x_2^n, U_2^n(l_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n), L_2 = l_2\}
\end{aligned}$$

$$\begin{aligned}
&\stackrel{(a)}{=} \sum_{l_2} \mathsf{P}\{L_2 = l_2 \mid X_2^n = x_2^n, U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\} \\
&\quad \cdot \mathsf{P}\{U_2^n(l_2) = u_2^n \mid U_2^n(l_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\} \\
&\stackrel{(b)}{\leq} \sum_{l_2} \mathsf{P}\{L_2 = l_2 \mid X_2^n = x_2^n, U_2^n(L_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\} \cdot 2^{-n(H(U_2|X_2)-\delta(\epsilon'))} \\
&= 2^{-n(H(U_2|X_2)-\delta(\epsilon'))},
\end{aligned}$$

where (a) follows since $U_2^n(m_2)$ is independent of X_2^n and $U_2^n(l'_2)$ for $l'_2 \neq l_2$, L_2 is a function of X_2^n and indicator variables of the events

$\{U_2^n(l_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\}$, $l_2 \in [1 : 2^{nR_2}]$, and hence given the event

$\{U_2^n(l_2) \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)\}$, $\{U_2^n(l_2) = u_2^n\}$ is conditionally independent of

$\{X_2^n = x_2^n, L_2 = l_2\}$, and (b) follows from the properties of the typical sequences

- Similarly, for every $u_2^n \in \mathcal{T}_{\epsilon'}^{(n)}(U_2|x_2^n)$ and n sufficiently large,

$$\mathsf{P}\{U_2^n(L_2) = u_2^n \mid X_2^n = x_2^n\} \geq (1 - \epsilon') 2^{-n(H(U_2|X_2)+\delta(\epsilon'))}$$

- This completes the proof of Lemma 2

Appendix: Proof of Lemma 3

- Since $D_2 \geq 1 - \rho^2 + \rho^2 D_1$,

$$\begin{aligned}\mathcal{R}_{12}(D_1, D_2) &\supseteq \mathcal{R}_{12}(D_1, 1 - \rho^2 + \rho^2 D_1) \\ &= \{(R_1, R_2) : R_1 + R_2 \geq R(1/D_1)\}\end{aligned}$$

If $(R_1, R_2) \in \mathcal{R}_1(D_1)$, then

$$R_1 + R_2 \geq g_1(R_2, D_1) + R_2 \geq g_1(0, D_1) = R(1/D_1)$$

since $g_1(R_2, D_1) + R_2$ is an increasing function of R_2 . Thus,

$$\mathcal{R}_1(D_1) \subseteq \mathcal{R}_{12}(D_1, D_2)$$

- On the other hand, the rate regions $\mathcal{R}_1(D_1)$ and $\mathcal{R}_2(D_2)$ can be expressed as

$$\mathcal{R}_1(D_1) = \left\{ (R_1, R_2) : R_1 \geq R \left(\frac{1 - \rho^2 + \rho^2 2^{-2R_2}}{D_1} \right) \right\},$$

$$\mathcal{R}_2(D_2) = \left\{ (R_1, R_2) : R_1 \geq R \left(\frac{\rho^2}{D_2 2^{2R_2} - 1 + \rho^2} \right) \right\}$$

But $D_2 \geq 1 - \rho^2 + \rho^2 D_1$ implies that

$$\frac{\rho^2}{D_2 2^{2R_2} - 1 + \rho^2} \leq \frac{1 - \rho^2 + \rho^2 2^{-2R_2}}{D_1}$$

Thus, $\mathcal{R}_1(D_1) \subseteq \mathcal{R}_2(D_2)$

Appendix: Proof of Lemma 5

- The proof has three steps. First, we show that $\hat{K} \succeq 0$ is diagonal. Second, we prove the matrix inequality $\hat{K} \preceq (\tilde{K}^{-1} + (1/N)\boldsymbol{\mu}^T \boldsymbol{\mu})^{-1}$. Since $\tilde{K} \preceq K(\theta)$, it can be further shown by the matrix inversion lemma in Appendix B that

$$\hat{K} \preceq (K^{-1}(\theta) + (1/N)\boldsymbol{\mu}^T \boldsymbol{\mu})^{-1} = \begin{bmatrix} (1 - \alpha)D_1 & (\theta - \alpha)\sqrt{D_1 D_2} \\ (\theta - \alpha)\sqrt{D_1 D_2} & (1 - \alpha)D_2 \end{bmatrix},$$

where $\alpha = (1 + \theta)^2 / (2(1 + \theta) + N)$. Finally, combining the above matrix inequality with the fact that \hat{K} is diagonal, we show that

$$|\hat{K}| \leq D_1 D_2 (1 + \theta - 2\alpha)^2 = D_1 D_2 N^2 (1 + \theta)^2 / (2(1 + \theta) + N)^2$$

- Step 1: Since $M_1 \rightarrow X_1^n \rightarrow Y^n \rightarrow X_2^n \rightarrow M_2$ form a Markov chain,

$$\mathbb{E}[(X_{1i} - \mathbb{E}(X_{1i}|Y^n, M_1, M_2))(X_{2i'} - \mathbb{E}(X_{2i'}|Y^n, M_1, M_2))]$$

$$= \mathbb{E}[(X_{1i} - \mathbb{E}(X_{1i}|Y^n, X_{2i'}, M_1, M_2))(X_{2i'} - \mathbb{E}(X_{2i'}|Y^n, M_1, M_2))] = 0$$

for all $i, i' \in [1 : n]$. Thus, $\hat{K} = \frac{1}{n} \sum_{i=1}^n K_{\mathbf{X}(i)|\mathbf{Y}^n, M_1, M_2} =: \text{diag}(\beta_1, \beta_2)$

- Step 2: Let $\tilde{\mathbf{Y}}(i) = (Y_i, \hat{\mathbf{X}}(i))$, where $\hat{\mathbf{X}}(i) = \mathbb{E}(\mathbf{X}(i)|M_1, M_2)$ for $i \in [1 : n]$, and

$$A := \left(\frac{1}{n} \sum_{i=1}^n K_{\mathbf{X}(i), \tilde{\mathbf{Y}}(i)} \right) \left(\frac{1}{n} \sum_{i=1}^n K_{\tilde{\mathbf{Y}}(i)} \right)^{-1}$$

Then,

$$\begin{aligned}
& \frac{1}{n} \sum_{i=1}^n K_{\mathbf{X}(i)|\mathbf{Y}^n, M_1, M_2} \\
& \stackrel{(a)}{\preceq} \frac{1}{n} \sum_{i=1}^n K_{\mathbf{X}(i) - A\tilde{\mathbf{Y}}(i)} \\
& \stackrel{(b)}{=} \left(\frac{1}{n} \sum_{i=1}^n K_{\mathbf{X}(i)} \right) - \left(\frac{1}{n} \sum_{i=1}^n K_{\mathbf{X}(i)\tilde{\mathbf{Y}}(i)} \right) \left(\frac{1}{n} \sum_{i=1}^n K_{\tilde{\mathbf{Y}}(i)} \right)^{-1} \left(\frac{1}{n} \sum_{i=1}^n K_{\tilde{\mathbf{Y}}(i)\mathbf{X}(i)} \right) \\
& \stackrel{(c)}{=} K_{\mathbf{X}} - \begin{bmatrix} K_{\mathbf{X}}\boldsymbol{\mu} & K_{\mathbf{X}} - \tilde{K} \end{bmatrix} \begin{bmatrix} \boldsymbol{\mu}^T K_{\mathbf{X}}\boldsymbol{\mu} + N & \boldsymbol{\mu}^T(K_{\mathbf{X}} - \tilde{K}) \\ (K_{\mathbf{X}} - \tilde{K})\boldsymbol{\mu} & K_{\mathbf{X}} - \tilde{K} \end{bmatrix}^{-1} \begin{bmatrix} \boldsymbol{\mu}^T K_{\mathbf{X}} \\ K_{\mathbf{X}} - \tilde{K} \end{bmatrix} \\
& \stackrel{(d)}{=} \left(\tilde{K}^{-1} + (1/N)\boldsymbol{\mu}\boldsymbol{\mu}^T \right)^{-1} \\
& \stackrel{(e)}{\preceq} \left(K^{-1}(\theta) + (1/N)\boldsymbol{\mu}\boldsymbol{\mu}^T \right)^{-1},
\end{aligned}$$

where (a) follows from the optimality of MMSE estimate $E(\mathbf{X}(i)|\mathbf{Y}^n, M_1, M_2)$ (compared to the estimate $A\tilde{\mathbf{Y}}(i)$), (b) follows from the definition of the matrix A , (c) follows since $\frac{1}{n} \sum_{i=1}^n K_{\hat{\mathbf{X}}(i)} = K_{\mathbf{X}} - \tilde{K}$, (d) follows from the matrix inversion formula in Appendix B, and (e) follows since $\tilde{K} \preceq K(\theta)$

Substituting for $\boldsymbol{\mu}$ and N , we have shown

$$\hat{K} = \text{diag}(\beta_1, \beta_2) \preceq \begin{bmatrix} (1-\alpha)D_1 & (\theta-\alpha)\sqrt{D_1 D_2} \\ (\theta-\alpha)\sqrt{D_1 D_2} & (1-\alpha)D_2 \end{bmatrix},$$

where $\alpha = (1+\theta)^2/(2(1+\theta) + N)$

- Step 3: We first note that if $b_1, b_2 \geq 0$ and

$$\begin{bmatrix} b_1 & 0 \\ 0 & b_2 \end{bmatrix} \preceq \begin{bmatrix} a & c \\ c & a \end{bmatrix},$$

then $b_1 b_2 \leq (a-c)^2$. This can be easily checked by simple algebra. Now let $\Lambda := \text{diag}(1/\sqrt{D_1}, -1/\sqrt{D_2})$. Then

$$\Lambda \text{diag}(\beta_1, \beta_2) \Lambda \preceq \Lambda \begin{bmatrix} (1-\alpha)D_1 & (\theta-\alpha)\sqrt{D_1 D_2} \\ (\theta-\alpha)\sqrt{D_1 D_2} & (1-\alpha)D_2 \end{bmatrix} \Lambda = \begin{bmatrix} 1-\alpha & \alpha-\theta \\ \alpha-\theta & 1-\alpha \end{bmatrix}$$

Therefore,

$$\frac{\beta_1 \beta_2}{D_1 D_2} \leq ((1-\alpha) - (\alpha-\theta))^2,$$

or equivalently,

$$\beta_1 \beta_2 \leq D_1 D_2 (1 + \theta - 2\alpha)^2$$

Plugging in α and simplifying, we obtain the desired inequality

Lecture Notes 14

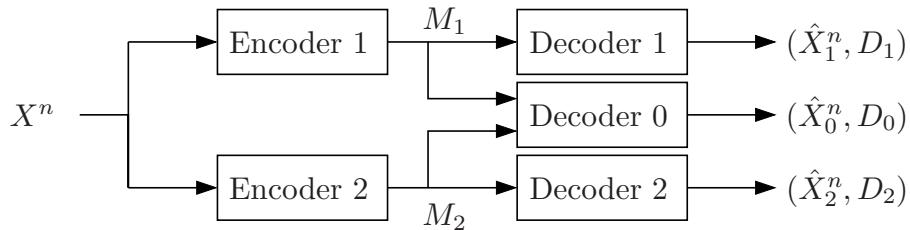
Multiple Descriptions

- Problem Setup
- Special Cases
- El Gamal–Cover Inner Bound
- Quadratic Gaussian Multiple Descriptions
- Successive Refinement
- Zhang–Berger Inner Bound
- Extensions to More than 2 Descriptions

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- Consider a DMS $(\mathcal{X}, p(x))$ and three distortion measures $d_j(x, \hat{x}_j)$, $\hat{x}_j \in \hat{\mathcal{X}}_j$ for $j = 0, 1, 2$
- Two descriptions of a source X are generated by two encoders, so that decoder 1 that receives only the first description can reproduce X with distortion D_1 , decoder 2 that receives only the second description can reproduce X with distortion D_2 , and decoder 0 that receives both descriptions can reproduce X with distortion D_0 . We wish to find the optimal description rates needed



- A $(2^{nR_1}, 2^{nR_2}, n)$ *multiple description* code consists of
 1. Two encoders: Encoder 1 assigns an index $m_1(x^n) \in [1 : 2^{nR_1}]$ and encoder 2 assigns an index $m_2(x^n) \in [1 : 2^{nR_2}]$ to each sequence $x^n \in \mathcal{X}^n$
 2. Three decoders: Decoder 1 assigns an estimate \hat{x}_1^n to each index m_1 .

Decoder 2 assigns an estimate \hat{x}_2^n to each index m_2 . Decoder 0 assigns an estimate \hat{x}_0^n to each pair (m_1, m_2)

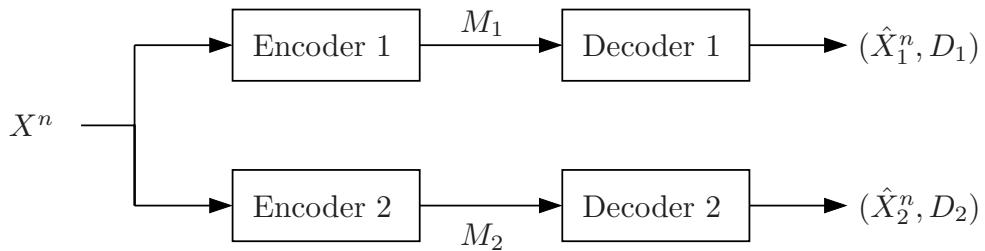
- A rate-distortion quintuple $(R_1, R_2, D_0, D_1, D_2)$ is said to be achievable (and a rate pair (R_1, R_2) is said to be achievable for distortion triple (D_0, D_1, D_2)), if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with average distortion

$$\limsup_{n \rightarrow \infty} E(d_j(X^n, \hat{X}_j^n)) \leq D_j \text{ for } j = 0, 1, 2$$

- The *rate-distortion region* $\mathcal{R}(D_0, D_1, D_2)$ for distortion triple (D_0, D_1, D_2) is the closure of the set of rate pairs (R_1, R_2) such that $(R_1, R_2, D_0, D_1, D_2)$ is achievable
- The tension in this problem arises from the fact that two good individual descriptions must be close to the source and so must be highly dependent. Thus the second description contributes little extra information beyond the first alone
On the other hand, to obtain more information by combining two descriptions, they must be far apart and so must be highly independent
Two independent descriptions, however, cannot in general be individually good
- The multiple description rate-distortion region is *not* known in general

Special Cases

1. No combined description ($D_0 = \infty$):

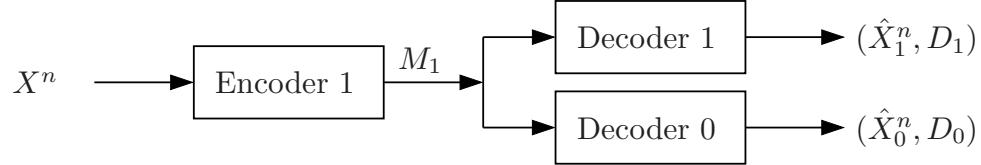


The rate-distortion region for distortion (D_1, D_2) is the set of rate pairs (R_1, R_2) such that

$$R_1 \geq I(X; \hat{X}_1), \quad R_2 \geq I(X; \hat{X}_2),$$

for some $p(\hat{x}_1|x)p(\hat{x}_2|x)$ such that $E(d_1(X; \hat{X}_1)) \leq D_1$, $E(d_2(X; \hat{X}_2)) \leq D_2$

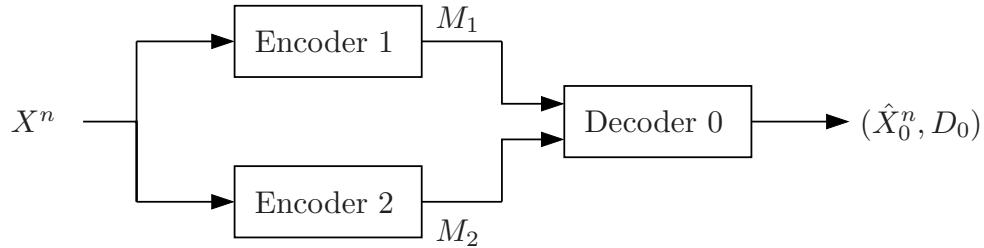
2. Single description with two reproductions ($R_2 = 0$):



The rate-distortion function is given by

$$R(D_1, D_0) = \min_{p(\hat{x}_1, \hat{x}_0|x): E(d_1(X, \hat{X}_1)) \leq D_1, E(d_0(X, \hat{X}_0)) \leq D_0} I(\hat{X}_1, \hat{X}_0; X)$$

3. Combined description only ($D_1 = D_2 = \infty$):



The rate-distortion region for distortion D_0 is the set of rate pairs (R_1, R_2) such that

$$R_1 + R_2 \geq I(\hat{X}_0; X) \text{ for some } p(\hat{x}_0|x) \text{ such that } E(d_0(\hat{X}_0, X)) \leq D_0$$

Simple Outer Bound

- If the rate pair (R_1, R_2) is achievable for distortion triple (D_0, D_1, D_2) , then it must satisfy the constraints

$$R_1 \geq I(X; \hat{X}_1),$$

$$R_2 \geq I(X; \hat{X}_2),$$

$$R_1 + R_2 \geq I(X; \hat{X}_0, \hat{X}_1, \hat{X}_2)$$

for some $p(\hat{x}_0, \hat{x}_1, \hat{x}_2|x)$ such that $E(d_j(X, \hat{X}_j)) \leq D_j$, $j = 0, 1, 2$

- This outer bound follows trivially from the converse for the lossy source coding theorem
- This outer bound is tight for all special cases considered above (check!)
- However, it is not tight in general

El Gamal–Cover Inner Bound

- *Theorem 1* (El Gamal–Cover Inner Bound) [1]: Let X be a DMS and $d_j(x, \hat{x}_j)$, $j = 0, 1, 2$, be three distortion measures. A rate pair (R_1, R_2) is achievable with distortion triple (D_0, D_1, D_2) if

$$R_1 > I(X; \hat{X}_1 | Q),$$

$$R_2 > I(X; \hat{X}_2 | Q),$$

$$R_1 + R_2 > I(X; \hat{X}_0, \hat{X}_1, \hat{X}_2 | Q) + I(\hat{X}_1; \hat{X}_2 | Q)$$

for some $p(q)p(\hat{x}_0, \hat{x}_1, \hat{x}_2 | x, q)$ such that

$$\mathbb{E}(d_0(X, \hat{X}_0)) \leq D_0,$$

$$\mathbb{E}(d_1(X, \hat{X}_1)) \leq D_1,$$

$$\mathbb{E}(d_2(X, \hat{X}_2)) \leq D_2$$

- It is easy to see that the above inner bound contains all special cases discussed above
- Excess rate: From the lossy source coding theorem, we know that $R_1 + R_2 \geq R(D_0)$, which is the rate–distortion function for X with respect to the distortion measure d_0 evaluated at D_0

The multiple descriptions are said to have *no excess rate* if $R_1 + R_2 = R(D_0)$; otherwise they have excess rate

- The El Gamal–Cover inner bound is optimal in some special case, including:
 - all previous special cases,
 - when $D_2 = \infty$ (successive refinement) discussed later,
 - when $d_1(x, \hat{x}_1) = 0$ if $\hat{x}_1 = g(x)$ and $d_1(x, \hat{x}_1) = 1$, otherwise, and $D_1 = 0$ (i.e., \hat{X}_1 recovers some deterministic function $g(X)$ losslessly) [2],
 - when there is no excess rate [3], and
 - the quadratic Gaussian case [4]
- However, the region is not optimal in general for the excess rate case [5]

Multiple Descriptions of a Bernoulli Source

- Consider the multiple descriptions problem for a $\text{Bern}(1/2)$ source X , where d_0, d_1, d_2 are Hamming distortion measures
- No-excess rate example: Assume we want $R_1 = R_2 = 1/2$ and $D_0 = 0$
Symmetry suggests that $D_1 = D_2 = D$
Define:

$$D_{\min} = \inf\{D : (1/2, 1/2) \text{ achievable for distortion } (0, D, D)\}$$

Note that $D_0 = 0$ requires the two descriptions, each at rate $1/2$, to be independent

- The lossy source coding theorem in this case gives $R = 1/2 \geq 1 - H(D)$, i.e., $D_{\min} \geq 0.11$
- Simple scheme: Split x^n into two equal length sequences (e.g., odd and even entries)
In this case $D_{\min} \leq D = 1/4$. Can we do better?
- Optimal scheme: Let \hat{X}_1 and \hat{X}_2 be independent $\text{Bern}(1/\sqrt{2})$ random variables, and $X = \hat{X}_1 \cdot \hat{X}_2$ and $\hat{X}_0 = X$, so $X \sim \text{Bern}(1/2)$ as it should be

Substituting in the inner bound rate constraints, we obtain

$$\begin{aligned} R_1 &\geq I(X; \hat{X}_1) \\ &= H(X) - H(X | \hat{X}_1) = 1 - \frac{1}{\sqrt{2}}H(1/\sqrt{2}) \approx 0.383, \end{aligned}$$

$$R_2 \geq I(X; \hat{X}_2) \approx 0.383,$$

$$\begin{aligned} R_1 + R_2 &\geq I(X; \hat{X}_1, \hat{X}_2) + I(\hat{X}_1; \hat{X}_2) \\ &= H(X) - H(X | \hat{X}_1, \hat{X}_2) + I(\hat{X}_1; \hat{X}_2) = 1 - 0 + 0 = 1 \end{aligned}$$

The average distortions are

$$\begin{aligned} E(d(X, \hat{X}_1)) &= P\{\hat{X}_1 \neq X\} \\ &= P\{\hat{X}_1 = 0, X = 1\} + P\{\hat{X}_1 = 1, X = 0\} = (\sqrt{2} - 1)/2 = 0.207, \end{aligned}$$

$$E(d(X, \hat{X}_2)) = (\sqrt{2} - 1)/2,$$

$$E(d(X, \hat{X}_0)) = 0$$

Thus $(R_1, R_2) = (1/2, 1/2)$ is achievable at distortions $(D_1, D_2, D_0) = ((\sqrt{2} - 1)/2, (\sqrt{2} - 1)/2, 0)$

- In [6] it was shown that indeed $D_{\min} = (\sqrt{2} - 1)/2$

Outline of Achievability

- Assume $|Q| = 1$ and fix $p(\hat{x}_0, \hat{x}_1, \hat{x}_2 | x)$. We independently generate $2^{nR_{11}}$ $\hat{x}_1^n(m_{11})$ sequences and $2^{nR_{22}}$ $\hat{x}_2^n(m_{22})$ sequences. For each sequence pair $(\hat{x}_1^n(m_{11}), \hat{x}_2^n(m_{22}))$, we generate 2^{nR_0} $\hat{x}_0^n(m_0, m_{11}, m_{22})$ sequences
- We use jointly typicality encoding. Given x^n , we find a jointly typical sequence pair $(\hat{x}_1^n(m_{11}), \hat{x}_2^n(m_{22}))$. By the multivariate covering lemma in Lecture Notes 9, if R_{11} and R_{22} are sufficiently large we can find with high probability a pair $\hat{x}_1^n(m_{11})$ and $\hat{x}_2^n(m_{22})$ that are jointly typical with x^n not only as individual pairs, but also as a triple

Given a jointly typical triple $(x^n, \hat{x}_1^n(m_{11}), \hat{x}_2^n(m_{22}))$, we find a jointly typical $\hat{x}_0^n(m_0, m_{11}, m_{22})$

The index m_0 is split into two independent parts m_{01} and m_{02} . Encoder 1 sends (m_{01}, m_{11}) to decoders 1 and 0, and encoder 2 sends (m_{02}, m_{22}) to decoders 2 and 0. The increase in rates beyond what is needed by decoders 1 and 2 to achieve their individual distortion constraints adds refinement information to help decoder 0 reconstruct x^n with (better) distortion D_0

Proof of Achievability

- Let $|Q| = 1$ and fix $p(\hat{x}_1, \hat{x}_2, \hat{x}_0 | x)$ such that

$$\mathbb{E}(d_j(X, \hat{X}_j)) \leq \frac{D_j}{(1 + \epsilon)} \text{ for } j = 0, 1, 2$$

Let $R_j = R_{0j} + R_{jj}$ and $R_0 = R_{01} + R_{02}$, where $R_{0j}, R_{jj} \geq 0$ for $j = 1, 2$

- Codebook generation: Randomly and independently generate $2^{nR_{11}}$ sequences $\hat{x}_1^n(m_{11})$, $m_{11} \in [1 : 2^{nR_{11}}]$, each according to $\prod_{i=1}^n p_{\hat{X}_1}(\hat{x}_{1i})$

Similarly generate $2^{nR_{22}}$ sequences $\hat{x}_2^n(m_{22})$, $m_{22} \in [1 : 2^{nR_{22}}]$, each according to $\prod_{i=1}^n p_{\hat{X}_2}(\hat{x}_{2i})$

For every $(\hat{x}_1^n(m_{11}), \hat{x}_2^n(m_{22})) \in \mathcal{T}_\epsilon^{(n)}$, $(m_{11}, m_{22}) \in [1 : 2^{nR_{11}}] \times [1 : 2^{nR_{22}}]$, randomly and conditionally independently generate 2^{nR_0} sequences $\hat{x}_0^n(m_{11}, m_{22}, m_0)$, $m_0 \in [1 : 2^{nR_0}]$, each according to $\prod_{i=1}^n p_{\hat{X}_0|\hat{X}_1, \hat{X}_2}(\hat{x}_{0i} | \hat{x}_{1i}, \hat{x}_{2i})$

- Encoding: To send x^n , find a triple (m_{11}, m_{22}, m_0) such that $(x^n, \hat{x}_1^n(m_{11}), \hat{x}_2^n(m_{22}), \hat{x}_0^n(m_{11}, m_{22}, m_0)) \in \mathcal{T}_\epsilon^{(n)}$

If no such triple exists set $(m_{11}, m_{22}, m_0) = (1, 1, 1)$

Represent $m_0 \in [1 : 2^{nR_0}]$ by $(m_{01}, m_{02}) \in [1 : 2^{nR_{01}}] \times [1 : 2^{nR_{02}}]$

Finally send (m_{11}, m_{01}) to decoder 1, (m_{22}, m_{02}) to decoder 2, and (m_{11}, m_{22}, m_0) to decoder 0

- Decoding: Decoder 1, given (m_{11}, m_{01}) , declares $\hat{x}_1^n(m_{11})$ as its estimate of x^n
 Decoder 2, given (m_{22}, m_{02}) , declares $\hat{x}_2^n(m_{22})$ as its estimate of x^n
 Decoder 0, given (m_{11}, m_{22}, m_0) , where $m_0 = (m_{01}, m_{02})$, declares $\hat{x}_0^n(m_{11}, m_{22}, m_0)$ as its estimate of x^n
- Expected distortion: Let (M_{11}, M_{22}) denote the pair of indices for covering codewords $(\hat{X}_1^n, \hat{X}_2^n)$. Define the “error” events:

$$\mathcal{E}_1 := \{(X^n, \hat{X}_1^n(m_{11}), \hat{X}_2^n(m_{22})) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } (m_{11}, m_{22})\},$$

$$\mathcal{E}_2 := \{(X^n, \hat{X}_1^n(M_{11}), \hat{X}_2^n(M_{22}), \hat{X}_0^n(M_{11}, M_{22}, m_0)) \notin \mathcal{T}_\epsilon^{(n)} \text{ for all } m_0\}$$

Thus the average probability of “error” is

$$P(\mathcal{E}) = P(\mathcal{E}_1) + P(\mathcal{E}_1^c \cap \mathcal{E}_2)$$

- By the multivariate covering lemma for 3-DMS and $r_3 = 0$ in Lecture Notes 7, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ if

$$R_{11} > I(X; \hat{X}_1) + \delta(\epsilon),$$

$$R_{22} > I(X; \hat{X}_2) + \delta(\epsilon),$$

$$R_{11} + R_{22} > I(X; \hat{X}_1, \hat{X}_2) + I(\hat{X}_1; \hat{X}_2) + 4\delta(\epsilon)$$

- By the covering lemma, $P(\mathcal{E}_1^c \cap \mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$ if
 $R_0 > I(X; \hat{X}_0 | \hat{X}_1, \hat{X}_2) + \delta(\epsilon)$
- Thus, $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$, if the inequalities specified in the theorem are satisfied
- Now by the law of total expectation and the typical average lemma,

$$E(d_j) \leq D_j + P(\mathcal{E})d_{\max}$$

for $j = 0, 1, 2$

If the inequalities in the theorem are satisfied, $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$ and thus $\limsup_{n \rightarrow \infty} E(d_j) \leq D_j$ for $j = 0, 1, 2$. In other words, the rate pair (R_1, R_2) satisfying the inequalities is achievable under distortion triple (D_0, D_1, D_2)

Finally, by the convexity of the inner bound, we have the desired achievability of (R_1, R_2) under (D_0, D_1, D_2)

Quadratic Gaussian Multiple Descriptions

- Consider the multiple descriptions problem for a $\text{WGN}(P)$ source X and squared error distortion measures d_0, d_1, d_2 . Without loss of generality, we consider the case $0 < D_0 \leq D_1, D_2 \leq P$
- Ozarow [4] showed that the El Gamal–Cover inner bound is tight in this case
Theorem 2 [1, 4]: The multiple description rate–distortion region $\mathcal{R}(D_0, D_1, D_2)$ for a $\text{WGN}(P)$ source X and mean squared error distortion measures is the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &\geq R\left(\frac{P}{D_1}\right), \\ R_2 &\geq R\left(\frac{P}{D_2}\right), \\ R_1 + R_2 &\geq R\left(\frac{P}{D_0}\right) + \Delta(P, D_0, D_1, D_2), \end{aligned}$$

where

$$\Delta = R\left(\frac{(P - D_0)^2}{(P - D_0)^2 - \left(\sqrt{(P - D_1)(P - D_2)} - \sqrt{(D_1 - D_0)(D_2 - D_0)}\right)^2}\right)$$

if $D_1 + D_2 < P + D_0$, and $\Delta = 0$ otherwise

- Proof of achievability: We choose $(X, \hat{X}_0, \hat{X}_1, \hat{X}_2)$ to be a Gaussian vector such that

$$\hat{X}_j = \left(1 - \frac{D_j}{P}\right)(X + Z_j), \quad j = 0, 1, 2,$$

where (Z_0, Z_1, Z_2) is a zero-mean Gaussian random vector, independent of X , with covariance matrix

$$K = \begin{bmatrix} N_0 & N_0 & N_0 \\ N_0 & N_1 & N_0 + \rho\sqrt{(N_1 - N_0)(N_2 - N_0)} \\ N_0 & N_0 + \rho\sqrt{(N_1 - N_0)(N_2 - N_0)} & N_2 \end{bmatrix},$$

$$N_j = \frac{PD_j}{P - D_j}, \quad j = 0, 1, 2$$

Note that $X \rightarrow \hat{X}_0 \rightarrow (\hat{X}_1, \hat{X}_2)$ form a Markov chain for all $\rho \in [-1, 1]$ (check)

High distortion: By relaxing the simple outer bound, any achievable rate pair (R_1, R_2) must satisfy

$$\begin{aligned} R_1 &\geq R\left(\frac{P}{D_1}\right), \\ R_2 &\geq R\left(\frac{P}{D_2}\right), \\ R_1 + R_2 &\geq R\left(\frac{P}{D_0}\right) \end{aligned}$$

Surprisingly these rates are achievable for high distortion, defined as

$$D_1 + D_2 \geq P + D_0$$

Under the above definition of high distortion and for $0 < D_0 \leq D_1, D_2 \leq P$, it can be easily verified that $(N_1 - N_0)(N_2 - N_0) \geq (P + N_0)^2$

Thus, there exists $\rho \in [-1, 1]$ such that $N_0 + \rho\sqrt{(N_1 - N_0)(N_2 - N_0)} = -P$. This shows that \hat{X}_1 and \hat{X}_2 can be made independent of each other, while achieving $E(d(X, \hat{X}_j)) = D_j$, $j = 0, 1, 2$, which proves the achievability of the simple outer bound

- Low distortion: When $D_1 + D_2 < P + D_0$, the consequent dependence of the descriptions causes an increase in the total description rate $R_1 + R_2$ beyond $R(P/D_0)$

Consider the above choice of $(\hat{X}_0, \hat{X}_1, \hat{X}_2)$ along with $\rho = -1$. Then by elementary algebra, one can show (check!) that

$$I(\hat{X}_1; \hat{X}_2) = \Delta(P, D_0, D_1, D_2)$$

- Proof of converse [4]: We only need to consider the low distortion case $D_0 + P > D_1 + D_2$. Again the inequalities $R_j \geq R(P/D_j)$, $j = 1, 2$, follow immediately from the lossy source coding theorem

To bound the sum rate, let $Y_i = X_i + Z_i$, where $\{Z_i\}$ is a WGN(N) process independent of $\{X_i\}$. Then

$$\begin{aligned} n(R_1 + R_2) &\geq H(M_1, M_2) + I(M_1; M_2) \\ &= I(X^n; M_1, M_2) + I(Y^n, M_1; M_2) - I(Y^n; M_2|M_1) \\ &\geq I(X^n; M_1, M_2) + I(Y^n; M_2) - I(Y^n; M_2|M_1) \\ &= I(X^n; M_1, M_2) + I(Y^n; M_2) + I(Y^n; M_1) - I(Y^n; M_1, M_2) \\ &= (I(X^n; M_1, M_2) - I(Y^n; M_1, M_2)) + I(Y^n; M_1) + I(Y^n; M_2) \end{aligned}$$

We first lower bound the second and third terms. Consider

$$\begin{aligned}
I(Y^n; M_1) &\geq \sum_{i=1}^n I(Y_i; \hat{X}_{1i}) \\
&\geq \sum_{i=1}^n \frac{1}{2} \log \frac{(P+N)}{\text{Var}(X_i + Z_i | \hat{X}_{1i})} \\
&= \sum_{i=1}^n \frac{1}{2} \log \frac{(P+N)}{(\text{Var}(X_i | \hat{X}_{1i}) + N)} \\
&\geq \frac{n}{2} \log \frac{(P+N)}{(D_1 + N)}
\end{aligned}$$

Similarly,

$$I(Y^n; M_2) \geq \frac{n}{2} \log \frac{(P+N)}{(D_2 + N)}$$

Next, we lower bound the first term. By the conditional EPI,

$$\begin{aligned}
h(Y^n | M_1, M_2) &\geq \frac{n}{2} \log \left(2^{2h(X^n | M_1, M_2)/n} + 2^{2h(Z^n | M_1, M_2)/n} \right) \\
&= \frac{n}{2} \log \left(2^{2h(X^n | M_1, M_2)/n} + 2\pi e N \right)
\end{aligned}$$

Since $h(X^n | M_1, M_2) \leq h(X^n | \hat{X}_0^n) \leq (n/2) \log(2\pi e D_0)$, we have

$$\begin{aligned}
h(Y^n | M_1, M_2) - h(X^n | M_1, M_2) &\geq \frac{n}{2} \log \left(1 + \frac{2\pi e N}{2^{2h(X^n | M_1, M_2)}} \right) \\
&\geq \frac{n}{2} \log \left(1 + \frac{N}{D_0} \right)
\end{aligned}$$

Hence

$$I(X^n; M_1, M_2) - I(Y^n; M_1, M_2) \geq \frac{n}{2} \log \left(\frac{P(D_0 + N)}{(P + N)D_0} \right)$$

Combining these inequalities and continuing with the lower bound on the sum rate, we have

$$R_1 + R_2 \geq \frac{1}{2} \log \left(\frac{P}{D_0} \right) + \frac{1}{2} \log \left(\frac{(P+N)(D_0+N)}{(D_1+N)(D_2+N)} \right)$$

Finally we maximize this sum-rate bound over $N > 0$ by taking

$$N = \frac{D_1 D_2 - D_0 P + \sqrt{(D_1 - D_0)(D_2 - D_0)(P - D_1)(P - D_2)}}{P + D_0 - D_1 - D_2},$$

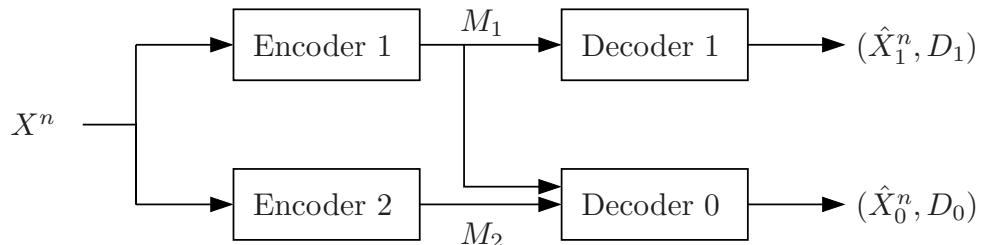
which yields the desired inequality

$$R_1 + R_2 \geq R \left(\frac{P}{D_0} \right) + \Delta(P, D_0, D_1, D_2)$$

- Remark: It can be shown that the optimized Y satisfies the Markov chain relationship $\hat{X}_1 \rightarrow Y \rightarrow \hat{X}_2$, where \hat{X}_1, \hat{X}_2 are the reproductions specified in the proof of achievability. As such, Y represents some form of *common information* between the optimal reproductions for the given distortion triple

Successive Refinement

- Consider the special case of the multiple descriptions problem without decoder 2 (i.e., $D_2 = \infty$ and $\hat{X}_2 = \emptyset$):



- Since there is no standalone decoder for the second description M_2 , there is no longer tension between two descriptions. As such, the second description can be viewed as a refinement of the first description that helps decoder 0 achieve a lower distortion

However, a tradeoff still exists between the two descriptions because if the first description is optimal for decoder 1, i.e., achieves the rate distortion function, the first and second descriptions combined may not be optimal for decoder 0

- *Theorem 3* [7, 8]: The successive refinement rate–distortion region $\mathcal{R}(D_0, D_1)$ for a DMS X and distortion measures d_0, d_1 is the set of rate pairs (R_1, R_2) such that

$$R_1 \geq I(X; \hat{X}_1),$$

$$R_1 + R_2 \geq I(X; \hat{X}_0, \hat{X}_1)$$

for some $p(\hat{x}_1, \hat{x}_0|x)$ satisfying

$$D_1 \geq E(d_1(X, \hat{X}_1)),$$

$$D_0 \geq E(d_0(X, \hat{X}_0))$$

- Achievability follows immediately from the proof of the El Gamal–Cover inner bound
- Proof of converse is also straightforward (check!)

Successively Refinable Sources

- Consider the successive refinement of a source under a common distortion measure $d_1 = d_0 = d$. If a rate pair (R_1, R_2) is achievable with distortion pair (D_0, D_1) for $D_0 \leq D_1$, then we must have

$$R_1 \geq R(D_1),$$

$$R_1 + R_2 \geq R(D_0),$$

where $R(D) = \min_{p(\hat{x}|x): E[d(X, \hat{X})] \leq D} I(X; \hat{X})$ is the rate–distortion function for a single description

In some cases, $(R_1, R_2) = (R(D_1), R(D_0) - R(D_1))$ is actually achievable for all $D_0 \leq D_1$ and there is no loss in describing the source in two successive parts. Such a source is referred to as *successively refinable*

- Example (Binary source and Hamming distortion): A binary source $X \sim \text{Bern}(p)$ can be shown to be successively refinable under Hamming distortion [7]. This is shown by considering a cascade of backward channels

$$X = \hat{X}_0 \oplus Z_0 = (\hat{X}_1 \oplus Z_1) \oplus Z_0,$$

where $Z_0 \sim \text{Bern}(D_0)$ and $Z_1 \sim \text{Bern}(D')$ such that $D' * D_0 = D_1$. Note that $\hat{X}_1 \rightarrow \hat{X}_0 \rightarrow X$ form a Markov chain

- Example (Gaussian source and squared error distortion): Consider a $\text{WGN}(P)$ source and squared error distortion d_0, d_1 . We can achieve $R_1 = R(P/D_1)$ and $R_1 + R_2 = R(P/D_0)$ (or equivalently $R_2 = R(D_1/D_2)$) simultaneously [7], by taking a cascade of backward channels $X = \hat{X}_0 + Z_0 = (\hat{X}_1 + Z_1) + Z_0$, where $\hat{X}_1 \sim N(0, 1 - D_1)$, $Z_1 \sim N(0, D_1 - D_0)$, $Z_0 \sim N(0, 1 - D_0)$ are independent of each other and $\hat{X}_0 = \hat{X}_1 + Z_1$. Again $\hat{X}_1 \rightarrow \hat{X}_0 \rightarrow X$ form a Markov chain
- Successive refinability of the WGN source can be shown more directly by the following heuristic argument:

From the quadratic Gaussian source coding theorem, using rate R_1 , the source sequence X^n can be described by \hat{X}_1^n with error $Y^n = X^n - \hat{X}_1^n$ and resulting distortion $D_1 = \frac{1}{n} \sum_{i=1}^n E(Y_i^2) \leq P2^{-2R_1}$. Then, using rate R_2 , the error sequence Y^n can be described by \hat{X}_0^n with resulting distortion $D_0 \leq D_1 2^{-2R_2} \leq P2^{-2(R_1+R_2)}$

Subsequently, the error of the error, the error of the error of the error, etc. can be successively described, providing further refinement of the source. Each stage represents a quadratic Gaussian source coding problem. Thus, successive refinement for a WGN source is, in a sense, dual to successive cancellation for the AWGN-MAC and AWGN-BC

This heuristic argument can be made rigorous [9]

- In general, we have the following result on successive refinability:

Proposition 1 [7]: A DMS X is successively refinable iff for each $D_0 \leq D_1$ there exists a conditional pmf $p(\hat{x}_0, \hat{x}_1|x) = p(\hat{x}_0|x)p(\hat{x}_1|\hat{x}_0)$ such that $p(\hat{x}_0|x)$, $p(\hat{x}_1|x)$ achieve the rate-distortion functions $R(D_0)$ and $R(D_1)$, respectively; in other words, $X \rightarrow \hat{X}_0 \rightarrow \hat{X}_1$ form a Markov chain and

$$E(d(X, \hat{X}_0)) \leq D_0,$$

$$E(d(X, \hat{X}_1)) \leq D_1,$$

$$I(X; \hat{X}_0) = R(D_0),$$

$$I(X; \hat{X}_1) = R(D_1)$$

Zhang–Berger Inner Bound

- The Zhang–Berger inner bound extends the El Gamal–Cover inner bound by adding a *common* description U to each description

Theorem 4 (Zhang–Berger Inner Bound) [5, 10]: Let $X \sim p(x)$ be a DMS and $d_j(x, \hat{x}_j)$, $j = 0, 1, 2$, be three distortion measures

A rate pair (R_1, R_2) is achievable for multiple descriptions with distortion triple (D_0, D_1, D_2) if

$$R_1 > I(X; \hat{X}_1, U),$$

$$R_2 > I(X; \hat{X}_2, U),$$

$$R_1 + R_2 > I(X; \hat{X}_0, \hat{X}_1, \hat{X}_2 | U) + 2I(U; X) + I(\hat{X}_1; \hat{X}_2 | U)$$

for some $p(u, \hat{x}_0, \hat{x}_1, \hat{x}_2 | x)$, where $|\mathcal{U}| \leq |\mathcal{X}| + 5$, such that

$$\mathbb{E}(d_0(X, \hat{X}_0)) \leq D_0,$$

$$\mathbb{E}(d_1(X, \hat{X}_1)) \leq D_1,$$

$$\mathbb{E}(d_2(X, \hat{X}_2)) \leq D_2$$

- This region is convex

- Outline of achievability: We first describe X^n with the common description U^n and then refine this description to obtain $\hat{X}_1^n, \hat{X}_2^n, \hat{X}_0^n$ as in the El Gamal–Cover coding scheme. The index of the common description U^n is sent by both encoders

Now, for some details

- Let $R_1 = R_0 + R_{11} + R_{01}$ and $R_2 = R_0 + R_{22} + R_{02}$
- Codebook generation: Fix $p(u, \hat{x}_1, \hat{x}_2, \hat{x}_0)$ that achieve the desired distortion triple (D_0, D_1, D_2) . Randomly generate 2^{nR_0} $u^n(m_0)$ sequences each according to $\prod_{i=1}^n p_U(u_i)$

For each $u^n(m_0)$, we randomly and conditional independently generate $2^{nR_{11}}$ $\hat{x}_1(m_0, m_{11})$ sequences each according to $\prod_{i=1}^n p_{\hat{X}_1|U}(\hat{x}_{1i}|u_i)$ and $2^{nR_{22}}$ $\hat{x}_2(m_0, m_{22})$ sequences each according to $\prod_{i=1}^n p_{\hat{X}_2|U}(\hat{x}_{2i}|u_i)$

For each $(u^n(m_0), \hat{x}_1^n(m_0, m_{11}), \hat{x}_2^n(m_0, m_{22}))$ randomly and conditionally independently generate $2^{n(R_{01}+R_{02})}$ $\hat{x}_0^n(m_0, m_{11}, m_{22}, m_{01}, m_{02})$ sequences, each according to $\prod_{i=1}^n p_{\hat{X}_0|U, \hat{X}_1, \hat{X}_2}(\hat{x}_{0i}|u_i, \hat{x}_{1i}, \hat{x}_{2i})$

- Encoding: Upon observing x^n , we find a jointly typical tuple $(u^n(m_0), \hat{x}_1(m_0, m_{11}), \hat{x}_2(m_0, m_{22}), \hat{x}_0^n(m_0, m_{11}, m_{22}, m_{01}, m_{02}))$. Encoder 1 sends (m_0, m_{11}, m_{01}) and encoder 2 sends (m_0, m_{22}, m_{02})
- Now using the covering lemma and a conditional version of the multivariate covering lemma, it can be shown that a rate tuple $(R_0, R_{11}, R_{22}, R_{01}, R_{02})$ is achievable if

$$\begin{aligned} R_0 &> I(X; U), \\ R_{11} &> I(X; \hat{X}_1|U), \\ R_{22} &> I(X; \hat{X}_2|U), \\ R_{11} + R_{22} &> I(X; \hat{X}_1, \hat{X}_2|U) + I(\hat{X}_1; \hat{X}_2|U), \\ R_{01} + R_{02} &> I(X; \hat{X}_0|U, \hat{X}_1, \hat{X}_2) \end{aligned}$$

for some $p(u, \hat{x}_0, \hat{x}_1, \hat{x}_2|x)$ such that $E(d_j(X, \hat{X}_j)) \leq D_j$, $j = 0, 1, 2$

- Using the Fourier–Motzkin procedure in Appendix D, we arrive at the conditions of the theorem

● Remarks

- It is not known whether the Zhang–Berger inner bound is tight
- The Zhang–Berger inner bound contains the El Gamal–Cover inner bound (take $U = \emptyset$). In fact, it can be strictly larger for the binary symmetric source in the case of excess rate [5]. Under $(D_0, D_1, D_2) = (0, 0.1, 0.1)$, the El Gamal–Cover region cannot achieve (R_1, R_2) such that $R_1 + R_2 \leq 1.2564$. On the other hand, the Zhang–Berger inner bound contains a rate pair (R_1, R_2) with $R_1 + R_2 = 1.2057$
- An equivalent region: The Zhang–Berger inner bound is equivalent to the set of rate pairs (R_1, R_2) such that

$$\begin{aligned} R_1 &> I(X; U_0, U_1), \\ R_2 &> I(X; U_0, U_2), \end{aligned}$$

$$R_1 + R_2 > I(X; U_1, U_2|U_0) + 2I(U_0; X) + I(U_1; U_2|U_0)$$

for some $p(u_0, u_1, u_2|x)$ satisfying

$$\begin{aligned} E(d_0(X, \hat{x}_0(U_0, U_1, U_2))) &\leq D_0, \\ E(d_1(X, \hat{x}_1(U_0, U_1))) &\leq D_1, \\ E(d_2(X, \hat{x}_2(U_0, U_2))) &\leq D_2 \end{aligned}$$

Clearly this region is contained in the inner bound in the above theorem

We now show that this alternative characterization contains the Zhang–Berger inner bound in the theorem [11]

Consider the following corner point of the Zhang–Berger inner bound:

$$R_1 = I(X; \hat{X}_1, U),$$

$$R_2 = I(X; \hat{X}_0, \hat{X}_2 | \hat{X}_1, U) + I(X; U) + I(\hat{X}_1; \hat{X}_2 | U)$$

for some $p(x, u, \hat{x}_0, \hat{x}_1, \hat{x}_2)$. By the functional representation lemma in Lecture Notes 7, there exists W independent of $(U, \hat{X}_1, \hat{X}_2)$ such that \hat{X}_0 is a function of $(U, \hat{X}_1, \hat{X}_2, W)$ and $X \rightarrow (U, \hat{X}_0, \hat{X}_1, \hat{X}_2) \rightarrow W$

Let $U_0 = U$, $U_1 = \hat{X}_1$, and $U_2 = (W, \hat{X}_2)$. Then

$$R_1 = I(X; \hat{X}_1, U) = I(X; U_0, U_1),$$

$$\begin{aligned} R_2 &= I(X; \hat{X}_0, \hat{X}_2 | \hat{X}_1, U) + I(X; U) + I(\hat{X}_1; \hat{X}_2 | U) \\ &= I(X; \hat{X}_2, W | \hat{X}_1, U) + I(X; U_0) + I(\hat{X}_1; \hat{X}_2, W | U) \\ &= I(X; U_2 | U_0, U_1) + I(X; U_0) + I(U_1; U_2 | U_0) \end{aligned}$$

and $\hat{X}_1, \hat{X}_2, \hat{X}_0$ are functions of $U_1, U_2, (U_0, U_1, U_2)$, respectively. Hence, (R_1, R_2) is also a corner point of the above region. The rest of the proof follows by time sharing

Extensions to More than 2 Descriptions

- The El Gamal–Cover and Zhang–Berger inner bounds can be easily extended to k descriptions and 2^{k-1} decoders [10]. This extension is optimal for the following special cases:
 - Successive refinement of k levels
 - Quadratic Gaussian multiple descriptions with individual decoders (each of which receives its own description) and a centralize decoder (which receives all descriptions) [12]
- It is known, however, that this extension is not optimal in general [13]

References

- [1] A. El Gamal and T. M. Cover, "Achievable rates for multiple descriptions," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 851–857, 1982.
- [2] F.-W. Fu and R. W. Yeung, "On the rate-distortion region for multiple descriptions," *IEEE Trans. Inf. Theory*, vol. 48, no. 7, pp. 2012–2021, July 2002.
- [3] R. Ahlswede, "The rate-distortion region for multiple descriptions without excess rate," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 721–726, 1985.
- [4] L. Ozarow, "On a source-coding problem with two channels and three receivers," *Bell System Tech. J.*, vol. 59, no. 10, pp. 1909–1921, 1980.
- [5] Z. Zhang and T. Berger, "New results in binary multiple descriptions," *IEEE Trans. Inf. Theory*, vol. 33, no. 4, pp. 502–521, 1987.
- [6] T. Berger and Z. Zhang, "Minimum breakdown degradation in binary source encoding," *IEEE Trans. Inf. Theory*, vol. 29, no. 6, pp. 807–814, 1983.
- [7] W. H. R. Equitz and T. M. Cover, "Successive refinement of information," *IEEE Trans. Inf. Theory*, vol. 37, no. 2, pp. 269–275, 1991, addendum in *IEEE Trans. Inf. Theory*, vol. IT-39, no. 4, pp. 1465–1466, 1993.
- [8] B. Rimoldi, "Successive refinement of information: Characterization of the achievable rates," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 253–259, Jan. 1994.
- [9] Y.-H. Kim and H. Jeong, "Sparse linear representation," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 329–333.

- [10] R. Venkataramani, G. Kramer, and V. K. Goyal, "Multiple description coding with many channels," *IEEE Trans. Inf. Theory*, vol. 49, no. 9, pp. 2106–2114, Sept. 2003.
- [11] L. Zhao, P. Cuff, and H. H. Permuter, "Consolidating achievable regions of multiple descriptions," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 51–54.
- [12] J. Chen, "Rate region of Gaussian multiple description coding with individual and central distortion constraints," *IEEE Trans. Inf. Theory*, vol. 55, no. 9, pp. 3991–4005, Sept. 2009.
- [13] R. Puri, S. S. Pradhan, and K. Ramchandran, " n -channel symmetric multiple descriptions—II: An achievable rate-distortion region," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1377–1392, 2005.

Lecture Notes 15

Joint Source–Channel Coding

- Transmission of 2-DMS over a DM-MAC
- Transmission of Correlated Sources over a BC
- Key New Ideas and Techniques
- Appendix: Proof of Lemma 1

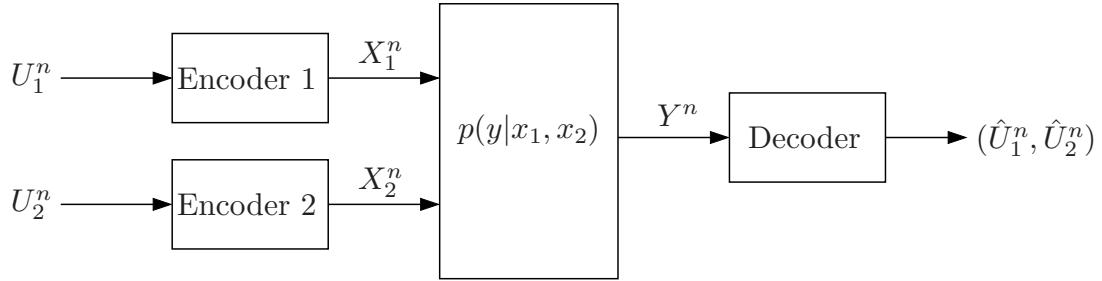
© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- As discussed in the introduction, the basic question in network information theory is to find the necessary and sufficient condition for reliable communication of a set of correlated sources over a noisy network
- Shannon showed that separate source and channel coding is sufficient for sending a DMS over a DMC. Does such separation theorem hold for sending multiple sources over a multiple user channel such as a MAC or BC?
- It turns out that such source–channel separation does not hold in general for sending multiple sources over multiple user channels. Thus in some cases it is advantageous to use joint source–channel coding
- We demonstrate this breakdown in separation through examples of lossless transmission of correlated sources over DM-MAC and DM-BC

Transmission of 2-DMS over a DM-MAC

- We wish to send a 2-DMS $(U_1, U_2) \sim p(u_1, u_2)$ losslessly over a DM-MAC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$



- A $(|\mathcal{U}_1|^{k_1}, |\mathcal{U}_2|^{k_2}, n)$ joint source–channel code of rate pair $(r_1 = k_1/n, r_2 = k_2/n)$ consists of:
 1. Two encoders: Encoder $j = 1, 2$ assigns a sequence $x_j^n(u_j^k) \in \mathcal{X}_j^n$ to each sequence $u_j^k \in \mathcal{U}_j^k$, and
 2. A decoder that assigns an estimate $(\hat{u}_1^k, \hat{u}_2^k) \in \hat{\mathcal{U}}_1^k \times \hat{\mathcal{U}}_2^k$ to each sequence $y^n \in \mathcal{Y}^n$
- For simplicity, assume the rates $r_1 = r_2 = 1$ symbol/transmission

- The probability of error is defined as $P_e^{(n)} = P\{(U_1^n, U_2^n) \neq (\hat{U}_1^n, \hat{U}_2^n)\}$
- The sources are transmitted losslessly over the DM-MAC if there exists a sequence of $(|\mathcal{U}_1|^n, |\mathcal{U}_2|^n, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The problem is to find the necessary and sufficient condition for lossless transmission
- We know that the capacity region of the DM-MAC is the set of rate pairs such that

$$R_1 \leq I(X_1; Y | X_2, Q),$$

$$R_2 \leq I(X_2; Y | X_1, Q),$$

$$R_1 + R_2 \leq I(X_1, X_2; Y | Q)$$

for some $p(q, x_1, x_2) = p(q)p(x_1|q)p(x_2|q)$

- Thus, it follows easily that if for some $p(q)p(x_1|q)p(x_2|q)$,

$$H(U_1) < I(X_1; Y | X_2, Q),$$

$$H(U_2) < I(X_2; Y | X_1, Q),$$

$$H(U_1) + H(U_2) < I(X_1, X_2; Y | Q),$$

then U_1 and U_2 can be sent losslessly

- This sufficient condition can be further improved. By the Slepian–Wolf theorem, it is again easy to show that if for some $p(q)p(x_1|q)p(x_2|q)$,

$$H(U_1|U_2) < I(X_1; Y|X_2, Q),$$

$$H(U_2|U_1) < I(X_2; Y|X_1, Q),$$

$$H(U_1, U_2) < I(X_1, X_2; Y|Q),$$

then the sources can be sent losslessly to the receiver

- In both cases source coding and channel coding are performed separately
- Can we do better? We know that separate source and channel coding is optimal for sending a DMS over a DMC. Is it optimal for the MAC as well?
- Example: Let the 2-DMS (U_1, U_2) be binary with joint pmf $p(0, 0) = p(0, 1) = p(1, 1) = 1/3$ and $p(1, 0) = 0$, and the channel be a binary erasure MAC with $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$, $\mathcal{Y} = \{0, 1, 2\}$, and $Y = X_1 + X_2$
 - Note that $H(U_1, U_2) = \log 3 = 1.58$ bits, but

$$\max_{p(x_1)p(x_2)} I(X_1, X_2; Y) = 1.5 \text{ bits}$$

Thus $H(U_1, U_2) > \max_{p(x_1)p(x_2)} I(X_1, X_2; Y)$ and even with Slepian–Wolf coding (or Cover's binning) we cannot send the sources losslessly over the channel

- Now consider the following joint source–channel coding scheme: Set $X_1 = U_1$ and $X_2 = U_2$
It is easy to see that error-free transmission is possible!
- So, we have an example of a DM-MAC for which using separate source coding and channel coding is *not* optimal
- A general necessary and sufficient condition for transmitting correlated sources over DM-MAC is not known
- We describe a suboptimal joint source–channel coding scheme

A Joint Source–Channel Coding Scheme

- *Theorem 1 [1]:* The 2-DMS $(\mathcal{U}_1 \times \mathcal{U}_2, p(u_1, u_2))$ can be sent losslessly over a DM-MAC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$ if

$$H(U_1|U_2) < I(X_1; Y|X_2, U_2, Q),$$

$$H(U_2|U_1) < I(X_2; Y|X_1, U_1, Q),$$

$$H(U_1, U_2) < I(X_1, X_2; Y|Q)$$

for some $p(q, x_1, x_2|u_1, u_2) = p(q)p(x_1|u_1, q)p(x_2|u_2, q)$

- Special cases:

- Slepian–Wolf optimal rate region: Consider a noiseless dummy channel with $Y = (X_1, X_2)$ and let $p(x_1, x_2|u_1, u_2) = p(x_1)p(x_2)$. Then

$$H(U_1|U_2) < I(X_1; Y|X_2, U_2) = H(X_1)(= R_1),$$

$$H(U_2|U_1) < I(X_2; Y|X_1, U_1) = H(X_2)(= R_2),$$

$$H(U_1, U_2) < I(X_1, X_2; Y) = H(X_1) + H(X_2)(= R_1 + R_2)$$

- DM-MAC capacity region: Let $(U_1, U_2) \sim p(u_1)p(u_2)$ be independent sources with entropies $H(U_1)$ and $H(U_2)$, respectively, and choose $p(q, x_1, x_2|u_1, u_2) = p(q)p(x_1|q)p(x_2|q)$. Then

$$H(U_1|U_2) = H(U_1)(= R_1) < I(X_1; Y|X_2, Q),$$

$$H(U_2|U_1) = H(U_2)(= R_2) < I(X_2; Y|X_1, Q),$$

$$H(U_1, U_2) = H(U_1) + H(U_2)(= R_1 + R_2) < I(X_1, X_2; Y|Q)$$

- For the binary sources over binary erasure MAC example, we set $Q = \emptyset$, $X_1 = U_1$, and $X_2 = U_2$

Proof of Achievability

- We show achievability for $|Q| = 1$; the rest of the proof follows using time-sharing

- Codebook generation: Fix $p(x_1|u_1)$ and $p(x_2|u_2)$

For each $u_1^n \in \mathcal{U}_1^n$, randomly and independently generate a sequence $x_1^n(u_1^n)$ according to $\prod_{i=1}^n p_{X_1|U_1}(x_{1i}|u_{1i})$

For each $u_2^n \in \mathcal{U}_2^n$, randomly and independently generate a sequence $x_2^n(u_2^n)$ 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 that $(\hat{u}_1^n, \hat{u}_2^n)$ 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: Define the events

$$\mathcal{E}_1 := \{(U_1^n, U_2^n, X_1^n(U_1^n), X_2^n(U_2^n), Y^n) \notin \mathcal{T}_\epsilon^{(n)}\}$$

$$\mathcal{E}_2 := \{(\tilde{u}_1^n, U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n\}$$

$$\mathcal{E}_3 := \{(U_1^n, \tilde{u}_2^n, X_1^n(U_1^n), X_2^n(\tilde{u}_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_2^n \neq U_2^n\}$$

$$\mathcal{E}_4 := \{(\tilde{u}_1^n, \tilde{u}_2^n, X_1^n(\tilde{u}_1^n), X_2^n(\tilde{u}_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n, \tilde{u}_2^n \neq U_2^n\}$$

The average probability of error is upper bounded by

$$P(\mathcal{E}) \leq P(\mathcal{E}_1) + P(\mathcal{E}_2) + P(\mathcal{E}_3) + P(\mathcal{E}_4)$$

Now we consider each term

- $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$ by the LLN
- Next, consider the second term. By the union of events bound,

$$P(\mathcal{E}_2)$$

$$= \sum_{u_1^n} p(u_1^n) P\{(\tilde{u}_1^n, U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{u}_1^n \neq u_1^n | U_1^n = u_1^n\}$$

$$\leq \sum_{u_1^n} p(u_1^n) \sum_{\tilde{u}_1^n \neq u_1^n} P\{(\tilde{u}_1^n, U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \in \mathcal{T}_\epsilon^{(n)} | U_1^n = u_1^n\}$$

Now, conditioned on $U_1^n = u_1^n$,

$$(U_2^n, X_1^n(\tilde{u}_1^n), X_2^n(U_2^n), Y^n) \sim p(u_2^n, x_2^n, y^n | u_1^n) p_{X_1^n | U_1^n}(x_1^n | \tilde{u}_1^n)$$

for all $\tilde{u}_1^n \neq u_1^n$. Thus

$$\begin{aligned} P(\mathcal{E}_2) &\leq \sum_{u_1^n} p(u_1^n) \sum_{\substack{\tilde{u}_1^n \neq u_1^n \\ (\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}}} p(u_2^n, x_2^n, y^n | u_1^n) p_{X_1^n | U_1^n}(x_1^n | \tilde{u}_1^n) \\ &= \sum_{(\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} \sum_{u_1^n \neq \tilde{u}_1^n} p(u_1^n, u_2^n, x_2^n, y^n) p_{X_1^n | U_1^n}(x_1^n | \tilde{u}_1^n) \\ &\leq \sum_{(\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} \sum_{u_1^n} p(u_1^n, u_2^n, x_2^n, y^n) p_{X_1^n | U_1^n}(x_1^n | \tilde{u}_1^n) \\ &= \sum_{(\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} p(u_2^n, x_2^n, y^n) p_{X_1^n | U_1^n}(x_1^n | \tilde{u}_1^n) \\ &\leq \sum_{(\tilde{u}_1^n, u_2^n, x_1^n, x_2^n, y^n) \in \mathcal{T}_\epsilon^{(n)}} 2^{-n(H(U_2, X_2, Y) - \delta(\epsilon))} 2^{-n(H(X_1 | U_1) - \delta(\epsilon))} \\ &\leq 2^{n(H(U_1, U_2, X_1, X_2, Y) + \delta(\epsilon))} 2^{-n(H(U_2, X_2, Y) + H(X_1 | U_1) - 2\delta(\epsilon))} \end{aligned}$$

Collecting the entropy terms, we have

$$\begin{aligned} H(U_1, X_1, X_2, Y | U_2) - H(X_2, Y | U_2) - H(X_1 | U_1) \\ &= H(U_1 | U_2) + H(X_1, X_2, Y | U_1, U_2) - H(X_2 | U_2) - H(X_1 | U_1) - H(Y | X_2, U_2) \\ &= H(U_1 | U_2) + H(Y | X_1, X_2, U_2) - H(Y | X_2, U_2) \\ &= H(U_1 | U_2) - I(X_1; Y | U_2, X_2) \end{aligned}$$

Thus $P(\mathcal{E}_2) \rightarrow 0$ as $n \rightarrow \infty$ if

$$H(U_1 | U_2) < I(X_1; Y | X_2, U_2) - 3\delta(\epsilon)$$

o Similarly $P(\mathcal{E}_3) \rightarrow 0$ as $n \rightarrow \infty$ if

$$H(U_2 | U_1) < I(X_2; Y | X_1, U_1) - 3\delta(\epsilon)$$

and $P(\mathcal{E}_4) \rightarrow 0$ as $n \rightarrow \infty$ if

$$\begin{aligned} H(U_1, U_2) &< I(U_1, U_2, X_1, X_2; Y) - 3\delta(\epsilon) \\ &= I(X_1, X_2; Y) - 3\delta(\epsilon) \end{aligned}$$

- This coding scheme is not optimal in general

For example, suppose $U_1 = U_2 = U$. Then we obtain

$$H(U) < \max_{p(q)p(x_1|q,u)p(x_2|q,u)} I(X_1, X_2; Y|Q) = \max_{p(x_1|u)p(x_2|u)} I(X_1, X_2; Y)$$

But, if both senders have the same message, it is easy to see that we can achieve complete cooperation, i.e.,

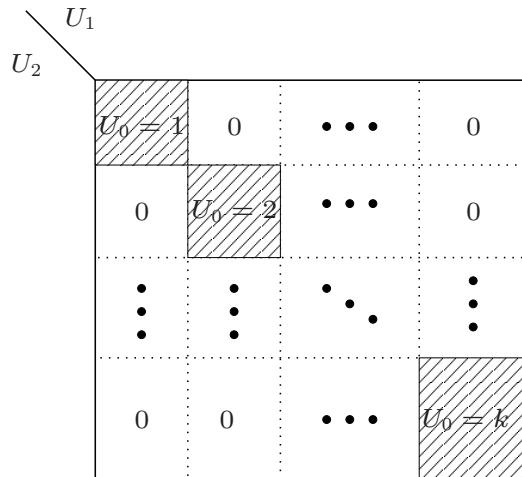
$$H(U) < \max_{p(x_1, x_2)} I(X_1, X_2; Y),$$

which is in general larger than the condition provided by the coding scheme

- The above coding scheme does not deal well with the case in which U_1 and U_2 have a *common part*

Common Part of U_1 and U_2 [2, 3]

- Arrange $p(u_1, u_2)$ in a block diagonal form with the maximum number $k \geq 1$ of non-zero blocks possible



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 alone or U_2 alone

- Formally, let $g_1 : \mathcal{U}_1 \rightarrow [1 : k]$ and $g_2 : \mathcal{U}_2 \rightarrow [1 : k]$ be two functions with the largest k such that $\mathbb{P}\{g_1(U_1) = u_0\} > 0$, $\mathbb{P}\{g_2(U_2) = u_0\} > 0$ for $u_0 \in [1 : k]$ and $\mathbb{P}\{g_1(U_1) = g_2(U_2)\} = 1$

The common part between U_1 and U_2 is $U_0 = g_1(U_1) = g_2(U_2)$

- Example:

		U_1		$U_0 = 1$	$U_0 = 2$
		1	2	3	4
U_2	1	0.1	0.2	0	0
	2	0.1	0.1	0	0
$U_0 = 1$	3	0.1	0.1	0	0

$U_0 = 2$	4	0	0	0.2	0.1

Here $k = 2$ and $\mathbb{P}\{U_0 = 1\} = 0.7$, $\mathbb{P}\{U_0 = 2\} = 0.3$

A More General Joint Source–Channel Coding Scheme

- Theorem 2 [1]:* A 2-DMS $(\mathcal{U}_1 \times \mathcal{U}_2, p(u_1, u_2))$ with common part $U_0 \sim p(u_0)$ can be sent losslessly over a DM-MAC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$ if

$$\begin{aligned} H(U_1|U_2) &< I(X_1; Y|X_2, U_2, W), \\ H(U_2|U_1) &< I(X_2; Y|X_1, U_1, W), \\ H(U_1, U_2|U_0) &< I(X_1, X_2; Y|U_0, W), \\ H(U_1, U_2) &< I(X_1, X_2; Y) \end{aligned}$$

for some $p(w)p(x_1|u_1, w)p(x_2|u_2, w)$

- In this coding scheme U_0 is represented by the independent *auxiliary random variable* W , which is chosen to maximize cooperation between the senders
- Remarks:

- 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 the source–channel separation theorem for sending a DMS over a DMC

- The sufficient condition does not change by introducing a time-sharing random variable Q
- The coding scheme is optimal for the DM-MAC with common message [4], where we have three independent messages $M_0 \in [1, 2^{nR_0}]$, $M_1 \in [1, 2^{nR_1}]$, $M_2 \in [1, 2^{nR_2}]$. Sender 1 has M_0, M_1 , sender 2 has M_0, M_2 , and the receiver wishes to decode all three messages reliably. It can be easily shown that the above sufficient condition simplifies to the capacity region, which is the set of rate triples (R_0, R_1, R_2) such that

$$\begin{aligned} R_1 &\leq I(X_1; Y|X_2, W), \\ R_2 &\leq I(X_2; Y|X_1, W), \\ R_1 + R_2 &\leq I(X_1, X_2; Y|W), \\ R_0 + R_1 + R_2 &\leq I(X_1, X_2; Y) \end{aligned}$$

for some $p(w)p(x_1|w)p(x_2|w)$, where $|\mathcal{W}| \leq \min\{|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 2, |\mathcal{Y}| + 3\}$

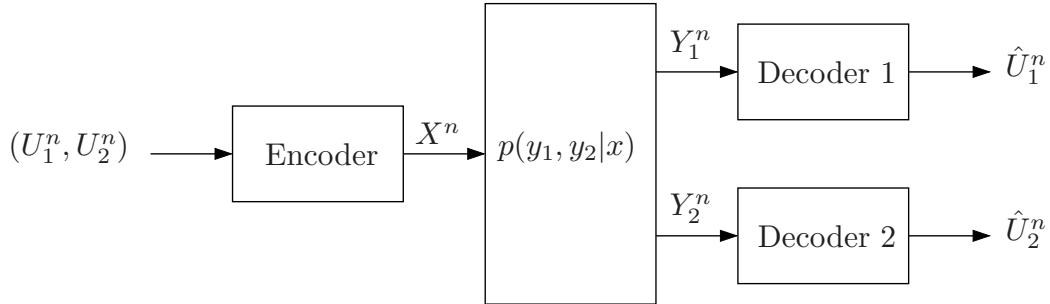
- The coding scheme is not optimal in general (see Dueck [5])
- Achievability outline: For each u_0^n , randomly and independently generate $w^n(u_0^n)$ according to $\prod_{i=1}^n p_W(w_i)$. For each (u_0^n, u_1^n) , randomly and independently generate $x_1^n(u_0^n, u_1^n)$ according to $\prod_{i=1}^n p_{X_1|U_1,W}(x_{1i}|u_{1i}, w_i(u_0^n))$. 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 $\rightarrow 0$ as $n \rightarrow \infty$

Transmission of Correlated Sources over a BC

- Now consider the problem of sending a 2-DMS $(U_1, U_2) \sim p(u_1, u_2)$ losslessly over a DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$



- As before, assume rates $r_1 = r_2 = 1$ symbol/transmission
- A code, probability of error, and lossless transmission are defined similarly to the MAC case
- We already know that even for the special case where U_1 and U_2 are independent (the private-message set DM-BC), the necessary and sufficient conditions for lossless transmission are not known in general

- Using Marton's coding scheme for the DM-BC, the sources can be transmitted losslessly if

$$H(U_1) < I(W_1; Y_1),$$

$$H(U_2) < I(W_2; Y_2),$$

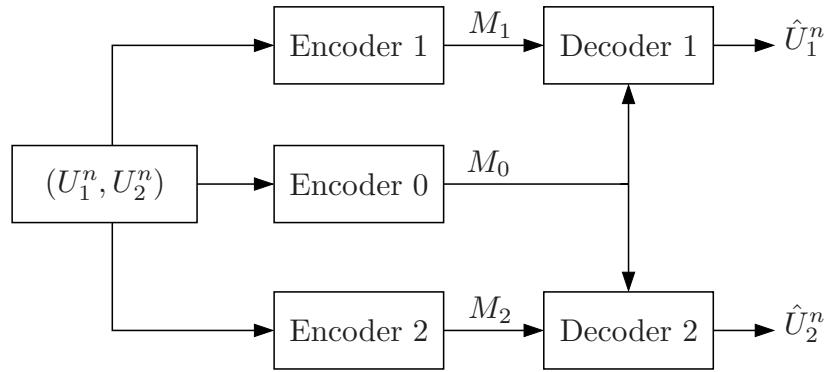
$$H(U_1) + H(U_2) < I(W_1; Y_1) + I(W_2; Y_2) - I(W_1; W_2)$$

for some $p(w_1, w_2, x)$

- As in the case of sending correlated sources over the MAC, the above condition can be further improved by incorporating some notion of *common information* between the two sources and using a joint source-channel coding

Gray–Wyner System

- To study the role of common information in broadcasting, we consider the following distributed lossless source coding problem (referred to as the Gray–Wyner system [6])
- Let (U_1, U_2) be a 2-DMS. The source pair is described by three encoders so that decoder 1, who receives descriptions 0 and 1 can losslessly recover U_1 and decoder 2, who receives descriptions 0 and 2 can losslessly recover U_2 . What is the optimal set of encoding rates?



- A $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ code for the Gray–Wyner system consists of:
 1. Three encoders: Encoders 0, 1, and 2 assign indices $m_0(u_1^n, u_2^n), m_1(u_1^n, u_2^n), m_2(u_1^n, u_2^n)$ to each sequence pair $(u_1^n, u_2^n) \in \mathcal{U}_1^n \times \mathcal{U}_2^n$, respectively
 2. Two decoders: Decoder 1 assigns an estimate $\hat{u}_1^n(m_0, m_1)$ to each index pair $(m_0, m_1) \in [1, 2^{nR_0}] \times [1, 2^{nR_1}]$ 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)} = P\{\(\hat{U}_1^n, \hat{U}_2^n) \neq (U_1^n, U_2^n)\}$
- The optimal rate region for the Gray–Wyner system is the closure of the set of rate triples (R_0, R_1, R_2) such that there exists a sequence of $(2^{nR_0}, 2^{nR_1}, 2^{nR_2}, n)$ codes with $P_e^{(n)} \rightarrow 0$
- *Theorem 3 [6]:* The optimal rate region for the Gray–Wyner system with a 2-DMS (U_1, U_2) is the set of rate triples (R_0, R_1, R_2) such that

$$R_0 \geq I(U_1, U_2; V),$$

$$R_1 \geq H(U_1 | V),$$

$$R_2 \geq H(U_2 | V)$$

for some $p(v|u_1, u_2)$, where $|\mathcal{V}| \leq |\mathcal{U}_1| \cdot |\mathcal{U}_2| + 2$

- The proof follows similar lines to the proof for the lossless coding with a helper theorem (see Lecture Notes 11)
- Achievability: Joint typicality encoding is used to describe (u_1^n, u_2^n) by a v^n sequence. This description is sent by decoder 0 at rate R_0 to both decoders. Given the description v^n , assign indices to $u_1^n \in \mathcal{T}_\epsilon^{(n)}(U_1|v^n)$ and $u_2^n \in \mathcal{T}_\epsilon^{(n)}(U_2|v^n)$, and send them to decoders 1 and 2, respectively
- Converse: We use the auxiliary random variable identification $V_i := (M_0, U_1^{i-1}, U_2^{i-1})$ (check!). The cardinality bound on V follows by using the standard technique in Appendix C
- Extreme points of the optimal rate region
 - $R_0 = 0$: By taking $V = \emptyset$, the region reduces to $R_1 \geq H(U_1)$, $R_2 \geq H(U_2)$
 - $R_1 = 0$: By taking $V = U_1$, the region reduces to $R_0 \geq H(U_1)$, $R_2 \geq H(U_2|U_1)$
 - $R_2 = 0$: By taking $V = U_2$, the region reduces to $R_0 \geq H(U_2)$, $R_1 \geq H(U_1|U_2)$
 - $(R_1, R_2) = (0, 0)$: By taking $V = (U_1, U_2)$, the region reduces to $R_0 \geq H(U_1, U_2)$

- A rate triple (R_0, R_1, R_2) in the optimal rate region must satisfy the following 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 which can be made equality as seen from the extreme points above. Interestingly, the corresponding common rate R_0 leads to several notions of *common information*

- Gacs–Körner–Witsenhausen common information [2, 3]: The maximum R_0 such that $R_0 + R_1 = H(U_1)$ and $R_0 + R_2 = H(U_2)$ are simultaneously achievable is the entropy $H(U_0)$ of the common part between U_1 and U_2 , denoted by $K(U_1; U_2)$
- Mutual information: The maximum R_0 such that $2R_0 + R_1 + R_2 = H(U_1) + H(U_2)$ is allowed by the outer bound is the mutual information $I(U_1; U_2)$

- Wyner's common information [7]: The minimum R_0 such that $R_0 + R_1 + R_2 = H(U_1, U_2)$ is achievable is
$$J(U_1; U_2) = \min I(U_1, U_2; V),$$
where the minimum is taken over all $p(v|u_1, u_2)$ such that $I(U_1; U_2|V) = 0$ (that is, U_1 and U_2 are conditionally independent given V) and $|\mathcal{V}| \leq |\mathcal{U}_1| \cdot |\mathcal{U}_2|$
- These three quantities represent common information between the random variables U_1 and U_2 in different contexts. For example, the Gacs–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. On the other hand, Wyner's common information captures the amount of common randomness that should be provided to generate U_1 and U_2 separately [7]
- It can be easily shown (check!) that

$$0 \leq K(U_1; U_2) \leq I(U_1; U_2) \leq J(U_1; U_2) \leq H(U_1, U_2)$$

and the inequalities can be strict in general. Furthermore,
 $K(U_1; U_2) = I(U_1; U_2) = J(U_1; U_2)$ if and only if $U_1 = (V, V_1)$ and $U_2 = (V, V_2)$ for some $V_1 \rightarrow V \rightarrow V_2$

- Examples:

- Let (U_1, U_2) be DSBS(p) with $0 \leq p \leq 1/2$. Then it can be shown [7] that $J(U_1; U_2) = 1 + H(p) - 2H(\alpha)$, where $\alpha * \alpha = p$. The minimum for the common information expression is achieved by taking $V \sim \text{Bern}(1/2)$, $V_1 \sim \text{Bern}(\alpha)$, $V_2 \sim \text{Bern}(\alpha)$ independent of each other and $U_j = V \oplus V_j$, $j = 1, 2$
- Let (U_1, U_2) be binary with $p(0, 0) = p(0, 1) = p(1, 1) = 1/3$. Then it can be shown [8] that $J(U_1; U_2) = 2/3$, which is achieved by taking $V \sim \text{Bern}(1/2)$, $U_1 = 0$, $U_2 \sim \text{Bern}(2/3)$ if $V = 0$, and $U_1 \sim \text{Bern}(1/3)$, $U_2 = 1$ if $V = 1$

Source–Channel Separation with Common Information

- By incorporating the common message into Marton’s coding and describing the sources by the Gray–Wyner coding, the sources can be transmitted losslessly if

$$I(U_1, U_2; V) + H(U_1|V) < I(W_0, W_1; Y_1),$$

$$I(U_1, U_2; V) + H(U_2|V) < I(W_0, W_2; Y_2),$$

$$\begin{aligned} I(U_1, U_2; V) + H(U_1|V) + H(U_2|V) &< I(W_0, W_1; Y_1) + I(W_2; Y_2|W_0) \\ &\quad - I(W_1; W_2|W_0), \end{aligned}$$

$$\begin{aligned} I(U_1, U_2; V) + H(U_1|V) + H(U_2|V) &< I(W_1; Y_1|W_0) + I(W_0, W_2; Y_2) \\ &\quad - I(W_1; W_2|W_0), \end{aligned}$$

$$\begin{aligned} 2I(U_1, U_2; V) + H(U_1|V) + H(U_2|V) &< I(W_0, W_1; Y_1) + I(W_0, W_2; Y_2) \\ &\quad - I(W_1; W_2|W_0) \end{aligned}$$

for some $p(w_0, w_1, w_2, x)$ and $p(v|u_1, u_2)$

- The source–channel separation is optimal for certain classes of sources and channels

- More capable BC: Suppose 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 source (U_1, U_2) can be transmitted losslessly if

$$H(U_1, U_2) < I(X; Y_1),$$

$$H(U_1, U_2) < I(X; Y_1|W) + I(W; Y_2),$$

$$H(U_2) < I(W; Y_2)$$

for some $p(w, x)$

- Degraded source sets: Suppose $U_1 = (V_1, V_2)$ and $U_2 = V_2$ for some $(V_1, V_2) \sim p(v_1, v_2)$. Then the source (U_1, U_2) can be transmitted losslessly if

$$H(V_1, V_2) = H(U_1) < I(X; Y_1),$$

$$H(V_1, V_2) = H(U_1) < I(X; Y_1|W) + I(W; Y_2),$$

$$H(V_2) = H(U_2) < I(W; Y_2)$$

for some $p(w, x)$

- In both cases, achievability follows by representing the source sequences by a pair of messages at rates $R_2 = H(U_2)$ and $R_1 = H(U_1|U_2)$ and sending them via superposition coding. The converse is essentially identical to that of the corresponding channel coding theorems for the DM-BC

- However, as in the case of the DM-MAC, source–channel separation is not optimal in general
- Example: Consider the binary sources (U_1, U_2) with $p(0, 0) = p(0, 1) = p(1, 1) = 1/3$ and the Blackwell channel (cf. Lecture Notes 9) defined by $\mathcal{X} = \{0, 1, 2\}$, $\mathcal{Y}_1 = \mathcal{Y}_2 = \{0, 1\}$, $p(0, 0|0) = p(0, 1|1) = p(1, 1|2) = 1$. In this case, setting $X = U_1 + U_2$ achieves error-free transmission since Y_1 and Y_2 uniquely determine U_1 and U_2 , respectively

On the other hand, an achievable rate triple (R_0, R_1, R_2) for the Blackwell channel must satisfy

$$R_0 + R_1 \leq H(Y_1) \leq 1,$$

$$R_0 + R_2 \leq H(Y_2) \leq 1,$$

$$R_0 + R_1 + R_2 \leq H(Y_1, Y_2) \leq \log 3$$

However, as we saw before, the sources require $R_0 \geq J(U_1; U_2) = 2/3$ when $R_0 + R_1 + R_2 \leq \log 3$, or equivalently, $2R_0 + R_1 + R_2 \geq \log 3 + 2/3 = 2.252$, which implies $R_0 + R_1 \geq 1.126$ or $R_0 + R_2 \geq 1.126$. Hence, source–channel separation fails

- Next we describe a general joint source–channel coding scheme that combines Marton’s coding with Gray–Wyner coding

A Joint Source–Channel Coding Scheme

- *Theorem 4* [9, 10]: The 2-DMS $(\mathcal{U}_1 \times \mathcal{U}_2, p(u_1, u_2))$ can be transmitted losslessly over a DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$ if
$$H(U_1|U_2) < I(U_1, W_0, W_1; Y_1) - I(U_1, W_0, W_1; U_2),$$

$$H(U_2|U_1) < I(U_2, W_0, W_2; Y_2) - I(U_2, W_0, W_2; U_1),$$

$$H(U_1, U_2) < I(U_1, W_0, W_1; Y_1) + I(U_2, W_2; Y_2|W_0) - I(U_1, W_1; U_2, W_2|W_0),$$

$$H(U_1, U_2) < I(U_1, W_1; Y_1|W_0) + I(U_2, W_0, W_2; Y_2) - I(U_1, W_1; U_2, W_2|W_0),$$

$$H(U_1, U_2) < I(U_1, W_0, W_1; Y_1) + I(U_2, W_0, W_2; Y_2) - I(U_1, W_1; U_2, W_2|W_0) - I(U_1, U_2; W_0)$$

for some $p(w_0, w_1, w_2|u_1, u_2)$ and function $x(u_1, u_2, w_0, w_1, w_2)$

- The given sufficient condition does not change by time sharing

- Special cases:
 - Gray–Wyner region: Consider a noiseless dummy channel with $X = (X_0, X_1, X_2)$, $Y_1 = (X_0, X_1)$, $Y_2 = (X_0, X_2)$ and let $W_0 = (V, X_0)$, $W_1 = X_1$, $W_2 = X_2$, where $(V, X_0, X_1, X_2) \sim p(v|u_1, u_2)p(x_0)p(x_1)p(x_2)$ with an additional auxiliary random variable V . Then the sufficient condition in the theorem simplifies (check!) to

$$R_0 + R_1 > I(U_1, U_2; V) + H(U_1|V),$$

$$R_0 + R_2 > I(U_1, U_2; V) + H(U_2|V),$$

$$R_0 + R_1 + R_2 > I(U_1, U_2; V) + H(U_1|V) + H(U_2|V),$$

$$2R_0 + R_1 + R_2 > 2I(U_1, U_2; V) + H(U_1|V) + H(U_2|V),$$

where $R_j = H(X_j)$, $j \in [0 : 2]$. It can be easily shown that this region includes (and in fact is equivalent to) the Gray–Wyner rate region characterized by

$$R_0 > I(U_1, U_2; V),$$

$$R_1 > H(U_1|V),$$

$$R_2 > H(U_2|V)$$

- Marton’s inner bound: Let $(V_0, V_1, V_2) \sim p(v_0)p(v_1)p(v_2)$ be independent sources of entropies R_0, R_1, R_2 , respectively, and let $U_1 = (V_0, V_1)$, $U_2 = (V_0, V_2)$. By taking $W_0 = (V_0, W'_0)$ and $p(w'_0, w_1, w_2, x|u_1, u_2) = p(w'_0, w_1, w_2, x)$, the sufficient condition simplifies (check!) to

$$R_0 + R_1 < I(W'_0, W_1; Y_1),$$

$$R_0 + R_2 < I(W'_0, W_2; Y_2),$$

$$R_0 + R_1 + R_2 < I(W'_0, W_1; Y_1) + I(W_2; Y_2|W'_0) - I(W_1; W_2|W'_0),$$

$$R_0 + R_1 + R_2 < I(W_1; Y_1|W'_0) + I(W'_0, W_2; Y_2) - I(W_1; W_2|W'_0),$$

$$2R_0 + R_1 + R_2 < I(W'_0, W_1; Y_1) + I(W'_0, W_2; Y_2) - I(W_1; W_2|W'_0)$$

- For the binary sources over the Blackwell channel example, set $W_0 = \emptyset$, $W_1 = U_1$, $W_2 = U_2$, $X = U_1 + U_2$

Proof of Achievability [11]

- Codebook generation: Fix $p(w_0, w_1, w_2 | u_1, u_2)$ and $x(u_1, u_2, w_0, w_1, w_2)$

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 source sequence $u_1^n \in \mathcal{U}_1^n$ and $w_0^n(m_0)$, 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 source sequence $u_2^n \in \mathcal{U}_2^n$ and $w_0^n(m_0)$, 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 source sequence (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 at time $i \in [1 : n]$, the encoder transmits

$$x_i = x(u_{1i}, u_{2i}, w_{0i}(m_0), w_{1i}(u_1^n, m_0, m_1), w_{2i}(u_2^n, m_0, m_2))$$

- Decoding: Decoder 1 declares that \hat{u}_1^n to be the estimate of the source 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 that \hat{u}_2^n to be the estimate of the source 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

Define the events

$$\begin{aligned} \mathcal{E}_0 &:= \{(U_1^n, U_2^n, W_0^n(m_0), W_1^n(U_1^n, m_0, m_1), W_2^n(U_2^n, m_0, m_2)) \notin \mathcal{T}_{\epsilon}^{(n)} \\ &\quad \text{for all } m_0, m_1, m_2\}, \end{aligned}$$

$$\mathcal{E}_{11} := \{(U_1^n, W_0^n(M_0), W_1^n(U_1^n, M_0, M_1), Y_1^n) \notin \mathcal{T}_{\epsilon}^{(n)}\},$$

$$\mathcal{E}_{12} := \{(\tilde{u}_1^n, W_0^n(M_0), W_1^n(\tilde{u}_1^n, M_0, m_1), Y_1^n) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n, m_1\},$$

$$\mathcal{E}_{13} := \{(\tilde{u}_1^n, W_0^n(m_0), W_1^n(\tilde{u}_1^n, m_0, m_1), Y_1^n) \in \mathcal{T}_{\epsilon}^{(n)} \text{ for some } \tilde{u}_1^n \neq U_1^n, m_0 \neq M_0, m_1\}$$

Then the average probability of error $P(\mathcal{E}_1)$ for decoder 1 is upper bounded by

$$P(\mathcal{E}_1) \leq P(\mathcal{E}_0) + P(\mathcal{E}_0^c \cap \mathcal{E}_{11}) + P(\mathcal{E}_{12}) + P(\mathcal{E}_{13})$$

- We prove the following variant of the multivariate covering lemma (cf. Lecture Notes 9) in the Appendix:

Lemma 1: $P(\mathcal{E}_0) \rightarrow 0$ as $n \rightarrow \infty$, if

$$R_0 > I(U_1, U_2; W_0) + \delta(\epsilon'),$$

$$R_0 + R_1 > I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + \delta(\epsilon'),$$

$$R_0 + R_2 > I(U_1, U_2; W_0) + I(U_1; W_2|U_2, W_0) + \delta(\epsilon'),$$

$$R_0 + R_1 + R_2 > I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + I(U_1, W_1; W_2|U_2, W_0) + \delta(\epsilon')$$

- By the conditional typicality lemma, $P(\mathcal{E}_0^c \cap \mathcal{E}_{11}) \rightarrow 0$ as $n \rightarrow \infty$
- Following steps similar to the DM-MAC joint source–channel coding, it can be shown that $P(\mathcal{E}_{12}) \rightarrow 0$ as $n \rightarrow \infty$ if $H(U_1) + R_1 < I(U_1, W_1; Y_1|W_0) + I(U_1; W_0) - \delta(\epsilon)$, and $P(\mathcal{E}_{13}) \rightarrow 0$ as $n \rightarrow \infty$ 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 $P(\mathcal{E}_2)$ for decoder 2 $\rightarrow 0$ as $n \rightarrow \infty$ if $H(U_2) + R_2 < I(U_2, W_2; Y_2|W_0) + I(U_2; W_0) - \delta(\epsilon)$ and $H(U_2) + R_0 + R_2 < I(U_2, W_0, W_1; Y_2) + I(U_2; W_0) - \delta(\epsilon)$
- The rest of the proof follows by combining the above inequalities and eliminating (R_0, R_1, R_2) using the Fourier–Motzkin procedure

Key New Ideas and Techniques

- Separation theorem does not hold in general for transmitting correlated sources over multiple user channels
- Common part between two random variables U_1 and U_2
- Gray–Wyner system
- Notions of common information
- Open problem: What are the necessary and sufficient conditions for transmitting correlated sources losslessly over a DM-MAC

Appendix: Proof of Lemma 1

- The proof follows similar steps to the multivariate covering lemma in Lecture Notes 9
- 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

$$\mathbb{P}(\mathcal{E}_0) \leq \mathbb{P}\{(U_1^n, U_2^n) \notin \mathcal{T}_{\epsilon'}^{(n)}\} + \sum_{(u_1^n, u_2^n) \in \mathcal{T}_{\epsilon'}^{(n)}} p(u_1^n, u_2^n) \mathbb{P}\{|\mathcal{A}(u_1^n, u_2^n)| = 0\}$$

- By the LLN, the first term $\rightarrow 0$ as $n \rightarrow \infty$
- To bound the second term, we recall that

$$\mathbb{P}\{|\mathcal{A}(u_1^n, u_2^n)| = 0\} \leq \frac{\text{Var}(|\mathcal{A}(u_1^n, u_2^n)|)}{(\mathbb{E}(|\mathcal{A}(u_1^n, u_2^n)|))^2}$$

Using the indicator variables, we can write

$$|\mathcal{A}(u_1^n, u_2^n)| = \sum_{m_0, m_1, m_2} E(m_0, m_1, m_2),$$

where

$$E(m_0, m_1, m_2) := \begin{cases} 1 & \text{if } (u_1^n, u_2^n, W_0^n(m_0), W_1^n(u_1^n, m_0, m_1), W_2^n(u_2^n, m_0, m_2)) \in \mathcal{T}_{\epsilon'}^{(n)}, \\ 0 & \text{otherwise} \end{cases}$$

for each (m_0, m_1, m_2) . Let

$$\begin{aligned} p_1 &:= \mathbb{E}(E(1, 1, 1)) \\ &= \mathbb{P}\{(u_1^n, u_2^n, W_0^n(m_0), W_1^n(u_1^n, m_0, m_1), W_2^n(u_2^n, m_0, m_2)) \in \mathcal{T}_{\epsilon'}^{(n)}\}, \\ p_2 &:= \mathbb{E}(E(1, 1, 1)E(1, 2, 1)), \\ p_3 &:= \mathbb{E}(E(1, 1, 1)E(1, 1, 2)), \\ p_4 &:= \mathbb{E}(E(1, 1, 1)E(1, 2, 2)), \\ p_5 &:= \mathbb{E}(E(1, 1, 1)E(2, 1, 1)) = \mathbb{E}(E(1, 1, 1)E(2, 1, 2)) \\ &= \mathbb{E}(E(1, 1, 1)E(2, 2, 1)) = \mathbb{E}(E(1, 1, 1)E(2, 2, 2)) = p_1^2 \end{aligned}$$

Then

$$\mathbb{E}(|\mathcal{A}(u_1^n, u_2^n)|) = \sum_{m_0, m_1, m_2} \mathbb{E}(E(m_0, m_1, m_2)) = 2^{n(R_0+R_1+R_2)} p_1,$$

$$\begin{aligned}
\mathsf{E}(|\mathcal{A}(u_1^n, u_2^n)|^2) &= \sum_{m_0, m_1, m_2} \mathsf{E}(E(m_0, m_1, m_2)) \\
&\quad + \sum_{m_0, m_1, m_2} \sum_{m'_1 \neq m_1} \mathsf{E}(E(m_0, m_1, m_2) E(m_0, m'_1, m_2)) \\
&\quad + \sum_{m_0, m_1, m_2} \sum_{m'_2 \neq m_2} \mathsf{E}(E(m_0, m_1, m_2) E(m_0, m_1, m'_2)) \\
&\quad + \sum_{m_0, m_1, m_2} \sum_{m'_1 \neq m_1, m'_2 \neq m_2} \mathsf{E}(E(m_0, m_1, m_2) E(m_0, m'_1, m'_2)) \\
&\quad + \sum_{m_0, m_1, m_2} \sum_{m'_0 \neq m_0, m'_1, m'_2} \mathsf{E}(E(m_0, m_1, m_2) E(m'_0, m'_1, m'_2)) \\
&\leq 2^{n(R_0+R_1+R_2)} p_1 + 2^{n(R_0+2R_1+R_2)} p_2 + 2^{n(R_0+R_1+2R_2)} p_3 \\
&\quad + 2^{n(R_0+2R_1+2R_2)} p_4 + 2^{2n(R_0+R_1+R_2)} p_5
\end{aligned}$$

Hence

$$\begin{aligned}
\text{Var}(|\mathcal{A}(u_1^n, u_2^n)|) &\leq 2^{n(R_0+R_1+R_2)} p_1 + 2^{n(R_0+2R_1+R_2)} p_2 \\
&\quad + 2^{n(R_0+R_1+2R_2)} p_3 + 2^{n(R_0+2R_1+2R_2)} p_4
\end{aligned}$$

Now by the joint typicality lemma, we have

$$\begin{aligned}
p_1 &\geq 2^{-n(I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + I(U_1, W_1; W_2|U_2, W_0) + \delta(\epsilon))}, \\
p_2 &\leq 2^{-n(I(U_1, U_2; W_0) + 2I(U_2, W_2; W_1|U_1, W_0) + I(U_1; W_2|U_2, W_0) + \delta(\epsilon))}, \\
p_3 &\leq 2^{-n(I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + 2I(U_1, W_1, U_1; W_2|U_2, W_0) + \delta(\epsilon))}, \\
p_4 &\leq 2^{-n(I(U_1, U_2; W_0) + 2I(U_2; W_1|U_1, W_0) + 2I(U_1, W_1; W_2|U_2, W_0) + \delta(\epsilon))}
\end{aligned}$$

Hence

$$\begin{aligned}
\frac{\text{Var}(|\mathcal{A}(u_1^n, u_2^n)|)}{(\mathsf{E}(|\mathcal{A}(u_1^n, u_2^n)|))^2} &\leq 2^{-n(R_0+R_1+R_2-I(U_1, U_2; W_0)-I(U_2; W_1|U_1, W_0)-I(U_1, W_1; W_2|U_2, W_0)-\delta(\epsilon))} \\
&\quad + 2^{-n(R_0+R_2-I(U_1, U_2; W_0)-I(U_1; W_2|U_2, W_0)-3\delta(\epsilon))} \\
&\quad + 2^{-n(R_0+R_1-I(U_1, U_2; W_0)-I(U_2; W_1|U_1, W_0)-3\delta(\epsilon))} \\
&\quad + 2^{-n(R_0-I(U_1, U_2; W_0)-3\delta(\epsilon))}
\end{aligned}$$

Therefore, $\mathsf{P}\{|\mathcal{A}(u_1^n, u_2^n)| = 0\} \rightarrow 0$ as $n \rightarrow \infty$ if

$$\begin{aligned}
R_0 &> I(U_1, U_2; W_0) + 3\delta(\epsilon), \\
R_0 + R_1 &> I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + 3\delta(\epsilon), \\
R_0 + R_2 &> I(U_1, U_2; W_0) + I(U_1; W_2|U_2, W_0) + 3\delta(\epsilon), \\
R_0 + R_1 + R_2 &> I(U_1, U_2; W_0) + I(U_2; W_1|U_1, W_0) + I(U_1, W_1; W_2|U_2, W_0) + \delta(\epsilon)
\end{aligned}$$

References

- [1] T. M. Cover, A. El Gamal, and M. Salehi, "Multiple access channels with arbitrarily correlated sources," *IEEE Trans. Inf. Theory*, vol. 26, no. 6, pp. 648–657, Nov. 1980.
- [2] P. Gács and J. Körner, "Common information is far less than mutual information," *Probl. Control Inf. Theory*, vol. 2, no. 2, pp. 149–162, 1973.
- [3] H. S. Witsenhausen, "On sequences of pairs of dependent random variables," *SIAM J. Appl. Math.*, vol. 28, pp. 100–113, 1975.
- [4] D. Slepian and J. K. Wolf, "A coding theorem for multiple access channels with correlated sources," *Bell System Tech. J.*, vol. 52, pp. 1037–1076, Sept. 1973.
- [5] G. Dueck, "A note on the multiple access channel with correlated sources," *IEEE Trans. Inf. Theory*, vol. 27, no. 2, pp. 232–235, 1981.
- [6] R. M. Gray and A. D. Wyner, "Source coding for a simple network," *Bell System Tech. J.*, vol. 53, pp. 1681–1721, 1974.
- [7] A. D. Wyner, "On source coding with side information at the decoder," *IEEE Trans. Inf. Theory*, vol. 21, pp. 294–300, 1975.
- [8] H. S. Witsenhausen, "Values and bounds for the common information of two discrete random variables," *SIAM J. Appl. Math.*, vol. 31, no. 2, pp. 313–333, 1976.
- [9] T. S. Han and M. M. H. Costa, "Broadcast channels with arbitrarily correlated sources," *IEEE Trans. Inf. Theory*, vol. 33, no. 5, pp. 641–650, Sept. 1987.
- [10] G. Kramer and C. Nair, "Comments on ‘broadcast channels with arbitrarily correlated

- "sources'," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 2777–2779.
- [11] P. Minero and Y.-H. Kim, "Correlated sources over broadcast channels," 2009.

Part III. Multi-hop Networks

Lecture Notes 16

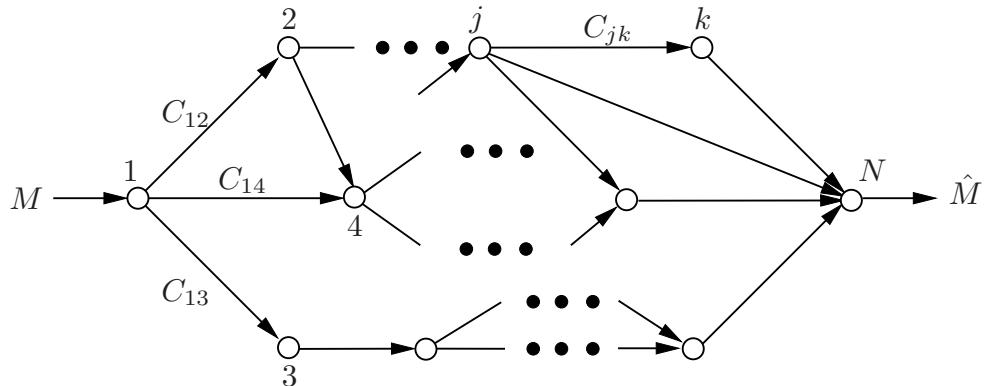
Noiseless Networks

- Noiseless Relay Network
- Noiseless Multicast Network
- Noiseless Multiple-Source Networks
- Key New Ideas and Techniques
- Appendix: Proof of Lemma 1

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

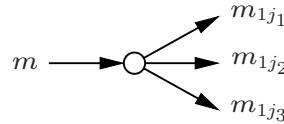
Noiseless Relay Network

- Consider a *noiseless relay network* modeled by a weighted directed acyclic graph $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{C})$. Here $\mathcal{N} = [1 : N]$ is the set of nodes, $\mathcal{E} \subset [1 : N] \times [1 : N]$ is the set of edges, and $\mathcal{C} = \{C_{jk} \in \mathbb{R}^+ : (j, k) \in \mathcal{E}\}$ is the set of weights. Each edge represents a noiseless communication link with capacity C_{jk}
- *Source node 1* wishes to send a message $M \in [1 : 2^{nR}]$ to *destination node N*

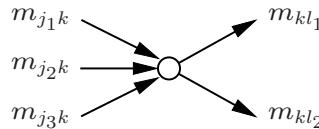


- A $(2^{nR}, n)$ code for a noiseless relay network $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{C})$ consists of:
 1. A source message set $[1 : 2^{nR}]$

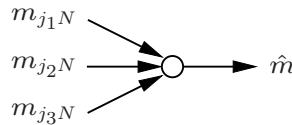
2. A source encoder that assigns an index $m_{1j}(m) \in [1 : 2^{nC_{1j}}]$ to each message $m \in [1 : 2^{nR}]$ for each edge $(1, j) \in \mathcal{E}$



3. A set of $(N - 2)$ relay encoders: Encoder k assigns an index $m_{kl} \in [1 : 2^{nC_{kl}}]$ to each received index tuple $\{m_{jk} : (j, k) \in \mathcal{E}\}$ for each $(k, l) \in \mathcal{E}$



4. A decoder that assigns a message $\hat{m} \in [1 : 2^{nR}]$ or an error message e to every received index tuple $\{m_{jN} : (j, N) \in \mathcal{E}\}$



- M is uniformly distributed over $[1 : 2^{nR}]$

- The probability of error is $P_e^{(n)} = P\{M \neq \hat{M}\}$
- A rate R is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The capacity (maximum flow) of the noiseless relay network is the supremum of the set of achievable rates

Max-flow Min-cut Theorem

- The capacity of the noiseless relay network is given by the following

Max-flow Min-cut Theorem [1, 2]: The capacity of the noiseless relay network $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{C})$ is

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

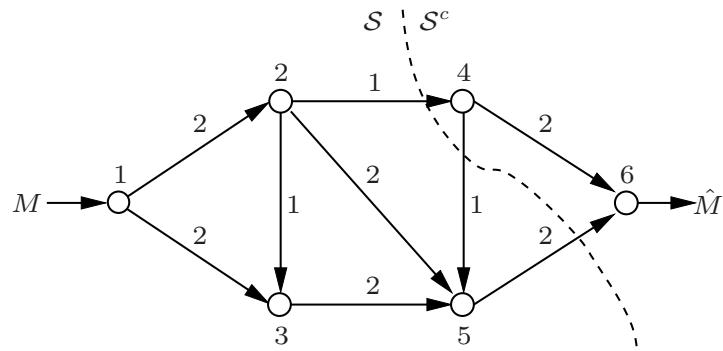
where

$$C(\mathcal{S}) := \sum_{\substack{(j,k) \in \mathcal{E} \\ j \in \mathcal{S}, k \in \mathcal{S}^c}} C_{jk}$$

is the capacity of a *cut* \mathcal{S}

In other words, the maximum flow is the minimum cut (capacity)

- Example: Consider the following noiseless relay network:



The capacity of this network is $C = 3$, with the minimum cut $\mathcal{S} = \{1, 2, 3, 5\}$.

The capacity is achieved by sending (routing) 1 bit along the path
 $1 \rightarrow 2 \rightarrow 4 \rightarrow 6$ and 2 bits along the path $1 \rightarrow 3 \rightarrow 5 \rightarrow 6$

- Proof of converse: Let \mathcal{S} be a cut, i.e., $\mathcal{S} \subset \mathcal{N}$ such that $1 \in \mathcal{S}$ and $N \in \mathcal{S}^c$. Then for any $(2^{nR}, n)$ code, \hat{M} is a function of $M(\mathcal{N}, \mathcal{S}^c) := \{M_{jk} : (j, k) \in \mathcal{E}, k \in \mathcal{S}^c\}$, which is in turn a function of $M(\mathcal{S}, \mathcal{S}^c) := \{M_{jk} : (j, k) \in \mathcal{E}, j \in \mathcal{S}, k \in \mathcal{S}^c\}$ (why?)

Thus by Fano's inequality,

$$\begin{aligned} nR &\leq I(M; \hat{M}) + n\epsilon_n \\ &\leq H(\hat{M}) + n\epsilon_n \\ &\leq H(M(\mathcal{S}, \mathcal{S}^c)) + n\epsilon_n \\ &\leq C(\mathcal{S}) + n\epsilon_n \end{aligned}$$

- Proof of Achievability:

- Suppose we allocate rate $r_{jk} \leq C_{jk}$ to each edge $(j, k) \in \mathcal{E}$ such that

$$\sum_{j:(j,k) \in \mathcal{E}} r_{jk} = \sum_{l:(k,l) \in \mathcal{E}} r_{kl} \text{ for all } k \neq 1, N$$

and

$$\sum_{k:(1,k) \in \mathcal{E}} r_{1k} = \sum_{j:(j,N) \in \mathcal{E}} r_{jN} = R$$

i.e., the total incoming information rate at the node is equal to the total outgoing information rate. Then it is straightforward to check that the rate R is achievable by splitting the message into multiple streams and routing them according to the rate allocation r_{jk} (as in commodity flows)

- Thus we can optimize the rate allocation as follows:

$$\begin{array}{ll} \text{maximize} & R \\ \text{subject to} & 0 \leq r_{jk} \leq C_{jk} \\ & \sum_j r_{jk} = \sum_l r_{kl}, \quad k \neq 1, N \\ & \sum_k r_{1k} = R \\ & \sum_j r_{jN} = R \end{array}$$

This is a linear programming problem and we can find its solution by solving its dual problem (another linear programming problem) [3]:

$$\begin{array}{ll} \text{minimize} & \sum_{j,k} \lambda_{jk} C_{jk} \\ \text{subject to} & \lambda_{jk} \geq 0 \\ & \nu_j - \nu_k = \lambda_{jk} \\ & \nu_1 - \nu_N = 1 \end{array}$$

with variables $\lambda_{jk}, (j, k) \in \mathcal{E}$ (weights for the link capacities) and $\nu_j, j \in \mathcal{N}$ (differences of the weights)

Now it can be shown that the dual optimum is achieved by

$$\nu_j^* = \begin{cases} 1 + c, & j \in \mathcal{S}, \\ c, & \text{otherwise,} \end{cases}$$

$$\lambda_{jk}^* = \begin{cases} 1, & j \in \mathcal{S}, k \in \mathcal{S}^c, \\ 0, & \text{otherwise} \end{cases}$$

for some c and $\mathcal{S} \in \mathcal{N}$ with $1 \in \mathcal{S}, N \in \mathcal{S}^c$, each of which gives nothing but a cut capacity $C(\mathcal{S})$. Hence, the dual optimum is the minimum cut capacity

- Finally, since both the primal and dual optimization problems satisfy *Slater's condition* (i.e., the feasible region has an interior point), the dual optimum is equal to the primal optimum, i.e.,

$$\max R = \min C(\mathcal{S})$$

This completes the proof of achievability

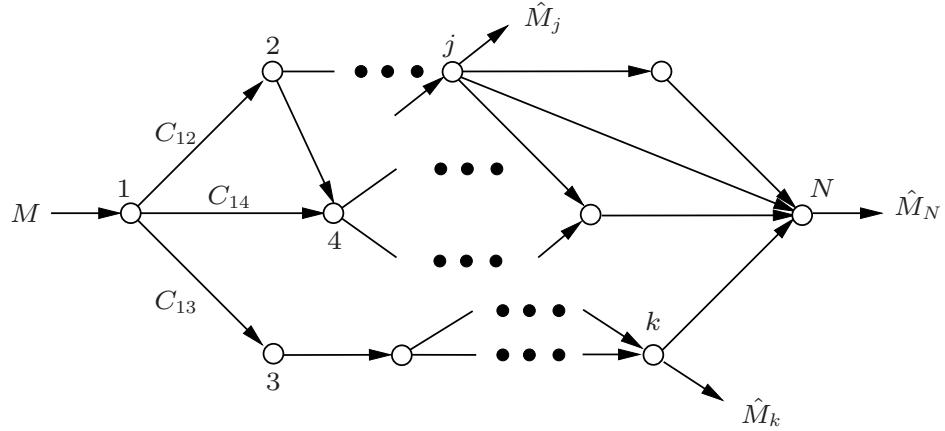
- Remarks:

- Capacity is achieved with zero error by simple routing (rate allocation) instead of more sophisticated encoding at relays. As we discuss in the next section, this is not the case in general when there are multiple destinations (multicast)

- The capacity and optimal routing can be found by the Ford–Fulkerson algorithm [1], which is constructive and more efficient than standard linear programming algorithms (the simplex method or interior point method)
- The max-flow min-cut theorem continues to hold for networks with cycles or delays (cf. Lecture Notes 19). For networks with cycles, the optimal routing found by the Ford–Fulkerson algorithm does not contain any cycle

Noiseless Multicast Network

- Now we consider the multicast extension of the noiseless relay network. Source node 1 wishes to send a message M to a set of destination nodes \mathcal{D}



- A $(2^{nR}, n)$ code, probability of error, achievability, and capacity are defined as for the single-destination case

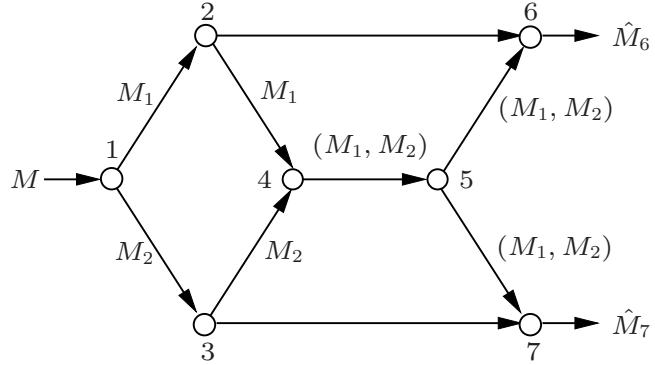
- Cut-set upper bound:* From the converse for the max-flow min-cut theorem, the capacity is upper bounded by

$$C \leq \min_{\substack{\mathcal{S} \subset \mathcal{N} \\ 1 \in \mathcal{S}, j \in \mathcal{S}^c}} C(\mathcal{S})$$

for each destination node $j \in \mathcal{D}$

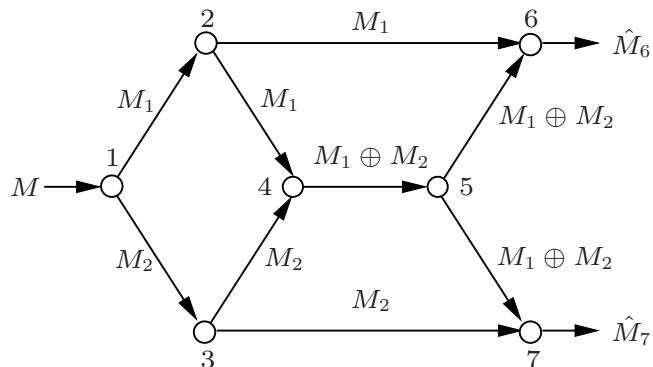
- If $\mathcal{D} = [2 : N]$, i.e., if every node wishes to receive the message, then it can be easily shown (check!) that this cutset upper bound is achievable by routing at intermediate nodes
- However, if $\mathcal{D} \subset [2 : N]$, the cutset upper bound is not in general achievable by routing only

- Example (butterfly network [4]): Consider the following noiseless multicast network with $C_{jk} = 1$ for all (j, k) and $\mathcal{D} = \{6, 7\}$
 - The cutset upper bound is $C \leq 2$
 - Split the message M into two independent messages M_1 at rate R_1 and M_2 at rate R_2 . Thus $R = R_1 + R_2$. If each relay node k simply routes incoming bitstreams (i.e., $\sum_j r_{jk} = \sum_l r_{kl}$ for each relay node k), then it can be easily seen that $R_1 + R_2$ must be ≤ 1 with $r_{45} \leq C_{45} = 1$ being the major bottleneck



- Even if we allow the relay nodes to forward multiple copies of incoming bitstreams, we still have $R_1 + R_2 \leq 1$

- Surprisingly, if we allow simple encoding operations at the relay nodes (network coding), we can achieve the cutset upper bound
Let $R_1 = R_2 = 1$. If relay nodes 2, 3, and 5 forward multiple copies of their incoming bitstreams and relay node 4 sends the binary sum (XOR) of its incoming bitstreams, then both destination nodes 6 and 7 can recover (M_1, M_2) with no errors, achieving the cutset upper bound



- This observation can be generalized to any noiseless multicast network

Network Coding Theorem

- *Network Coding Theorem* [4]: The capacity of the noiseless multicast network $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{C})$ with destination set \mathcal{D} is

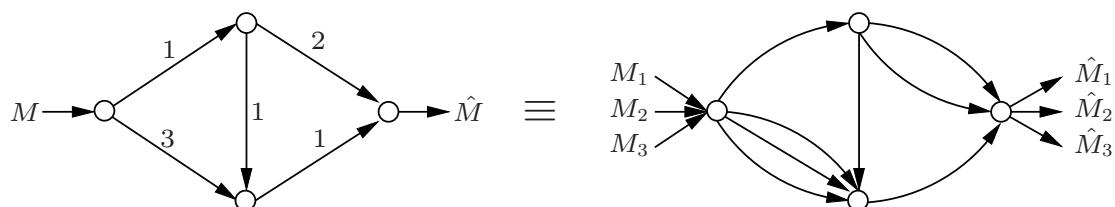
$$C = \min_{j \in \mathcal{D}} \min_{\substack{\mathcal{S} \subset \mathcal{N} \\ 1 \in \mathcal{S}, j \in \mathcal{S}^c}} C(\mathcal{S}),$$

where $C(\mathcal{S})$ is the capacity of the cut \mathcal{S}

- Capacity coincides with the cutset upper bound
- Interestingly, capacity can be achieved with zero error by simple linear operations at the relay nodes (*linear network coding*) [5, 6]

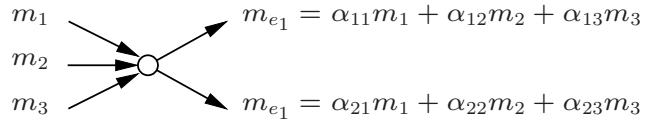
Linear Network Coding

- For simplicity, we first consider a noiseless multicast network with integer link capacities, represented by a directed acyclic *multigraph* $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ with links of the same 1-bit capacity. Therefore, each link of the multigraph \mathcal{G} can carry n bits of information (a symbol from \mathbb{F}_{2^n}) per n -transmission block. Further, we assume that R is an integer so that the message can be represented as $M = (M_1, \dots, M_R)$ with $M_j \in \mathbb{F}_{2^n}$, $j \in [1 : R]$
- Example: Assume $R = 3$

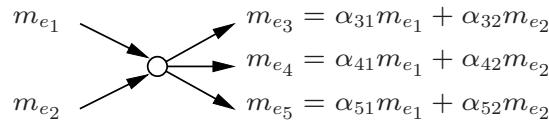


- Given a network modeled by a multigraph $(\mathcal{N}, \mathcal{E})$, we denote the set of outgoing edges from a node $k \in \mathcal{N}$ by $\mathcal{E}_{k \rightarrow}$ and the set of incoming edges to a node k by $\mathcal{E}_{\rightarrow k}$

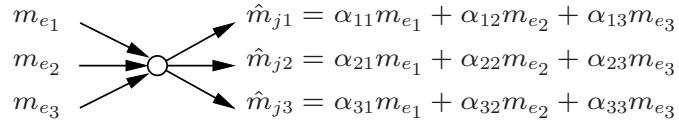
- For this setup, a $(2^{nR}, n)$ linear code consists of
 1. A message set $\mathbb{F}_{2^n}^R$, that is, each message is represented by a vector in the R -dimensional vector space over the finite field \mathbb{F}_{2^n}
 2. A linear source encoder that assigns an index tuple
 $m(\mathcal{E}_{1 \rightarrow}) := \{m_e \in \mathbb{F}_{2^n} : e \in \mathcal{E}_{1 \rightarrow}\}$ to each $(m_1, \dots, m_R) \in \mathbb{F}_{2^n}^R$ via a linear transformation with coefficient $\alpha_{jk} \in \mathbb{F}_{2^n}$



- 3. A set of linear relay encoders: Encoder k assigns an index tuple $m(\mathcal{E}_{k \rightarrow})$ to each $m(\mathcal{E}_{\rightarrow k})$ via a linear transformation



- 4. A set of linear decoders: Decoder j , $j \in \mathcal{D}$, assigns \hat{m}_j^R to each $m(\mathcal{E}_{\rightarrow j})$

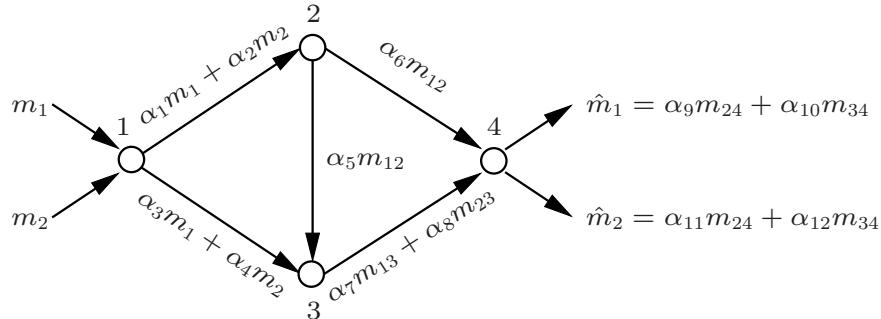


- Thus, for each destination node $j \in \mathcal{D}$, a linear code induces a linear transformation

$$\hat{m}_j^R = A_j(\boldsymbol{\alpha})m^R$$

for some $A_j(\boldsymbol{\alpha}) \in \mathbb{F}_{2^n}^{R \times R}$, where $\boldsymbol{\alpha}$ is a vector of linear encoding/decoding coefficients with elements taking values in \mathbb{F}_{2^n}

For example, consider the following network with $\mathcal{D} = \{4\}$



A linear network code with $R = 2$ induces the linear transformation

$$\begin{pmatrix} \hat{m}_1 \\ \hat{m}_2 \end{pmatrix} = \begin{pmatrix} \alpha_9 & \alpha_{10} \\ \alpha_{11} & \alpha_{12} \end{pmatrix} \begin{pmatrix} \alpha_6 & 0 \\ \alpha_5 \alpha_8 & \alpha_7 \end{pmatrix} \begin{pmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 & \alpha_4 \end{pmatrix} \begin{pmatrix} m_1 \\ m_2 \end{pmatrix}$$

- The rate R is achievable with zero error if there exist an integer n and a vector α such that $A_j(\alpha) = I_R$ for every $j \in \mathcal{D}$. Note that any invertible $A_j(\alpha)$ suffices since the decoder can multiply \hat{m}_j^R by $A_j^{-1}(\alpha)$ to recover m

The resulting decoder is still linear (with a different α). In the above example, it corresponds to the linear transformation

$$A^{-1}(\alpha) \begin{pmatrix} \alpha_9 & \alpha_{10} \\ \alpha_{11} & \alpha_{12} \end{pmatrix}$$

- A general network with noninteger link capacities can be approximated by a multigraph with links of the same n/k bit capacities (each link carries n information bits per k transmissions). A $(2^{nR}, k)$ linear code with rate nR/k is defined as before with vector space dimension R

Proof of Achievability

- We show that a linear code can achieve the cutset bound using an elegant proof by Koetter and Medard [6]
- First consider a noiseless relay network (a multicast network with $\mathcal{D} = \{N\}$). A $(2^{nR}, n)$ linear code induces $\hat{m}^R = A(\alpha)m^R$ for some matrix $A(\alpha)$, where α denotes the coefficients in the encoder and decoder maps

Now replace the coefficients α with indeterminate vector \mathbf{x} and consider the determinant $|A(\mathbf{x})|$ as a multivariate polynomial in \mathbf{x}

In the previous example, $\mathbf{x} = (x_1, \dots, x_{12})$

$$\begin{aligned} A(\mathbf{x}) &= \begin{pmatrix} x_9 & x_{10} \\ x_{11} & x_{12} \end{pmatrix} \begin{pmatrix} x_6 & 0 \\ x_5x_8 & x_7 \end{pmatrix} \begin{pmatrix} x_1 & x_2 \\ x_3 & x_4 \end{pmatrix} \\ &= \begin{pmatrix} x_1(x_6x_9 + x_5x_8x_{10}) + x_3x_7x_{10} & x_2(x_6x_9 + x_5x_8x_{10}) + x_4x_7x_{10} \\ x_1(x_6x_{11} + x_5x_8x_{12}) + x_3x_7x_{12} & x_2(x_6x_{11} + x_5x_8x_{12}) + x_4x_7x_{12} \end{pmatrix} \end{aligned}$$

and

$$\begin{aligned} |A(\mathbf{x})| &= (x_1(x_6x_9 + x_5x_8x_{10}) + x_3x_7x_{10})(x_2(x_6x_{11} + x_5x_8x_{12}) + x_4x_7x_{12}) \\ &\quad - (x_1(x_6x_{11} + x_5x_8x_{12}) + x_3x_7x_{12})(x_2(x_6x_9 + x_5x_8x_{10}) + x_4x_7x_{10}) \end{aligned}$$

In general, $|A(\mathbf{x})|$ is a polynomial in \mathbf{x} with binary coefficients, that is, $|A(\mathbf{x})| \in \mathbb{F}_2[\mathbf{x}]$, the polynomial ring over \mathbb{F}_2 . This polynomial depends on the network topology and the rate R , but not on n

We first show that the rate R is achievable iff $|A(\mathbf{x})|$ is nonzero in $\mathbb{F}_2[\mathbf{x}]$

- o Suppose $R \leq C$ (i.e., R is achievable by the max-flow min-cut theorem). Then R is achievable by routing, which is a special class of linear codes (with zero or one coefficients). Hence, there exists a coefficient vector α with components in \mathbb{F}_2 such that $A(\alpha) = I_R$ (because the message is received with zero error at the destination). In particular, $|A(\alpha)| = |I_R| = 1$, which implies that $|A(\mathbf{x})|$ is nonzero in the polynomial ring $\mathbb{F}_2[\mathbf{x}]$
- o Conversely, suppose $|A(\mathbf{x})|$ is a nonzero polynomial in $\mathbb{F}_2[\mathbf{x}]$ for some R . Then there exist an integer n and a vector α with components taking values in \mathbb{F}_{2^n} such that $A(\alpha)$ is invertible

To show this, we prove the following fact in the Appendix

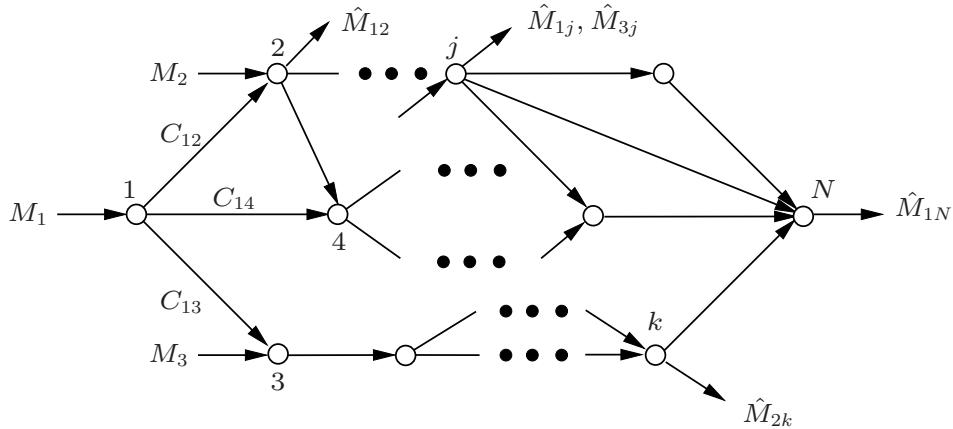
Lemma 1: If $P(\mathbf{x})$ is a nonzero polynomial in $\mathbb{F}_2[\mathbf{x}]$. Then there exist an integer n and a vector α with components taking values in \mathbb{F}_{2^n} such that $P(\alpha) \neq 0$

Now from the lemma, $|A(\alpha)|$ is nonzero, that is, $A(\alpha)$ is invertible

- Next consider the multicast network with destination nodes \mathcal{D}
 - o If $R \leq C$, then from the above, each of $|A_j(\mathbf{x})|$, $j \in \mathcal{D}$, is a nonzero polynomial in $\mathbb{F}_2[\mathbf{x}]$. Since $\mathbb{F}_2[\mathbf{x}]$ is an integral domain (i.e., the product of any two nonzero elements is nonzero) [7], this implies that $\prod_{j \in \mathcal{D}} |A_j(\mathbf{x})|$ is also a nonzero polynomial
 - o As before, this shows that there exist n and α with elements in \mathbb{F}_{2^n} such that $|A_j(\alpha)|$ is nonzero for all $j \in \mathcal{D}$, that is, $A_j^{-1}(\alpha)$ is invertible for all $j \in \mathcal{D}$
- Remarks:
 - o It can be shown [6] that it suffices to take $n \leq \lceil \log(|\mathcal{D}|R + 1) \rceil$
 - o There exists an efficient algorithm [8] to find a vector α (which makes $A_j(\alpha)$ invertible for each $j \in \mathcal{D}$). In comparison, finding the optimal routing is an NP-complete problem of packing Steiner trees [9]
 - o For sufficiently large n , a *randomly* generated linear network code achieves capacity with high probability. This random linear network coding can be used as both a construction tool and a method of attaining robustness to link failures and network topology changes [10, 9]

Noiseless Multiple-Source Networks

- As before, consider a noiseless network modeled by a directed acyclic graph $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{C})$. Assume that the nodes are ordered so that there is no path from node k to node j if $j < k$
- Each node $j \in [1 : N - 1]$ wishes to send a message M_j to a set $\mathcal{D}_j \subseteq [j + 1 : N]$ of destination nodes



This setup includes the case where only a subset of nodes are sending messages by taking $M_j = \emptyset$ (zero rate) for each nonsource node j

- Formally, a $(2^{nR_1}, \dots, 2^{nR_{N-1}}, n)$ code for the noiseless network $\mathcal{G} = (\mathcal{N}, \mathcal{E}, \mathcal{C})$ consists of:
 - Message sets $[1 : 2^{nR_1}], \dots, [1 : 2^{nR_{N-1}}]$
 - A set of encoders: Encoder $k \in [1 : N - 1]$ assigns an index $m_{kl} \in [1 : 2^{nC_{kl}}]$ to each received index tuple $\{m_{jk} : (j, k) \in \mathcal{E}\}$ and its own message m_k
 - A set of decoders: Decoder $l \in [2 : N]$ assigns a message \hat{m}_{jl} or an error message e to each received index tuple $\{m_{kl} : (k, l) \in \mathcal{E}\}$ for j such that $l \in \mathcal{D}_j$
- Assume that M_1, \dots, M_{N-1} are uniformly distributed over $[1 : 2^{nR_1}] \times \dots \times [1 : 2^{nR_{N-1}}]$
- The probability of error is $P_e^{(n)} = \mathbb{P}\{M_j \neq \hat{M}_{jk} \text{ for some } j \in [1 : N - 1], k \in \mathcal{D}_j\}$
- A rate tuple (R_1, \dots, R_{N-1}) is said to be achievable if there exists a sequence of $(2^{nR_1}, \dots, 2^{nR_{N-1}}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The capacity region of the noiseless network is the closure of the set of achievable rates tuples

- Cutset outer bound: If the rate tuple (R_1, \dots, R_{N-1}) is achievable, then it must satisfy the following conditions:

$$\sum_{j \in \mathcal{S}: \mathcal{D}_j \cap \mathcal{S}^c \neq \emptyset} R_j \leq C(\mathcal{S})$$

for all $\mathcal{S} \subseteq \mathcal{N}$ such that $\mathcal{D}_j \cap \mathcal{S}^c \neq \emptyset$ for some j . Here $C(\mathcal{S})$ is the capacity of the cut \mathcal{S} as before

Note that the cutset bound continues to hold even when the network has cycles and interaction between nodes is allowed (cf. Lecture Notes 19)

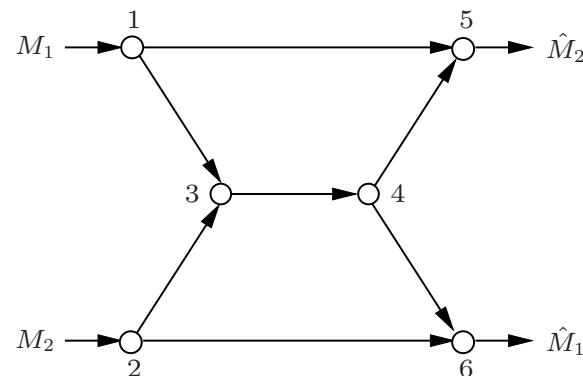
- Special cases

- Multicast: When $R_2 = \dots = R_{N-1} = 0$, the network reduces to a noiseless multicast network. More generally, assume that only a subset $[1 : k]$, $k \leq N - 1$, of the nodes are sources and let $\mathcal{D}_j = [k + 1 : N]$ for all $j \in \mathcal{N}$. In this general multi-source multicast setup, every destination node in $[k + 1 : N]$ wishes to decode all the sources. It can be shown [11] that the capacity region is again equal to the cutset outer bound. We discuss a generalization of this case in more detail in Lecture Notes 19

- Multiple unicast: Consider a network with $|\mathcal{D}_j| = 1$ for all j . If the operations at the nodes are restricted to forwarding, then the problem reduces to the well-studied *multi-commodity flow* [12]. The necessary and sufficient conditions for optimal multi-commodity flow can be found by linear programming as in the max-flow min-cut theorem. This provides an inner bound to the capacity region of the multiple unicast network, which is not optimal in general

More generally, each node can perform linear network coding

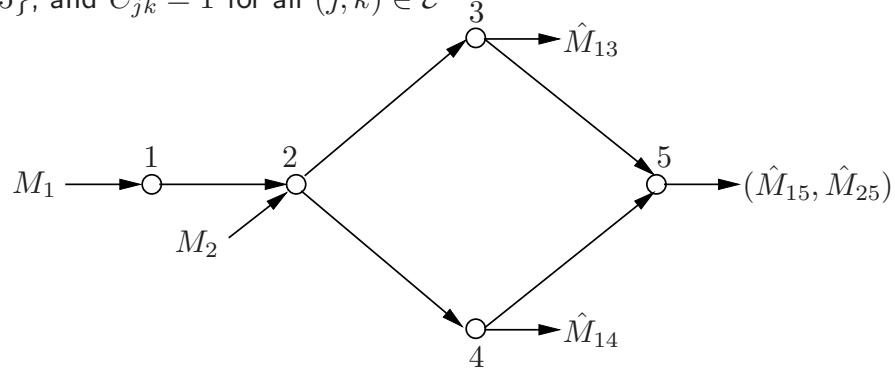
Example: Consider the following variant of the butterfly network with $R_3 = \dots = R_6 = 0$, $\mathcal{D}_1 = \{5\}$, $\mathcal{D}_2 = \{6\}$, and $C_{jk} = 1$ for all $(j, k) \in \mathcal{E}$



By the cutset outer bound, $R_1, R_2 \leq 1$ (by taking $\mathcal{J} = \{1, 3, 4, 5\}$ and $\mathcal{J} = \{2, 3, 4, 6\}$), which is achievable by linear network coding. In comparison, routing can achieve at most $R_1 + R_2 \leq 1$, because of the bottleneck edge $(3, 4)$

The capacity region of the multiple unicast network is not known in general

- For a general multiple-source multicast network, both the linear network coding inner bound and the cutset outer bound are loose
 - Example: To see that the cutset outer bound is loose in general, consider the following network [13, Figure 21.3] with $R_3 = R_4 = R_5 = 0$, $\mathcal{D}_1 = \{3, 4, 5\}$, $\mathcal{D}_2 = \{5\}$, and $C_{jk} = 1$ for all $(j, k) \in \mathcal{E}$



It can be easily shown that the cutset outer bound is the set of rate pairs (R_1, R_2) such that $R_1 \leq 1$, $R_1 + R_2 \leq 2$

On the other hand, the capacity region is the set of rate pairs (R_1, R_2) such that $R_1 \leq 1$, $2R_1 + R_2 \leq 2$, which is achieved by forwarding

- In [14], it is shown via an ingenuous construction of a counterexample network that linear network coding is strictly suboptimal

Key New Ideas and Techniques

- Max-flow min-cut theorem
- Network coding is better than routing
- Linear network coding can achieve the capacity of noiseless multicast networks (with zero error and finite block size)
- Cutset outer bound for general multi-source multicast networks
- Open problem: Is linear network coding optimal for multiple unicast networks?

References

- [1] L. R. Ford, Jr. and D. R. Fulkerson, “Maximal flow through a network,” *Canad. J. Math.*, vol. 8, pp. 399–404, 1956.
- [2] P. Elias, A. Feinstein, and C. E. Shannon, “A note on the maximum flow through a network,” *IRE Trans. Inf. Theory*, vol. 2, no. 4, pp. 117–119, Dec. 1956.
- [3] D. G. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, 3rd ed. New York: Springer, 2008.
- [4] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, “Network information flow,” *IEEE Trans. Inf. Theory*, vol. 46, no. 4, pp. 1204–1216, 2000.
- [5] S.-Y. R. Li, R. W. Yeung, and N. Cai, “Linear network coding,” *IEEE Trans. Inf. Theory*, vol. 49, no. 2, pp. 371–381, 2003.
- [6] R. Koetter and M. Médard, “An algebraic approach to network coding,” *IEEE/ACM Trans. Networking*, vol. 11, no. 5, pp. 782–795, 2003.
- [7] R. Lidl and H. Niederreiter, *Finite fields*, 2nd ed. Cambridge: Cambridge University Press, 1997.
- [8] S. Jaggi, P. Sanders, P. A. Chou, M. Effros, S. Egner, K. Jain, and L. M. G. M. Tolhuizen, “Polynomial time algorithms for multicast network code construction,” *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1973–1982, 2005.
- [9] P. A. Chou, Y. Wu, and K. Jain, “Practical network coding,” in *Proc. 41st Annual Allerton Conference on Communications, Control, and Computing*, Monticello, IL, Sept. 2003.

- [10] T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi, and B. Leong, "A random linear network coding approach to multicast," *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.
- [11] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 789–804, 2006.
- [12] T. C. Hu, "Multi-commodity network flows," *Operations Research*, vol. 11, no. 3, pp. 344–360, 1963.
- [13] R. W. Yeung, *Information Theory and Network Coding*. New York: Springer, 2008.
- [14] R. Dougherty, C. Freiling, and K. Zeger, "Insufficiency of linear coding in network information flow," *IEEE Trans. Inf. Theory*, vol. 51, no. 8, pp. 2745–2759, 2005.

Appendix: Proof of Lemma 1

- Let $P(x_1, \dots, x_k)$ be a nonzero polynomial in $\mathbb{F}_2[x_1, \dots, x_k]$. We show that if n is sufficiently large, then there exist $\alpha_1, \dots, \alpha_k \in \mathbb{F}_{2^n}$ such that $P(\alpha_1, \dots, \alpha_k) \neq 0$
- If $k = 1$, then the statement follows from the fact that the number of zeros of a polynomial cannot exceed the degree of the polynomial [7], which implies that there exists $\alpha_1 \in \mathbb{F}_{2^n}$ with $P(\alpha_1) \neq 0$, provided that 2^n is larger than the degree of the polynomial
- We proceed by induction on the number of variables k . Write the polynomial as

$$P(x_1, \dots, x_k) = \sum_{j=0}^d P_j(x_2, \dots, x_k) x_1^j$$

Since $P(x_1, \dots, x_k) \neq 0$, $P_j(x_2, \dots, x_k) \neq 0$ for some j . Therefore, by the induction hypothesis, if n is sufficiently large, there exist $\alpha_2, \dots, \alpha_k \in \mathbb{F}_{2^n}$ such that $P_j(\alpha_2, \dots, \alpha_k) \neq 0$ for some j . But this implies that $P(x_1, \alpha_2, \dots, \alpha_k)$ is a nonzero polynomial in x_1 . Hence, from the single-variable case, $P(\alpha_1, \alpha_2, \dots, \alpha_k)$ is nonzero for some α_1 , if n is sufficiently large

Lecture Notes 17

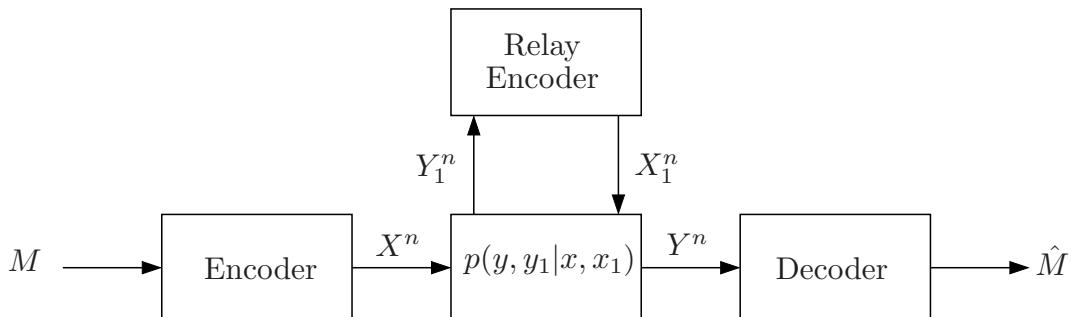
Relay Channels

- Problem Setup
- Cutset Upper Bound
- Simple Lower Bounds
- Decode–Forward Lower Bound
- AWGN Relay Channel
- Partial Decode–Forward Lower Bound
- Compress–Forward Lower Bound
- Linear Relaying for RFD-AWGN-RC
- Relay With Lookahead
- Key New Ideas and Techniques
- Appendices

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Problem Setup

- A discrete memoryless relay channel (DM-RC) $(\mathcal{X} \times \mathcal{X}_1, p(y, y_1|x, x_1), \mathcal{Y} \times \mathcal{Y}_1)$ consists of four finite sets \mathcal{X} , \mathcal{X}_1 , \mathcal{Y} , \mathcal{Y}_1 , and a collection of conditional pmfs $p(y, y_1|x, x_1)$ on $\mathcal{Y} \times \mathcal{Y}_1$
- Sender X wishes to send a message M to receiver Y with the help of the relay (X_1, Y_1)



- A $(2^{nR}, n)$ code for a DM-RC consists of:
 1. A message set $[1 : 2^{nR}]$
 2. An encoder that assigns a codeword $x^n(m)$ to each message $m \in [1 : 2^{nR}]$

- 3. A relay encoder that assigns at time $i \in [1 : n]$ a symbol $x_{1i}(y_1^{i-1})$ to each past received sequence $y_1^{i-1} \in \mathcal{Y}_1^{i-1}$
- 4. A decoder that assigns a message \hat{m} or an error message e to each received sequence $y^n \in \mathcal{Y}^n$
- The channel is memoryless in the sense that the current received symbols (Y_i, Y_{1i}) and the past symbols $(X^{i-1}, X_1^{i-1}, Y^{i-1}, Y_1^{i-1})$ are conditionally independent given the current transmitted symbols (X_i, X_{1i})
- We assume that the message M is uniformly distributed over $[1 : 2^{nR}]$
- The average probability of error is $P_e^{(n)} = P\{\hat{M} \neq M\}$
- The rate R is said to be achievable for the DM-RC if there exists a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$
- The *capacity* C of the DM-RC is the supremum of all achievable rates

- A multi-letter characterization of the capacity [1] is

$$C = \lim_{k \rightarrow \infty} C_k,$$

where

$$C_k := \sup_{p(x^k), \{x_{1j}(y_1^{j-1})\}_{j=1}^k} \frac{1}{k} I(X^k; Y^k)$$

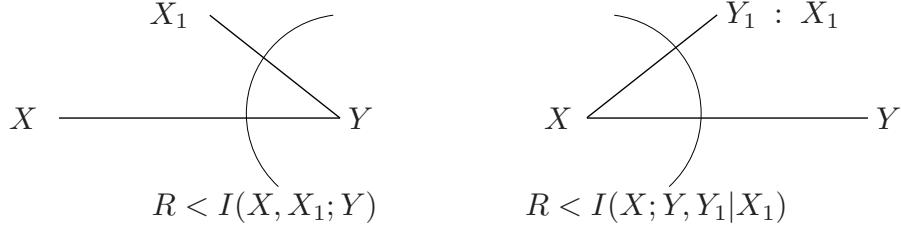
- A single-letter characterization for the capacity of the DM-RC is not known in general
- We discuss upper and lower bounds on the capacity for the DM and AWGN relay channels that are tight for some special classes

Cutset Upper Bound

- The following upper bound is motivated by the cutset upper bound discussed in Lecture Notes 16
- Theorem 1 (Cutset Bound) [2]:* The capacity of the DM-RC is upper bounded as

$$C \leq \max_{p(x,x_1)} \min \{I(X, X_1; Y), I(X; Y, Y_1 | X_1)\}$$

- Min-cut interpretation:



“Cooperative MAC bound” “Cooperative BC bound”

- This bound is tight for almost all classes of DM-RCs with known capacity. It is not tight in general as we show later [3]

- Proof: By Fano's inequality, we have

$$nR = H(M) = I(M; Y^n) + H(M|Y^n) \leq I(M; Y^n) + n\epsilon_n$$

We now show that

$$I(M; Y^n) \leq \min \left\{ \sum_{i=1}^n I(X_i, X_{1i}; Y_i), \sum_{i=1}^n I(X_i; Y_{1i}, Y_i | X_{1i}) \right\}$$

To show the first inequality, consider

$$\begin{aligned} I(M; Y^n) &= \sum_{i=1}^n I(M; Y_i | Y^{i-1}) \\ &= \sum_{i=1}^n I(M, Y^{i-1}; Y_i) \\ &\leq \sum_{i=1}^n I(X_i, X_{1i}, M, Y^{i-1}; Y_i) \\ &= \sum_{i=1}^n I(X_i, X_{1i}; Y_i) \end{aligned}$$

To show the second inequality, consider

$$\begin{aligned}
I(M; Y^n) &\leq I(M; Y^n, Y_1^n) \\
&= \sum_{i=1}^n I(M; Y_i, Y_{1i} | Y^{i-1}, Y_1^{i-1}) \\
&\stackrel{(a)}{=} \sum_{i=1}^n I(M; Y_{1i}, Y_i | Y^{i-1}, Y_1^{i-1}, X_{1i}) \\
&\leq \sum_{i=1}^n I(M, Y^{i-1}, Y_1^{i-1}; Y_{1i}, Y_i | X_{1i}) \\
&= \sum_{i=1}^n I(X_i, M, Y^{i-1}, Y_1^{i-1}; Y_{1i}, Y_i | X_{1i}) \\
&= \sum_{i=1}^n I(X_i; Y_i, Y_{1i} | X_{1i}),
\end{aligned}$$

where (a) follows by the fact that X_{1i} is a function of Y_1^{i-1}

Finally, let $Q \sim \text{Unif}[1 : n]$ be independent of X^n, X_1^n, Y^n, Y_1^n and set $X := X_Q, X_1 := X_{1Q}, Y := Y_Q, Y_1 := Y_{1Q}$

Since $Q \rightarrow (X, X_1) \rightarrow (Y, Y_1)$, we have

$$\begin{aligned}
\sum_{i=1}^n I(X_i, X_{1i}; Y_i) &= nI(X, X_1; Y | Q) \leq nI(X, X_1; Y), \\
\sum_{i=1}^n I(X_i; Y_i, Y_{1i} | X_{1i}) &= nI(X; Y, Y_1 | X_1, Q) \leq nI(X; Y, Y_1 | X_1)
\end{aligned}$$

Thus

$$R \leq \min \{I(X, X_1; Y), I(X; Y, Y_1 | X_1)\} + \epsilon_n$$

This completes the proof of the cutset bound

Direct Transmission Lower Bound

- If the relay is not used, we obtain the lower bound

$$C \geq \max_{p(x), x_1} I(X; Y | X_1 = x_1)$$

- This bound is tight if the DM-RC is *reversely degraded*, i.e.,

$$p(y, y_1 | x, x_1) = p(y|x, x_1)p(y_1|y, x_1)$$

- Converse follows from the cutset upper bound and noting that $I(X; Y, Y_1 | X_1) = I(X; Y | X_1)$ when the relay is reversely degraded

Simple Multi-hop Lower Bound

- In this scheme, the relay decodes the message received from the sender in each block and retransmits it in the following block. This yields the following lower bound on the capacity of the DM-RC

$$C \geq \max_{p(x)p(x_1)} \min\{I(X_1; Y), I(X; Y_1 | X_1)\}$$

- It is not difficult to show that this lower bound is tight for a DM-RC consisting of the cascade of two DMCs, i.e., $p(y, y_1 | x, x_1) = p(y_1 | x)p(y | x_1)$. In this case the capacity expression simplifies to

$$\begin{aligned} C &= \max_{p(x)p(x_1)} \min\{I(X_1; Y), I(X; Y_1 | X_1)\} \\ &= \max_{p(x)p(x_1)} \min\{I(X_1; Y), I(X; Y_1)\} = \min\{\max_{p(x_1)} I(X_1; Y), \max_{p(x)} I(X; Y_1)\} \end{aligned}$$

- Achievability uses the following multiple transmission block coding scheme:

Consider b transmission blocks, each consisting of n transmissions

A sequence of $b - 1$ messages, $m_j \in [1 : 2^{nR}]$, $j \in [1 : b - 1]$, each selected independently and uniformly over $[1 : 2^{nR}]$ is sent over the channel in nb transmissions. We assume $m_b = 1$ by convention



So the average rate is $R(b - 1)/b$, which approaches R as $b \rightarrow \infty$

- Codebook generation: Fix $p(x)p(x_1)$ that achieves the lower bound. We randomly and independently generate a codebook for each block

For each $j \in [1 : b]$, randomly and independently generate 2^{nR} sequences $x^n(m_j)$, $m_j \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p(x_i)$. Similarly, generate 2^{nR} sequences $x_1^n(m_{j-1})$, $m_{j-1} \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p(x_{1i})$

This defines the codebooks $\mathcal{C}_j = \{(x^n(m_j), x_1^n(m_{j-1})) : m_{j-1}, m_j \in [1 : 2^{nR}]\}$ for $j \in [1 : b]$

The codebooks \mathcal{C}_j are revealed to all parties

- Encoding: Let $m_j \in [1 : 2^{nR}]$ be the new message to be sent in block j , the encoder transmits $x^n(m_j)$ from the codebook \mathcal{C}_j

At the end of block j , the relay has an estimate \tilde{m}_j of the message m_j . In block $j + 1$, it transmits $x_1^n(\tilde{m}_j)$ from the codebook \mathcal{C}_{j+1} , where $\tilde{m}_0 = 1$ by convention

- Decoding and analysis of the probability of error: The decoding procedures for message m_j are as follows

- Upon receiving $y_1^n(j)$, the relay receiver declares that \tilde{m}_j is sent if it is the unique message such that $(x^n(\tilde{m}_j), x_1^n(\tilde{m}_{j-1}), y_1^n(j)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error

We analyze the probability of decoding error for message M_j averaged over codes. Assume without loss of generality that $M_j = 1$

Let \tilde{M}_{j-1} be the relay's decoded message in block $j - 1$. Define the following error events for the relay at the end of block j

$$\tilde{\mathcal{E}}_1(j) = \{(X^n(1), X_1^n(\tilde{M}_{j-1}), Y_1^n(j)) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\tilde{\mathcal{E}}_2(j) = \{(X^n(m_j), X_1^n(\tilde{M}_{j-1}), Y_1^n(j)) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_j \neq 1\}$$

Thus, the total probability of error is upper bounded as

$$P\{\tilde{M}_j \neq 1\} \leq P(\tilde{\mathcal{E}}_1(j)) + P(\tilde{\mathcal{E}}_2(j))$$

Note that by the independence of the codebooks, the relay message estimate \tilde{M}_{j-1} , which is a function of $Y_1^n(j - 1)$ and the codebook \mathcal{C}_{j-1} , is independent of the codewords $X^n(m_j)$, $X_1^n(m_{j-1})$, $m_j, m_{j-1} \in [1 : 2^{nR}]$, in the codebook \mathcal{C}_j

Thus, by the LLN, $P(\tilde{\mathcal{E}}_1(j)) \rightarrow 0$ as $n \rightarrow \infty$, and by the packing lemma, $P(\tilde{\mathcal{E}}_2(j)) \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1|X_1) - \delta(\epsilon)$

Therefore, $P\{\tilde{M}_j \neq 1\} \rightarrow 0$ as $n \rightarrow \infty$ for all $j \in [1 : b - 1]$ if $R < I(X; Y_1|X_1) - \delta(\epsilon)$

2. Upon receiving $y^n(j+1)$, the receiver declares that \hat{m}_j is sent if it is the unique message such that $(x_1^n(\hat{m}_j), y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error

Define the following error events for the receiver in block $j+1$

$$\mathcal{E}_1(j) = \{(X_1^n(\tilde{M}_j), Y^n(j+1)) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\mathcal{E}_2(j) = \{(X_1^n(m_j), Y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_j \neq \tilde{M}_j\}$$

The probability of decoding error for message M_j is upper bounded as

$$P\{\hat{M}_j \neq 1\} \leq P(\mathcal{E}_1(j) \cup \mathcal{E}_2(j) \cup \{\tilde{M}_j \neq 1\}) \leq P\{\tilde{M}_j \neq 1\} + P(\mathcal{E}_1(j)) + P(\mathcal{E}_2(j))$$

We know that $P\{\tilde{M}_j \neq 1\} \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1|X_1) - \delta(\epsilon)$

By the independence of the codebooks and the LLN, $P(\mathcal{E}_1(j)) \rightarrow 0$ as $n \rightarrow \infty$

By the same independence and the packing lemma, $P(\mathcal{E}_2(j)) \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X_1; Y) - \delta(\epsilon)$

- Thus we have shown that under the given constraints on the rate, $P(\hat{M}_j \neq M_j) \rightarrow 0$ for each $j \in [1 : b - 1]$

Coherent Multi-hop Lower Bound

- The simple multi-hop coding scheme can be improved by having the sender and relay *coherently* cooperate in transmitting their codewords. This improvement gives the following lower bound on the capacity of the DM-RC

$$C \geq \max_{p(x, x_1)} \min\{I(X_1; Y), I(X; Y_1|X_1)\}$$

Again we consider b blocks each consisting of n transmissions, where a sequence of $b - 1$ i.i.d. messages M_j , $j \in [1 : b - 1]$, is to be sent in nb transmissions.

We use a *block Markov coding* scheme where the codeword transmitted in a block depends statistically on the codeword transmitted in the previous block

- Codebook generation: Fix $p(x, x_1)$ that achieves the lower bound. Again, we randomly and independently generate a codebook for each block

For $j \in [1 : b]$, randomly and independently generate 2^{nR} sequences $x_1^n(m_{j-1})$, $m_{j-1} \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_{X_1}(x_{1i})$

For each $x_1^n(m_{j-1})$, generate 2^{nR} conditionally independent sequences $x_1^n(m_j|m_{j-1})$, $m_j \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_{X|X_1}(x_i|x_{1i}(m_{j-1}))$

This defines the codebook

$$\mathcal{C}_j = \{(x_1^n(m_j|m_{j-1}), x_1^n(m_{j-1})) : m_{j-1}, m_j \in [1 : 2^{nR}]\} \text{ for } j \in [1 : b]$$

The codebooks \mathcal{C}_j are revealed to all parties

- Encoding and decoding are explained with the help of the following table:

Block	1	2	3	\dots	$b - 1$	b
X	$x^n(m_1 1)$	$x^n(m_2 m_1)$	$x^n(m_3 m_2)$	\dots	$x^n(m_{b-1} m_{b-2})$	$x^n(1 m_{b-1})$
Y_1	\tilde{m}_1	\tilde{m}_2	\tilde{m}_3	\dots	\tilde{m}_{b-1}	1
X_1	$x_1^n(1)$	$x_1^n(\tilde{m}_1)$	$x_1^n(\tilde{m}_2)$	\dots	$x_1^n(\tilde{m}_{b-2})$	$x_1^n(\tilde{m}_{b-1})$
Y	1	\hat{m}_1	\hat{m}_2	\dots	\hat{m}_{b-2}	\hat{m}_{b-1}

- Encoding: Let $m_j \in [1 : 2^{nR}]$ be the message to be sent in block j , the encoder transmits $x^n(m_j|m_{j-1})$ from the codebook \mathcal{C}_j

At the end of block j , the relay has an estimate \tilde{m}_j of the message m_j . In block $j + 1$, it transmits $x_1^n(\tilde{m}_j)$ from the codebook \mathcal{C}_{j+1}

- Decoding and analysis of the probability of error: The decoding procedures for message m_j are as follows

1. Upon receiving $y_1^n(j)$, the relay receiver declares that \tilde{m}_j is sent if it is the unique message such that $(x^n(\tilde{m}_j|\tilde{m}_{j-1}), x_1^n(\tilde{m}_{j-1}), y_1^n(j)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error

Assume without loss of generality that $(M_{j-1}, M_j) = (1, 1)$ and let \tilde{M}_{j-1} be the relay's decoded message in block $j - 1$. Define the following error events for the relay at the end of block j

$$\begin{aligned}\tilde{\mathcal{E}}_1(j) &= \{(X^n(1|\tilde{M}_{j-1}), X_1^n(\tilde{M}_{j-1}), Y_1^n(j)) \notin \mathcal{T}_\epsilon^{(n)}\}, \\ \tilde{\mathcal{E}}_2(j) &= \{(X^n(m_j|\tilde{M}_{j-1}), X_1^n(\tilde{M}_{j-1}), Y_1^n(j)) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_j \neq 1\}\end{aligned}$$

The probability of decoding error for the relay at the end of block j is upper bounded as

$$\begin{aligned}\mathbb{P}\{\tilde{M}_j \neq 1\} &\leq \mathbb{P}(\tilde{\mathcal{E}}_1(j) \cup \tilde{\mathcal{E}}_2(j) \cup \{\tilde{M}_{j-1} \neq 1\}) \\ &\leq \mathbb{P}\{\tilde{M}_{j-1} \neq 1\} + \mathbb{P}(\tilde{\mathcal{E}}_1(j) \cap \{\tilde{M}_{j-1} = 1\}) + \mathbb{P}(\tilde{\mathcal{E}}_2(j))\end{aligned}$$

Consider the second term

$$\begin{aligned}\mathbb{P}(\tilde{\mathcal{E}}_1(j) \cap \{\tilde{M}_{j-1} = 1\}) &= \mathbb{P}\{(X^n(1|\tilde{M}_{j-1}), X_1^n(\tilde{M}_{j-1}), Y_1^n(j)) \notin \mathcal{T}_\epsilon^{(n)}, \tilde{M}_{j-1} = 1\} \\ &\leq \mathbb{P}\{(X^n(1|1), X_1^n(1), Y_1^n(j)) \notin \mathcal{T}_\epsilon^{(n)} | \tilde{M}_{j-1} = 1\}\end{aligned}$$

$\rightarrow 0$ as $n \rightarrow \infty$ by the independence of the codebooks and the LLN (why?)

By the packing lemma, $\mathbb{P}(\tilde{\mathcal{E}}_2(j)) \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1|X_1) - \delta(\epsilon)$.

Note that $\tilde{M}_0 = 1$. Hence, by induction, $\mathbb{P}\{\tilde{M}_j \neq 1\} \rightarrow 0$ as $n \rightarrow \infty$ for each $j \in [1 : b - 1]$

- Upon receiving $y^n(j+1)$, the receiver declares that \hat{m}_j is sent if it is the unique message such that $(x_1^n(\hat{m}_j), y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error. Following the steps of bounding $P(\mathcal{E}_1(j) \cup \mathcal{E}_2(j) \cup \{\tilde{M}_j \neq 1\})$ for the simple multi-hop coding scheme, $P\{\hat{M}_j \neq 1\} \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X_1; Y) - \delta(\epsilon)$ and $R < I(X; Y_1|X_1) - \delta(\epsilon)$

Decode–Forward Lower Bound

- The coherent multi-hop scheme can be improved by combining the information received through the direct path with the information received from the relay. This leads to the following *decode–forward* lower bound on capacity
- Theorem 2* (Decode–Forward Lower Bound) [2]:

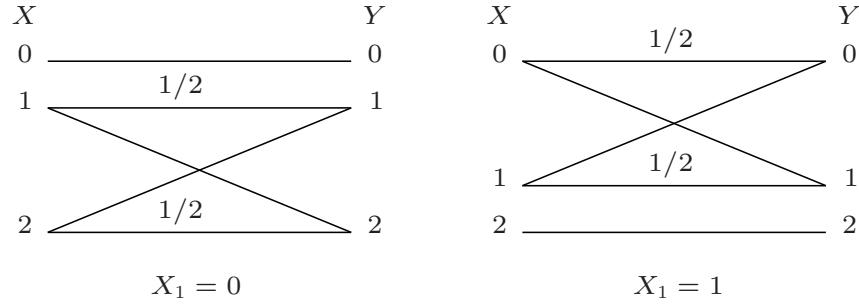
$$C \geq \max_{p(x,x_1)} \min \{I(X, X_1; Y), I(X; Y_1|X_1)\}$$

- The decode–forward lower bound is tight when the DM-RC is *physically degraded*, i.e.,

$$p(y, y_1|x, x_1) = p(y_1|x, x_1)p(y|y_1, x_1)$$

Converse: Follows from the cutset upper bound by noting that degradedness implies that $I(X; Y, Y_1|X_1) = I(X; Y_1|X_1)$

- Example (Sato relay channel) [4]: Consider the degraded DM-RC with $Y_1 = X \in \{0, 1, 2\}$, $X_1 \in \{0, 1\}$



- Direct transmission: $R = 1$ bits/transmission can be achieved by setting $X_1 = 0$ (or 1)
- Optimal first-order Markov relay function [4], $x_{1i}(y_{1,i-1})$, yields $R_1 = 1.0437$ bits/transmission
- Optimal second-order Markov relay function [4], $x_{1i}(y_{1,i-1}, y_{1,i-2})$, yields $R_2 = 1.0549$ bits/transmission
- The capacity is $C = 1.161878$ bits/transmission [2]

Proof of Achievability

-
- Again we consider b transmission blocks, each consisting of n transmissions and use a block Markov coding scheme
A sequence of $b - 1$ i.i.d. messages $M_j \in [1 : 2^{nR}]$, $j \in [1 : b - 1]$, is to be sent over the channel in nb transmissions
 - Codebook generation: Fix $p(x, x_1)$ that achieves the lower bound. As in the coherent multi-hop coding scheme, we randomly and independently generate codebooks $\mathcal{C}_j = \{(x^n(m_j|m_{j-1}), x_1^n(m_{j-1})) : m_{j-1}, m_j \in [1 : 2^{nR}]\}$ for $j \in [1 : b]$
Encoding: Encoding is again the same as in coherent multi-hop
To send m_j in block j , the encoder transmits $x^n(m_j|m_{j-1})$
At the end of block j , the relay has an estimate \tilde{m}_j of message m_j
It transmits $x_1^n(\tilde{m}_j)$ in block $j + 1$

Backward Decoding [5]

- Decoding at the receiver is done backwards after all b blocks are received
- Encoding and decoding is explained with the help of the following table:

Block	1	2	3	\dots	$b - 1$	b
X	$x^n(m_1 1)$	$x^n(m_2 m_1)$	$x^n(m_3 m_2)$	\dots	$x^n(m_{b-1} m_{b-2})$	$x^n(1 m_{b-1})$
Y_1	$\tilde{m}_1 \rightarrow$	$\tilde{m}_2 \rightarrow$	$\tilde{m}_3 \rightarrow$	\dots	\tilde{m}_{b-1}	1
X_1	$x_1^n(1)$	$x_1^n(\tilde{m}_1)$	$x_1^n(\tilde{m}_2)$	\dots	$x_1^n(\tilde{m}_{b-2})$	$x_1^n(\tilde{m}_{b-1})$
Y	1	\hat{m}_1	$\leftarrow \hat{m}_2$	\dots	$\leftarrow \hat{m}_{b-2}$	$\leftarrow \hat{m}_{b-1}$

- Decoding and analysis of the probability of error: The decoding procedures for message m_j are as follows

- Decoding of message m_j at the relay is done as in coherent multi-hop

Upon receiving $y_1^n(j)$, the relay receiver declares that \tilde{m}_j is sent if it is the unique message such that $(x^n(\tilde{m}_j|\tilde{m}_{j-1}), x_1^n(\tilde{m}_{j-1}), y_1^n(j)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error

Following the analysis of error for the relay in the coherent multi-hop scheme, $P\{\tilde{M}_j \neq 1\} \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1|X_1) - \delta(\epsilon)$

- Decoding at the receiver is done successively backwards

Based on the received $y^n(j+1)$, the receiver finds the unique message \hat{m}_j such that $(x^n(\hat{m}_{j+1}|\hat{m}_j), x_1^n(\hat{m}_j), y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error

Assume $(M_j, M_{j+1}) = (1, 1)$ is sent and define the following error events for message M_j

$$\mathcal{E}_1(j) = \{(X^n(\hat{M}_{j+1}|\tilde{M}_j), X_1^n(\tilde{M}_j), Y^n(j+1)) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\mathcal{E}_2(j) = \{(X^n(\hat{M}_{j+1}|m_j), X_1^n(m_j), Y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_j \neq \tilde{M}_j\}$$

The total probability of error is upper bounded as

$$\begin{aligned} P\{\hat{M}_j \neq 1\} &\leq P(\mathcal{E}_1(j) \cup \mathcal{E}_2(j) \cup \{\tilde{M}_j \neq 1\} \cup \{\hat{M}_{j+1} \neq 1\}) \\ &\leq P\{\tilde{M}_j \neq 1\} + P\{\hat{M}_{j+1} \neq 1\} + P(\mathcal{E}_1(j) \cap \{\hat{M}_{j+1} = 1\} \cap \{\tilde{M}_j = 1\}) \\ &\quad + P(\mathcal{E}_2(j)) \end{aligned}$$

The first term $P\{\tilde{M}_j \neq 1\} \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1|X_1) - \delta(\epsilon)$

By the independence of the codebooks and the LLN,

$$\begin{aligned}
& \mathbb{P}(\mathcal{E}_1(j) \cap \{\hat{M}_{j+1} = 1\} \cap \{\tilde{M}_j = 1\}) \\
&= \mathbb{P}\{(X^n(1|\tilde{M}_j), X_1^n(\tilde{M}_j), Y^n(j+1)) \notin \mathcal{T}_\epsilon^{(n)}, \hat{M}_{j+1} = 1, \tilde{M}_j = 1\} \\
&\leq \mathbb{P}\{(X^n(1|\tilde{M}_j), X_1^n(\tilde{M}_j), Y^n(j+1)) \notin \mathcal{T}_\epsilon^{(n)}, \tilde{M}_j = 1\} \\
&\leq \mathbb{P}\{(X^n(1|1), X_1^n(1), Y^n(j+1)) \notin \mathcal{T}_\epsilon^{(n)} | \tilde{M}_j = 1\}
\end{aligned}$$

$\rightarrow 0$ as $n \rightarrow \infty$

By the same independence and the packing lemma, $\mathbb{P}(\mathcal{E}_2(j)) \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X, X_1; Y) - \delta(\epsilon)$

Note that $\hat{M}_b = M_b = 1$. Hence, by induction, $\mathbb{P}\{\hat{M}_j \neq 1\} \rightarrow 0$ as $n \rightarrow \infty$ for each $j \in [1 : b-1]$ if the conditions in the theorem are satisfied. This completes the proof of achievability

- Remark: The excessive delay of backward decoding can be alleviated via *binning* [2] or *sliding window decoding* [6]. We describe the binning scheme, which was used in the original proof of the the decode-forward lower bound

Decode–Forward via Binning [2]

- In this scheme, the senders use codebooks with doubly-indexed set of codewords: $\mathcal{C}_j = \{(x^n(m_j|l_{j-1}), x_1^n(l_{j-1})) : m_j \in [1 : 2^{nR}], l_{j-1} \in [1 : 2^{nR_1}]\}$ for $j \in [1 : b]$, where l_j is a function of m_j that is sent *cooperatively* by both senders in block $j+1$ to help the receiver decode the message m_j
- Encoding and decoding are explained with the help of the following table:

Block	1	2	3	...	$b-1$	b
X	$x^n(m_1 1)$	$x^n(m_2 l_1)$	$x^n(m_3 l_2)$...	$x^n(m_{b-1} l_{b-2})$	$x^n(1 l_{b-1})$
Y_1	\tilde{m}_1, \tilde{l}_1	\tilde{m}_2, \tilde{l}_2	\tilde{m}_3, \tilde{l}_3	...	$\tilde{m}_{b-1}, \tilde{l}_{b-1}$	1
X_1	$x_1^n(1)$	$x_1^n(\tilde{l}_1)$	$x_1^n(\tilde{l}_2)$...	$x_1^n(\tilde{l}_{b-2})$	$x_1^n(\tilde{l}_{b-1})$
Y	1	\hat{l}_1, \hat{m}_1	\hat{l}_2, \hat{m}_2	...	$\hat{l}_{b-2}, \hat{m}_{b-2}$	$\hat{l}_{b-1}, \hat{m}_{b-1}$

- Codebook generation: Fix $p(x, x_1)$ that achieves the lower bound
For each $j \in [1 : b]$, randomly and independently generate 2^{nR_1} sequences $x_1^n(l_{j-1})$, $l_{j-1} \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{X_1}(x_{1i})$
For each $x_1^n(l_{j-1})$, randomly and conditionally independently generate 2^{nR} sequences $x^n(m_j | l_{j-1})$, $m_j \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_{X|X_1}(x_i | x_{1i})$
Partition the set of messages into 2^{nR_1} equal size bins
 $\mathcal{B}(l) = [(l-1)2^{n(R-R_1)} + 1 : l2^{n(R-R_1)}], l \in [1 : 2^{nR_1}]$
The codebook and bin assignments are revealed to all parties
- Encoding: Let $m_j \in [1 : 2^{nR}]$ be the new message to be sent in block j and assume that $m_{j-1} \in \mathcal{B}(l_{j-1})$, the encoder sends $x^n(m_j | l_{j-1})$
At the end of block j , the relay has an estimate \tilde{m}_j of m_j
Assume that $\tilde{m}_j \in \mathcal{B}(\tilde{l}_j)$, the relay sends $x_1^n(\tilde{l}_j)$ in block $j+1$
- Decoding and analysis of the probability of error: The decoding procedures for message m_j are as follows
 - Upon receiving $y_1^n(j)$, the relay receiver declares that \tilde{m}_j is sent if it is the unique message such that $(x_1^n(\tilde{m}_j | \tilde{l}_{j-1}), x_1^n(\tilde{l}_{j-1}), y_1^n(j)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error

- Following similar steps to the analysis of error for the relay in the coherent multi-hop scheme with \tilde{L}_{j-1} replacing \tilde{M}_{j-1} , $P\{\tilde{M}_j \neq M_j\} \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1 | X_1) - \delta(\epsilon)$, and hence $P\{\tilde{L}_j \neq L_j\} \rightarrow 0$ as $n \rightarrow \infty$
- Upon receiving $y^n(j+1)$, the receiver declares that \hat{l}_j is sent if it is the unique message such that $(x_1^n(\hat{l}_j), y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)}$; otherwise it declares an error
- Assume without loss of generality assume that $(M_j, L_j) = (1, 1)$ and let \tilde{L}_j be the relay estimate of L_j . Consider the following error events for the receiver at the end of block $j+1$

$$\begin{aligned}\mathcal{E}_1(j) &= \{(X_1^n(\tilde{L}_j), Y^n(j+1)) \notin \mathcal{T}_\epsilon^{(n)}\}, \\ \mathcal{E}_2(j) &= \{(X_1^n(l_j), Y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } l_j \neq \tilde{L}_j\}\end{aligned}$$

Then

$$\begin{aligned}P\{\hat{L}_j \neq 1\} &\leq P(\mathcal{E}_1(j) \cup \mathcal{E}_2(j) \cup \{\tilde{L}_j \neq 1\}) \\ &\leq P\{\tilde{L}_j \neq 1\} + P(\mathcal{E}_1(j)) + P(\mathcal{E}_2(j))\end{aligned}$$

The first term $\rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1 | X_1) - \delta(\epsilon)$. By the independence of the codebooks, the LLN, and the packing lemma $P(\mathcal{E}_1(j)) \rightarrow 0$ and $P(\mathcal{E}_2(j)) \rightarrow 0$ as $n \rightarrow \infty$ if $R_1 < I(X_1; Y) - \delta(\epsilon)$

3. The receiver then declares that \hat{m}_j is sent if it is the unique message such that $(x^n(\hat{m}_j|\hat{l}_{j-1}), x_1^n(\hat{l}_{j-1}), y^n(j)) \in \mathcal{T}_\epsilon^{(n)}$ and $\hat{m}_j \in \mathcal{B}(\hat{l}_j)$; otherwise it declares an error

Assume without loss of generality that $(L_{j-1}, L_j, M_j) = (1, 1, 1)$ and let $(\hat{L}_{j-1}, \hat{L}_j)$ be the receiver's estimates of (L_{j-1}, L_j) . Consider the following error events for the receiver

$$\begin{aligned}\mathcal{E}_3(j) &= \{(X^n(1|\hat{L}_{j-1}), X_1^n(\hat{L}_{j-1}), Y^n(j)) \notin \mathcal{T}_\epsilon^{(n)}\}, \\ \mathcal{E}_4(j) &= \{(X^n(m_j|\hat{L}_{j-1}), X_1^n(\hat{L}_{j-1}), Y^n(j)) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_j \neq 1, m_j \in \mathcal{B}(\hat{L}_j)\}\end{aligned}$$

The probability of decoding error is upper bounded as

$$\begin{aligned}\mathsf{P}\{\hat{M}_j \neq 1\} &\leq \mathsf{P}(\mathcal{E}_3(j) \cup \mathcal{E}_4(j) \cup \{\hat{L}_{j-1} \neq 1\} \cup \{\hat{L}_j \neq 1\} \cup \{\tilde{L}_{j-1} \neq 1\}) \\ &\leq \mathsf{P}\{\hat{L}_{j-1} \neq 1\} + \mathsf{P}\{\hat{L}_j \neq 1\} + \mathsf{P}\{\tilde{L}_{j-1} \neq 1\} \\ &\quad + \mathsf{P}(\mathcal{E}_3(j) \cap \{\hat{L}_{j-1} = 1\} \cap \{\tilde{L}_{j-1} = 1\}) + \mathsf{P}(\mathcal{E}_4(j))\end{aligned}$$

The first three terms $\rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1|X_1) - \delta(\epsilon)$ and $R_1 < I(X_1; Y) - \delta(\epsilon)$. By the independence of the codebooks and the LLN

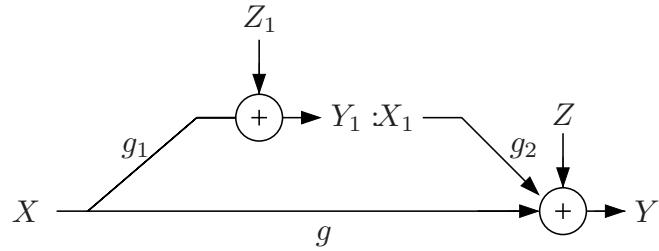
$$\begin{aligned}\mathsf{P}(\mathcal{E}_3(j) \cap \{\hat{L}_{j-1} = 1\} \cap \{\tilde{L}_{j-1} = 1\}) \\ \leq \mathsf{P}\{(X^n(1|1), X_1^n(1), Y^n(j)) \notin \mathcal{T}_\epsilon^{(n)} | \tilde{L}_{j-1} = 1\} \rightarrow 0 \text{ as } n \rightarrow \infty\end{aligned}$$

By the same independence and the packing lemma, $\mathsf{P}(\mathcal{E}_4(j)) \rightarrow 0$ as $n \rightarrow \infty$, if $R - R_1 < I(X; Y|X_1) - \delta(\epsilon)$ (since there are $2^{n(R-R_1)}$ codewords $X^n(m_j|\hat{L}_{j-1})$, $m_j \in \mathcal{B}(\hat{L}_j)$)

Combining the bounds, we have shown that $\mathsf{P}\{\hat{M}_j \neq M_j\} \rightarrow 0$ as $n \rightarrow \infty$ for all j if $R < I(X; Y_1|X_1) - \delta(\epsilon)$ and $R < I(X; Y|X_1) + I(X_1; Y) - 2\delta(\epsilon) = I(X, X_1; Y) - 2\delta(\epsilon)$. This completes the proof of achievability

AWGN Relay Channel

- Consider the following general AWGN-RC model



At time i : $Y_{1i} = g_1 X_i + Z_{1i}$, $Y_i = g X_i + g_2 X_{1i} + Z_i$, where $g, g_1, g_2 > 0$ are channel gains, $\{Z_{1i}\}$ and $\{Z_i\}$ are independent WGN processes each with average power $N_0/2 = 1$, $\{X_i, X_{1i}\}$ are independent of $\{Z_{1i}\}$ and $\{Z_i\}$ for all i . Assume equal average power constraint P on X and on X_1

- Denote the SNR of the direct channel as $S := g^2 P$, the SNR of the channel from the sender to the relay receiver as $S_1 := g_1^2 P$, and the SNR of the channel from the relay to the receiver as $S_2 := g_2^2 P$
- Note that with this model, the channel cannot be physically degraded or reversely degraded. In fact capacity is not known for any $S, S_1, S_2 > 0$

- A multi-letter characterization of the capacity as a function of power P is given by

$$C(P) = \lim_{k \rightarrow \infty} C_k(P),$$

where

$$C_k(P) := \sup_{\substack{F(x^k), \{x_{1j}\}_{j=1}^k: \\ \sum_{j=1}^k \mathbb{E}(X_j^2) \leq kP, \sum_{j=1}^k \mathbb{E}(X_{1j}^2) \leq kP}} \frac{1}{k} I(X^k; Y^k)$$

Properties of $C(P)$ are discussed in the Appendix

Upper and Lower Bounds on Capacity of AWGN-RC

- Cutset upper bound: The cutset upper bound reduces to

$$C \leq \max_{0 \leq \rho \leq 1} \min \left\{ C \left(S + S_2 + 2\rho\sqrt{SS_2} \right), C \left((S + S_1)(1 - \rho^2) \right) \right\}$$

$$= \begin{cases} C \left((\sqrt{S_1 S_2} + \sqrt{S + S_1 - S_2})^2 / (S + S_1) \right) & \text{if } S_1 \geq S_2 \\ C(S + S_1) & \text{otherwise} \end{cases}$$

- Direct transmission lower bound: If the relay is not used, we obtain

$$C \geq C(S)$$

- Simple multi-hop lower bound: If independent Gaussian sender and relay signals are used and the receiver treats the signal from the direct channel as noise, we obtain the lower bound

$$C \geq \min \{ C(S_1), C(S_2/(S+1)) \}$$

- Decode-forward lower bound: Decode-forward yields

$$C \geq \max_{0 \leq \rho \leq 1} \min \left\{ C \left(S + S_2 + 2\rho\sqrt{SS_2} \right), C \left(S_1(1 - \rho^2) \right) \right\}$$

$$= \begin{cases} C \left(\left(\sqrt{S(S_1 - S_2)} + \sqrt{S_2(S_1 - S)} \right)^2 / S_1 \right) & \text{if } S_1 \geq S + S_2 \\ C(S_1) & \text{otherwise} \end{cases}$$

Achievability follows by setting $X_1 \sim N(0, P)$ and $X = \rho X_1 + X'$, where $X' \sim N(0, (1 - \rho^2)P)$ is independent of X_1 and carries the new message to be decoded first by the relay

- For $S_1 < S$, the decode-forward rate is lower than the capacity of the direct channel $C(S)$
- Non-coherent decode-forward: Since implementing coherent communication is difficult in wireless systems, one may consider a *non-coherent* decode-forward scheme, where X and X_1 are independent. This gives the lower bound

$$C \geq \min \{ C(S + S_2), C(S_1) \}$$

This scheme uses the same codebook and encoding as the simple multi-hop scheme, but achieves higher rate by performing more sophisticated decoding

Partial Decode–Forward Lower Bound

- In decode–forward, the relay fully decodes the message, which is optimal for physically degraded DM-RC because the relay receives a strictly better version of X than the receiver. But in some cases (e.g., the AWGN-RC with $S_1 < S$), the channel to the relay can be a bottleneck and decode–forward may in fact perform worse than direct transmission
- In *partial-decode-forward*, the relay decodes only part of the message. This provides a more general lower bound on capacity

Theorem 3 (Partial Decode–Forward Lower Bound) [2]: The following is a lower bound on the capacity of the DM-RC

$$C \geq \max_{p(u,x,x_1)} \min\{I(X, X_1; Y), I(U; Y_1|X_1) + I(X; Y|X_1, U)\},$$

where $|\mathcal{U}| \leq |\mathcal{X}| \cdot |\mathcal{X}_1|$

- Outline of achievability: We use block Markov coding and binning

Split the message m into two independent messages with rates R' and R'' . Thus $R = R' + R''$. Fix $p(u, x, x_1)$ that achieves the lower bound

U carries the part of the current message (with rate R') decoded by the relay at the end of the current block (replacing X in decode–forward). This requires that $R' < I(U; Y_1|X_1) - \delta(\epsilon)$

X carries the rest of the message, which is decoded only by the receiver at the end of the following block

X_1 carries the additional information (bin number) needed by the receiver to fully decode U sent in the previous block. The relay and sender cooperate to send X_1 to Y

The receiver first decodes X_1 . This requires that $R_1 < I(X_1; Y) - \delta(\epsilon)$. It then finds the previous U . This requires that $R' - R_1 < I(U; Y|X_1) - \delta(\epsilon)$. Finally, it decodes X to find the rest of the message sent in the previous block. This requires that $R'' < I(X; Y|X_1, U) - \delta(\epsilon)$

Eliminating R_1 , R' and R'' gives the inequalities in the partial decode–forward lower bound

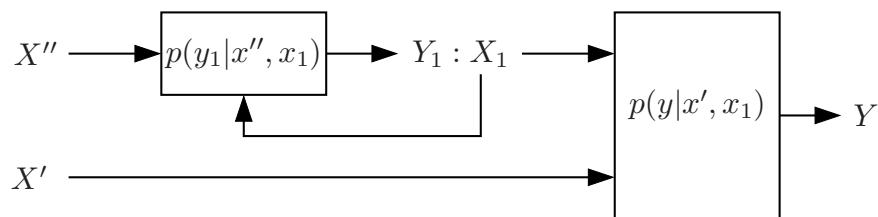
- Note that if we substitute $U = X$, the above lower bound reduces the decode-and forward lower bound, and if we substitute $U = \emptyset$, it reduces to the direct transmission lower bound

Semi-deterministic DM-RC[7]

- A DM-RC is referred to as *semi-deterministic* if $Y_1 = g(X, X_1)$
- The capacity of the semi-deterministic DM-RC is
$$C = \max_{p(x, x_1)} \min\{I(X, X_1; Y), H(Y_1|X_1) + I(X; Y|X_1, Y_1)\}$$
- The capacity is achieved using partial decode-forward bound. We set $U = Y_1$ in the partial decode-forward bound, which is feasible because the sender knows both X and X_1 and thus Y_1
- The converse follows by the cutset upper bound

Relay Channel with Orthogonal Sender Components

- This model is motivated by the practical constraint in wireless communication that a node cannot send and receive at the same time or in the same frequency band
- First consider the DM-RC with *orthogonal sender components* [8]: Here $X = (X', X'')$ and $p(y, y_1|x, x_1) = p(y|x', x_1)p(y_1|x'', x_1)$



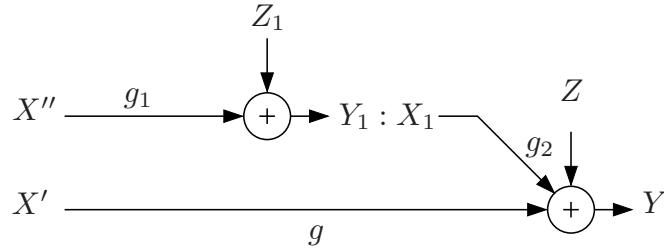
- The capacity for the DM-RC with orthogonal sender components is

$$C = \max_{p(x_1)p(x'|x_1)p(x''|x_1)} \min\{I(X', X_1; Y), I(X''; Y_1|X_1) + I(X'; Y|X_1)\}$$

- Achievability uses partial decode-forward with $U = X''$
- The converse follows by the cutset upper bound (check)

SFD-AWGN Relay Channel

- Consider the AWGN-RC with orthogonal sender components [8], which we refer to as Sender Frequency-Division (SFD) AWGN-RC



Here $X = (X', X'')$

- The capacity for this class is

$$C = \max_{0 \leq \alpha, \rho \leq 1} \min \left\{ C \left(\alpha S + S_2 + 2\rho\sqrt{\alpha S S_2} \right), C(\bar{\alpha} S_1) + C(\alpha(1 - \rho^2)S) \right\}$$

- Achievability again uses partial-decode-forward with $U = X'' \sim N(0, \bar{\alpha}P)$, and $X' \sim N(0, \alpha P)$ are independent and $X_1 \sim N(0, P)$ is jointly Gaussian with X' with correlation coefficient ρ , and independent of X''
- The converse follows by the cutset bound

- Remark: It can be shown (see Appendix) that the partial decode-forward lower bound for the AWGN-RC is equal to the maximum of the decode-forward lower bound and the direct channel lower bound [9]. As such, partial decode-forward does not offer any improvement in rate over these simpler schemes

Compress–Forward Lower Bound

- In the decode–forward coding scheme, the relay decodes the entire message (or part of it). If the channel from the sender to the relay is worse than the direct channel to the receiver, this requirement can make the transmission rate lower than the direct transmission rate, i.e., that rate when the relay is not used at all
- In the *compress–forward* coding scheme, the relay helps communication by sending a description of its received signal to the receiver. Because this description is correlated with the received sequence, Wyner–Ziv coding is used to reduce the rate needed to send it to the receiver. This coding scheme achieves the following lower bound on the capacity of the DM-RC

Theorem 4 (Compress–Forward Lower Bound) [2, 9]: The following is a lower bound on the capacity of the DM-RC

$$C \geq \max_{p(x)p(x_1)p(\hat{y}_1|y_1, x_1)} \min \left\{ I(X, X_1; Y) - I(Y_1; \hat{Y}_1 | X, X_1, Y), I(X; Y, \hat{Y}_1 | X_1) \right\},$$

where $|\hat{\mathcal{Y}}_1| \leq |\mathcal{X}_1| \cdot |\mathcal{Y}_1| + 1$

- Compared to the cutset bound,
 - the first term is the multiple access bound without coherent cooperation (X and X_1 are independent) and with a subtracted term,
 - the second term looks similar to the broadcast bound but with Y_1 replaced by the description \hat{Y}_1
- Outline of achievability:
 - A block Markov coding scheme is used to send $b - 1$ i.i.d. messages in b blocks
 - At the end of block j , a description $\hat{y}_1^n(j)$ of $y_1^n(j)$ conditioned on $x_1^n(j)$, which is known to both the relay and receiver, is constructed by the relay
 - Since the receiver has side information $y^n(j)$ about $\hat{y}_1^n(j)$, we use binning as in Wyner–Ziv coding to reduce the rate necessary to send $\hat{y}_1^n(j)$. The bin index is sent to the receiver in block $j + 1$ via $x_1^n(j + 1)$
 - At the end of block $j + 1$, the receiver decodes $x_1^n(j + 1)$. It then uses $y^n(j)$ and $x_1^n(j)$ to decode $\hat{y}_1^n(j)$ and $x^n(m_j)$ simultaneously

- Codebook generation: Fix $p(x)p(x_1)p(\hat{y}_1|y_1, x_1)$ that achieves the lower bound. Again, we randomly and independently generate a codebook for each block $j \in [1 : b]$
 1. Randomly and independently generate 2^{nR} sequences $x^n(m_j)$, $m_j \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_X(x_i)$
 2. Randomly and independently generate 2^{nR_1} sequences $x_1^n(l_{j-1})$, $l_{j-1} \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p_{X_1}(x_{1i})$
 3. For each $x_1^n(l_{j-1})$, $l_{j-1} \in [1 : 2^{nR_1}]$, randomly and conditionally independently generate $2^{n\tilde{R}_1}$ sequences $\hat{y}_1^n(k_j|l_{j-1})$, $k_j \in [1 : 2^{n\tilde{R}_1}]$, each according to $\prod_{i=1}^n p_{Y_1|X_1}(\hat{y}_{1i}|x_{1i}(l_{j-1}))$
 4. Partition the set $[1 : 2^{n\tilde{R}_1}]$ into 2^{nR_1} equal size bins $\mathcal{B}(l_j)$, $l_j \in [1 : 2^{nR_1}]$

- Encoding and decoding are explained with the help of the following table:

Block	1	2	3	...	$b - 1$	b
X	$x^n(m_1)$	$x^n(m_2)$	$x^n(m_3)$...	$x^n(m_{b-1})$	$x^n(1)$
Y_1	$\hat{y}_1^n(k_1 1), l_1$	$\hat{y}_1^n(k_2 l_1), l_2$	$\hat{y}_1^n(k_3 l_2), l_3$...	$\hat{y}_1^n(k_{b-1} l_{b-2}), l_{b-1}$	\emptyset
X_1	$x_1^n(1)$	$x_1^n(l_1)$	$x_1^n(l_2)$...	$x_1^n(l_{b-2})$	$x_1^n(l_{b-1})$
Y	\emptyset	$\hat{l}_1, \hat{k}_1, \hat{m}_1$	$\hat{l}_2, \hat{k}_2, \hat{m}_2$...	$\hat{l}_{b-2}, \hat{k}_{b-2}, \hat{m}_{b-2}$	$\hat{l}_{b-1}, \hat{k}_{b-1}, \hat{m}_{b-1}$

- Encoding: To send m_j , the sender transmits $x^n(m_j)$ in block j . The relay, upon receiving $y_1^n(j)$, finds an index k_j such that $(\hat{y}_1^n(k_j|l_{j-1}), y_1^n(j), x_1^n(l_{j-1})) \in \mathcal{T}_{\epsilon'}^{(n)}$. Assuming that such k_j is found and $k_j \in \mathcal{B}(l_j)$, the relay sends $x_1^n(l_j)$ in block $j + 1$. By the covering lemma, the probability $P(\tilde{\mathcal{E}}(j))$ that there is no such k_j tends to 0 as $n \rightarrow \infty$, if $\tilde{R}_1 > I(\hat{Y}_1; Y_1|X_1) + \delta(\epsilon')$.

- Decoding and analysis of the probability of error: The decoding procedures for message m_j are as follows

- Upon receiving $y^n(j+1)$, the receiver finds a unique \hat{l}_j such that $(x_1^n(\hat{l}_j), y^n(j+1)) \in \mathcal{T}_\epsilon^{(n)}$

Let L_j denote the bin index chosen by the relay. Following the analysis of the error probability in step 2 of decode-forward via binning, $P\{\hat{L}_j \neq L_j\} \rightarrow 0$ as $n \rightarrow \infty$, if $R_1 < I(X_1; Y) - \delta(\epsilon)$

- Let $\epsilon > \epsilon'$. The receiver finds a unique \hat{m}_j such that

$$(x^n(\hat{m}_j), x_1^n(\hat{l}_{j-1}), \hat{y}_1^n(\hat{k}_j | \hat{l}_{j-1}), y^n(j)) \in \mathcal{T}_\epsilon^{(n)}$$

for some $\hat{k}_j \in \mathcal{B}(\hat{l}_j)$

Assume without loss of generality that $M_j = 1$ and let L_{j-1}, L_j, K_j denote the indices chosen by the relay. Define the events

$$\begin{aligned}\mathcal{E}_1(j) &:= \{X^n(1), X_1^n(\hat{L}_{j-1}), \hat{Y}_1^n(K_j | \hat{L}_{j-1}), Y^n(j)) \notin \mathcal{T}_\epsilon^{(n)}\}, \\ \mathcal{E}_2(j) &:= \{X^n(m_j), X_1^n(\hat{L}_{j-1}), \hat{Y}_1^n(K_j | \hat{L}_{j-1}), Y^n(j)) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } m_j \neq 1\}, \\ \mathcal{E}_3(j) &:= \{X^n(m_j), X_1^n(\hat{L}_{j-1}), \hat{Y}_1^n(\hat{k}_j | \hat{L}_{j-1}), Y^n(j)) \in \mathcal{T}_\epsilon^{(n)} \\ &\quad \text{for some } \hat{k}_j \in \mathcal{B}(\hat{L}_j), \hat{k}_j \neq K_j, m_j \neq 1\}\end{aligned}$$

The probability of error is bounded as

$$\begin{aligned}P\{\hat{M}_j \neq 1\} &\leq P(\cup_{q=1}^3 \mathcal{E}_q(j) \cup \tilde{\mathcal{E}}(j) \cup \{(\hat{L}_{j-1}, \hat{L}_j) \neq (L_{j-1}, L_j)\}) \\ &\leq P(\tilde{\mathcal{E}}(j)) + P\{(\hat{L}_{j-1}, \hat{L}_j) \neq (L_{j-1}, L_j)\} \\ &\quad + P(\mathcal{E}_1(j) \cap \{\hat{L}_{j-1} = L_{j-1}\} | \tilde{\mathcal{E}}^c(j)) + P(\mathcal{E}_2(j)) \\ &\quad + P(\mathcal{E}_3(j) \cap \{(\hat{L}_{j-1}, \hat{L}_j) = (L_{j-1}, L_j)\})\end{aligned}$$

The first two terms $\rightarrow 0$ as $n \rightarrow \infty$ if $\tilde{R}_1 > I(\hat{Y}_1; Y_1 | X_1) + \delta(\epsilon')$ and $R < I(X_1; Y) - \delta(\epsilon)$, respectively

By the independence of codebooks and the conditional typicality lemma, $P(\mathcal{E}_1(j) \cap \{\hat{L}_{j-1} = L_{j-1}\} | \tilde{\mathcal{E}}^c(j)) \rightarrow 0$ as $n \rightarrow \infty$

By the same independence and the packing lemma, $P(\mathcal{E}_2(j)) \rightarrow 0$ as $n \rightarrow \infty$, if $R < I(X; Y, \hat{Y}_1, X_1) + \delta(\epsilon) = I(X; Y, \hat{Y}_1 | X_1) + \delta(\epsilon)$

Following similar steps as in Lemma 1 in the Wyner–Ziv achievability proof, we have

$$\begin{aligned}
& \mathbb{P}(\mathcal{E}_3 \cap \{(\hat{L}_{j-1}, \hat{L}_j) = (L_{j-1}, L_j)\}) \\
& \leq \mathbb{P}\{(X^n(m_j), X_1^n(L_{j-1}), \hat{Y}_1^n(\hat{k}_j|L_{j-1}), Y^n(j)) \in \mathcal{T}_\epsilon^{(n)} \\
& \quad \text{for some } \hat{k}_j \in \mathcal{B}(L_j), \hat{k}_j \neq K_j, m_j \neq 1\} \\
& \leq \mathbb{P}\{(X^n(m_j), X_1^n(L_{j-1}), \hat{Y}_1^n(\hat{k}_j|L_{j-1}), Y^n(j)) \in \mathcal{T}_\epsilon^{(n)} \\
& \quad \text{for some } \hat{k}_j \in \mathcal{B}(1), m_j \neq 1\}
\end{aligned}$$

By the independence of the codebooks, the joint typicality lemma (twice), and the union of events bound (the packing lemma here is not general enough), it can be easily shown (check!) that this probability $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R + \tilde{R}_1 - R_1 < I(X; Y|X_1) + I(\hat{Y}_1; X, Y|X_1) - \delta(\epsilon)$$

- Combining the bounds, $\mathbb{P}\{\hat{M}_j \neq M_j\} \rightarrow 0$ as $n \rightarrow \infty$ for all j if
$$\begin{aligned}
R &< I(X, X_1; Y) + I(\hat{Y}_1; X, Y|X_1) - I(\hat{Y}_1; Y_1|X_1) - 2\delta(\epsilon) - \delta(\epsilon') \\
&= I(X, X_1; Y) + I(\hat{Y}_1; X, Y|X_1) - I(\hat{Y}_1; Y_1, X, Y|X_1) - \delta'(\epsilon) \\
&= I(X, X_1; Y) - I(\hat{Y}_1; Y_1|X, X_1, Y) - \delta'(\epsilon)
\end{aligned}$$
- This completes the achievability proof

- An equivalent characterization: The original characterization of the compress–forward lower bound established in [2] is

$$C \geq \max I(X; Y, \hat{Y}_1|X_1),$$

where the maximization is over $p(x)p(x_1)p(\hat{y}_1|y_1, x_1)$ subject to
 $I(X_1; Y) \geq I(Y_1; \hat{Y}_1|X_1, Y)$

We show in the Appendix [9] that this characterization is equivalent to that in Theorem 4

Extensions

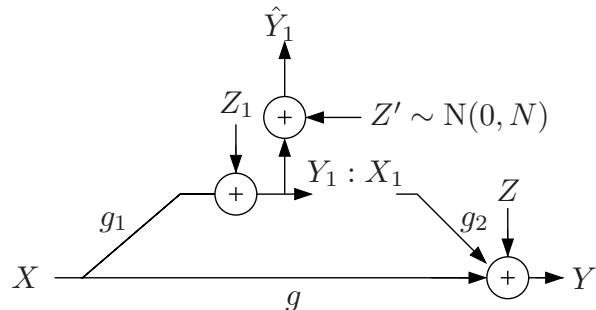
- The compress-forward lower bound (before maximization) is not in general convex in $p(x)p(x_1)p(\hat{y}_1|y_1, x_1)$. As such, the lower bound can be improved via time-sharing [9] to obtain the time-sharing compress-forward bound

$$C \geq \max_{p(q)p(x|q)p(x_1|q)p(\hat{y}_1|y_1, x_1, q)} \min \left\{ I(X, X_1; Y|Q) - I(Y_1; \hat{Y}_1|X, X_1, Y, Q), I(X; Y, \hat{Y}_1|X_1, Q) \right\}$$

- Compress-forward can be combined with partial decode-forward to yield a lower bound on the capacity of the relay channel [2, Theorem 7]

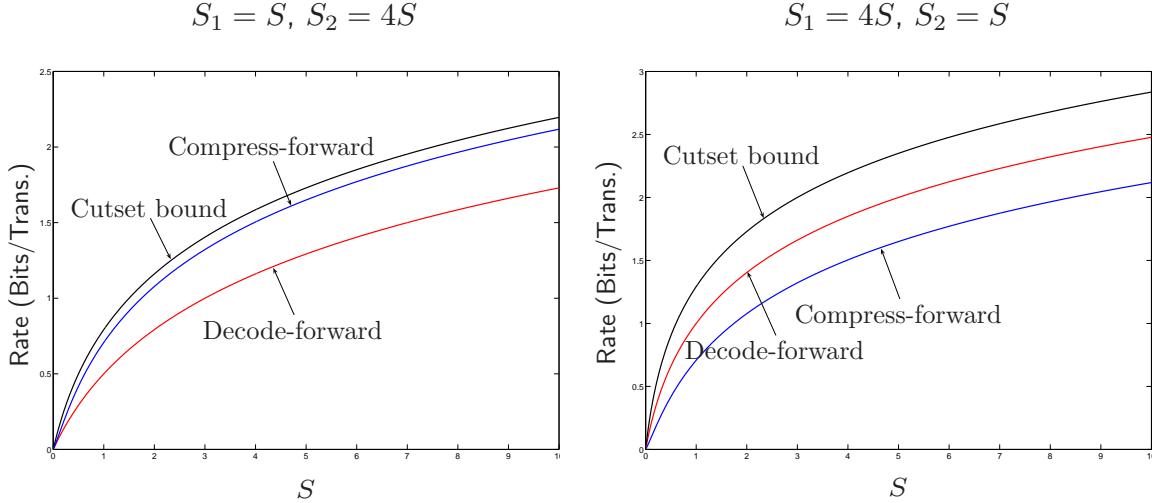
Compress–Forward for AWGN-RC

- The distribution $F(x_1)F(x_2)F(\hat{y}_1|y_1, x_1)$ that achieves the compress-forward lower bound for the AWGN-RC is not known and may not be Gaussian
- Assume $X \sim N(0, P)$, $X_1 \sim N(0, P)$, $Z' \sim N(0, Q)$ to be independent, and $\hat{Y}_1 = Y_1 + Z'$. Substituting in the compress-forward expression and optimizing over N , we obtain the lower bound $C \geq C(S + S_1 S_2 / (S + S_1 + S_2 + 1))$



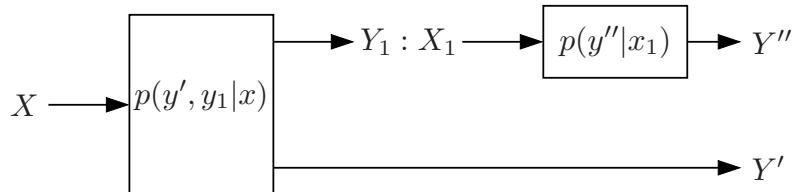
- Remarks:
 - As $S_2 \rightarrow \infty$, this bound becomes tight
 - When S_1 is small, the bound can be improved via time-sharing at the sender side

Comparison of the Bounds



Relay Channel with Orthogonal Receiver Components

- As a dual model to the DM-RC with orthogonal sender components, consider the DM-RC with orthogonal receiver components



Here $Y = (Y', Y'')$ and $p(y, y_1 | x, x_1) = p(y', y_1 | x)p(y'' | x_1)$, decoupling the BC from the sender to the receivers from the relay-to-receiver channel

- Capacity of the relay channel with orthogonal receiver components is in general not known. The cutset upper bound on the capacity reduces to

$$C \leq \max_{p(x)p(x_1)} \min\{I(X; Y') + I(X_1; Y''), I(X; Y', Y_1)\}$$

Thus, if we denote the capacity of the relay-to-receiver channel by $C_0 := \max_{p(x_1)} I(X_1; Y'')$, then the cutset bound can be expressed as

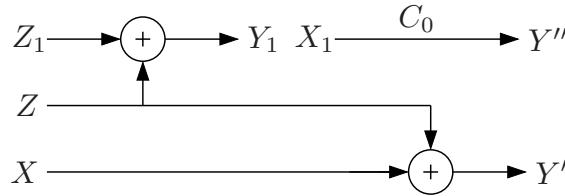
$$C \leq \max_{p(x)} \min\{I(X; Y') + C_0, I(X; Y', Y_1)\}$$

Note that C depends on $p(y'' | x_1)$ only through C_0

- Consider the following special cases:
 - Example (Receiver-orthogonal semi-deterministic RC [10]): Let Y_1 be a deterministic function of (X, Y') . Then by setting $\hat{Y}_1 = Y_1$ and using the fact that $H(Y_1|X, Y') = 0$, the compress-forward achievable rate coincides with the cutset upper bound

$$\begin{aligned} R &= \max_{p(x)p(x_1)p(\hat{y}_1|y_1, x_1)} \min \left\{ I(X, X_1; Y) - I(Y_1; \hat{Y}_1|X, X_1, Y), I(X; Y, \hat{Y}_1|X_1) \right\} \\ &= \max_{p(x)} \min \{I(X; Y') + C_0, I(X; Y', Y_1)\} = C \end{aligned}$$

- Example (Cutset bound is not tight [3]): Let $Y' = X \oplus Z$ and $Y_1 = Z \oplus Z_1$, where $Z \sim \text{Bern}(1/2)$ and $Z_1 \sim \text{Bern}(p)$ and X are independent. Assume that the relay-to-receiver channel $p(y''|x_1)$ has capacity $C_0 \in [0, 1]$



The capacity of this relay channel is

$$C = 1 - H(p * H^{-1}(1 - C_0)),$$

where $H^{-1}(x) \in [0, 1/2]$ is the inverse of the binary entropy function

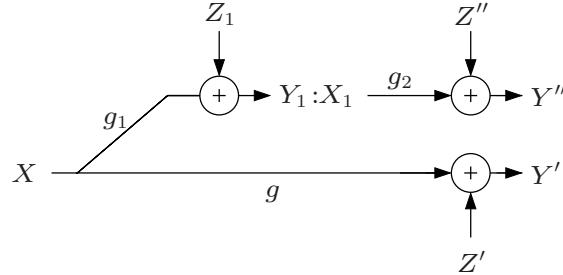
Achievability follows by setting $\hat{Y}_1 = Y_1 \oplus V$, where $V \sim \text{Bern}(\alpha)$ is independent of (X, Z, Z_1) and $\alpha = H^{-1}(1 - C_0)$, in the compress-forward lower bound. For the converse, consider

$$\begin{aligned} nR &\leq I(X^n; Y'^n, Y''^n) + n\epsilon_n \\ &\stackrel{(a)}{=} I(X^n; Y'^n | Y''^n) + n\epsilon_n \\ &\leq n - H(Y'^n | X^n, Y''^n) + n\epsilon_n \\ &= n - H(Z^n | Y''^n) + n\epsilon_n \\ &\stackrel{(b)}{\leq} n - nH(p * H^{-1}(H(Y_1^n | Y''^n)/n)) + n\epsilon_n \\ &\stackrel{(c)}{\leq} n - nH(p * H^{-1}(1 - C_0)) + n\epsilon_n, \end{aligned}$$

where (a) follows from independence of X^n and $(Z^n, Z_1^n, X_1^n, Y''^n)$, (b) follows from the vector version of Mrs. Gerber's lemma with $Z^n = Y_1^n \oplus Z_1^n$, which yields $H(Z^n | Y''^n) \geq H(p * H^{-1}(H(Y_1^n | Y''^n)/n))$, and (c) follows from the fact that $nC_0 \geq I(X_1^n; Y''^n) \geq I(Y_1^n; Y''^n) = n - H(Y_1^n | Y''^n)$. Note that the cutset upper bound for this channel is $\min\{1 - H(p), C_0\}$, which is strictly larger than the capacity if $p \in (0, 1)$ and $1 - H(p) \leq C_0$. This shows that the cutset upper bound is not tight in general

RFD-AWGN Relay Channel

- The Receiver Frequency-Division (RFD) AWGN-RC [9] has orthogonal receiver components



Here $Y = (Y', Y'')$ and $\{Z'_i\}$ and $\{Z''_i\}$ are independent WGN processes with average powers equal to 1

- The capacity of this channel is not known in general
- The cutset upper bound reduces to

$$C \leq \begin{cases} C(S + S_2(S + 1)) & \text{if } S_1 \geq S_2(1 + S) \\ C(S + S_1) & \text{otherwise} \end{cases}$$

- The decode-forward lower bound reduces to

$$C \geq \begin{cases} C(S + S_2(S + 1)) & \text{if } S_1 \geq S + S_2(S + 1) \\ C(S_1) & \text{otherwise} \end{cases}$$

- The bounds coincide if $S_1 \geq S + S_2(S + 1)$ and $C = C(S) + C(S_2)$. Thus capacity is known in this case and is achieved via decode-forward
- If $S_1 \leq S$, decode-forward bound is worse than the direct transmission lower bound
- As for the general AWGN-RC model, the rate of partial-decode-forward does not exceed the maximum the decode-forward and direct transmission rates
- Compress-forward with Gaussian signals reduces to

$$C \geq C(S + S_1 S_2(S + 1)/(S_1 + (S + 1)(S_2 + 1)))$$

Remarks:

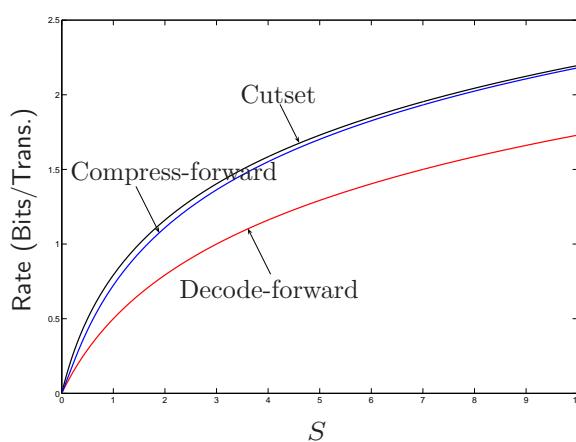
- The bound becomes tight if $S \rightarrow \infty$ or $S_2 \rightarrow \infty$
- At small S_1 (low SNR for the channel to the relay), compress-forward outperforms both direct transmission and decode-forward, even though more noise is sent over the channel to the receiver. In this case, the rate can be improved via time sharing at the sender side (X sends at power P/α for a fraction $\alpha \in [0, 1]$ of the time and at power 0 the rest of the time)
- Remark: Note that while the receiver orthogonal DM-RC is a special case of the DM-RC, the RFD-AWGN-RC is not a special case of the AWGN-RC introduced earlier

However, it is a special case of the product of two AWGN-RCs $Y'_1 = g_1 X' + Z'_1$, $Y' = gX' + g_2 X'_1 + Z'$ and $Y''_1 = g_1 X'' + Z''_1$, $Y'' = gX'' + g_2 X''_1 + Z''$ with power constraint P on (X', X'') and on (X'_1, X''_1) (Why?)

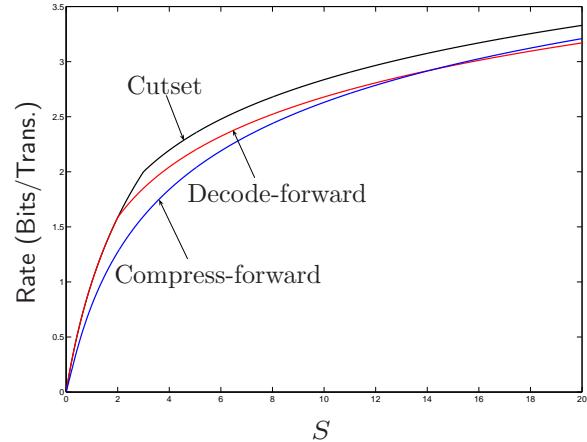
We can generalize the RFD-AWGN model by assuming that the channel from the relay sender to the receiver has a different "frequency band" from the channel with input X and outputs Y_1, Y' . The above results can be readily extended to this generalized model [11]

Comparison of Bounds for RFD-AWGN Relay Channel

$$S_1 = S, S_2 = 4S$$

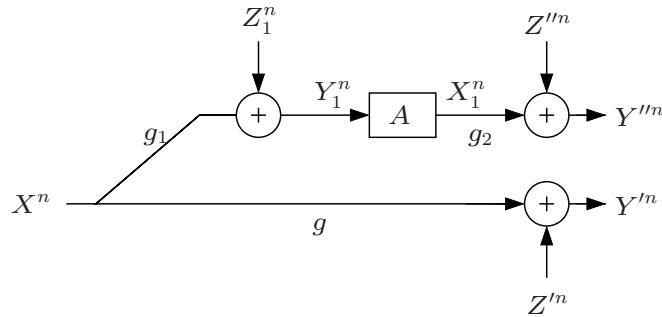


$$S_1 = 4S, S_2 = S$$



Linear Relaying for RFD-AWGN-RC

- Assume the relay functions are restricted to linear combinations of past received symbols, i.e., $x_{1i} = \sum_{j=1}^i a_{ij}y_{1j}$, $i \in [1 : n]$. Note that we can eliminate the delay in relay encoding by simple relabeling of transmission time over the channel from X_1 to Y''
- This scheme is considerably simpler than decode-forward and compress-forward, but can it perform well?
- Using vector notation $X_1^n = AY_1^n$, where the A is an $n \times n$ lower triangular matrix



- *Multi-letter characterization:* The capacity with linear relaying, $C^{(l)}$, can be expressed as

$$C^{(l)} = \lim_{k \rightarrow \infty} C_k^{(l)}$$

where

$$C_k^{(l)} := \sup_{F(x^k), A} \frac{1}{k} I(X^k; Y^k)$$

subject to sender and relay power constraint P and A lower triangular

- Note that $C^{(l)}(P)$ satisfies the properties of $C(P)$ discussed in the Appendix
- It can be shown that $C_k^{(l)}$ is achieved using Gaussian X^k (why?)

Amplify–Forward

- Consider $C_1^{(l)}$, which is the maximum rate achieved via a simple *amplify–forward* relaying scheme

- It can be easily shown that $C_1^{(l)}$ is achieved by $X \sim N(0, P)$ and $X_1 = \sqrt{P/(S_2 + 1)} Y_1$. Therefore,

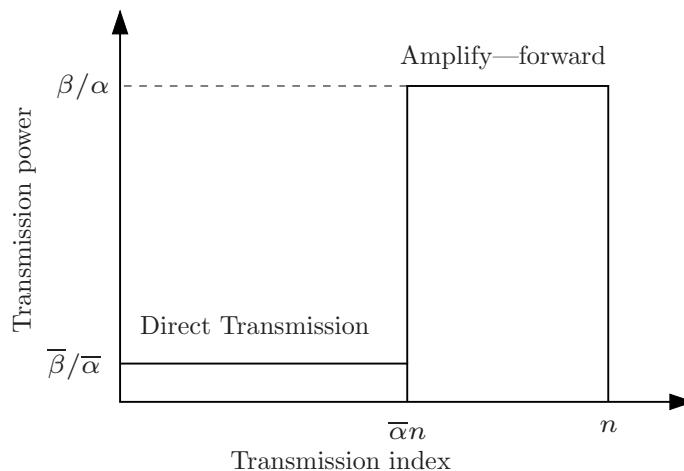
$$C_1^{(l)} = C(S + S_1 S_2 / (S_1 + S_2 + 1))$$

- This rate approaches capacity as $S_2 \rightarrow \infty$!

- $C_1^{(l)}$ is not convex in P . In fact it is concave for small P and convex for large P . Thus the rate can be improved by time sharing between direct transmission only and amplify–forward, and we obtain the improved lower bound

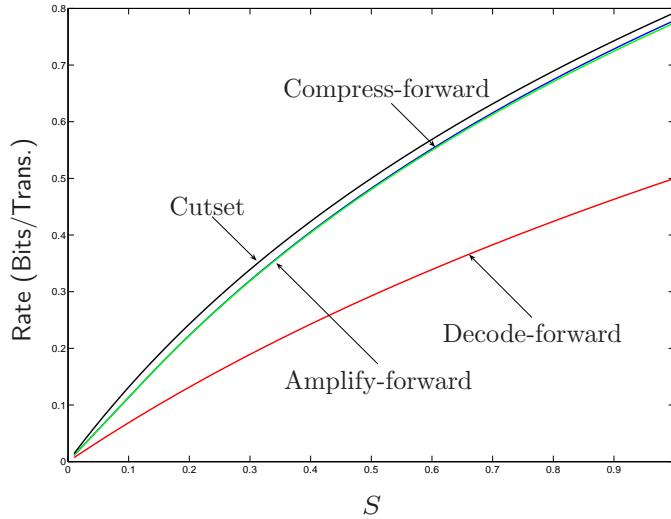
$$C^l \geq \max_{0 < \alpha, \beta \leq 1} (\bar{\alpha} C(\bar{\beta} S / \bar{\alpha}) + \alpha C((\beta/\alpha)(S + S_1 S_2 / (\beta S_1 + S_2 + \alpha))))$$

Note that the relay transmits at power P/α during amplify–forward



Comparison to Other Schemes

- Example: $S_1 = S$, $S_2 = 25S$



- Compress-forward outperforms amplify-forward, but is significantly more complex to implement

Linear Relaying Capacity of RFD-AWGN Relay Channel

- *Theorem 5 [9]:* The linear relaying capacity of the RFD-AWGN relay channel is

$$C^{(l)} = \max \left(\alpha_0 C \left(\frac{\beta_0 P}{\alpha_0} \right) + \sum_{j=1}^4 \alpha_j C \left(\frac{\beta_j P}{\alpha_j} \left(1 + \frac{g_1^2 g_2^2 \eta_j}{1 + g_2^2 \eta_j} \right) \right) \right),$$

where the maximum is taken over $\alpha_j, \beta_j \geq 0$, and $\eta_j > 0$, such that $\sum_{j=0}^4 \alpha_j = \sum_{j=0}^4 \beta_j = 1$, and $\sum_{j=1}^4 \eta_j (g_1^2 \beta_j + \alpha_j) = P$

- In the following, we provide an outline of the proof
- Gaussian X^k maximizes $C_k^{(l)} = (1/k) \sup_{F(x^k), A} I(X^k; (Y')^k, (Y'')^k)$ subject to power constraint P and lower triangle matrix A

- Assume without loss of generality that $g = 1$. Then,

$$C_k^{(l)} = \text{Maximum} \frac{1}{2k} \log \frac{\left| \begin{bmatrix} I + K_X & g_1 g_2 K_X A^T \\ g_1 g_2 A K_X & I + g_1^2 g_2^2 A K_X A^T + g_2^2 A A^T \end{bmatrix} \right|}{\left| \begin{bmatrix} I & 0 \\ 0 & I + g_2^2 A A^T \end{bmatrix} \right|}$$

Subject to $K_X \succeq 0$

$$\text{tr}(K_X) \leq kP$$

$$\text{tr}(g_1^2 K_X A^T A + A^T A) \leq kP, \text{ and } A \text{ lower triangle}$$

- $K_X = E(X^k (X^k)^T)$ and A are the optimization variables
- This is a nonconvex problem in (K_X, A) with $k^2 + k$ variables
- For a fixed A , the problem is convex in K_X (similar to waterfilling); however, finding A for a fixed K_X is a nonconvex problem
- Can show that diagonal K_X and A suffice

- Then,

$$C_k^{(l)} = \text{Maximum} \frac{1}{2k} \log \prod_{j=1}^k \left(1 + \sigma_j \left(1 + \frac{g_1^2 g_2^2 a_j^2}{1 + g_2^2 a_j^2} \right) \right)$$

Subject to $\sigma_j \geq 0$, for $j \in [1 : k]$, $\sum_{j=1}^k \sigma_j \leq kP$, and

$$\sum_{j=1}^k a_j^2 (1 + g_1^2 \sigma_j) \leq kP$$

- This still is a nonconvex optimization problem, but with $2k$ variables only
- At the optimum point:
 - If $\sigma_j = 0$ it is easy to show that $a_j = 0$
 - If $a_j = a_{j'} = 0$ then $\sigma_j = \sigma_{j'}$ (by concavity of log function)

- Thus,

$$C_k^{(l)} = \text{Maximum} \frac{1}{2k} \log (1 + k\beta_0 P/k_0)^{k_0} \prod_{j=k_0+1}^k (1 + \sigma_j (1 + g_1^2 g_2^2 a_j^2 / (1 + g_2^2 a_j^2)))$$

Subject to $a_j > 0$, for $j \in [k_0 + 1 : k]$, $\sum_{j=k_0}^k \sigma_j \leq k(1 - \beta_0)P$,

$$\sum_{j=k_0+1}^k a_j^2 (1 + g_1^2 \sigma_j) \leq kP$$

- By KKT conditions, at the optimum, there are ≤ 4 distinct nonzero (σ_j, a_j) pairs, thus

$$C_k^{(l)} = \text{Maximum} \frac{1}{2k} \log (1 + k\beta_0 P/k_0)^{k_0} \prod_{j=1}^4 (1 + \sigma_j (1 + g_1^2 g_2^2 a_j^2 / (1 + g_2^2 a_j^2)))^{k_j}$$

Subject to $a_j > 0$ for $j \in [1 : 4]$, $\sum_{j=1}^4 k_j \sigma_j \leq k(1 - \beta_0)P$, and

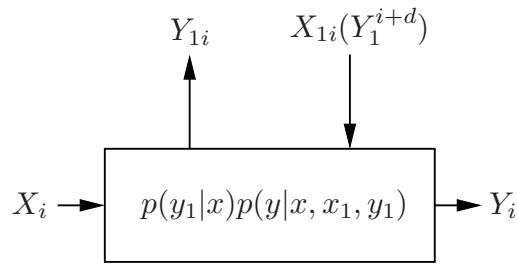
$$\sum_{j=1}^4 k_j a_j^2 (1 + g_1^2 \sigma_j) \leq kP, \quad \sum_{j=0}^4 k_j = k,$$

where k_j is the number of times the pair (σ_j, a_j) is used during transmission and is a new optimization variable in the problem

- Taking the limit as $k \rightarrow \infty$ completes the proof
- Remarks:
 - This is a rare example where we do not have a single-letter mutual information characterization of capacity but are able to obtain a computable characterization *directly* from the multi-letter characterization
 - The equivalent problem for the general AWGN-RC with linear relaying is still open (i.e, there is no similar single-letter characterization)

Relay With Lookahead

- The *discrete-memoryless relay with lookahead channel* $(\mathcal{X}, \mathcal{X}_1, p(y_1|x)p(y|x, x_1, y_1), \mathcal{Y}, \mathcal{Y}_1, d)$ [12] consists of four finite alphabets $\mathcal{X}, \mathcal{X}_1, \mathcal{Y}, \mathcal{Y}_1$, a collection of conditional pmfs $p(y_1|x)p(y|x, x_1, y_1)$ on $\mathcal{Y}, \mathcal{Y}_1$, and lookahead $d \in \mathbb{Z}$ in relay encoding. Recall that the conditional pmf for the DM-RC is defined as $p(y, y_1|x, x_1)$. The restriction on the conditional pmf for the relay-with-lookahead channel is needed to prevent instantaneous or lookahead dependency of X_1 on Y_1



- The channel is memoryless in the sense that

$$p(y_1^n | x^n) p(y^n | x^n, x_1^n, y_1^n) = \prod_{i=1}^n p_{Y_1|X}(y_{1i} | x_{i+d}) p_{Y|X, X_1, Y_1}(y_i | x_i, x_{1i}, y_{1i}),$$

where the pmfs with symbols that do not have positive time indices or time indices greater than n are arbitrary

- A $(2^{nR}, n)$ code for the relay-with-lookahead channel consists of:
 - A message set $[1 : 2^{nR}]$
 - An encoder that assigns to a codeword $x^n(m)$ to each message $m \in [1 : 2^{nR}]$
 - A relay encoder that assigns a symbol $x_{1i}(y_1^{i+d})$ to each sequence y_1^{i+d} for $i \in [1 : n]$
 - A decoder that assigns an estimate $\hat{m}(y^n)$ or an error message e to each received sequence y^n
- The message $M \sim \text{Unif}[1 : 2^{nR}]$
- The definition of probability of error, achievability, and capacity C_d are as before

- The lookahead in the above relay model may be, for example, due to a difference between the arrival times of the signal from the sender to the receiver and to the relay. If the signal arrives at both the relay and receiver at the same time, we have a lookahead of $d = -1$. In general, if the signal arrives at the receiver $d + 1$ transmissions after it arrives at the relay, we have a lookahead of d
- Remarks:
 - Since lookahead $d = -1$ corresponds to the (classical) DM-RC model, $C_{-1} = C$, the capacity of the DM-RC
 - The channel with $d = 0$ will be referred to as the DM-RC without delay (DM-RWD)
 - C_d is monotonically nondecreasing in d
- We define the DM-RC with unlimited lookahead as a relay channel where the relay encoder can depend noncausally on the entire relay received sequence y_1^n and denote its capacity by C_∞ . The purpose of studying this extreme case is to understand the limits on relaying with arbitrary lookahead
- C_d for any finite d and C_∞ are not known in general
- We present results for the DM-RC with unlimited lookahead and the DM-RWD

Relay With Unlimited Lookahead

- We show that C_∞ can be strictly larger than the capacity of the DM-RC, C , and can exceed the cutset bound
- Upper bound on C_∞ :

Theorem 6 (Unlimited-Lookahead Cutset Bound) [12]: The following is an upper bound on the capacity of the DM-RC with unlimited lookahead

$$C_\infty \leq \max_{p(x,x_1)} \min\{I(X, X_1; Y), I(X; Y_1) + I(X; Y|X_1, Y_1)\}$$

- Noncausal decode-forward lower bound [12]:

$$C_\infty \geq \max_{p(x,x_1)} \min\{I(X; Y_1), I(X, X_1; Y)\}$$

To prove achievability fix a pmf $p(x, x_1)$ and randomly generate 2^{nR} sequence pairs $(x^n, x_1^n)(m)$, $m \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p(x_t, x_{1i})$

Since the relay knows y_1^n in advance, it decodes m before transmission commences. By the LLN and the packing lemma, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if $R < I(X; Y_1) - \delta(\epsilon)$

The sender and relay then cooperatively transmit $(x^n, x_1^n)(m)$

The receiver can reliably decode m if $R < I(X, X_1; Y)$. Combining the two bounds completes the proof

- The above lower bound is tight for the degraded DM-RC with unlimited lookahead, where $X \rightarrow (X_1, Y_1) \rightarrow Y$ form a Markov chain. The converse follows from the upper bound on C_∞
- Example: Consider the Sato relay channel [4] with unlimited lookahead. We know that $C = 1.161878$ bits/transmission and coincides with the cutset bound

Since the channel is degraded, the capacity with unlimited lookahead coincides with the unlimited-lookahead cutset bound and is achieved by noncausal decode-forward. Evaluating the capacity expression, we obtain

$C_\infty = \log(9/4) = 1.169925$ bits/transmission. The optimizing pmf $p(x, x_1)$ is given in the following table

	$X = 0$	$X = 1$	$X = 2$
$X_1 = 0$	7/18	1/18	1/18
$X_1 = 1$	1/18	1/18	7/18

Thus for this example $C_\infty > C$ and exceeds the cutset bound. This also shows that the above upper bound can be strictly larger than the cutset bound

- Remark: A partial noncausal decode-forward lower bound can be similarly established and can be shown to achieve the capacity of the semi-deterministic relay-with-unlimited lookahead

$$C_\infty = \max_{p(x, x_1)} \min\{I(X, X_1; Y), H(Y_1) + I(X; Y|X_1, Y_1)\}$$

- *AWGN-RC with unlimited lookahead:* Consider the AWGN-RC and assume that the relay encoding functions can depend noncausally on the received sequence y_1^n

By evaluating the above upper bound and the decode-forward lower bound on C_∞ with average power constraints P on X and on X_1 , we can show that capacity

$$C_\infty = C((g + g_2)^2 P) = C(S + S_2 + 2\sqrt{SS_2})$$

if $g_1 \geq g + g_2$

Relay Without Delay

- Consider the DM-RWD. For this case, $d = 0$, i.e., for each $i \in [1 : n]$, the relay encoder assigns a symbol $x_{1i}(y_1^i)$. We show that rates higher than the cutset bound can be achieved
- *Theorem 7* (Relay-Without-Delay Cutset Bound) [12]: The following is an upper bound on the capacity of the DM-RWD

$$C_0 \leq \max_{p(v,x), x_1(u,y_1)} \min\{I(U, X; Y), I(X; Y, Y_1|U)\},$$

where $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{X}_1| + 1$

- Remarks:

- The above bound is also an upper bound on the capacity of the DM-RC. However, since in this case X_{1i} is a function only of U_i , the bound reduces to the cutset bound
- The above bound can be expressed as a cutset bound for a DM-RC with relay sender alphabet \mathcal{X}'_1 that consists of all mappings $x'_1 : \mathcal{Y}_1 \rightarrow \mathcal{X}'_1$. The bound reduces to $C_0 \leq \max_{p(x,x'_1)} \min\{I(X; Y, Y_1|X'_1), I(X, X'_1; Y)\}$, which is analogous to Shannon expression of the capacity of the DMC with DM state available causally at the encoder

Instantaneous Relaying Lower Bound

- Note that any lower bound on the capacity of the DM-RC, e.g., using partial decode-forward or compress-forward, is a lower bound on the capacity of the DM-RWD. We expect, however, that higher rates can be achieved by depending on present in addition to past received relay symbols
- In *instantaneous relaying* the relay symbol at time i is a function only of y_{1i} . This simple scheme yields the lower bound

$$C_0 \geq \max_{p(x), x_1(y_1)} I(X; Y)$$

- We now show that instantaneous relaying can be optimal and can achieve a higher rate than the cutset bound

Example: Again consider the Sato relay channel. We have shown that $C = 1.161878$ bits/transmission and $C_\infty = \log(9/4) = 1.169925$ bits/transmission

Consider the instantaneous relaying lower bound with pmf $(3/9, 2/9, 4/9)$ on X and a mapping from X to X_1 of $0 \rightarrow 0$, $1 \rightarrow 1$, $2 \rightarrow 1$

It can be easily shown that these choices yield $I(X; Y) = 1.169925$ bits/transmission. Thus the capacity of the Sato relay channel without delay $C_0 = C_\infty^* = 1.169925$ bits/transmission

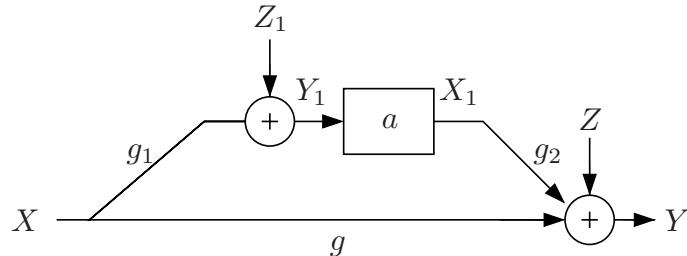
- Remarks:
 - This result is not too surprising. Since the channel from the sender to the relay is noiseless, complete cooperation, which requires knowledge of the entire received sequence in advance, can be achieved simply via instantaneous relaying
 - Since for this example $C_0 > C$ and C coincides with the cutset bound, this result shows that instantaneous relaying alone can achieve a higher rate than the cutset bound!
- Superposition of instantaneous relaying with partial decode-forward yield the lower bound

$$C_0 \geq \max_{p(u,v,x), x_1(v,y_1)} \min\{I(V,X;Y), I(U;Y_1|V) + I(X;Y|V,U)\},$$

which is optimal for degraded and semi-deterministic RWD channels

AWGN Relay-Without-Delay

- Consider the AWGN-RC, where at the time i , the relay encoder depends on y_1^i
- *Amplify—forward* lower bound on C_0 :



- To satisfy the power the relay constraint we must have $a^2 \leq P/(g_1^2 P + 1)$
- The capacity of the equivalent point-to-point AWGN channel with average received power $(g_1 g_2 a + g)^2 P$ and average noise power $(g_2^2 a^2 + 1)$ yields the lower bound

$$C_0 \geq C \left(\frac{(g_1 g_2 a + g)^2 P}{g_2^2 a^2 + 1} \right)$$

Now, if $g_2^2 \geq g_1^2(g_1^2P + 1)/(g^2P)$ and $gg_1 \geq 0$, then it can be shown that the bound is optimized for $a^* = g_1/gg_2$ and simplifies to

$$C_0 \geq C((g^2 + g_1^2)P)$$

Evaluating the upper bound on C_∞ for the AWGN case yields

$$C_0 \leq C((g^2 + g_1^2)P) \text{ for } g_1 \leq g_2$$

Thus the bounds coincide if $g_1^2 \leq g_2^2 \min\{1, P/(g_1^2P + 1)\}$, and

$$C_0 = C_\infty = C((g^2 + g_1^2)P) = C(S_1 + S_2)$$

- Remarks:

- The above result shows that amplify-forward alone can be *optimal* for both the AWGN RWD and the AWGN relay with unlimited lookahead. This is surprising given the extreme simplicity of this scheme
- Combining results, we have shown that the capacity of the AWGN relay with unlimited lookahead is known if $g_1 \geq (g + g_2)$ or if $g_1^2 \leq g_2^2 \min\{1, P/(g_1^2P + 1)\}$. Note that the capacity in this range coincides with the cutset bound
- It can be shown using superposition of amplify-forward and decode-forward that the capacity of the AWGN RWD can exceed the cutset bound

Coherent Cooperation

- In studying the relay channel with and without delay, we have introduced three types of coherent cooperation:
 - *Decode-forward*: Here the relay decodes part or all of the message and the sender and relay cooperate on sending the *previous* message. This requires knowledge only of past received relay symbols and therefore is possible to implement for any finite relay encoding delay $-l$
 - *Instantaneous relaying*: Here the relay sends a function only of its current received symbol. This is possible when the relay has access to the current received symbol, which is the case for any $l \geq 0$
 - *Noncausal decode-forward*: This scheme is possible only when the relay has unlimited lookahead. The relay pre-decodes part or all of the message before communication commences and cooperates with the sender to transmit the message to the receiver
- Although instantaneous relaying alone can be optimal (e.g., the Sato and AWGN RWD), a combination of decode-forward and instantaneous relaying achieves higher rate in general

Key New Ideas and Techniques

- Cutset upper bound on capacity
- Coherent cooperation (similar to MAC with common message)
- Block Markov coding
- Use of multiple independent codebooks
- Decode-forward
- Backward decoding
- Use of binning in channel coding
- Compress-forward
- Amplify-forward
- Linear relaying

References

- [1] E. C. van der Meulen, "Three-terminal communication channels," *Adv. Appl. Prob.*, vol. 3, pp. 120–154, 1971.
- [2] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sept. 1979.
- [3] M. Aleksic, P. Razaghi, and W. Yu, "Capacity of a class of modulo-sum relay channel," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 596–600.
- [4] H. Sato, "Information transmission through a channel with relay," The Aloha Systems, University of Hawaii, Honolulu, HI, Technical Report B76-7, Mar. 1976.
- [5] F. M. J. Willems and E. C. van der Meulen, "The discrete memoryless multiple-access channel with cribbing encoders," *IEEE Trans. Inf. Theory*, vol. 31, no. 3, pp. 313–327, 1985.
- [6] L.-L. Xie and P. R. Kumar, "An achievable rate for the multiple-level relay channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1348–1358, 2005.
- [7] A. El Gamal and M. R. Aref, "The capacity of the semideterministic relay channel," *IEEE Trans. Inf. Theory*, vol. 28, no. 3, p. 536, May 1982.
- [8] A. El Gamal and S. Zahedi, "Capacity of a class of relay channels with orthogonal components," *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp. 1815–1817, 2005.
- [9] A. El Gamal, M. Mohseni, and S. Zahedi, "Bounds on capacity and minimum energy-per-bit for AWGN relay channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1545–1561, 2006.

- [10] Y.-H. Kim, "Capacity of a class of deterministic relay channels," *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 1328–1329, Mar. 2008.
- [11] Y. Liang and V. V. Veeravalli, "Gaussian orthogonal relay channels: Optimal resource allocation and capacity," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3284–3289, Sept. 2005.
- [12] A. El Gamal, N. Hassanpour, and J. Mammen, "Relay networks with delays," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3413–3431, Oct. 2007.

Appendix: Properties of $C(P)$

- The capacity of the AWGN-RC with average power constraints satisfies the following:
 - (i) $C(P) > 0$ if $P > 0$ and approaches ∞ as $P \rightarrow \infty$.
 - (ii) $C(P) \rightarrow 0$ as $P \rightarrow 0$.
 - (iii) $C(P)$ is concave and strictly increasing in P .
- Proof:
 - (i) This follows from the fact that $C(P) \geq C(g^2P)$, the capacity of the direct channel, which is strictly greater than zero for $P > 0$, and approaches infinity as $P \rightarrow \infty$.
 - (ii) This follows from the fact that the cutset bound, which is greater than or equal to $C(P)$ approaches zero as $P \rightarrow 0$

- (iii) Concavity follows by the following “time-sharing” argument. For any $P, P' > 0$ and $\epsilon > 0$, there exists k and k' such that $C(P) < C_k(P) + \epsilon$ and $C(P') < C_{k'}(P') + \epsilon$. Now, for any integers a, b , define $\alpha := ak/(ak + bk')$, where,

$$\begin{aligned}\alpha C(P) + \bar{\alpha} C(P') &\leq \alpha C_k(P) + \bar{\alpha} C_{k'}(P') + \epsilon \\ &\leq C_{ak+bk'}(\alpha P + \bar{\alpha} P') + \epsilon \\ &\leq C(\alpha P + \bar{\alpha} P') + \epsilon,\end{aligned}$$

where the second inequality follows from the fact that $\alpha C_k(P) + \bar{\alpha} C_{k'}(P')$ is achieved arbitrarily closely for some pmf $p(x^{ak+bk'})$ and some relaying functions $\{\tilde{x}_{1j}\}_{j=1}^{ak+bk'}$ that is a mixture of the pmf $p(x^k)$ and relaying functions $\{x_{1i}\}_{j=1}^k$ that achieve $C_k(P)$ and the $p(x^{k'})$ and $\{x'_{1j}\}_{j=1}^{k'}$ that achieve $C_{k'}(P')$ (corresponding to “time-sharing”). Clearly, the set of pmfs and functions achieved by “time-sharing” is a subset of the set of all possible $p(x^{ak+bk'})$ and $\{x_{1i}\}_{i=1}^{ak+bk'}$. Note that even though $C_k(P) = (1/k) \max_{p(x^k), \{x_{1i}\}_{j=1}^k} I(X^k; Y^k)$ may not be concave, $C(P) = \sup_k C_k(P)$ is concave

That $C(P)$ is strictly monotonically increasing in P follows from parts (i), (ii), and concavity.

Appendix: Cutset Bound for AWGN-RC

- It can be easily shown that the cutset bound for the AWGN-RC is

$$C \leq \sup_{F(x, x_1): E(X^2) \leq P, E(X_1^2) \leq P} \min\{I(X, X_1; Y), I(X; Y, Y_1 | X_1)\}$$

We perform the maximization by first establishing an upper bound on the RHS expression and then showing that it is attained by jointly Gaussian X, X_1

- We begin with the first mutual information. Without loss of generality assume that $E(X) = E(X_1) = 0$. Consider

$$\begin{aligned}I(X, X_1; Y) &= h(Y) - h(Y | X, X_1) = h(Y) - \frac{1}{2} \log(2\pi e) \\ &\leq \frac{1}{2} \log(E(Y^2)) \\ &\leq \frac{1}{2} \log(1 + g^2 E(X^2) + g_2^2 E(X_1^2) + 2gg_2 E(XX_1)) \\ &\leq \frac{1}{2} \log(1 + S + S_2 + 2\rho\sqrt{SS_2}) = C(S + S_2 + 2\rho\sqrt{SS_2}),\end{aligned}$$

where $\rho := E(XX_1)/\sqrt{E(X^2)E(X_1^2)}$, is the correlation coefficient between X and X_1 (the random variables are assumed to have zero means)

- Next, we consider the second mutual information term in the cutset bound

$$\begin{aligned}
I(X; Y, Y_1 | X_1) &= h(Y, Y_1 | X_1) - h(Y, Y_1 | X, X_1) \leq h(Y, Y_1 | X_1) - \log(2\pi e) \\
&= h(Y | X_1) + h(Y_1 | Y, X_1) - \log(2\pi e) \\
&\leq \frac{1}{2} \log(\mathbb{E}(\text{Var}(Y | X_1))) + \frac{1}{2} \log(\mathbb{E}(\text{Var}(Y_1 | Y, X_1))) \\
&\stackrel{(a)}{\leq} \frac{1}{2} \log(1 + g^2(\mathbb{E}(X^2) - (\mathbb{E}(XX_1))^2 / \mathbb{E}(X_1^2))) \\
&\quad + \frac{1}{2} \log\left(\frac{1 + (g^2 + g_1^2)(\mathbb{E}(X^2) - (\mathbb{E}(XX_1))^2 / \mathbb{E}(X_1^2))}{1 + g^2(\mathbb{E}(X^2) - (\mathbb{E}(XX_1))^2 / \mathbb{E}(X_1^2))}\right) \\
&= \frac{1}{2} \log(1 + (g^2 + g_1^2)(\mathbb{E}(X^2) - (\mathbb{E}(XX_1))^2 / \mathbb{E}(X_1^2))) \\
&\leq \frac{1}{2} \log(1 + (S + S_1)(1 - \rho^2)) = C((S + S_1)(1 - \rho^2)),
\end{aligned}$$

where (a) follows from the fact that the mean-squared error of the best linear MSE estimates of Y given X_1 and of Y_1 given (Y, X_1) are greater than or equal to the expected conditional variances $\mathbb{E}(\text{Var}(Y | X_1))$ and $\mathbb{E}(\text{Var}(Y_1 | Y, X_1))$, respectively.

- Now, it is clear that jointly Gaussian (X, X_1) each with average power P and correlation coefficient ρ achieve the above upper bounds

Appendix: Partial Decode–Forward for AWGN-RC

- It is straightforward to verify that

$$I(X, X_1; Y) \leq C(S + S_2 + 2\rho\sqrt{SS_2}),$$

where ρ is the correlation coefficient between X and X_1

- Next consider

$$\begin{aligned}
&I(U; Y_1 | X_1) + I(X; Y | X_1, U) \\
&= h(Y_1 | X_1) - h(Y_1 | X_1, U) + h(Y | X_1, U) - h(Y | X, X_1, U) \\
&\leq \frac{1}{2} \log(2\pi e \mathbb{E}(\text{Var}(Y_1 | X_1))) - h(Y_1 | X_1, U) + h(Y | X_1, U) - \frac{1}{2} \log(2\pi e) \\
&\leq \frac{1}{2} \log(1 + g_1^2(\mathbb{E}(X^2) - (\mathbb{E}(XX_1))^2 / \mathbb{E}(X_1^2))) - h(Y_1 | X_1, U) + h(Y | X_1, U) \\
&= C(S_1(1 - \rho^2)) - h(Y_1 | X_1, U) + h(Y | X_1, U)
\end{aligned}$$

- We now upper bound $(h(Y|X_1, U) - h(Y_1|X_1, U))$

First consider the case of $S_1 > S$, i.e., $|g_1| > |g|$. In this case

$$\begin{aligned} h(Y_1|X_1, U) &= h(g_1 X + Z_1|X_1, U) \\ &= h(g_1 X + Z|X_1, U) \\ &\geq h(gX + Z|X_1, U) = h(Y|X_1, U) \end{aligned}$$

Hence, $h(Y|X_1, U) - h(Y_1|X_1, U) \leq 0$, and

$$I(U; Y_1|X_1) + I(X; Y|X_1, U) \leq C((1 - \rho^2)S_1)$$

Thus the rate of the partial decode-forward rate reduces to that of the decode-forward

Next, consider the case of $S_1 \leq S$. Note that

$$\frac{1}{2} \log(2\pi e) \leq h(Y_1|X_1, U) \leq h(Y_1) = \frac{1}{2} \log(2\pi e(1 + S_1))$$

Therefore, there exists a constant $0 \leq \beta \leq 1$ such that

$$h(Y_1|X_1, U) = \frac{1}{2} \log(2\pi e(1 + S_1\beta))$$

Now, consider

$$\begin{aligned} h(g_1 X + Z_1|X_1, U) &= h((g_1/g)(gX + (g/g_1)Z_1)|X_1, U) \\ &= h(gX + (g/g_1)Z_1|X_1, U) + \log |g_1/g| \\ &\stackrel{(a)}{=} h(gX + Z' + Z''|X_1, U) + \log |g_1/g| \\ &\stackrel{(b)}{\geq} \frac{1}{2} \log \left(2^{2h(gX + Z'|X_1, U)} + 2^{2h(Z''|X_1, U)} \right) + \log |g_1/g| \\ &= \frac{1}{2} \log \left(2^{2h(gX + Z'|X_1, U)} + 2\pi e (g^2/g_1^2 - 1) \right) + \log |g_1/g| \\ &= \frac{1}{2} \log \left(2^{2h(Y|X_1, U)} + 2\pi e (S/S_1 - 1) \right) + \frac{1}{2} \log(S_1/S), \end{aligned}$$

where in (a), $Z' \sim N(0, 1)$ and $Z'' \sim N(0, g^2/g_1^2 - 1)$ are independent, and (b) follows by the entropy power inequality (EPI). Since

$$h(g_1 X + Z_1|X_1, U) = \frac{1}{2} \log(2\pi e(1 + S_1\beta)),$$

we obtain

$$2\pi e (S/S_1 + \beta S) \geq 2^{2h(Y|X_1, U)} + 2\pi e (S/S_1 - 1)$$

Thus

$$h(Y|X_1, U) \leq \frac{1}{2} \log(2\pi e(1 + \beta S)),$$

and

$$h(Y|X_1, U) - h(Y_1|X_1, U) \leq \frac{1}{2} \log \left(\frac{1 + \beta S}{1 + \beta S_1} \right) \stackrel{(a)}{\leq} \frac{1}{2} \log \left(\frac{1 + S}{1 + S_1} \right),$$

where (a) follows since if $S_1 \leq S$, $(1 + \beta S)/(1 + \beta S_1)$ is a strictly increasing function of β and achieves its maximum when $\beta = 1$. Substituting, we obtain

$$\begin{aligned} I(U; Y_1|X_1) + I(X; Y|X_1, U) &\leq \frac{1}{2} \log (1 + S_1(1 - \rho^2)) + \frac{1}{2} \log \left(\frac{1 + S}{1 + S_1} \right) \\ &\leq \frac{1}{2} \log (1 + S_1) + \frac{1}{2} \log \left(\frac{1 + S}{1 + S_1} \right) \\ &= C(S), \end{aligned}$$

which is the capacity of the direct channel. This completes the proof

Appendix: Equivalence of Compress–Forward Lower Bound Characterizations

- To show that the two characterizations are equal, denote the first characterization by R_1 and the second by R_2
- First we show that $R_2 \leq R_1$. At the optimum joint pmf

$$\begin{aligned} R_2 &= I(X; Y, \hat{Y}_1|X_1) \\ &= H(Y, \hat{Y}_1|X_1) - H(Y, \hat{Y}_1|X, X_1) \\ &= H(Y|X_1) + H(\hat{Y}_1|X_1, Y) - H(Y|X, X_1) - H(\hat{Y}_1|X, X_1, Y) \\ &= I(X, X_1; Y) - I(X_1; Y) + I(\hat{Y}_1; X|X_1, Y) \\ &\stackrel{(a)}{\leq} I(X, X_1; Y) - I(Y_1; \hat{Y}_1|X_1, Y) + I(\hat{Y}_1; X|X_1, Y) \\ &= I(X, X_1; Y) + H(\hat{Y}_1|X_1, Y_1, Y) - H(\hat{Y}_1|X_1, X, Y) \\ &= I(X, X_1; Y) + H(\hat{Y}_1|X_1, X, Y_1, Y) - H(\hat{Y}_1|X_1, X, Y) \\ &= I(X, X_1; Y) - I(Y_1; \hat{Y}_1|X, X_1, Y), \end{aligned}$$

where (a) follows from the constraint in the expression of R_2

- To show that $R_1 \leq R_2$, first note that this is the case if at the optimum, $I(X; Y, \hat{Y}_1|X_1) \leq I(X, X_1; Y) - I(Y_1; \hat{Y}_1|X, X_1, Y)$

Now assume that at the optimum, $I(X; Y, \hat{Y}_1|X_1) > I(X, X_1; Y) - I(Y_1; \hat{Y}_1|X, X_1, Y)$. We show that higher rate can be achieved. Fix $p(x)p(x_1)$ and let $\hat{Y}'_1 = \hat{Y}_1$ w.p. p and $\hat{Y}'_1 = \emptyset$ w.p. $(1-p)$

Then $\hat{Y}'_1 \rightarrow \hat{Y}_1 \rightarrow (Y_1, X_1)$ form a Markov chain. Note that the two mutual information terms are continuous in p and that as p increases, the first term decreases and the second increases. Thus there exists a p^* such that

$$I(X; Y, \hat{Y}'_1|X_1) = I(X, X_1; Y) - I(Y_1; \hat{Y}'_1|X, X_1, Y)$$

and the rate using $p(\hat{y}'_1|y_1, x_1)$ is larger than that using $p(\hat{y}_1|y_1, x_1)$

By the above argument, at the optimum joint pmf,

$$I(X, X_1; Y) - I(Y_1; \hat{Y}_1|X, X_1, Y) = I(X; Y, \hat{Y}_1|X_1)$$

Thus

$$\begin{aligned} I(X_1; Y) &= I(X; Y, \hat{Y}_1|X_1) + I(Y_1; \hat{Y}_1|X, X_1, Y) - I(X; Y|X_1) \\ &= I(X; \hat{Y}_1|X_1, Y) + I(Y_1; \hat{Y}_1|X, X_1, Y) \\ &= H(\hat{Y}_1|X_1, Y) - H(\hat{Y}_1|X, X_1, Y, Y_1) \\ &= H(\hat{Y}_1|X_1, Y) - H(\hat{Y}_1|X_1, Y, Y_1) = I(Y_1; \hat{Y}_1|X_1, Y) \end{aligned}$$

Lecture Notes 18

Interactive Communication

- Capacity of DMC with Feedback
- Iterative Refinement
- Multiple Access Channel with Feedback
- Broadcast Channel with Feedback
- Relay Channel with Feedback
- Two-Way Channel
- Massey's Directed Information
- Key New Ideas and Techniques

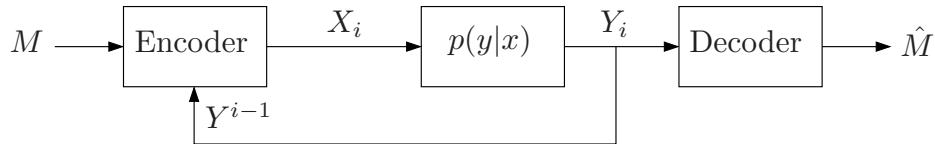
© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Introduction

- So far, we have discussed one-way communication only. Many communication systems are inherently two-way, allowing for cooperation through feedback and interactive exchange of information between nodes
- In this lecture notes, we study the effect of feedback on the capacity of single-hop channels and then present results on the two-way channel, which was introduced by Shannon [1] as the first multiple-user network model

Capacity of DMC with Feedback

- Consider a DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ with noiseless causal feedback



Recall that the memoryless property is defined as $p(y_i|x^i, y^{i-1}) = p_{Y|X}(y_i|x_i)$ for $i \in [1 : n]$

- A $(2^{nR}, n)$ feedback code for the DMC consists of
 - a message set $[1 : 2^{nR}]$
 - an encoder that assigns a symbol $x_i(m, y^{i-1})$ to each message $m \in [1 : 2^{nR}]$ and received sequence $y^{i-1} \in \mathcal{Y}^{i-1}$ for $i \in [1 : n]$
 - a decoder that assigns a message $\hat{m} \in [1 : 2^{nR}]$ or an error message e to each received sequence y^n
- We assume that the message M is uniformly distributed over $[1 : 2^{nR}]$

- Average probability of error, achievability, and capacity are defined as in the nonfeedback case
- Shannon [2] showed that feedback does not increase the capacity of a DMC
- Theorem 1:* The capacity of the DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ with noiseless causal feedback is

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

- Proof: We only need to prove the converse. Note that by the memoryless property, $(M, Y^{i-1}) \rightarrow X_i \rightarrow Y_i$ form a Markov chain for all $i \in [1 : n]$. Hence, the proof of converse in Lecture Notes 3 holds for the DMC with feedback
- Nonetheless, feedback can help communication in several important ways
 - Feedback can greatly simplify coding and improve its performance [3, 4, 5]
 - Feedback can increase the capacity of channels with memory, e.g., [6]
 - Feedback can enlarge the capacity region of DM multiple user channels, e.g., [7, 8]
- Study of feedback also gives insights on the fundamental limit of two-way communication

Iterative Refinement

- Consider a BEC with erasure probability p . Without feedback, we need to use block error correcting codes to approach the channel capacity $C = (1 - p)$ bits/transmission. With feedback, however, we can achieve capacity by simply retransmitting each bit immediately after it is erased. It can be shown that roughly $n = k/(1 - p)$ transmissions suffice to send k bits of information reliably. Thus, with feedback there is no need for sophisticated error correcting codes
- This simple observation can be extended to other channels with feedback. The basic idea is to first send a message at a higher rate than channel capacity, and then to iteratively refine the receiver's knowledge about the message
- We discuss this general paradigm of feedback communication through three key examples

Schalkwijk–Kailath Coding for the AWGN Channel

- Consider an AWGN channel with noiseless causal feedback, where the channel output at time i is $Y_i = X_i + Z_i$, and the noise $\{Z_i\}$ is a WGN(1) process. Assume the *expected* average transmitted power constraint

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

We present a simple coding scheme by Schalkwijk and Kailath [3, 4] that achieves any rate $R < C(P)$

- Codebook: Divide the interval $[-1, 1]$ into 2^{nR} equal-length “message intervals.” Represent each message $m \in [1 : 2^{nR}]$ by the midpoint $\theta(m)$ of its interval with distance $\Delta = 2 \cdot 2^{-nR}$ between neighboring message points
- Encoding and decoding: To simplify notation, we assume that the transmission commences at time $i = 0$. To send message m :
 - Initial transmission: At time $i = 0$, the encoder transmits $X_0 = \theta(m)$, so $Y_0 = \theta(m) + Z_0$. Because of the feedback of Y_0 , the encoder can learn the noise $Z_0 = Y_0 - X_0$

- At time $i = 1$, the encoder transmits $X_1 = \gamma_1 Z_0$, where $\gamma_1 = \sqrt{P}$ is chosen such that $E(X_1^2) = P$
- At time $i \in [2 : n]$, the encoder forms the minimum mean squared error (MMSE) estimate $E(Z_0|Y^{i-1})$ of Z_0 given $Y^{i-1} = (Y_1, \dots, Y_{i-1})$, and transmits

$$X_i = \gamma_i (Z_0 - E(Z_0|Y^{i-1})),$$

where γ_i is chosen such that $E(X_i^2) = P$ for each i . So $Y_i \sim N(0, P + 1)$ for all $i \in [1 : n]$

- The total (expected) power consumption over $n + 1$ transmissions is upper bounded by

$$\sum_{i=0}^n E(X_i^2) \leq 1 + nP$$

- Finally at time n , the receiver estimates $\theta(m)$ by

$$\hat{\theta}_n := Y_0 - E(Z_0|Y^n) = \theta(m) + Z_0 - E(Z_0|Y^n)$$

and declares \hat{m} is sent if $\theta(\hat{m})$ is the closest message point to $\hat{\theta}_n$

- Analysis of the probability of error: Since Z_0 and Z_1 are independent and Gaussian, and $Y_1 = \gamma_1 Z_0 + Z_1$, it follows that $E(Z_0|Y_1)$ is linear in Y_1 . Thus by orthogonality, $X_2 = \gamma_2 (Z_0 - E(Z_0|Y_1))$ is Gaussian and independent of Y_1 . Since Z_2 is Gaussian and independent of (Y_1, X_2) , $Y_2 = X_2 + Z_2$ is also Gaussian and independent of Y_1

In general, for $i \geq 1$, $E(Z_0|Y^{i-1})$ is linear in Y^{i-1} , and Y_i is Gaussian and independent of Y^{i-1} . Thus the output sequence Y^n is i.i.d. with

$$Y_i \sim N(0, P + 1)$$

Now consider $I(Z_0; Y^n)$. On one hand,

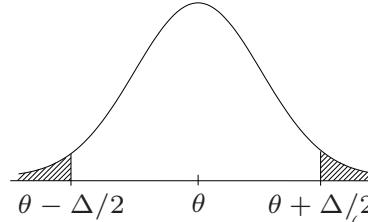
$$\begin{aligned} I(Z_0; Y^n) &= \sum_{i=1}^n I(Z_0; Y_i | Y^{i-1}) \\ &= \sum_{i=1}^n (h(Y_i | Y^{i-1}) - h(Y_i | Z_0, Y^{i-1})) \\ &= \sum_{i=1}^n (h(Y_i) - h(Z_i | Z_0, Y^{i-1})) \\ &= \sum_{i=1}^n (h(Y_i) - h(Z_i)) = \frac{n}{2} \log(1 + P) = n C(P) \end{aligned}$$

On the other hand, we have

$$I(Z_0; Y^n) = h(Z_0) - h(Z_0|Y^n) = \frac{1}{2} \log \frac{1}{\text{Var}(Z_0|Y^n)}$$

Thus, $\text{Var}(Z_0|Y^n) = 2^{-2nC(P)}$ and $\hat{\theta}_n \sim N(\theta, 2^{-2nC(P)})$

It is easy to see that decoding error occurs only if $\hat{\theta}_n$ is closer to the nearest neighbors of θ than to θ , that is, if $|\theta - \hat{\theta}_n| > \Delta/2 = 2^{-nR}$



The probability of error is thus upper bounded as $P_e^{(n)} \leq 2Q(2^{n(C(P)-R)})$, where

$$Q(x) := \int_x^\infty \frac{1}{\sqrt{2\pi}} e^{-t^2/2} dt \leq e^{-x^2/2} \text{ for } x \geq 0$$

Therefore, if $R < C(P)$, we have

$$P_e^{(n)} \leq 2 \exp\left(-\frac{2^{2n(C(P)-R)}}{2}\right),$$

that is, the probability of error decays double-exponentially fast in block size n !

- Remarks:

- At each transmission i , the Schalkwijk–Kailath encoding $X_i = \gamma_i(Z_0 - E(Z_0|Y^{i-1}))$ can be interpreted as adjusting the receiver's knowledge about the initial noise Z_0 (or equivalently the message $\theta(m)$) at the given moment. The encoding can be alternatively expressed as

$$\begin{aligned} X_i &= \gamma_i(Z_0 - E(Z_0|Y^{i-1})) \\ &= \gamma_i(Z_0 - E(Z_0|Y^{i-2}) + E(Z_0|Y^{i-2}) - E(Z_0|Y^{i-1})) \\ &= \frac{\gamma_i}{\gamma_{i-1}}(X_{i-1} - E(X_{i-1}|Y^{i-1})) \\ &= \frac{\gamma_i}{\gamma_{i-1}}(X_{i-1} - E(X_{i-1}|Y_{i-1})) \end{aligned}$$

Thus the sender iteratively corrects the receiver's error in estimating the previous transmission

- Consider the channel with input X_1 and output $\hat{X}_1(Y^n) = E(X_1|Y^n)$. Because the MMSE estimate $\hat{X}_1(Y^n)$ is a linear function of X_1 and Z^n with $I(X_1; \hat{X}_1) = nC(P)$ for Gaussian X_1 , the channel from \hat{X}_1 to X_1 is equivalent to an AWGN channel with effective SNR $2^{2nC(P)} - 1$ (independent of the specific input distribution on X_1). Hence the Schalkwijk–Kailath coding transforms n uses of the AWGN channel with SNR P into a single use

of the channel with SNR $2^{2nC(P)} - 1$. Thus to achieve the capacity, the sender can transmit $X_1 = \theta(m)$ directly without any initial transmission and iterations on Z_0

- Another implication of the linearity of the Schalkwijk–Kaliath coding is that it can be used as is when the additive noise is not Gaussian. In this case, by Chebychev's inequality, $P_e^{(n)} \leq P\{|\theta - \hat{\theta}_n| > 2^{-2nR}\} \leq 2^{-2n(C(P)-R)}$, which $\rightarrow 0$ as $n \rightarrow \infty$ if $R < C(P)$
- The Schalkwijk–Kailath coding has been generalized to AWGN-MAC and AWGN-BC with feedback (as will be discussed shortly), and additive colored Gaussian noise channels with feedback [9, 10]
- The doubly exponential decay of error probability depends crucially on the expected power constraint $\sum_{i=1}^n E(x_i^2(m, Y^{i-1})) \leq nP$. Under the more stringent power constraint $P\{\sum_{i=1}^n x_i^2(m, Y^{i-1}) \leq nP\} = 1$ assumed in the nonfeedback case, the doubly exponential decay is no longer achievable [11, 12], although the Schalkwijk–Kailath coding can be still used with a slight modification [13] to provide a simple constructive coding scheme

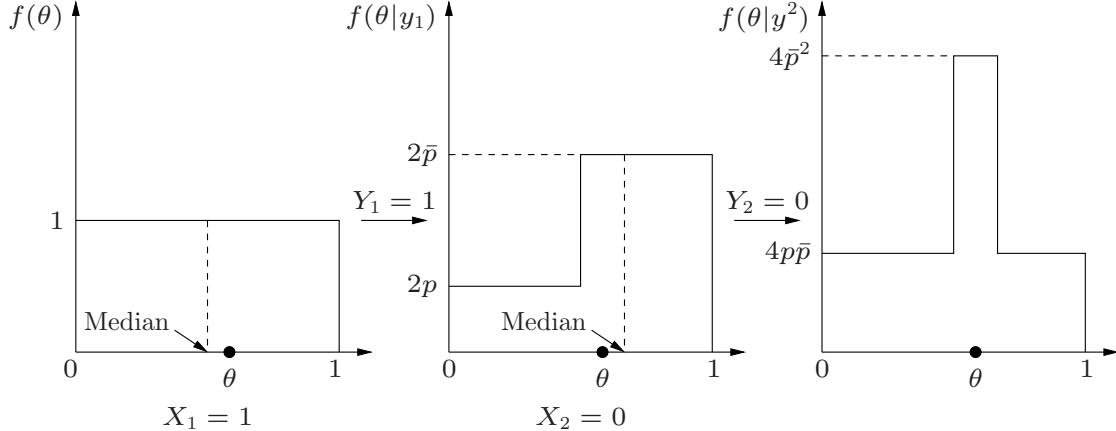
Horstein Coding for the BSC

- Consider a BSC(p), where the channel output at time i is $Y_i = X_i \oplus Z_i$ and the noise $\{Z_i\}$ is a Bern(p) process. We present a simple coding scheme by Horstein [14] that achieves any rate $R < 1 - H(p)$ [15]
- Codebook: Represent each message $m \in [1 : 2^{nR}]$ by one of 2^{nR} equidistance points $\theta(m) = \alpha + (m - 1)2^{-nR} \in [0, 1]$, where the offset $\alpha \in [0, 2^{-nR})$ is to be specified later
- Encoding: We define the encoding map for every $\theta_0 \in [0, 1]$ (not only message points). For each $\theta \in [0, 1]$ and pdf f on $[0, 1]$, define $\phi(\theta, f) := 1$ if θ is greater than the median of f , and 0, otherwise
 - Let $f_0 = f(\theta)$ be the uniform pdf (prior) on $[0, 1]$ (i.e., $\Theta \sim \text{Unif}[0, 1]$). The encoder transmits $x_1 = 1$ if $\theta_0 > 1/2$, and $x_1 = 0$, otherwise. In other words, $x_1 = \phi(\theta_0, f_0)$
 - At time $i \in [2 : n]$, upon receiving $Y^{i-1} = y^{i-1}$, the encoder calculates the conditional pdf (posterior)

$$f_{i-1} = f(\theta | y^{i-1}) = \frac{f(\theta) p(y^{i-1} | \theta)}{p(y^{i-1})}$$

$$\begin{aligned}
&= f(\theta|y^{i-2}) \cdot \frac{p(y_{i-1}|y^{i-2}, \theta)}{\int p(y_{i-1}|y^{i-2}, \theta) f(\theta|y^{i-2}) d\theta} \\
&= \begin{cases} 2\bar{p}f_{i-2} & \text{if } y_{i-1} = \phi(\theta, f_{i-2}), \\ 2pf_{i-2} & \text{otherwise} \end{cases}
\end{aligned}$$

The encoder then transmits $x_i = \phi(\theta_0, f_{i-1})$. Note f_{i-1} is a function of y^{i-1}



- Decoding: Upon receiving $Y^n = y^n$, the decoder finds the interval $[\beta, \beta + 2^{-nR}]$ of length 2^{-nR} that maximizes the posterior probability

$$\int_{\beta}^{\beta+2^{-nR}} f(\theta|y^n) d\theta$$

If there is a tie, it chooses the smallest such β . Then it declares that \hat{m} is sent if $\theta(\hat{m}) \in [\beta, \beta + 2^{-nR}]$

- Outline of the analysis of the probability of error: We first consider the average probability of error with $\Theta_0 \sim \text{Unif}[0, 1]$. Note that $X_1 \sim \text{Bern}(1/2)$ and $Y_1 \sim \text{Bern}(1/2)$. Moreover, for every y^{i-1} , we have

$$\begin{aligned}
\mathbb{P}\{X_i = 1 | Y^{i-1} = y^{i-1}\} &= \mathbb{P}\{\Theta_0 > \text{Median}(f_{\Theta|Y^{i-1}}(\cdot | y^{i-1})) \mid Y^{i-1} = y^{i-1}\} \\
&= 1/2
\end{aligned}$$

Thus $X_i \sim \text{Bern}(1/2)$ is independent of Y^{i-1} and hence $Y_i \sim \text{Bern}(1/2)$ is also independent of Y^{i-1} . Therefore

$$I(\Theta_0; Y^n) = H(Y^n) - H(Z^n) = n(1 - H(p)) = nC,$$

which implies that $h(\Theta_0|Y^n) = -nC$. Moreover, by the LLN and the recursive definitions of the encoding maps and conditional pdfs, it can be easily verified that

$$\mathbb{P}\{f_{\Theta|Y^n}(\Theta_0|Y^n) \doteq 2^{nC}\} \rightarrow 1$$

as $n \rightarrow \infty$, or more precisely,

$$\frac{1}{n} \log f_{\Theta|Y^n}(\Theta_0|Y^n) \rightarrow C \text{ in probability}$$

These two facts strongly suggest (albeit not prove) that the probability of error, $P\{\Theta_0 \notin [\beta, \beta + 2^{-nR}]\} \rightarrow 0$ as $n \rightarrow \infty$, if $R < C$. By a more refined analysis of the evolution of $f_{\Theta|Y^i}(\Theta_0|Y^i)$, $i \in [1 : n]$, based on iterated function systems, it can be shown [15] that indeed the probability of error $E_\Theta(P\{\Theta \notin [\beta, \beta + 2^{-nR}]\}|\Theta) \rightarrow 0$ as $n \rightarrow \infty$ if $R < C$

Therefore, there must exist an $\alpha_n \in [0, 2^{-nR}]$ such that

$$P_e^{(n)} = \frac{1}{2^{nR}} \sum_{m=1}^{2^{nR}} P\{\Theta \notin [\beta, \beta + 2^{-nR}] | \Theta = \alpha_n + (m-1)2^{-nR}\} \rightarrow 0$$

as $n \rightarrow \infty$, if $R < C$. Thus with high probability, Θ is the unique message point within the $[\beta, \beta + 2^{-nR}]$ interval. This completes the outline of the proof of achievability

- The Horstein coding is a special case of a more general posterior matching coding scheme by Shayevitz and Feder [15], which can be applied to any DMC. It can be also shown that the posterior matching scheme includes the Schalkwijk–Kailath coding as a special case. In this coding scheme, to send a

message point $\theta_0 \in [0, 1]$, the encoder at time i transmits

$$X_i = F_X^{-1}(F_{\Theta|Y^{i-1}}(\theta_0|Y^{i-1})),$$

where $F_X^{-1}(u) = \inf\{x : F(x) \geq u\}$ denotes the inverse of the capacity-achieving input cdf $F(x)$ and the iteration begins with the uniform prior on Θ . Note that $X_i \sim F_X(x_i)$ is independent of Y^{i-1}

Letting $U_i(\theta_0, Y^{i-1}) := F_{\Theta|Y^{i-1}}(\theta_0|Y^{i-1})$, the coding scheme can be expressed recursively as

$$\begin{aligned} U_i &= F_{U|Y}(U_{i-1}|Y_{i-1}), \\ X_i &= F_X^{-1}(U_i), \end{aligned}$$

where $F_{U|Y}(u|y)$ is the backward channel cdf corresponding to $U \sim \text{Unif}[0, 1]$, $X = F_X^{-1}(U)$, $Y|X=x \sim p(y|x)$. Thus $\{(U_i, Y_i)\}$ is a Markov process

Using the Markovity of $\{(U_i, Y_i)\}$ and iterated function systems, it can be shown [15] that the same maximal-probability interval decoding achieves the capacity of a DMC under a certain relabeling of \mathcal{X} (which determines the shape of F_X^{-1})

Block Feedback Coding for the BSC

- In the previous two coding schemes, the encoder sends a large (undecodable) amount of uncoded information in the initial few transmissions and then iteratively refines the receiver's knowledge in subsequent transmissions

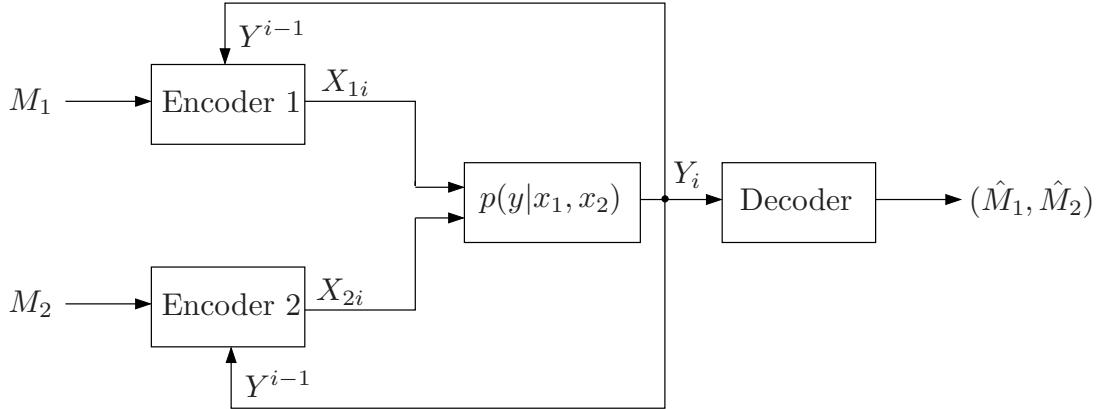
Here we present a coding scheme that implements iterative refinement at the block level rather than the transmission level. In this coding scheme, the encoder initially transmits an uncoded *block* of information and then refines the receiver's knowledge of it in subsequent blocks

- Again consider a $BSC(p)$, where the channel output at time i is $Y_i = X_i \oplus Z_i$ and the noise $\{Z_i\}$ is a $Bern(p)$ process
- Codebook generation and encoding:
 - To send message $m \in [1 : 2^n]$, the encoder first transmits the binary representation $\mathbf{X}_1 = X^n(m)$ of the message m
 - Upon receiving the feedback signal \mathbf{Y}_1 , the encoder compresses $\mathbf{Z}_1 = \mathbf{X}_1 \oplus \mathbf{Y}_1$ losslessly and transmits the index $\mathbf{X}_2(\mathbf{Z}_1)$ over the next $n(H(p) + \delta(\epsilon))$ transmissions

- Upon receiving the resulting feedback signal \mathbf{Y}_2 , the encoder transmits the corresponding noise index $\mathbf{X}_3(\mathbf{Z}_2)$ over the next $n(H(p) + \delta(\epsilon))^2$ transmissions
- Continuing in the same manner, in the j -th block, the encoder transmits the noise index $\mathbf{X}_j(\mathbf{Z}_{j-1})$ over $n(H(p) + \delta(\epsilon))^{j-1}$ transmissions
- After k_1 such unequal-length block transmissions, the encoder transmits the index of \mathbf{Z}_{k_1} over $n(H(p) + \delta(\epsilon))^{k_1-1} \cdot k_2$ transmissions using repetition coding (i.e., transmits the noise index k_2 times without any coding)
- The rate of this code is $1/(\sum_{j=1}^{k_1} (H(p) + \delta(\epsilon))^{j-1} + (H(p) + \delta(\epsilon))^{k_1} \cdot k_2)$
- Decoding and the analysis of the probability of error: Decoding is performed backwards. The decoder first finds \mathbf{Z}_{k_1} (by the majority decoding rule), then \mathbf{Z}_{k_1-1} through $\mathbf{X}(\mathbf{Z}_{k_1-1}) = \mathbf{Y}_{k_1} \oplus \mathbf{Z}_{k_1}$, then \mathbf{Z}_{k_1-2} , and so on, until \mathbf{Z}_1 is decoded. The message is finally decoded through $\mathbf{X}_1(m) = \mathbf{Y}_1 \oplus \mathbf{Z}_1$
By choosing $k_1 = \log(n/\log n)$ and $k_2 = \log^2 n$, it can be shown (check!) that the probability of error over all transmission blocks $\rightarrow 0$ while the achieved rate approaches $1/(\sum_{j=1}^{\infty} (H(p) + \delta(\epsilon))^{j-1}) = 1 - H(p) - \delta(\epsilon)$ as $n \rightarrow \infty$
- This simple coding scheme is originally due to Weldon [16] and has been extended to arbitrary DMCs [17, 5]

Multiple Access Channel with Feedback

- Consider a DM-MAC with noiseless causal feedback to both senders. The code is defined by two message sets $[1 : 2^{nR_j}]$, $j = 1, 2$, two encoders $x_{ji}(M_j, Y^{i-1})$ for $j = 1, 2$ and $i \in [1 : n]$, and a decoder $\hat{m}(y^n)$. The probability of error, achievability, and capacity region are defined as before



- Feedback can enlarge the capacity region (by creating cooperation between senders)

- Capacity region with feedback is not known in general
- Capacity region with feedback is known for 2-sender AWGN-MAC [8]
- Cooperative outer bound: Any achievable rate pair (R_1, R_2) for the DM-MAC with feedback must satisfy the conditions

$$\begin{aligned} R_1 &\leq I(X_1; Y|X_2), \\ R_2 &\leq I(X_2; Y|X_1), \\ R_1 + R_2 &\leq I(X_1, X_2; Y) \end{aligned}$$

for some $p(x_1, x_2)$

To prove this outer bound, note that by the memoryless property, $(M_1, M_2, Y^{i-1}) \rightarrow (X_{1i}, X_{2i}) \rightarrow Y_i$ form a Markov chain. Hence, as in the proof of converse for the DM-MAC without feedback in Lecture Notes 4, the following conditions continue to hold

$$\begin{aligned} R_1 &\leq I(X_{1Q}; Y_Q | X_{2Q}, Q), \\ R_2 &\leq I(X_{2Q}; Y_Q | X_{1Q}, Q), \\ R_1 + R_2 &\leq I(X_{1Q}, X_{2Q}; Y_Q, Q) \end{aligned}$$

Now, since $Q \rightarrow (X_{1Q}, X_{2Q}) \rightarrow Y_Q$ form a Markov chain, the above inequalities can be further relaxed to

$$\begin{aligned} R_1 &\leq I(X_{1Q}; Y_Q | X_{2Q}), \\ R_2 &\leq I(X_{2Q}; Y_Q | X_{1Q}), \\ R_1 + R_2 &\leq I(X_{1Q}, X_{2Q}; Y_Q) \end{aligned}$$

Identifying $X_1 := X_{1Q}$, $X_2 := X_{2Q}$, and $Y := Y_Q$ completes the proof

Note that unlike the nonfeedback case X_1 and X_2 are no longer conditionally independent given Q . Hence, the outer bound is evaluated over all joint pmfs $p(x_1, x_2)$

- Later we find constraints on the set of joint pmfs that can be induced between X_1 and X_2 through feedback, which yield a tighter outer bound in general

Cover–Leung Inner Bound

- *Theorem 2 (Cover–Leung Inner Bound)* [18]: A rate pair (R_1, R_2) is achievable for a DM-MAC with feedback if it satisfies the conditions

$$R_1 < I(X_1; Y | X_2, U),$$

$$R_2 < I(X_2; Y | X_1, U),$$

$$R_1 + R_2 < I(X_1, X_2; Y)$$

for some $p(u)p(x_1|u)p(x_2|u)$, where $|\mathcal{U}| \leq \min\{|\mathcal{X}_1| \cdot |\mathcal{X}_2| + 1, |\mathcal{Y}| + 2\}$

- This region is convex and has a very similar form to the nonfeedback capacity region given by the set of (R_1, R_2) pairs satisfying

$$R_1 \leq I(X_1; Y | X_2, Q),$$

$$R_2 \leq I(X_2; Y | X_1, Q),$$

$$R_1 + R_2 \leq I(X_1, X_2; Y | Q)$$

for some $p(q)p(x_1|q)p(x_2|q)$, where $|\mathcal{Q}| \leq 2$. In fact, the only difference comes from the conditioning in the sum-rate bound

- This region was shown to be optimal for the class of DM-MAC for which X_1 is a deterministic function of (X_2, Y) [19]. However, it is not optimal in general

Example: Binary Erasure MAC

- Consider the binary erasure DM-MAC discussed in Lecture Notes 4, in which the channel input symbols X_1, X_2 are binary and the channel output symbol $Y = X_1 + X_2$ is ternary
- We know that the capacity region without feedback is given by

$$\begin{aligned}R_1 &\leq 1, \\R_2 &\leq 1, \\R_1 + R_2 &\leq 3/2\end{aligned}$$

- First we show that this region can be achieved by a simple feedback coding scheme reminiscent of Weldon's coding. We focus on the symmetric rate pair $R_1 = R_2 = R$

Suppose each encoder sends k independent bits uncoded. Then roughly $k/2$ bits are erased (i.e., $Y = 0 + 1 = 1 + 0 = 1$ is received). Since encoder 1 knows the exact locations of the erasures through feedback, it can retransmit the erased bits over the next $k/2$ transmissions (while encoder 2 sends $X_2 = 0$). The decoder now can decode both messages. Since k bits are sent over $k + k/2$ transmissions, the rate $R = 2/3$ is achievable

Since encoder 2 also knows the $k/2$ erased bits for encoder 1 through feedback, the two encoders can cooperate by each sending half of the $k/2$ erased bits over the following $k/4$ transmissions. These retransmissions result in roughly $k/8$ erased bits, which can be retransmitted again over the following $k/16$ transmissions, and so on. Proceeding recursively, we can achieve a rate arbitrarily close to $k/(k + k/4 + k/16 + \dots) = 3/4$

- The above coding scheme can be improved by inducing further cooperation between the encoders [7]. Again suppose k independent bits are sent initially. Since both encoders know the $k/2$ erased bits, they can cooperate to send them over the next $(k/2)/\log 3$ transmissions. Hence we can achieve the rate $R = k/(k + k/\log 9) = 0.7602 > 3/4$!
- Now evaluating the Cover–Leung inner bound with $U \sim \text{Bern}(1/2)$ and $X_j = U \oplus V_j, j = 1, 2$, where $V_j \sim \text{Bern}(0.2377)$ and U, V_1, V_2 are independent of each other, we can achieve $R = 0.7911$

This rate can be shown to be optimal [19]

Proof of Achievability [20]

- The proof of achievability involves superposition coding, block Markov coding, and backward decoding

- We consider b blocks, each consisting of n transmissions

A sequence of $b - 1$ i.i.d. message pairs $(M_{1j}, M_{2j}) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$, $j \in [1 : b - 1]$, is sent over nb transmissions

At the end of block $j - 1$, sender 1 decodes $M_{2,j-1}$ and then in block j both senders cooperatively transmit information to the receiver (carried by U) to resolve the remaining uncertainty about $M_{2,j-1}$, superimposed with information about the new messages (M_{1j}, M_{2j})

- Codebook generation: Fix $p(u)p(x_1|u)p(x_2|u)$. As in block Markov coding for the relay channel, we randomly and independently generate a codebook for each block

For $j \in [1 : b]$, randomly and independently generate 2^{nR_2} sequences $u^n(m_{2,j-1})$, $m_{2,j-1} \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_U(u_i)$

For each $u^n(m_{2,j-1})$, randomly and conditionally independently generate 2^{nR_1} sequences $x_1^n(m_{1j}|m_{2,j-1})$, $m_{1j} \in [1, 2^{nR_1}]$, each according to

$\prod_{i=1}^n p_{X_1|U}(x_{1i}|u_i)$, and 2^{nR_2} sequences $x_2^n(m_{2j}|m_{2,j-1})$, $m_{2j} \in [1, 2^{nR_2}]$, each according to $\prod_{i=1}^n p_{X_2|U}(x_{2i}|u_i)$

- Encoding and decoding are explained with the help of the following table

Block	1	2	...	$b - 1$	b
X_1 (X_1, Y)	$x_1^n(m_{11} 1)$ $\tilde{m}_{21} \rightarrow$	$x_1^n(m_{12} \tilde{m}_{21})$ $\tilde{m}_{22} \rightarrow$...	$x_1^n(m_{1,b-1} \tilde{m}_{2,b-2})$ $\tilde{m}_{2,b-1} \rightarrow$	$x_1^n(m_{1b} \tilde{m}_{2,b-1})$
X_2	$x_2^n(m_{21} 1)$	$x_2^n(m_{22} m_{21})$...	$x_2^n(m_{2,b-1} m_{2,b-2})$	$x_2^n(1 m_{2,b-1})$
Y	\hat{m}_{11}, \emptyset	$\leftarrow \hat{m}_{12}, \hat{m}_{21}$...	$\leftarrow \hat{m}_{1,b-1}, \hat{m}_{2,b-2}$	$\leftarrow \hat{m}_{1b}, \hat{m}_{2,b-1}$

- Encoding: Encoder 2 transmits $x_2^n(m_{2j}|m_{2,j-1})$ in block j

At the end of block $j - 1$, encoder 1 has an estimate $\tilde{m}_{2,j-1}$ of the message $m_{2,j-1}$. In block j , encoder 1 transmits $x_1^n(m_{1j}|\tilde{m}_{2,j-1})$

- Decoding and analysis of the probability of error:

1. Based on $y^n(j)$, encoder 1 finds the unique message \tilde{m}_{2j} such that $(u^n(\tilde{m}_{2,j-1}), x_1^n(m_{1j}|\tilde{m}_{2,j-1}), x_2^n(\tilde{m}_{2j}|\tilde{m}_{2,j-1}), y^n(j)) \in \mathcal{T}_\epsilon^{(n)}$

Following steps similar to the analysis of the coherent multi-hop coding scheme in Lecture Notes 17, by the independence of the codebook, the LLN,

the packing lemma, and induction, $\mathbb{P}\{\tilde{M}_{2j} \neq M_{2j}\} \rightarrow 0$ as $n \rightarrow \infty$ for all $j \in [1 : b - 1]$, if $R_2 < I(X_2; Y|X_1|U) - \delta(\epsilon) = I(X_2; Y|X_1, U) - \delta(\epsilon)$

2. Decoding at the receiver is done successively backwards after all blocks are received

Based on the received signal $y^n(j)$, the decoder finds the unique message pair $(\hat{m}_{1j}, \hat{m}_{2,j-1})$ such that

$$(u^n(\hat{m}_{2,j-1}), x_1^n(\hat{m}_{1j}|\hat{m}_{2,j-1}), x_2^n(\hat{m}_{2j}|\hat{m}_{2,j-1}), y^n(j)) \in \mathcal{T}_\epsilon^{(n)}$$

Following steps similar to the analysis of backward decoding for decode-forward in Lecture Notes 17, by the independence of the codebook, the LLN, the packing lemma, and induction,

$\mathbb{P}\{(\hat{M}_{1j}, \hat{M}_{2,j-1}) \neq (M_{1j}, M_{2,j-1})\} \rightarrow 0$ for all $j \in [1 : b]$, as $n \rightarrow \infty$ if

$R_1 < I(X_1; Y|X_2, U) - \delta(\epsilon)$ and

$$R_1 + R_2 < I(U, X_1, X_2; Y) - \delta(\epsilon) = I(X_1, X_2; Y) - \delta(\epsilon)$$

- Remark: The above coding scheme uses only one-sided feedback. Therefore, it is not surprising that the corresponding region is suboptimal in general

AWGN-MAC with Feedback

- Consider the AWGN-MAC $Y_i = g_1 X_{1i} + g_2 X_{2i} + Z_i$ with expected average power P on each transmitter (as defined for the AWGN channel)

For the AWGN-MAC with feedback, the Cover–Leung theorem yields the achievable rate region consisting of all (R_1, R_2) such that

$$R_1 \leq C(\bar{\alpha}_1 S_1),$$

$$R_2 \leq C(\bar{\alpha}_2 S_2),$$

$$R_1 + R_2 \leq C\left(S_1 + S_2 + 2\sqrt{\alpha_1 \alpha_2 S_1 S_2}\right)$$

for some $0 \leq \alpha_1, \alpha_2 \leq 1$, where $S_1 = g_1^2 P$ and $S_2 = g_2^2 P$

- Achievability follows by setting $U \sim N(0, 1)$, $X_1 = \sqrt{\alpha_1 P} U + X'_1$, and $X_2 = \sqrt{\alpha_2 P} U + X'_2$, where $X'_1 \sim N(0, \bar{\alpha}_1 P)$, $X'_2 \sim N(0, \bar{\alpha}_2 P)$, and U, X'_1, X'_2 are independent

- This region turned out to be strictly suboptimal

- *Theorem 3 [8]:* The capacity region of the AWGN-MAC with feedback is the set of (R_1, R_2) such that

$$\begin{aligned} R_1 &\leq C((1 - \rho^2)S_1), \\ R_2 &\leq C((1 - \rho^2)S_2), \\ R_1 + R_2 &\leq C(S_1 + S_2 + 2\rho\sqrt{S_1S_2}) \end{aligned}$$

for some $0 \leq \rho \leq 1$

- The converse is quite straightforward. It follows by evaluating the general cooperative outer bound. For the AWGN-MAC, it suffices to consider zero mean jointly Gaussian (X_1, X_2) with equal average power P and correlation coefficient ρ , which yields the capacity region

Proof of Achievability

- Achievability is proved using an interesting extension of the Schalkwijk–Kailath coding scheme

We show that the maximum sum rate

$$\max_{0 \leq \rho \leq 1} \min\{C((1 - \rho^2)S_1) + C((1 - \rho^2)S_2), C(S_1 + S_2 + 2\rho\sqrt{S_1S_2})\}$$

is achievable. Since the first term in the minimum decreases with ρ while the second term increases with ρ , the maximum is achieved by a unique $\rho^* \in (0, 1)$ such that

$$C((1 - (\rho^*)^2)S_1) + C((1 - (\rho^*)^2)S_2) = C(S_1 + S_2 + 2\rho^*\sqrt{S_1S_2})$$

This corresponds to

$$\begin{aligned} R_1 &= I(X_1; Y) = I(X_1; Y|X_2), \\ R_2 &= I(X_2; Y) = I(X_2; Y|X_1) \end{aligned}$$

for jointly Gaussian X_1, X_2 with zero mean, equal power P , and correlation coefficient ρ^*

For simplicity of exposition, we consider the symmetric case $g_1 = g_2 = g$, i.e., $S_1 = S_2 = S = g^2P$; the general case follows similarly (check!)

- Codebook: As in the Schalkwijk–Kailath coding for the AWGN channel with feedback, divide the interval $[-1, 1]$ into 2^{nR_1} message intervals and 2^{nR_2} message intervals. For $j = 1, 2$, represent each message $m_j \in [1 : 2^{nR_j}]$ by a midpoint $\theta_j(m_j)$ of an interval with distance $\Delta_j = 2 \cdot 2^{-nR_j}$ between neighboring messages
- Encoding and decoding: To send the message pair (m_1, m_2) , in the initial 3 transmissions, the encoders transmit

$$\begin{aligned} X_{1,-2} &= 0, & X_{2,-2} &= \theta_2(m_2), \\ X_{1,-1} &= \theta_1(m_1), & X_{2,-1} &= 0, \\ X_{1,0} &= 0, & X_{2,0} &= 0 \end{aligned}$$

From the noiseless feedback, encoder 1 knows the initial noise values (Z_{-1}, Z_0) and encoder 2 knows (Z_{-2}, Z_0) . For appropriately chosen $\lambda > 0$, let $U_1 = Z_{-1} + \lambda Z_0$ and $U_2 = Z_{-2} + \lambda Z_0$ be jointly Gaussian with zero mean, equal average powers, and correlation coefficient ρ^*

At time $i = 1$, the encoders transmit $X_{11} = \gamma_1 U_1$ and $X_{21} = \gamma_1 U_2$, respectively, where γ_1 is chosen such that $E(X_{11}^2) = E(X_{21}^2) = P$

For time $i \geq 2$, the encoders transmit

$$\begin{aligned} X_{1i} &= \gamma_i(X_{1,i-1} - E(X_{1,i-1}|Y_{i-1})), \\ X_{2i} &= -\gamma_i(X_{2,i-1} - E(X_{2,i-1}|Y_{i-1})), \end{aligned}$$

where γ_i , $i \in [2 : n]$, is chosen such that $E(X_{1i}^2) = E(X_{2i}^2) = P$ for each i . Such γ_i exists since the “errors” $(X_{1i} - E(X_{1i}|Y_i))$ and $(X_{2i} - E(X_{2i}|Y_i))$ have the same power. Note that the errors are scaled with opposite signs

The total (expected) power consumption for each sender over the $n + 3$ transmissions is upper bounded by

$$\sum_{i=-2}^n E(X_{ji}^2) \leq 1 + nP \text{ for } j = 1, 2$$

After time n , the decoder estimates $\theta_1(m_1)$ and $\theta_2(m_2)$ as

$$\begin{aligned} \hat{\theta}_{1n}(m_1) &= Y_{-1} + \lambda Y_0 - E(U_1|Y^n) = \theta_1(m_1) + U_1 - E(U_1|Y^n), \\ \hat{\theta}_{2n}(m_2) &= Y_{-2} + \lambda Y_0 - E(U_2|Y^n) = \theta_2(m_2) + U_2 - E(U_2|Y^n) \end{aligned}$$

- Analysis of the probability of error: First note that we can rewrite X_{1i}, X_{2i} as

$$X_{1i} = \gamma'_i(U_1 - \mathbb{E}(U_1|Y^{i-1})),$$

$$X_{2i} = (-1)^{i-1}\gamma'_i(U_2 - \mathbb{E}(U_2|Y^{i-1}))$$

(Recall the first remark after the Schalkwijk–Kailath coding for the AWGN channel)

Hence X_{1i}, X_{2i}, Y_i are independent of Y^{i-1}

Now consider

$$\begin{aligned} I(U_1; Y^n) &= \sum_{i=1}^n I(U_1; Y_i | Y^{i-1}) \\ &= \sum_{i=1}^n h(Y_i) - h(Y_i | U_1, Y^{i-1}) \\ &= \sum_{i=1}^n h(Y_i) - h(Y_i | X_{1i}, Y^{i-1}) \\ &\stackrel{(a)}{=} \sum_{i=1}^n h(Y_i) - h(Y_i | X_{1i}) = \sum_{i=1}^n I(X_{1i}; Y_i), \end{aligned}$$

where (a) follows since X_{1i}, Y_i are independent of Y^{i-1}

We show by induction that

$$I(X_{1i}; Y_i) = C \left(\frac{(1 + \rho^*)^2 S}{(1 - (\rho^*)^2)S + 1} \right) = C((1 - (\rho^*)^2)S) = I(X_{1i}; Y_i | X_{2i})$$

for all i , or equivalently, the correlation coefficient ρ_i between X_{1i} and X_{2i} stays constant as $\rho_i = \rho^*$ for all $i \in [1 : n]$

By construction, $\rho_1 = \rho^*$. For $i \geq 2$, consider

$$\begin{aligned} I(X_{1i}; X_{2i}) &\stackrel{(a)}{=} I(X_{1i}; X_{2i} | Y_{i-1}) \\ &= I(X_{1,i-1}; X_{2,i-1} | Y_{i-1}) \\ &= I(X_{1,i-1}; X_{2,i-1}) + I(X_{1,i-1}; Y_{i-1} | X_{2,i-1}) - I(X_{1,i-1}; Y_{i-1}) \\ &\stackrel{(b)}{=} I(X_{1,i-1}; X_{2,i-1}), \end{aligned}$$

where (a) follows since the pair (X_{1i}, X_{2i}) is independent of Y_{i-1} , (b) follows from the induction hypothesis $I(X_{1,i-1}; Y_{i-1} | X_{2,i-1}) = I(X_{1,i-1}; Y_{i-1})$. Hence, we have $\rho_i^2 = \rho_{i-1}^2$

To show that $\rho_i = \rho_{i-1}$ (same sign), consider

$$\begin{aligned}
I(X_{1i}; X_{1i} + X_{2i}) &= I(X_{1i}; X_{1i} + X_{2i} | Y_{i-1}) \\
&\stackrel{(a)}{=} I(X_{1,i-1}; X_{1,i-1} - X_{2,i-1} | Y_{i-1}) \\
&\stackrel{(b)}{=} I(X_{1,i-1}, Y_{i-1}; X_{1,i-1} - X_{2,i-1}) \\
&= I(X_{1,i-1}; X_{1,i-1} - X_{2,i-1}) + I(X_{2,i-1}; Y_{i-1} | X_{1,i-1}) \\
&> I(X_{1,i-1}; X_{1,i-1} - X_{2,i-1}),
\end{aligned}$$

where (a) follows from the definitions of X_{1i}, X_{2i} and (b) follows because $X_{1,i-1} - X_{2,i-1}$ is independent of Y_{i-1} (why?). Hence we must have $\rho_i \geq 0$, which implies that $\rho_i = \rho_{i-1} = \rho^*$

Therefore,

$$I(U_1; Y^n) = n C((1 - (\rho^*)^2)S),$$

which implies that

$$\hat{\theta}_{1n} - \theta_1 = U_1 - E(U_1 | Y^n) \sim N(0, 2^{-2n C((1 - (\rho^*)^2)S)})$$

Similarly, we have

$$\hat{\theta}_{2n} - \theta_2 = U_2 - E(U_2 | Y^n) \sim N(0, 2^{-2n C((1 - (\rho^*)^2)S)})$$

Hence, as in the Schalkwijk–Kailath coding, $P_e^{(n)} \rightarrow 0$ doubly-exponentially as $n \rightarrow \infty$, if $R_1, R_2 < C((1 - (\rho^*)^2)S)$

- Remarks:

- Since the covariance matrix K_{X_i} of $\mathbf{X} = (X_{1i}, X_{2i})$ is constant over time, the error scaling factor $\gamma_i \equiv \gamma$ is also constant for $i \geq 2$. Let

$$A := \begin{bmatrix} \gamma & 0 \\ 0 & -\gamma \end{bmatrix}, \quad B := [g \ g]$$

and consider

$$\begin{aligned}
X_{1i} &= \gamma(X_{1,i-1} - E(X_{1,i-1} | Y_{i-1})), \\
X_{2i} &= -\gamma(X_{2,i-1} - E(X_{2,i-1} | Y_{i-1}))
\end{aligned}$$

Then K_{X_i} can be expressed recursively (check!) as

$$K_{X_i} = AK_{X_{i-1}}A^T - (AK_{X_{i-1}}B^T)(1 + BK_{X_{i-1}}B^T)^{-1}(AK_{X_{i-1}}B^T)^T$$

Now from the properties of discrete algebraic Riccati equations [21], it can be shown that

$$K_{X_i} \rightarrow K^* = \begin{bmatrix} P & P\rho^* \\ P\rho^* & P \end{bmatrix}$$

as $i \rightarrow \infty$ for any positive definite K_{X_1} . Equivalently,

$$n^{-1}I(X_{11}; Y^n), n^{-1}I(X_{21}; Y^n) \rightarrow C((1 - (\rho^*)^2)S)$$

Thus by the same argument for the Schalkwijk–Kailath coding, this implies that we do not need any initial transmission phase and that we can use the same linear coding for any non-Gaussian additive noise MAC with feedback to achieve the same rate

- The entire capacity region can be achieved by combining rate splitting, superposition coding, and successive cancellation decoding with the above feedback coding scheme [8] as follows:

Encoder 1 splits M_1 into two independent messages M_{10} and M_{11} , and sends M_{10} using a Gaussian random code with power αP_1 and M_{11} using the above feedback coding scheme while treating the codeword for M_{10} as noise. Encoder 2 sends M_2 using the above feedback coding scheme. The decoder first decodes (M_{11}, M_2) as in the above feedback scheme and then decodes M_{10} by successive cancellation decoding

It can be easily shown (check!) that the rate triple (R_{10}, R_{11}, R_2) is achievable if

$$R_{10} < C(\alpha S_1),$$

$$R_{11} < C\left(\frac{(1 - (\rho^*)^2)\bar{\alpha}S_1}{1 + \alpha S_1}\right),$$

$$R_2 < C\left(\frac{(1 - (\rho^*)^2)S_2}{1 + \alpha S_1}\right),$$

where $\rho^* \in [0, 1]$ satisfies

$$C\left(\frac{(1 - (\rho^*)^2)\bar{\alpha}S_1}{1 + \alpha S_1}\right) + C\left(\frac{(1 - (\rho^*)^2)S_2}{1 + \alpha S_1}\right) = C\left(\frac{\bar{\alpha}S_1 + S_2 + 2\rho\sqrt{\bar{\alpha}S_1S_2}}{1 + \alpha S_1}\right)$$

By combining $R_1 = R_{10} + R_{11}$, taking $\rho = \sqrt{\bar{\alpha}}\rho^*$, and varying $\alpha \in [0, 1]$, we can show the achievability of (R_1, R_2) such that

$$R_1 < C((1 - \rho^2)S_1),$$

$$R_2 < C(S_1 + S_2 + 2\rho\sqrt{S_1S_2}) - C((1 - \rho^2)S_2)$$

for all $\rho \leq \rho^*$. By symmetry, we can similarly show the achievability of (R_1, R_2) such that

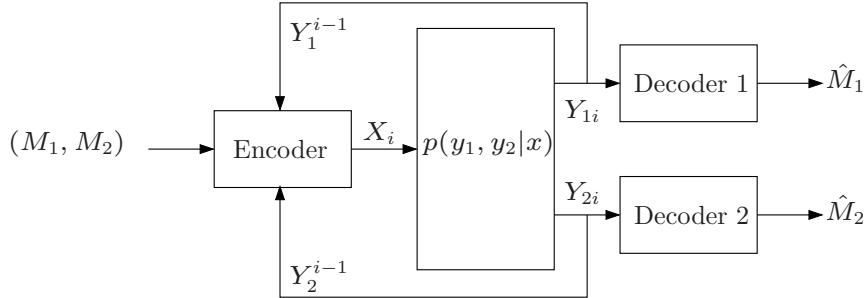
$$R_1 < C(S_1 + S_2 + 2\rho\sqrt{S_1S_2}) - C((1 - \rho^2)S_1),$$

$$R_2 < C((1 - \rho^2)S_2)$$

for all $\rho \leq \rho^*$. Finally, taking the union over all these regions and noting that inequalities in the capacity region are inactive for $\rho > \rho^*$ completes the proof

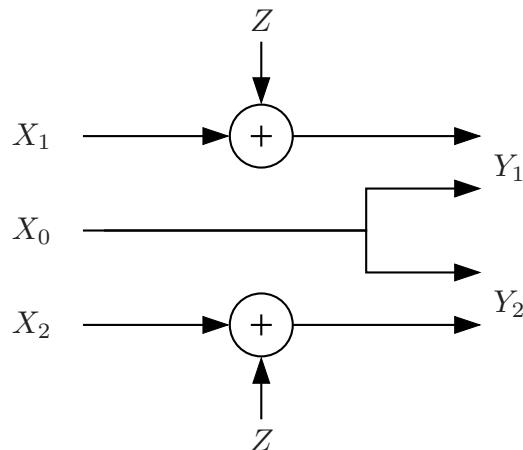
Broadcast Channel with Feedback

- Consider a DM-BC with causal feedback from both receivers



- The capacity region of this channel is not known in general
- Theorem 4 [22]:* The capacity region of the *physically degraded* DM-BC does not increase with feedback
Remark: The converse we proved for the case without feedback needs to be modified to establish this result
- Feedback can enlarge the capacity region of DM and AWGN broadcast channels in general [23, 24]

- Example [23]: Consider a DM broadcast channel with input $X = (X_0, X_1, X_2)$ and outputs $Y_1 = (X_0, X_1 \oplus Z)$ and $Y_2 = (X_0, X_2 \oplus Z)$, where $\mathcal{X}_0 = \mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$ and $Z \sim \text{Bern}(1/2)$



- It is easy to show that the capacity region of this channel without feedback is $\{(R_1, R_2) : R_1 + R_2 \leq 1\}$

- With feedback it can be shown that $(R_1, R_2) = (1, 1)$ is achievable:
 Suppose we want to send the binary sequences x_1^n and x_2^n to receivers Y_1 and Y_2 , respectively
 Begin by sending $(0, x_{11}, x_{21})$ over the channel
 Using the feedback link, the sender can determine the outcome z_1 of the random variable Z_1
 The triple (z_1, x_{12}, x_{22}) is then sent over the channel
 Upon receiving the common information z_1 , the decoders recover x_{11} and x_{21}
 Thus using the feedback link, the sender and receivers can recover z^n and therefore each receiver can recover its intended sequence perfectly, and $(R_1, R_2) = (1, 1)$ is achievable with feedback
 As shown in this example, feedback can increase the capacity by letting the encoder broadcast common channel information to all decoders

- Example (AWGN-BC [24]): Consider the symmetric AWGN-BC

$$Y_{1i} = X_i + Z_{1i}, \quad Y_{2i} = X_i + Z_{2i},$$
 where $\{Z_{1i}\}, \{Z_{2i}\}$ are independent WGN(1) processes, and assume expected average power constraint P
 - Without feedback, the capacity region is $\{(R_1, R_2) : R_1 + R_2 \leq C(P)\}$
 - With feedback, we can use the following variation of the Schalkwijk–Kailath coding. After proper initialization, send $X_i = X_{1i} + X_{2i}$, where
$$X_{1i} = \gamma_i(X_{1,i-1} - E(X_{1,i-1}|Y_{1,i-1})),$$

$$X_{2i} = -\gamma_i(X_{2,i-1} - E(X_{2,i-1}|Y_{2,i-1}))$$
 and γ_i is chosen such that $E(X_i^2) \leq P$ for each i

It can be shown that

$$R_1 = R_2 = \frac{1}{2} C \left(\frac{P(1 + \rho^*)/2}{1 + P(1 - \rho^*)/2} \right)$$

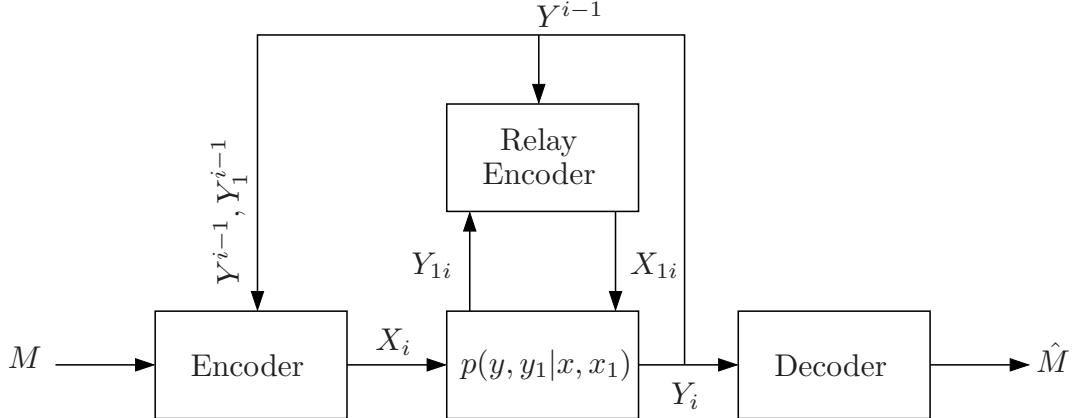
is achievable, where ρ^* satisfies

$$\rho^* \left(1 + (P + 1) \left(1 + \frac{P(1 - \rho^*)}{2} \right) \right) = \frac{P(P + 2)}{2}(1 - \rho^*)$$

For example, when $P = 1$, $(R_1, R_2) = (0.2803, 0.2803)$ is achievable with feedback, which is strictly outside the nonfeedback capacity region

Relay Channel with Feedback

- Consider the DM-RC with noiseless causal feedback from both receivers to the senders



Here, for each i , the relay encoder assigns a symbol $x_{1i}(y^{i-1}, y_1^{i-1})$ to each pair (y^{i-1}, y_1^{i-1}) and the encoder assigns a symbol $x_i(m, y^{i-1}, y_1^{i-1})$ to each triple (m, y^{i-1}, y_1^{i-1})

- *Theorem 5 [25]:* The capacity of DM-RC with feedback is given by

$$C_{\text{FB}} = \sup_{p(x,x_1)} \min \{I(X, X_1; Y), I(X; Y, Y_1 | X_1)\}$$

- The converse follows from the cutset upper bound to the capacity given in Lecture Notes 17, which applies when feedback is present (check!)
 - Achievability: We know that for a degraded relay channel, the capacity is

$$C = \max_{p(x,x_1)} \min\{I(X, X_1; Y), I(X; Y_1 | X_1)\},$$

and is achieved using decode-forward

Feedback in effect converts an arbitrary relay channel into a degraded relay channel, in which the relay at time i observes (Y^{i-1}, Y_1^{i-1}) instead of Y_1^{i-1} only

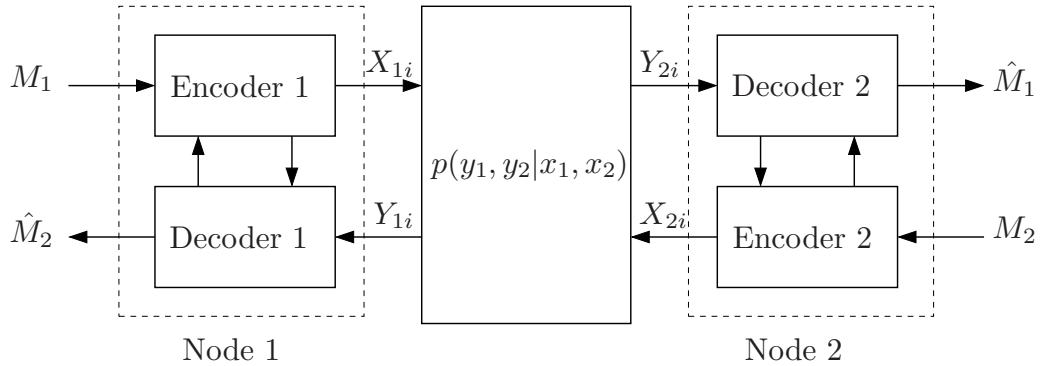
Clearly Y is a degraded form of (Y, Y_1)

Replacing Y_1 by (Y, Y_1) in the above expression, it follows that the rate is achievable with feedback

- Remark: To achieve this capacity, we only need feedback from the receiver to the relay, so adding other feedback links does not increase the capacity

Two-Way Channel

- A *discrete memoryless two-way channel* (DM-TWC) $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ 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 $\mathcal{Y}_1 \times \mathcal{Y}_2$
- Each node wishes to send a message to the other node



- A $(2^{nR_1}, 2^{nR_2}, n)$ code for the DM-TWC consists of:
 1. Two message sets $[1 : 2^{nR_1}]$ and $[1 : 2^{nR_2}]$
 2. Two encoders: For each $i \in [1 : n]$, encoder 1 assigns a symbol $x_{1i}(m_1, y_1^{i-1})$ to each pair (m_1, y_1^{i-1}) and encoder 2 assigns a symbol $x_{2i}(m_2, y_2^{i-1})$ to each pair (m_2, y_2^{i-1})
 3. Two decoders: Decoder 1 assigns an estimate \hat{m}_2 to each pair (m_1, y_1^n) , and decoder 2 assigns an estimate \hat{m}_1 to each pair (m_2, y_2^n)
 - The channel is memoryless in the sense that given $(X_{1i}, X_{2i}), (Y_{1i}, Y_{2i})$ is independent of the past symbols $(X_1^{i-1}, X_2^{i-1}, Y_1^{i-1}, Y_2^{i-1})$
 - 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
- $$P_e^{(n)} = P\{(\hat{M}_1, \hat{M}_2) \neq (M_1, M_2)\}$$
- The *capacity region* of the DM-TWC is the closure of the set of achievable rate pairs (R_1, R_2)

- The capacity of the DM-TWC is not known in general

The difficulty arises from the fact that two information flows share the same channel, inflicting interference to each other. In addition, each node has to play two competing roles of communicating its own message and providing feedback to help the other node

Simple Inner and Outer Bounds on the Capacity Region

- *Shannon's Inner Bound* [2]: A rate pair (R_1, R_2) is achievable for a DM-TWC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ if

$$R_1 < I(X_1; Y_2|X_2, Q), \quad R_2 < I(X_2; Y_1|X_1, Q)$$

for some $p(q)p(x_1|q)p(x_2|q)$

- The proof follows by the usual achievability argument using random codebook generation, joint typicality decoding, and the packing lemma. The encoders completely ignore the received outputs (no feedback)
- This inner bound is tight when the channel is decoupled into two separate DMCs, that is, $p(y_1, y_2|x_1, x_2) = p(y_1|x_2)p(y_2|x_1)$
- The bound is not tight in general, as shown by a counterexample [26]

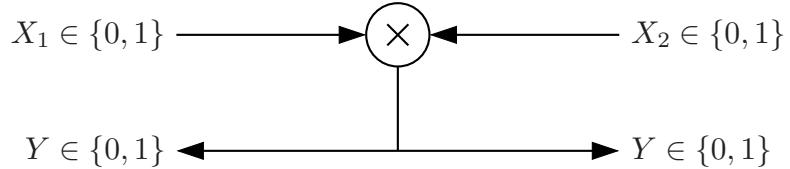
- *Shannon's Outer Bound* [2]: Any achievable rate pair (R_1, R_2) for a DM-TWC $(\mathcal{X}_1 \times \mathcal{X}_2, p(y_1, y_2|x_1, x_2), \mathcal{Y}_1 \times \mathcal{Y}_2)$ must satisfy the conditions

$$R_1 \leq I(X_1; Y_2|X_2), \quad R_2 \leq I(X_2; Y_1|X_1)$$

for some $p(x_1, x_2)$

- This outer bound can be easily established using standard weak converse techniques

- This outer bound is a special case of the cutset outer bound that will be discussed in Lecture Notes 19 and is not tight in general
- Example: Consider the *binary multiplier channel (BMC)* defined by $\mathcal{X}_1 = \mathcal{X}_2 = \{0, 1\}$ and $Y_1 = Y_2 = Y = X_1 \cdot X_2$



- The Shannon inner bound is the set of rate pairs such that

$$R_1 < p_2 H(p_1),$$

$$R_2 < p_1 H(p_2)$$

for some $1/2 \leq p_1, p_2 \leq 1$. We set $p_{X_1}(1) = p_1$ and $p_{X_2}(1) = p_2$

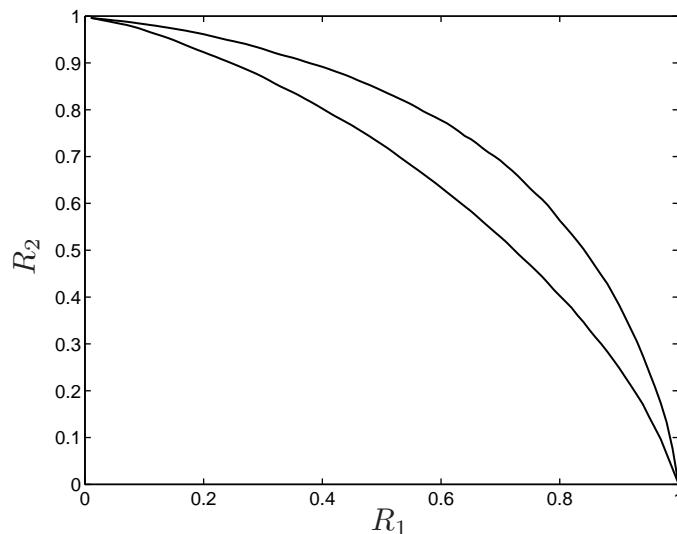
- The Shannon outer bound is the set of rate pairs such that

$$R_1 \leq (1 - p_1)H\left(\frac{p_2}{1 - p_1}\right),$$

$$R_2 \leq (1 - p_2)H\left(\frac{p_1}{1 - p_2}\right)$$

for some $p_1, p_2 \geq 0$ such that $p_1 + p_2 \leq 1$. We set $p_{X_1, X_2}(1, 0) = p_1$, $p_{X_1, X_2}(0, 1) = p_2$, $p_{X_1, X_2}(1, 1) = 1 - p_1 - p_2$

- Plot of the bounds:



- This leads to bounds on the symmetric capacity $C = \max\{R : (R, R) \in \mathcal{C}\}$ as

$$0.6170 \leq C \leq 0.6942$$

Dependence Balance Outer Bound

- Consider the DM-TWC with common output $Y_1 = Y_2 = Y$
- *Theorem 6 [27]:* If a rate pair (R_1, R_2) is achievable for the DM-TWC with common output $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$, then it must satisfy the conditions

$$R_1 \leq I(X_1; Y|X_2, U),$$

$$R_2 \leq I(X_2; Y|X_1, U)$$

for some $p(u, x_1, x_2)$ such that

$$I(X_1; X_2|U) \leq I(X_1; X_2|Y, U)$$

and $|\mathcal{U}| \leq 3$

- The proof follows (check!) from standard weak converse techniques by identifying $U_i = Y^{i-1}$
- The dependence balance outer bound is identical to Shannon's outer bound, except for the extra *dependence balance* condition
 $I(X_1; X_2|U) \leq I(X_1; X_2|Y, U)$. This condition limits the set of possible joint pmfs that can be formed through sequential transmissions
- This bound is not tight in general

- For the case of the BMC, the dependence balance bound gives the same upper bound on the symmetric capacity. However, an ingenuous modification [27] of the technique leads to the tighter upper bound $C \leq 0.6463$
- A similar outer bound can be derived for the DM-MAC with feedback. In this case, we add the inequality

$$R_1 + R_2 \leq I(X_1, X_2; Y|U)$$

to those already in the DM-TWC case. This outer bound is in general tighter than the cooperative outer bound for the DM-MAC with feedback, due to the dependence balance condition on the set of joint pmfs on (X_1, X_2)

Massey's Directed Information

- Directed information, introduced by Massey [28] and further refined by Kramer [29], is a useful notion to provide a nontrivial multi-letter characterization of the capacity region of the DM-TWC
- *Directed information from a random vector X^n to another random vector Y^n of the same length* is defined as

$$I(X^n \rightarrow Y^n) := \sum_{i=1}^n I(X^i; Y_i | Y^{i-1})$$

Similarly, directed information from X^n to Y^n causally conditioned on Z^n is defined as

$$I(X^n \rightarrow Y^n || Z^n) := \sum_{i=1}^n I(X^i; Y_i | Y^{i-1}, Z^i)$$

- As a related notion, the pmf of X^n causally conditioned on Y^n is defined as

$$p(x^n || y^n) := \prod_{i=1}^n p(x_i | x^{i-1}, y^i)$$

By convention, the pmf of X^n causally conditioned on (\emptyset, Y^{n-1}) is expressed as

$$p(x^n || y^{n-1}) := \prod_{i=1}^n p(x_i | x^{i-1}, y^{i-1})$$

- Directed information and causally conditional probabilities arise as a canonical answer to many other problems with causality constraints [30]. Most notably, it captures the feedback capacity of channels with memory [31, 32]

Multiletter Characterization of DM-TWC Capacity Region

- *Theorem 7 [29]:* Let \mathcal{C}_k , $k \geq 1$, be the set of rate pairs (R_1, R_2) such that

$$R_1 \leq \frac{1}{k} I(X_1^k \rightarrow Y^k || X_2^k), \quad R_2 \leq \frac{1}{k} I(X_2^k \rightarrow Y^k || X_1^k)$$

for some joint (causally conditional) pmf $p(x_1^k || y^{k-1})p(x_2^k || y^{k-1})$. Then the capacity region of the DM-TWC with common output $(\mathcal{X}_1 \times \mathcal{X}_2, p(y|x_1, x_2), \mathcal{Y})$ is $\mathcal{C} = \cup_k \mathcal{C}_k$

- A similar characterization can be found for the general DM-TWC $p(y_1, y_2 | x_1, x_2)$ and the DM-MAC with feedback
- Note that each choice of k and $p(x_1^k || y^{k-1})p(x_2^k || y^{k-1})$ leads to an inner bound on the capacity region
- Example: For the BMC $Y = X_1 \cdot X_2$, we consider the input pmf $p(x_1^k || y^{k-1})p(x_2^k || y^{k-1})$ defined as follows: Let $U_0 = \emptyset$ and $U_i := u_i(Y^i) \in \{0, 1, 2\}$, $i \geq 1$, such that

$$U_i = \begin{cases} 0 & \text{if } (U_{i-1} = 0, Y_i = 1) \text{ or } (U_{i-1} = 1, Y_i = 0) \text{ or } U_i = 2, \\ 1 & \text{if } U_{i-1} = 0, Y_i = 0, \\ 2 & \text{otherwise} \end{cases}$$

and for $j = 1, 2$,

$$\begin{aligned} p(x_{ji} = 1 | u_{i-1} = 0) &= \alpha, \\ p(x_{ji} = 1 | u_{i-1} = 1, x_{j,i-1} = 1) &= \beta, \\ p(x_{ji} = 1 | u_{i-1} = 1, x_{j,i-1} = 0) &= 1, \\ p(x_{ji} = 1 | u_{i-1} = 2, x_{j,i-1} = 1) &= 0, \\ p(x_{ji} = 1 | u_{i-1} = 2, x_{j,i-1} = 0) &= 1 \end{aligned}$$

for some $\alpha, \beta \in [0, 1]$ (i.e., both of causally conditional input pmfs are identical). Then, by optimizing α, β , it can be shown [?] that

$$\lim_{k \rightarrow \infty} \frac{1}{k} I(X_1^k \rightarrow Y^k || X_2^k) = \lim_{k \rightarrow \infty} \frac{1}{k} I(X_2^k \rightarrow Y^k || X_1^k) = 0.6191,$$

which is tighter than Shannon's lower bound. This lower bound was originally obtained by Schalkwijk [33] using a constructive coding scheme in the flavor of Horstein coding. It can be further improved [34] to $C \geq 0.6306$

Proof of Converse

- Using Fano's inequality, we have

$$\begin{aligned}
 nR_1 &\leq I(M_1; Y^n, M_2) + n\epsilon_n = I(M_1; Y^n | M_2) + n\epsilon_n \\
 &= \sum_{i=1}^n I(M_1; Y_i | M_2, Y^{i-1}) + n\epsilon_n \\
 &= \sum_{i=1}^n I(X_{1i}; Y_i | X_2^n, Y^{i-1}) + n\epsilon_n \\
 &\leq \sum_{i=1}^n I(X_{1i}; Y^i | X_2^n) + n\epsilon_n = I(X_1^n \rightarrow Y^n || X_2^n) + n\epsilon_n
 \end{aligned}$$

Similarly, $nR_2 \leq I(X_2^n \rightarrow Y^n || X_1^n) + n\epsilon_n$

Also it can be shown (check!) that $I(M_1; M_2 | X_2^i, Y^i) \leq I(M_1; M_2 | X_2^{i-1}, Y^{i-1})$ for all $i \in [1 : n]$. Hence,

$$I(X_1^i; X_{2i} | X_2^{i-1}, Y^{i-1}) \leq I(M_1; M_2 | X_2^{i-1}, Y^{i-1}) \leq I(M_1; M_2) = 0$$

or equivalently, $X_{2i} \rightarrow (X_2^{i-1}, Y^{i-1}) \rightarrow X_1^i$ form a Markov chain, which implies that the joint pmf is of the form $p(x_1^n || y^{n-1})p(x_2^n || y^{n-1})$. Therefore, for any $\epsilon > 0$, $(R_1 - \epsilon, R_2 - \epsilon) \in \mathcal{C}_n$ for n sufficiently large. This completes the proof

Proof of Achievability

- We communicate over k interleaved blocks, each used for one of k independent message pairs $(M_{1j}, M_{2j}) \in [1 : 2^{nR_{1j}}] \times [1 : 2^{nR_{2j}}]$, $j \in [1 : k]$. Block j consists of transmission time $j, k+j, 2k+j, \dots, (n-1)k+j$

For each block, we treat the channel input and output sequences from previous blocks as causal state information available at respective encoder-decoder pairs and use the multiplexing technique in Lecture Notes 7

- Codebook generation: Fix k and

$$p(x_1^k || y^{k-1})p(x_2^k || y^{k-1}) = \prod_{j=1}^k p(x_{1j} | x_1^{j-1}, y^{j-1})p(x_{2j} | x_2^{j-1}, y^{j-1}). \text{ Let } S_{1j} := (X_1^{j-1}, Y^{j-1}) \text{ and } S_{2j} := (X_2^{j-1}, Y^{j-1})$$

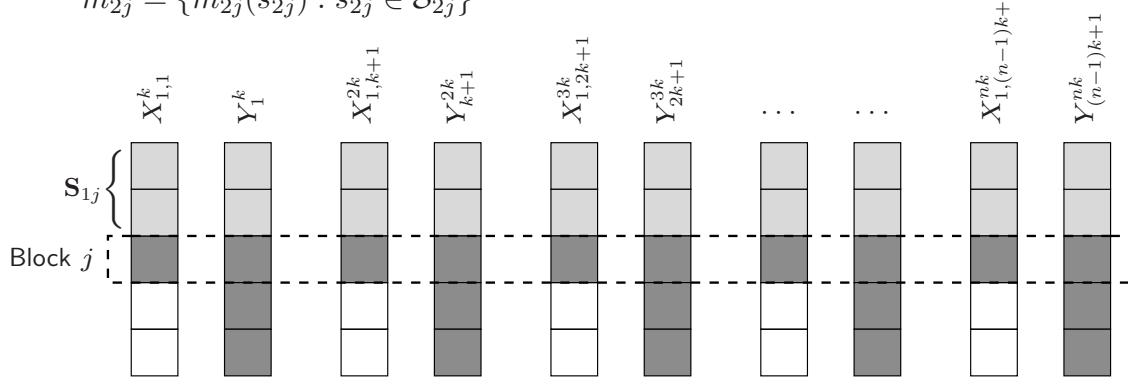
Split the message m_1 into k independent messages: m_{11}, \dots, m_{1k} . Then split each message m_{1j} , $j \in [1 : k]$, further into the

messages $\{m_{1j}(s_{1j}) : s_{1j} \in \mathcal{S}_{1j}\} = \mathcal{X}_1^{j-1} \times \mathcal{Y}^{j-1}$. Thus

$$R_1 = \sum_{j=1}^k \sum_{s_{1j} \in \mathcal{S}_{1j}} R_{1j}(s_{1j})$$

For $j \in [1 : k]$ and $s_{1j} \in \mathcal{S}_{1j}$, randomly and conditionally independently generate $2^{nR_{1j}(s_{1j})}$ sequences $\mathbf{x}_{1j}(m_{1j}(s_{1j}), s_{1j})$, $m_{1j}(s_{1j}) \in [1 : 2^{nR_{1j}(s_{1j})}]$ according to $\prod_{i=1}^n p_{X_{1j}|S_{1j}}(x_{1,(i-1)k+j} | s_{1j})$. These sequences form the codebook $\mathcal{C}_{1j}(s_j)$

Similarly, generate random codebooks $\mathcal{C}_{2j}(s_{2j})$, $j \in [1 : k]$,
 $s_{2j} \in \mathcal{S}_{2j} = \mathcal{X}_1^{j-1} \times \mathcal{Y}^{j-1}$ for $m_2 = (m_{21}, \dots, m_{2k})$ and
 $m_{2j} = \{m_{2j}(s_{2j}) : s_{2j} \in \mathcal{S}_{2j}\}$



- Encoding: For each block $j \in [1 : k]$ (i.e., time $j, k+j, 2k+j, \dots, (n-1)k+j$), encoder 1 treats the sequences $(\mathbf{x}_1^{j-1}, \mathbf{y}^{j-1}) \in \mathcal{S}_{1j}^n$ as causal state information available at both encoder 1 and decoder 2. Encoder 1 stores the codewords $\mathbf{x}_{1j}(m_{1j}(s_{1j}), s_{1j})$, $s_{1j} \in \mathcal{X}_1^{j-1} \times \mathcal{Y}^{j-1}$, in FIFO buffers and transmits a symbol from the buffer that corresponds to the state symbol of the given time. Similarly, encoder 2 stores the codewords in FIFO buffers and uses the multiplexing over them according to its state sequence

- Decoding and the analysis of the probability of error: Upon receiving y^{kn} , decoder 2 decodes m_{11}, \dots, m_{1k} successively. For interleaved block j , decoder 2 first forms the state sequence $\hat{s}_{1j} = (\hat{\mathbf{x}}_1^{j-1}, \mathbf{y}^{j-1})$ from the decoded codewords and output sequences from previous blocks, and demultiplexes the output sequence for block j into $|\mathcal{S}_{1j}|$ subsequences accordingly. Then it finds the unique index $\hat{m}_{1j}(s_{1j})$ for each subsequence corresponding to the state s_{1j}

Following the same argument in Lecture Notes 7, the probability of error for $m_{1j} \rightarrow 0$ as $n \rightarrow \infty$, if previous decoding steps are successful and

$$\begin{aligned} R_{1j} &< I(X_{1j}; X_2^k, Y_j^k | S_{1j}) - \delta(\epsilon) \\ &\stackrel{(a)}{=} I(X_{1j}; X_{2,j+1}^k, Y_j^k | X_2^j, X_1^{j-1}, Y^{j-1}) - \delta(\epsilon) \\ &= \sum_{i=j}^k I(X_{1j}; X_{2,i+1}, Y_i | X_2^i, X_1^{j-1}, Y^{i-1}) - \delta(\epsilon) \\ &\stackrel{(b)}{=} \sum_{i=j}^k I(X_{1j}; Y_i | X_2^i, X_1^{j-1}, Y^{i-1}) - \delta(\epsilon) \end{aligned}$$

where (a) follows by the Markov relation $X_{1j} \rightarrow (X_1^{j-1}, Y^{j-1}) \rightarrow X_2^j$ and (b) follows by the Markov relation $X_{2,i+1} \rightarrow (X_2^i, Y^i) \rightarrow X_1^{i+1}$

Therefore, by induction, the probability of error over all time slots $j \in [1 : k]$ $\rightarrow 0$ as $n \rightarrow \infty$ if

$$\begin{aligned}
\sum_{j=1}^k R_{1j} &< \sum_{j=1}^k \sum_{i=j}^k I(X_{1j}; Y_i | X_2^i, X_1^{j-1}, Y^{i-1}) - k\delta(\epsilon) \\
&= \sum_{i=1}^k \sum_{j=1}^i I(X_{1j}; Y_i | X_2^i, X_1^{j-1}, Y^{i-1}) - k\delta(\epsilon) \\
&= \sum_{i=1}^k I(X_1^i; Y_i | X_2^i, Y^{i-1}) - k\delta(\epsilon) \\
&= I(X_1^k \rightarrow Y^k | X_2^k) - k\delta(\epsilon)
\end{aligned}$$

Similarly, the probability of error for decoder 1 $\rightarrow 0$ as $n \rightarrow \infty$ if

$$\sum_{j=1}^k R_{2j} < I(X_2^k \rightarrow Y^k | X_1^k) - k\delta(\epsilon)$$

This completes the proof of achievability

Key New Ideas and Techniques

- Feedback does not increase the capacity of a DMC
- Iterative refinement
- Feedback can increase capacity of DM multiple user channels
- Directed information
- Open problems:
 - What is the feedback capacity region of the AWGN-MAC with more than 2 senders?
 - What is the feedback capacity region of the AWGN BC? (Why does feedback increase capacity here?)

References

- [1] C. E. Shannon, "Two-way communication channels," in *Proc. 4th Berkeley Sympos. Math. Statist. Prob.* Berkeley, Calif.: Univ. California Press, 1961, vol. I, pp. 611–644.
- [2] ——, "The zero error capacity of a noisy channel," *IRE Trans. Inf. Theory*, vol. 2, no. 3, pp. 8–19, Sept. 1956.
- [3] J. P. M. Schalkwijk and T. Kailath, "A coding scheme for additive noise channels with feedback—I: No bandwidth constraint," *IEEE Trans. Inf. Theory*, vol. 12, pp. 172–182, Apr. 1966.
- [4] J. P. M. Schalkwijk, "A coding scheme for additive noise channels with feedback—II: Band-limited signals," *IEEE Trans. Inf. Theory*, vol. 12, pp. 183–189, Apr. 1966.
- [5] J. M. Ooi and G. W. Wornell, "Fast iterative coding techniques for feedback channels," *IEEE Trans. Inf. Theory*, vol. 44, no. 7, pp. 2960–2976, 1998.
- [6] S. Butman, "A general formulation of linear feedback communication systems with solutions," *IEEE Trans. Inf. Theory*, vol. 15, no. 3, pp. 392–400, May 1969.
- [7] N. T. Gaarder and J. K. Wolf, "The capacity region of a multiple-access discrete memoryless channel can increase with feedback," *IEEE Trans. Inf. Theory*, vol. 21, pp. 100–102, 1975.
- [8] L. H. Ozarow, "The capacity of the white Gaussian multiple access channel with feedback," *IEEE Trans. Inf. Theory*, vol. 30, no. 4, pp. 623–629, 1984.
- [9] S. Butman, "Linear feedback rate bounds for regressive channels," *IEEE Trans. Inf. Theory*, vol. 22, no. 3, pp. 363–366, May 1976.

- [10] Y.-H. Kim, "Feedback capacity of stationary Gaussian channels," to appear in *IEEE Trans. Inf. Theory*, Jan. 2010.
- [11] M. S. Pinsker, "The probability of error in block transmission in a memoryless Gaussian channel with feedback," *Probl. Inf. Transm.*, vol. 4, no. 4, pp. 3–19, 1968.
- [12] L. A. Shepp, J. K. Wolf, A. D. Wyner, and J. Ziv, "Binary communication over the Gaussian channel using feedback with a peak energy constraint," *IEEE Trans. Inf. Theory*, vol. 15, pp. 476–478, 1969.
- [13] A. D. Wyner, "On the Schalkwijk–Kailath coding scheme with a peak energy constraint," *IEEE Trans. Inf. Theory*, vol. 14, pp. 129–134, Jan. 1968.
- [14] M. Horstein, "Sequential transmission using noiseless feedback," *IEEE Trans. Inf. Theory*, vol. 9, no. 3, pp. 136–143, July 1963.
- [15] O. Shayevitz and M. Feder, "Optimal feedback communication via posterior matching," 2009, submitted to *IEEE Trans. Inf. Theory*.
- [16] E. J. Weldon, Jr., "Asymptotic error coding bounds for the binary symmetric channel with feedback," Ph.D. Thesis, University of Florida, Gainesville, FL, Nov. 1963.
- [17] R. Ahlswede, "A constructive proof of the coding theorem for discrete memoryless channels in case of complete feedback," in *Transactions of the Sixth Prague Conference on Information Theory, Statistical Decision Functions, Random Processes (Tech Univ., Prague, 1971; dedicated to the memory of Antonín Špaček)*. Prague: Academia, 1973, pp. 1–22.
- [18] T. M. Cover and C. S. K. Leung, "An achievable rate region for the multiple-access channel with feedback," *IEEE Trans. Inf. Theory*, vol. 27, no. 3, pp. 292–298, 1981.
- [19] F. M. J. Willems, "The feedback capacity region of a class of discrete memoryless multiple access channels," *IEEE Trans. Inf. Theory*, vol. 28, no. 1, pp. 93–95, 1982.

- [20] C.-M. Zeng, F. Kuhlmann, and A. Buzo, "Achievability proof of some multiuser channel coding theorems using backward decoding," *IEEE Trans. Inf. Theory*, vol. 35, no. 6, pp. 1160–1165, 1989.
- [21] P. Lancaster and L. Rodman, *Algebraic Riccati Equations*. New York: Oxford University Press, 1995.
- [22] A. El Gamal, "The feedback capacity of degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 379–381, 1978.
- [23] G. Dueck, "Partial feedback for two-way and broadcast channels," *Inf. Control*, vol. 46, no. 1, pp. 1–15, 1980.
- [24] L. H. Ozarow and S. K. Leung-Yan-Cheong, "An achievable region and outer bound for the Gaussian broadcast channel with feedback," *IEEE Trans. Inf. Theory*, vol. 30, no. 4, pp. 667–671, 1984.
- [25] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sept. 1979.
- [26] G. Dueck, "The capacity region of the two-way channel can exceed the inner bound," *Inf. Control*, vol. 40, no. 3, pp. 258–266, 1979.
- [27] A. P. Hekstra and F. M. J. Willems, "Dependence balance bounds for single-output two-way channels," *IEEE Trans. Inf. Theory*, vol. 35, no. 1, pp. 44–53, 1989.
- [28] J. L. Massey, "Causality, feedback, and directed information," in *Proc. International Symposium on Information Theory and its Applications*, Honolulu, Hawaii, Nov. 1990, pp. 303–305.
- [29] G. Kramer, "Capacity results for the discrete memoryless network," *IEEE Trans. Inf. Theory*, vol. 49, no. 1, pp. 4–21, 2003.

- [30] H. H. Permuter, Y.-H. Kim, and T. Weissman, "Interpretations of directed information in portfolio theory, data compression, and hypothesis testing," 2009.
- [31] Y.-H. Kim, "A coding theorem for a class of stationary channels with feedback," *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1488–1499, Apr. 2008.
- [32] H. H. Permuter, T. Weissman, and A. Goldsmith, "Finite state channels with time-invariant deterministic feedback," *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 644–662, Feb. 2009.
- [33] J. P. M. Schalkwijk, "The binary multiplying channel—a coding scheme that operates beyond Shannon's inner bound region," *IEEE Trans. Inf. Theory*, vol. 28, no. 1, pp. 107–110, Jan. 1982.
- [34] ———, "On an extension of an achievable rate region for the binary multiplying channel," *IEEE Trans. Inf. Theory*, vol. 29, no. 3, pp. 445–448, 1983.

Lecture Notes 19

Discrete Memoryless Networks

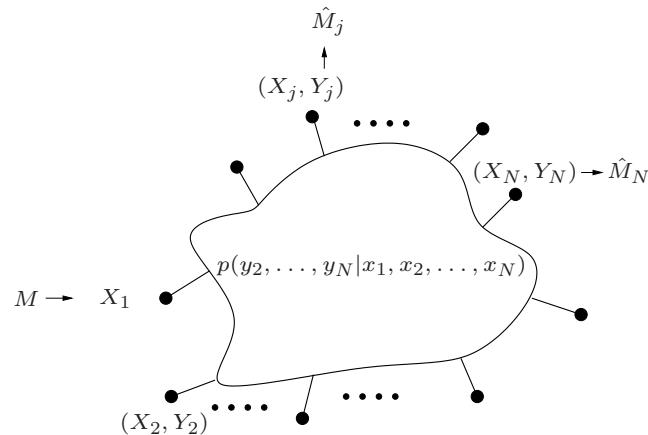
- Discrete Memoryless Multicast Network
- Decode–Forward Lower Bound
- Noisy Network Coding Lower Bound
- Discrete Memoryless Multiple Source Network
- Key New Ideas and Techniques

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Discrete Memoryless Multicast Network

- An N -node *discrete memoryless multicast network* (DM-MN) $(\mathcal{X}_1 \times \dots \times \mathcal{X}_N, p(y_2, \dots, y_N | x_1, \dots, x_N), \mathcal{Y}_2 \times \dots \times \mathcal{Y}_N)$ consists of a source alphabet \mathcal{X}_1 , $N - 1$ sender–receiver alphabet pairs $(\mathcal{X}_j, \mathcal{Y}_j)$, $j \in [2 : N]$, and a collection of conditional pmfs $p(y_2, \dots, y_N | x_1, \dots, x_N)$

Source node 1 wishes to send a message M to a set $\mathcal{D} \subseteq [2 : N]$ of destination nodes



- Formally, a $(2^{nR}, n)$ code for a DM-MN consists of:
 1. A message set $[1 : 2^{nR}]$
 2. A source encoder that assigns a codeword $x_1^n(m)$ to each message $m \in [1 : 2^{nR}]$
 3. A set of $N - 1$ relay encoders: Encoder k assigns a symbol $x_{ki}(y_k^{i-1})$ to every received sequence y_k^{i-1} for $i \in [1 : n]$
 4. A set of decoders: Decoder $k, k \in \mathcal{D}$, assigns \hat{m}_k to each y_k^n
- M is uniformly distributed over $[1 : 2^{nR}]$
- The probability of error is $P_e^{(n)} = \mathbb{P} \left\{ \hat{M}_k \neq M \text{ for some } k \in \mathcal{D} \right\}$
- A rate R is said to be achievable if there exists a sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The capacity of the DM-MN is the supremum of the set of achievable rates

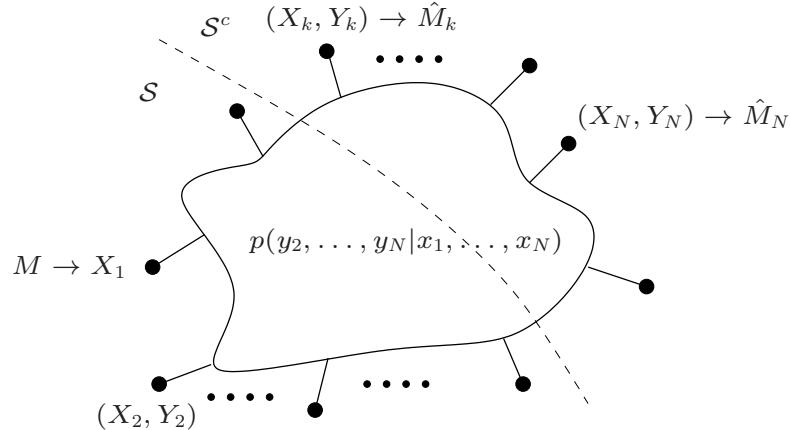
- Examples:
 - If $\mathcal{D} = [2 : N]$ and $p(y_2, \dots, y_N | x_1, \dots, x_N) = p(y_2, \dots, y_N | x_1)$, then this is a DM-BC with common message only
 - If $N = 3$, $X_3 = \emptyset$, and $\mathcal{D} = \{3\}$, then this is a DM-RC
 - If $\mathcal{D} = \{N\}$, then we denote the network as a discrete memoryless relay network (DM-RN)
- There is no single-letter (i.e., computable) characterization of the capacity of a general DM-MN (recall that the relay channel is a special case of the multicast network)

Cutset Bound on the Multicast Capacity

- Motivated by the max-flow min-cut theorem, we establish the following cutset bound on capacity

Theorem 1 (Cutset Bound) [1]: The capacity of the DM-MN $p(y_2, \dots, y_N | x^N)$ is upper bounded by

$$C \leq \max_{p(x^N)} \min_{k \in \mathcal{D}} \min_{\mathcal{S}: 1 \in \mathcal{S}, k \in \mathcal{S}^c} I(X(\mathcal{S}); Y(\mathcal{S}^c) | X(\mathcal{S}^c))$$



- Proof: We generalize the cutset bound for the relay channel in Lecture Notes 17

Let $k \in \mathcal{D}$ and $\mathcal{S} \subseteq [1 : N]$ such that $1 \in \mathcal{S}$ and $k \in \mathcal{S}^c$. Then by Fano's inequality, $H(M|Y^n(\mathcal{S}^c)) \leq H(M|Y_k^n) \leq n\epsilon_n$ with $\epsilon_n \rightarrow 0$ as $P_e^{(n)} \rightarrow 0$

Now consider

$$\begin{aligned} nR &= H(M) \leq I(M; Y^n(\mathcal{S}^c)) + n\epsilon_n \\ &= \sum_{i=1}^n I(M; Y_i(\mathcal{S}^c) | Y^{i-1}(\mathcal{S}^c)) + n\epsilon_n \\ &= \sum_{i=1}^n I(M; Y_i(\mathcal{S}^c) | Y^{i-1}(\mathcal{S}^c), X_i(\mathcal{S}^c)) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(M, Y^{i-1}(\mathcal{S}^c); Y_i(\mathcal{S}^c) | X_i(\mathcal{S}^c)) + n\epsilon_n \\ &\leq \sum_{i=1}^n I(X_i(\mathcal{S}), M, Y^{i-1}(\mathcal{S}^c); Y_i(\mathcal{S}^c) | X_i(\mathcal{S}^c)) + n\epsilon_n \\ &= \sum_{i=1}^n I(X_i(\mathcal{S}); Y_i(\mathcal{S}^c) | X_i(\mathcal{S}^c)) + n\epsilon_n \end{aligned}$$

By introducing a time-sharing random variable $Q \sim \text{Unif}[1 : n]$ and independent of all other random sequences, and defining $X(\mathcal{S}) := X_Q(\mathcal{S})$, $Y(\mathcal{S}^c) := Y_Q(\mathcal{S}^c)$, $X(\mathcal{S}^c) := X_Q(\mathcal{S}^c)$, we have

$$\begin{aligned} nR &\leq nI(X_Q(\mathcal{S}), Y_Q(\mathcal{S}^c) | X_Q(\mathcal{S}^c), Q) + n\epsilon_n \\ &\leq nI(X_Q(\mathcal{S}), Y_Q(\mathcal{S}^c) | X_Q(\mathcal{S}^c)) + n\epsilon_n = nI(X(\mathcal{S}), Y(\mathcal{S}^c) | X(\mathcal{S}^c)) + n\epsilon_n, \end{aligned}$$

which completes the proof

- As discussed in Lecture notes 17, the cutset bound is tight for several classes of relay channels, but is not tight in general

Decode–Forward Lower Bound

- *Theorem 2 (Decode–Forward Lower Bound)* [2, 3]: The capacity of the DM-MN $p(y_2, \dots, y_N | x^N)$ with any set $\mathcal{D} \subseteq [2 : N]$ of destination nodes is lower bounded by

$$C \geq \max_{p(x^N)} \min_{k \in [1:N-1]} I(X^k; Y_{k+1} | X_{k+1}^N)$$

- The decode–forward lower bound is tight when the DM-MN is *physically degraded* [2, 3], i.e.,

$$p(y_k^N | x^N, y^{k-1}) = p(y_k^N | x_{k-1}^N, y_{k-1}) \quad \text{for } k \in [2 : N],$$

where $y_1 = \emptyset$ by convention

Converse follows from the cutset upper bound with cutsets of the form $\mathcal{S} = [1 : k]$, $k \in [1 : N - 1]$, only (instead of all possible cutsets):

$$C \leq \max_{p(x^N)} \min_{k \in [1:N-1]} I(X^k; Y_{k+1}^N | X_{k+1}^N) = \max_{p(x^N)} \min_{k \in [1:N-1]} I(X^k; Y_{k+1} | X_{k+1}^N),$$

where the equality follows by the condition for channel degradedness
 $X^k \rightarrow (Y_{k+1}, X_{k+1}^N) \rightarrow Y_{k+2}^N$

- The decode-forward lower bound is also tight for the relay channel $p(y_2, y_3|x_1, x_2)$ with $\mathcal{D} = \{2, 3\}$. Here the capacity is

$$C = \max_{p(x_1, x_2)} \min\{I(X_1; Y_2|X_2), I(X_1, X_2; Y_3)\}$$

- The decode-forward lower bound holds for any set $\mathcal{D} \subseteq [2 : N]$ of destination nodes
- The bound can be further improved by removing some relay nodes or reordering nodes and taking the best subset/permuation

Sliding Window Decoding

- Achievability of the multicast decode-forward lower bound involves the new idea of *sliding-window decoding* [4, 5]
- We first revisit the single-relay case as an example and prove the decode-forward lower bound using an alternative decoding scheme to backward decoding in Lecture Notes 17
- As usual, we consider b transmission blocks, each consisting of n transmissions and use a block Markov coding scheme
A sequence of $b - 1$ i.i.d. messages, $m_j \in [1 : 2^{nR}]$, $j \in [1 : b - 1]$, is to be sent over the channel in nb transmissions
- Codebook generation: We use the same codebook generation as in cooperative multi-hop in Lecture Notes 17
Fix $p(x_1, x_2)$ that achieves the lower bound. We randomly and independently generate a codebook for each block $j \in [1 : b]$:
 1. Randomly and independently generate 2^{nR} sequences $x_2^n(m_{j-1})$, $m_{j-1} \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_{X_2}(x_{2i})$

2. For each $x_2^n(m_{j-1})$, randomly and conditionally independently generate 2^{nR} sequences $x_1^n(m_j|m_{j-1})$, $m_j \in [1 : 2^{nR}]$, each according to
 $\prod_{i=1}^n p_{X_1|X_2}(x_{1i}|x_{2i}(m_{j-1}))$

This defines the codebook

$$\mathcal{C}_j = \{x_1^n(m_j|m_{j-1}), x_2^n(m_{j-1}) : m_{j-1}, m_j \in [1 : 2^{nR}]\} \text{ for } j \in [1 : b]$$

The codebooks C_j , $j \in [1 : b]$, are revealed to all parties

- Encoding and decoding are explained with the help of the following table:

Block	1	2	3	...	$b - 1$	b
X_1	$x_1^n(m_1 1)$	$x_1^n(m_2 m_1)$	$x_1^n(m_3 m_2)$...	$x_1^n(m_{b-1} m_{b-2})$	$x_1^n(1 m_{b-1})$
Y_2	\hat{m}_{21}	\hat{m}_{22}	\hat{m}_{23}	...	$\hat{m}_{2,b-1}$	1
X_2	$x_2^n(1)$	$x_2^n(\hat{m}_{21})$	$x_2^n(\hat{m}_{22})$...	$x_2^n(\hat{m}_{2,b-2})$	$x_2^n(\hat{m}_{2,b-1})$
Y_3	1	\hat{m}_{31}	\hat{m}_{32}	...	$\hat{m}_{3,b-2}$	$\hat{m}_{3,b-1}$

- Encoding: Again encoding is the same as in the cooperative multi-hop

Let $m_j \in [1 : 2^{nR}]$ be the message to be sent in block j , the encoder transmits $x_1^n(m_j|m_{j-1})$ from the codebook \mathcal{C}_j

At the end of block j , the relay has an estimate \hat{m}_{2j} of the message m_j . In block $j + 1$, it transmits $x_2^n(\hat{m}_{2j})$ from the codebook \mathcal{C}_{j+1}

- Decoding and analysis of the probability of error: The decoding procedures for message m_j are as follows

- Decoding at the relay is the same as in the cooperative multi-hop. Hence,
 $P\{\hat{M}_{2j} \neq M_j\} \rightarrow 0$ as $n \rightarrow \infty$ for all $j \in [1 : b - 1]$ if
 $R < I(X_1; Y_2|X_2) - \delta(\epsilon)$

- Unlike backward decoding, however, the receiver decodes the message sequence in the forward direction using a different procedure

Upon receiving $y_3^n(j + 1)$, the receiver finds a unique message \hat{m}_{3j} that satisfies the following two conditions simultaneously:

$$(X_1^n(\hat{m}_{3j}|\hat{m}_{3,j-1}), X_2^n(\hat{m}_{3,j-1}), Y_3^n(j)) \in \mathcal{T}_\epsilon^{(n)},$$

$$(X_2^n(\hat{m}_{3j}), Y_3^n(j + 1)) \in \mathcal{T}_\epsilon^{(n)}$$

Since the codebooks are generated independently for each block, these two events are independent. Hence, by the LLN, the joint typicality lemma, and induction, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R < I(X_1; Y_3|X_2) + I(X_2; Y_3) = I(X_1, X_2; Y_3) - 2\delta(\epsilon) \text{ and}$$

$$R < I(X_1; Y_2|X_2) - \delta(\epsilon)$$

Achievability of the Multicast Decode–Forward Lower Bound

- We extend the decode–forward coding scheme to the DM-MN using sliding-window decoding. Each relay node $k \in [2 : N - 1]$ decodes the message and forwards it to the next node
- A sequence of $b - N + 2$ messages $m_j \in [1 : 2^{nR}]$, $j \in [1 : b - N + 2]$, each selected independently and uniformly over $[1 : 2^{nR}]$, is to be sent over the channel in b blocks of n transmissions
- Codebook generation: Fix $p(x^N)$. We randomly and independently generate a codebook for each block $j \in [1 : b]$
 1. Randomly generate a sequence $x_N^n(j)$ according to $\prod_{i=1}^n p_{X_N}(x_{Ni})$
 2. For each relay node $k = N - 1, N - 2, \dots, 1$ and for each $(x_{k+1}^n(m_{j-k}|m_{j-N+2}^{j-k-1}), \dots, x_{N-1}^n(m_{j-N+2}), x_N^n(j))$, generate 2^{nR} conditionally independent sequences $x_k^n(m_{j-k+1}|m_{j-N+2}^{j-k})$, $m_{j-k+1} \in [1 : 2^{nR}]$, each according to $\prod_{i=1}^n p_{X_k|X_{k+1}^N}(x_{ki}|x_{k+1,i}(m_{j-k}|m_{j-N+2}^{j-k-1}), \dots, x_{N-1,i}(m_{j-N+2}), x_{Ni}(j))$

This defines the codebooks

$$\mathcal{C}_j = \{(x_1^n(m_j|m_{j-N+2}^{j-1}), x_2^n(m_{j-1}|m_{j-N+2}^{j-2}), \dots, x_{N-1}^n(m_{j-N+2}), x_N^n(j)) : m_{j-N+2}, \dots, m_j \in [1 : 2^{nR}]\}$$

for each block $j \in [1 : b]$, which are revealed to all parties

- Encoding and decoding for $N = 4$ are explained with the help of the following table

Block	1	2	3	...	j
X_1	$x_1^n(m_1 1, 1)$	$x_1^n(m_2 1, m_1)$	$x_1^n(m_3 m_1^2)$...	$x_1^n(m_j m_{j-2}^{j-1})$
Y_2	\hat{m}_{21}	\hat{m}_{22}	\hat{m}_{23}	...	\hat{m}_{2j}
X_2	$x_2^n(1 1)$	$x_2^n(\hat{m}_{21} 1)$	$x_2^n(\hat{m}_{22} \hat{m}_{21})$...	$x_2^n(\hat{m}_{2,j-1} \hat{m}_{2,j-2})$
Y_3	\emptyset	\hat{m}_{31}	\hat{m}_{32}	...	$\hat{m}_{3,j-1}$
X_3	1	1	$x_3^n(\hat{m}_{31})$...	$x_3^n(\hat{m}_{3,j-2})$
Y_4	\emptyset	\emptyset	\hat{m}_{41}	...	$\hat{m}_{4,j-2}$

Block	$j + 1$	\dots	$b - 2$	$b - 1$	b
X_1	$x_1^n(m_{j+1} m_{j-1}^{j-1})$	\dots	$x_1^n(m_{b-2} m_{b-4}^{b-3})$	$x_1^n(1 m_{b-3}^{b-2})$	$x_1^n(1 m_{b-2}, 1)$
Y_2	$\hat{m}_{2,j+1}$	\dots	$\hat{m}_{2,b-2}$	\emptyset	\emptyset
X_2	$x_2^n(\hat{m}_{2,j} \hat{m}_{2,j-1})$	\dots	$x_2^n(\hat{m}_{2,b-3} \hat{m}_{2,b-4})$	$x_2^n(\hat{m}_{2,b-2} \hat{m}_{2,b-3})$	$x_2^n(1 \hat{m}_{2,b-2})$
Y_3	$\hat{m}_{3,j}$	\dots	$\hat{m}_{3,b-3}$	$\hat{m}_{3,b-2}$	\emptyset
X_3	$x_3^n(\hat{m}_{3,j-1})$	\dots	$x_3^n(\hat{m}_{3,b-4})$	$x_3^n(\hat{m}_{3,b-3})$	$x_3^n(\hat{m}_{3,b-2})$
Y_4	$\hat{m}_{4,j-1}$	\dots	$\hat{m}_{4,b-4}$	$\hat{m}_{4,b-3}$	$\hat{m}_{4,b-2}$

- Encoding: Let $m_j \in [1 : 2^{nR}]$ be the new message to be sent in block j , the encoder transmits $x_1^n(m_j|m_{j-N+2}^{j-1})$ from the codebook \mathcal{C}_j . At the end of block $j+k-2$, node $k \in [2 : N-1]$ has an estimate (\hat{m}_{kj}) of the message m_j . In block $j+k-1$, it transmits $x_k^n(\hat{m}_{kj}|\hat{m}_{k,j+k-N+1}^{j-1})$ from the codebook \mathcal{C}_{j+k-1} . Node N sends $x_N^n(j)$ in block $j \in [1 : N]$.

- Decoding and analysis of the probability of error: The decoding procedures for message m_j are as follows

Upon receiving $y_k^n(j+k-2)$ at the end of block $j+k-2$, node k finds a unique message \hat{m}_{kj} that satisfies the following conditions simultaneously (here the dependence of codewords on previous message indices $\hat{m}_{k,j-N+2}^{j-1}$ is suppressed for brevity):

$$\begin{aligned} (X_1^n(\hat{m}_{kj}), X_2^n, \dots, X_N^n(j), Y_k^n(j)) &\in \mathcal{T}_\epsilon^{(n)}, \\ (X_2^n(\hat{m}_{kj}), X_3^n, \dots, X_N^n(j+1), Y_k^n(j+1)) &\in \mathcal{T}_\epsilon^{(n)}, \\ &\vdots \\ (X_{k-1}^n(\hat{m}_{kj}), X_k^n, \dots, X_N^n(j+k-1), Y_k^n(j+k-1)) &\in \mathcal{T}_\epsilon^{(n)} \end{aligned}$$

For example, in the case $N = 4$, node 4 at the end of block $j+2$ finds a unique message $\hat{m}_{4,j}$ such that

$$\begin{aligned} (X_1^n(\hat{m}_{4,j}|\hat{m}_{4,j-2}^{j-1}), X_2^n(\hat{m}_{4,j-1}|\hat{m}_{4,j-2}), X_3^n(\hat{m}_{4,j-2}), X_4^n(j), Y_4^n(j)) &\in \mathcal{T}_\epsilon^{(n)}, \\ (X_2^n(\hat{m}_{4,j}|\hat{m}_{4,j-1}), X_3^n(\hat{m}_{4,j-1}), X_4^n(j+1), Y_4^n(j+1)) &\in \mathcal{T}_\epsilon^{(n)}, \\ (X_3^n(\hat{m}_{4,j}), X_4^n(j+2), Y_4^n(j+2)) &\in \mathcal{T}_\epsilon^{(n)} \end{aligned}$$

Following similar steps to the proof of the sliding-window decoding for the relay channel, by the independence of the codebooks, the LLN, the joint typicality lemma, and induction, it can be shown that the probability of error tends to 0 as $n \rightarrow \infty$, provided that

$$R < \sum_{k'=1}^{k-1} I(X_{k'}; Y_k | X_{k'+1}^N) - \delta(\epsilon) = I(X^{k-1}; Y_k | X_k^N) - \delta(\epsilon)$$

This completes the proof of achievability

Noisy Network Coding Lower Bound

- We generalize the network coding theorem to obtain the following

Theorem 3 (Noisy Network Coding Lower Bound) [6]: The capacity of the DM-MN $p(y_2, \dots, y_N | x^N)$ is lower bounded by

$$C \geq \max_{\prod_{k=1}^N p(x_k)p(\hat{y}_k|y_k, x_k)} \min_{k \in \mathcal{D}} \min_{\substack{\mathcal{S} \subseteq [1:N] \\ 1 \in \mathcal{S}, k \in \mathcal{S}^c}} (I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_k | X(\mathcal{S}^c)) - I(Y(\mathcal{S}); \hat{Y}(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c), Y_k)),$$

where the maximum is taken over all pmfs $\prod_{k=1}^N p(x_k)p(\hat{y}_k|y_k, x_k)$ and $Y_1 = \hat{Y}_1 = \emptyset$ by convention

- The noisy network coding lower bound can be compared to the cutset upper bound:
 - the first term is similar to the cutset bound with $Y(\mathcal{S}^c)$ replaced by the “compressed version” $\hat{Y}(\mathcal{S}^c)$,
 - the second term is subtracted, and
 - the maximization is over independent X^N (no coherent cooperation)
- Note that this lower bound reduces to the compress-forward lower bound for the relay channel [7, 8], which was discussed in Lecture Notes 17

Deterministic Multicast Network

- Consider the class of deterministic multicast networks where the received symbol Y_k at each node $k \in [2 : N]$ is a deterministic function of transmitted symbols, i.e., $Y_k = y_k(X^N)$
- The cutset upper bound simplifies to

$$C \leq \max_{p(x^N)} \min_{k \in \mathcal{D}} \min_{\mathcal{S}: 1 \in \mathcal{S}, k \in \mathcal{S}^c} H(Y(\mathcal{S}^c) | X(\mathcal{S}^c))$$

- On the other hand, by taking $\hat{Y}_k = Y_k$ for all $k \in [2 : N]$, the noisy network coding lower bound reduces to the following lower bound [9]:

$$C \geq \max_{\prod_{k=1}^N p(x_k)} \min_{k \in \mathcal{D}} \min_{\mathcal{S}: 1 \in \mathcal{S}, k \in \mathcal{S}^c} H(Y(\mathcal{S}^c) | X(\mathcal{S}^c))$$

where the maximization is over product pmfs instead of arbitrary joint pmf as in the cutset bound

- In general, these two bounds do not coincide. But there are several interesting special cases where they coincide

- Examples

- Noiseless multicast network: A noiseless multicast network $(\mathcal{N}, \mathcal{E}, \mathcal{C})$ with destinations \mathcal{D} in Lecture Notes 16 is a special case of deterministic multicast networks with $Y_k = X(\mathcal{N}_k)$, where $\mathcal{N}_k = \{j : (j, k) \in \mathcal{E}\}$ for $k \in [2 : N]$. Each link $(j, k) \in \mathcal{E}$ carries an input symbol $x_{jk} \in \mathcal{X}_{jk}$ with link capacity $C_{jk} = \log |\mathcal{X}_{jk}|$

In this case, the capacity is given by the max-flow min-cut theorem, which coincides with the cutset bound achieved by the uniform pmf on all input symbols

- Deterministic multicast network with no interference [2, 10]: Suppose each node receives a collection of single-variable functions of input symbols, i.e., $Y_k = (y_{k1}(X_1), \dots, y_{kN}(X_N))$, $k \in [2 : N]$. Then the cutset bound is achieved by a product input pmf and the capacity is

$$C = \max_{\prod_{k=1}^N p(x_k)} \min_{k \in \mathcal{D}} \min_{\mathcal{S}: 1 \in \mathcal{S}, k \in \mathcal{S}^c} \sum_{j \in \mathcal{S}} H(\{Y_{lj} : l \in \mathcal{S}^c\})$$

For example, if $N = 3$, $\mathcal{D} = \{2, 3\}$,
 $Y_2 = (y_{21}(X_1), y_{23}(X_3))$, $Y_3 = (y_{31}(X_1), y_{32}(X_2))$, then

$$C = \max_{p(x_1)p(x_2)p(x_3)} \min\{H(Y_{21}, Y_{31}), H(Y_{21}) + H(Y_{23}), H(Y_{31}) + H(Y_{32})\}$$

- Finite-field deterministic multicast network (FFD-MN): Suppose each node receives linear functions

$$Y_k = \sum_{j=1}^N g_{jk} X_j,$$

where g_{jk} , $j, k \in [1 : N]$ and X_j , $j \in [1 : N]$ take values in the finite field \mathbb{F}_q

Then it can be easily shown (check!) that that the cutset bound is achieved by the uniform product pmf [9] and

$$C = \min_{k \in \mathcal{D}} \max_{\mathcal{S}: 1 \in \mathcal{S}, k \in \mathcal{S}^c} \text{rank}(G(\mathcal{S})) \log q,$$

where $G(\mathcal{S})$ is defined such that

$$Y(\mathcal{S}^c) = G(\mathcal{S})X(\mathcal{S}) + G'(\mathcal{S})X(\mathcal{S}^c)$$

- Deterministic relay channel: Suppose the network has three nodes with output symbols

$$Y_2 = y_2(X_1, X_2), Y_3 = y_3(X_1, X_2)$$

Then the capacity is

$$C = \max_{p(x_1, x_2)} \min\{H(Y_3), H(Y_2, Y_3 | X_2)\},$$

which is achieved by partial decode-and-forward (cf. Lecture Notes 17). In this case, the compress–forward lower bound is not tight in general

Message Repetition Compress–Forward Coding

- Achievability of the noisy network coding lower bound involves the new idea of message repetition compress–forward coding. Unlike other block Markov coding techniques we have seen so far, the message repetition coding sends the same message $m \in [1 : 2^{nbR}]$ over b blocks (nb transmissions), while the relays send compressed versions of the channel observation of the previous block. Equivalently, the encoder transmits a long codeword of length nb , while relays compress and forward observations of length n (over b blocks)
- We first consider the single-relay case as an example and then develop the main idea into the general DM-MN subsequently
- Consider the DM-RC $p(y_2, y_3 | x_1, x_2)$ with source node 1, relay node 2, and destination node 3. By convention $Y_1 = X_3 = \emptyset$. We prove the achievability of the compress–forward lower bound:

$$C \geq \max_{p(x_1)p(x_2)p(\hat{y}_2|y_2, x_2)} \min\{I(X_1, X_2; Y_3) - I(Y_2; \hat{Y}_2 | X_1, X_2, Y_3), I(X_1; \hat{Y}_2, Y_3 | X_2)\}$$

- Codebook generation: Fix $p(x_1)p(x_2)p(\hat{y}_2|y_2, x_2)$. For each $j \in [1 : b]$, we generate an independent codebook as follows:

1. Randomly and independently generate 2^{nbR} sequences $x_1^n(j, m)$, $m \in [1 : 2^{nbR}]$, each according to $\prod_{i=1}^n p_{X_1}(x_{1i})$
2. Randomly and independently generate 2^{nR_2} sequences $x_2^n(l_{j-1})$, $l_{j-1} \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_{X_2}(x_{2i})$
3. For each $x_2^n(l_{j-1})$, $l_{j-1} \in [1 : 2^{nR_2}]$, randomly and conditionally independently generate 2^{nR_2} sequences $\hat{y}_2^n(l_j|l_{j-1})$, $l_j \in [1 : 2^{nR_2}]$, each according to $\prod_{i=1}^n p_{\hat{Y}_2|X_2}(\hat{y}_{2i}|x_{2i}(l_{j-1}))$

- Encoding and decoding are explained with the help of the following table:

Block	1	2	3	...	$b - 1$	b
X_1	$x_1^n(1, m)$	$x_1^n(2, m)$	$x_1^n(3, m)$...	$x_1^n(b - 1, m)$	$x_1^n(b, m)$
Y_2	$\hat{y}_2^n(l_1 1), l_1$	$\hat{y}_2^n(l_2 l_1), l_2$	$\hat{y}_2^n(l_3 l_2), l_3$...	$\hat{y}_2^n(l_{b-1} l_{b-2}), l_{b-1}$	$\hat{y}_2^n(l_b l_{b-1}), l_b$
X_2	$x_2^n(1)$	$x_2^n(l_1)$	$x_2^n(l_2)$...	$x_2^n(l_{b-2})$	$x_2^n(l_{b-1})$
Y_3	\emptyset	\emptyset	\emptyset	...	\emptyset	\hat{m}

- Encoding: To send m , the sender transmits $x^n(j, m)$ in block j
The relay, upon receiving $y_2^n(j)$, finds an index l_j such that
 $(\hat{y}_2^n(l_j|l_{j-1}), y_2^n(j), x_2^n(l_{j-1})) \in \mathcal{T}_{\epsilon'}^{(n)}$
Assuming that such l_j is found, the relay sends $x_2^n(l_j)$ in block $j + 1$
By the covering lemma, the probability $P(\tilde{\mathcal{E}}(j))$ that there is no such l_j tends to 0 as $n \rightarrow \infty$, if $R_2 > I(\hat{Y}_2; Y_2|X_2) + \delta(\epsilon')$
- Decoding and analysis of the probability of error: At the end of block b , the receiver finds a unique index \hat{m} such that

$$(x_1^n(j, \hat{m}), \hat{y}_2^n(l_j|l_{j-1}), x_2^n(l_{j-1}), y_3^n(j)) \in \mathcal{T}_{\epsilon}^{(n)} \quad \text{for all } j \in [1 : b]$$

for some l_1, l_2, \dots, l_b . Here $l_0 = 1$ by convention

To bound the probability of error, assume without loss of generality that $M = 1$ and $L_1 = L_2 = \dots = L_b = 1$. Define the events

$$\mathcal{E}_j(m, l_{j-1}, l_j) := \{(X_1^n(j, m), \hat{Y}_2^n(l_j|l_{j-1}), X_2^n(l_{j-1}), Y_3^n(j)) \in \mathcal{T}_{\epsilon}^{(n)}\}$$

Then the probability of the event of interest (conditioned on the event that $(X_2^n(j, 1), \hat{Y}_2^n(j, 1|1), Y_2^n(j)) \in \mathcal{T}_{\epsilon'}^{(n)}$ for all $j \in [1 : b]$) is bounded as

$$\begin{aligned} \mathsf{P}(\mathcal{E}) &\leq \mathsf{P}(\bigcup_{j=1}^b \mathcal{E}_j^c(1, 1, 1)) + \mathsf{P}(\bigcup_{m \neq 1} \bigcup_{l^b} \cap_{j=1}^b \mathcal{E}_j(m, l_{j-1}, l_j)) \\ &\leq \sum_{j=1}^b \mathsf{P}(\mathcal{E}_j^c(1, 1, 1)) + \sum_{m \neq 1} \sum_{l^b} \mathsf{P}(\cap_{j=1}^b \mathcal{E}_j(m, l_{j-1}, l_j)) \\ &\stackrel{(a)}{=} \sum_{j=1}^b \mathsf{P}(\mathcal{E}_j^c(1, 1, 1)) + \sum_{m \neq 1} \sum_{l^b} \prod_{j=1}^b \mathsf{P}(\mathcal{E}_j(m, l_{j-1}, l_j)) \\ &\leq \sum_{j=1}^b \mathsf{P}(\mathcal{E}_j^c(1, 1, 1)) + \sum_{m \neq 1} \sum_{l^b} \prod_{j=2}^b \mathsf{P}(\mathcal{E}_j(m, l_{j-1}, l_j)), \end{aligned}$$

where (a) follows since the codebook is generated independently for each block $j \in [1 : b]$

By the Markov lemma, the first term $\rightarrow 0$ as $n \rightarrow \infty$

For the second term, note that if $m \neq 1$ and $l_{j-1} = 1$, then

$X_1^n(j, m) \sim \prod_{i=1}^n p_{X_1}(x_{1i})$ is independent of $(\hat{Y}_2^n(j, l_j | l_{j-1}), X_2^n(j, l_{j-1}), Y_3^n(j))$ and hence by the joint typicality lemma

$$\begin{aligned} \mathsf{P}(\mathcal{E}_j(m, l_{j-1}, l_j)) &= \mathsf{P}\{X_1^n(j, m), \hat{Y}_2^n(j, l_j | l_{j-1}), X_2^n(j, l_{j-1}), Y_3^n(j) \in \mathcal{T}_{\epsilon}^{(n)}\} \\ &\leq 2^{-n(I(X_1; \hat{Y}_2, Y_3 | X_2) - \delta(\epsilon))} =: 2^{-n(I_1 - \delta(\epsilon))} \end{aligned}$$

Similarly, if $m \neq 1$ and $l_{j-1} \neq 1$, then

$(X_1^n(j, m), \hat{Y}_2^n(j, l_j | l_{j-1}), X_2^n(j, l_{j-1})) \sim \prod_{i=1}^n (p_{X_1}(x_{1i}) p_{\hat{Y}_2, X_2}(\hat{y}_{2i}, x_{2i}))$ is independent of $Y_3^n(j)$ and hence

$$\mathsf{P}(\mathcal{E}_j(m, l_{j-1}, l_j)) \leq 2^{-n(I(X_1, X_2; Y_3) + I(\hat{Y}_2; X_1, Y_3 | X_2) - \delta(\epsilon))} =: 2^{-n(I_2 - \delta(\epsilon))}$$

Hence, if $\pi(1 | l^{b-1}) = k/(b-1)$, i.e., l^{b-1} has k 1s, then

$$\prod_{j=2}^b \mathsf{P}(\mathcal{E}_j(m, l_{j-1}, l_j)) \leq 2^{-n(kI_1 + (b-1-k)I_2 - (b-1)\delta(\epsilon))}$$

Therefore

$$\begin{aligned}
& \sum_{m \neq 1} \sum_{l^b} \prod_{j=2}^b \mathbb{P}(\mathcal{E}_j(m, l_{j-1}, l_j)) \\
& \leq \sum_{m \neq 1} \sum_{l_b} \sum_{j=0}^{b-1} \binom{b-1}{j} 2^{n(b-1-j)R_2} \cdot 2^{-n(jI_1 + (b-1-j)I_2 - (b-1)\delta(\epsilon))} \\
& = \sum_{m \neq 1} \sum_{l_b} \sum_{j=0}^{b-1} \binom{b-1}{j} 2^{-n(jI_1 + (b-1-j)(I_2 - R_2) - (b-1)\delta(\epsilon))} \\
& \leq \sum_{m \neq 1} \sum_{l_b} \sum_{j=0}^{b-1} \binom{b-1}{j} 2^{-n((b-1)(\min\{I_1, I_2 - R_2\} - \delta(\epsilon)))} \\
& \leq 2^{nbR} \cdot 2^{nR_2} \cdot 2^b \cdot 2^{-n(b-1)(\min\{I_1, I_2 - R_2\} - \delta(\epsilon))},
\end{aligned}$$

which $\rightarrow 0$ as $n \rightarrow \infty$, provided that

$$R < \frac{b-1}{b}(\min\{I_1, I_2 - R_2\} - \delta'(\epsilon)) - \frac{R_2}{b}$$

- Finally, by eliminating $R_2 > I(\hat{Y}_2; Y_2|X_2) + \delta(\epsilon')$, letting $b \rightarrow \infty$, and substituting

$$\begin{aligned}
I_1 &= I(X_1; \hat{Y}_2, Y_3|X_2), \\
I_2 &= I(X_1, X_2; Y_3) + I(\hat{Y}_2; X_1, Y_3|X_2)
\end{aligned}$$

we have shown that the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R < \min\{I(X_1; \hat{Y}_2, Y_3|X_2), I(X_1, X_2; Y_3) - I(\hat{Y}_2; Y_2|X_1, X_2, Y_3)\} - \delta'(\epsilon) - \delta(\epsilon')$$

Achievability of the Noisy Network Coding Lower Bound

- We generalize the message repetition compress-forward coding to a general DM-RN $p(y_2, \dots, y_N | x^N)$

- First we consider the case with single destination node N and $N - 2$ relay nodes $k \in [2 : N - 1]$

Assume without loss of generality that $X_N = \emptyset$ (otherwise, we can consider a new destination node $N + 1$ with $Y_{N+1} = Y_N$ and $X_{N+1} = \emptyset$). To simplify notation, we define $Y_1 = \hat{Y}_1 = \emptyset$ and let $\hat{Y}_N = Y_N$

- Codebook generation: Fix $\prod_{k=1}^{N-1} p(x_k)p(\hat{y}_k|y_k, x_k)$. For each $j \in [1 : b]$, generate an independent codebook as follows:

1. Randomly and independently generate 2^{nbR} sequences $x_1^n(j, m)$, $m \in [1 : 2^{nbR}]$, each according to $\prod_{i=1}^n p_{X_1}(x_{1i})$
2. For each relay node $k \in [2 : N - 1]$, randomly and independently generate 2^{nR_k} sequences $x_k^n(l_{k,j-1})$, $l_{k,j-1} \in [1 : 2^{nR_k}]$, each according to $\prod_{i=1}^n p_{X_k}(x_{ki})$

3. For each $k \in [2 : N - 1]$ and each $x_k^n(l_{k,j-1})$, $l_{k,j-1} \in [1 : 2^{nR_k}]$, randomly and conditionally independently generate 2^{nR_k} sequences $\hat{y}_k^n(l_{kj}|l_{k,j-1})$, $l_{kj} \in [1 : 2^{nR_k}]$, each according to $\prod_{i=1}^n p_{\hat{Y}_k|X_k}(\hat{y}_{ki}|x_{ki}(l_{k,j-1}))$

- Encoding and decoding are explained with the help of the following table:

Block	1	2	...	$b - 1$	b
X_1	$x_1^n(1, m)$	$x_1^n(2, m)$...	$x_1^n(b - 1, m)$	$x_1^n(b, m)$
Y_k	$\hat{y}_k^n(l_{k1} 1), l_{k1}$	$\hat{y}_k^n(l_{k2} l_{k1}), l_{k2}$...	$\hat{y}_k^n(l_{kb-1} l_{kb-2}), l_{kb-1}$	\emptyset
X_k	$x_k^n(1)$	$x_k^n(l_{k1})$...	$x_k^n(l_{kb-2})$	$x_k^n(l_{kb-1})$
Y_N	\emptyset	\emptyset	...	\emptyset	\hat{m}

- Encoding: To send m , source node 1 transmits $x_1^n(j, m)$ is block j

Relay node k , upon receiving $y_k^n(j)$, finds an index l_{kj} such that $(\hat{y}_k^n(l_{kj}|l_{k,j-1}), y_k^n(j), x_k^n(l_{k,j-1})) \in \mathcal{T}_{\epsilon'}^{(n)}$

Assuming that such l_{kj} is found, relay node k sends $x_k^n(l_{kj})$ in block $j + 1$

By the covering lemma, the probability $P(\tilde{\mathcal{E}}_k(j))$ that there is no such l_{kj} tends to 0 as $n \rightarrow \infty$, if $R_k > I(\hat{Y}_k; Y_k|X_k) + \delta(\epsilon')$

- Decoding and analysis of the probability of error: At the end of block b , the receiver finds a unique index \hat{m} such that there exists some $\mathbf{l}^b := (\mathbf{l}_1, \dots, \mathbf{l}_b)$ satisfying

$$(x_1^n(j, \hat{m}), x_2^n(l_{2,j-1}), \dots, x_{N-1}(l_{N-1,j-1}), \\ \hat{y}_2^n(l_{2,j}|l_{2,j-1}), \dots, \hat{y}_{N-1}^n(l_{N-1,j}|l_{N-1,j-1}), y_N^n(j)) \in \mathcal{T}_\epsilon^{(n)}$$

for all $j \in [1 : b]$. Here $\mathbf{l}_j := (l_{2,j}, \dots, l_{N-1,j})$, $j \in [1 : b]$, and $l_{k0} = 1$, $k \in [2 : N - 1]$, by convention

To bound the probability of error, assume without loss of generality that $M = 1$ and $L_{kj} = 1$, $k \in [2 : N - 1], j \in [1 : b]$. Define the events

$$\mathcal{E}_j(m, \mathbf{l}_{j-1}, \mathbf{l}_j) := \{(X_1^n(j, m), X_2^n(l_{2,j-1}), \dots, X_{N-1}^n(l_{N-1,j-1}), \\ \hat{Y}_2^n(l_{2,j}|l_{2,j-1}), \dots, \hat{Y}_{N-1}^n(l_{N-1,j}|l_{N-1,j-1}), Y_N^n(j)) \in \mathcal{T}_\epsilon^{(n)}\}$$

Then the probability of the event of interest (conditioned on the event that $(X_k^n(j, 1), \hat{Y}_k^n(1|1), Y_k^n(j)) \in \mathcal{T}_\epsilon^{(n)}$ for all $k \in [2 : N - 1], j \in [1 : b]$) is bounded by

$$\begin{aligned} \mathsf{P}(\mathcal{E}) &\leq \mathsf{P}(\bigcup_{j=1}^b \mathcal{E}_j^c(1, \dots, 1)) + \mathsf{P}(\bigcup_{m \neq 1} \bigcup_{\mathbf{l}^b} \bigcap_{j=1}^b \mathcal{E}_j(m, \mathbf{l}_{j-1}, \mathbf{l}_j)) \\ &\leq \sum_{j=1}^b \mathsf{P}(\mathcal{E}_j^c(1, \dots, 1)) + \sum_{m \neq 1} \sum_{\mathbf{l}^b} \mathsf{P}(\bigcap_{j=1}^b \mathcal{E}_j(m, \mathbf{l}_{j-1}, \mathbf{l}_j)) \\ &\stackrel{(a)}{=} \sum_{j=1}^b \mathsf{P}(\mathcal{E}_j^c(1, \dots, 1)) + \sum_{m \neq 1} \sum_{\mathbf{l}^b} \prod_{j=1}^b \mathsf{P}(\mathcal{E}_j(m, \mathbf{l}_{j-1}, \mathbf{l}_j)) \\ &\leq \sum_{j=1}^b \mathsf{P}(\mathcal{E}_j^c(1, \dots, 1)) + \sum_{m \neq 1} \sum_{\mathbf{l}^b} \prod_{j=2}^b \mathsf{P}(\mathcal{E}_j(m, \mathbf{l}_{j-1}, \mathbf{l}_j)), \end{aligned}$$

where (a) follows since the codebook is generated independently for each block

By the Markov lemma, the first term $\rightarrow 0$ as $n \rightarrow \infty$

To bound the second term, for each \mathbf{l}^b and $j \in [2 : b]$, define $\mathcal{S}_j(\mathbf{l}^b) \subseteq [1 : N]$ such that $1 \in \mathcal{S}_j(\mathbf{l}^b)$, $N \in \mathcal{S}_j^c(\mathbf{l}^b)$, and $k \in [2 : N - 1] \cap \mathcal{S}_j(\mathbf{l}^b)$ iff $l_{k,j-1} \neq 1$. Note that $\mathcal{S}_j(\mathbf{l}^b)$ depends only on \mathbf{l}_{j-1} and is written as $\mathcal{S}_j(\mathbf{l}_{j-1})$

Now by the joint typicality lemma (check!)

$$P(\mathcal{E}_j(m, \mathbf{l}_{j-1}, \mathbf{l}_j)) \leq 2^{-n(I_1(\mathcal{S}_j(\mathbf{l}_{j-1})) + I_2(\mathcal{S}_j(\mathbf{l}_{j-1})) - \delta(\epsilon))},$$

where $I_1(\mathcal{S}) := (I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c)|X(\mathcal{S}^c))$ and
 $I_2(\mathcal{S}) := \sum_{k \in \mathcal{S}} I(\hat{Y}_k; \hat{Y}(\mathcal{S}^c \cup \{k' \in \mathcal{S} : k' < k\}), X^N|X_k)$. Furthermore,

$$\begin{aligned} & \sum_{\mathbf{l}_{j-1}} 2^{-n(I_1(\mathcal{S}_j(\mathbf{l}_{j-1})) + I_2(\mathcal{S}_j(\mathbf{l}_{j-1})) - \delta(\epsilon))} \\ & \leq \sum_{\substack{\mathcal{S} \subseteq [1:N] \\ 1 \in \mathcal{S}, N \in \mathcal{S}^c}} \sum_{\mathbf{l}_{j-1}: \mathcal{S}_j(\mathbf{l}_{j-1}) = \mathcal{S}} 2^{-n(I_1(\mathcal{S}_j(\mathbf{l}_{j-1})) + I_2(\mathcal{S}_j(\mathbf{l}_{j-1})) - \delta(\epsilon))} \\ & \leq \sum_{\substack{\mathcal{S} \subseteq [1:N] \\ 1 \in \mathcal{S}, N \in \mathcal{S}^c}} 2^{-n(I_1(\mathcal{S}) + I_2(\mathcal{S}) - \sum_{k \in \mathcal{S}} R_k - \delta(\epsilon))} \\ & \leq 2^{N-2} \cdot 2^{-n(\min_{\mathcal{S}}(I_1(\mathcal{S}) + I_2(\mathcal{S}) - \sum_{k \in \mathcal{S}} R_k - \delta(\epsilon)))} \end{aligned}$$

Hence,

$$\begin{aligned} & \sum_{m \neq 1} \sum_{\mathbf{l}^b} \prod_{j=2}^b P(\mathcal{E}_j(m, \mathbf{l}_{j-1}, \mathbf{l}_j)) \\ & \leq \sum_{m \neq 1} \sum_{\mathbf{l}^b} \cdot \prod_{j=2}^b \left(\sum_{\mathbf{l}_{j-1}} 2^{-n(I_1(\mathcal{S}_j(\mathbf{l}_{j-1})) + I_2(\mathcal{S}_j(\mathbf{l}_{j-1})) - \delta(\epsilon))} \right) \\ & \leq 2^{(N-2)(b-1)} \cdot 2^{n(bR + \sum_{k=2}^{N-1} R_k - (b-1) \min_{\mathcal{S}}(I_1(\mathcal{S}) + I_2(\mathcal{S}) - \sum_{k \in \mathcal{S}} R_k - \delta(\epsilon)))}, \end{aligned}$$

which $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R < \frac{b-1}{b} \left(\min_{\mathcal{S}} \left(I_1(\mathcal{S}) + I_2(\mathcal{S}) - \sum_{k \in \mathcal{S}} R_k \right) - \delta(\epsilon) \right) - \frac{1}{b} \left(\sum_{k=2}^{N-1} R_k \right)$$

By eliminating $R_k > I(\hat{Y}_k; Y_k|X_k) + \delta(\epsilon')$ and letting $b \rightarrow \infty$, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R < \min_{\mathcal{S}} \left(I_1(\mathcal{S}) + I_2(\mathcal{S}) - \sum_{k \in \mathcal{S}} I(\hat{Y}_k; Y_k|X_k) \right) - (N-2)\delta(\epsilon') - \delta(\epsilon)$$

Finally, note that

$$\begin{aligned}
I_2(\mathcal{S}) - \sum_{k \in \mathcal{S}} I(\hat{Y}_k; Y_k | X_k) &= \sum_{k \in \mathcal{S}} I(\hat{Y}_k; Y_k | X^N, \hat{Y}(\mathcal{S}^c), \hat{Y}(\{k' \in \mathcal{S} : k' < k\})) \\
&= \sum_{k \in \mathcal{S}} I(\hat{Y}_k; Y(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c), \hat{Y}(\{k' \in \mathcal{S} : k' < k\})) \\
&= I(\hat{Y}(\mathcal{S}); Y(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c))
\end{aligned}$$

Therefore, the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$R < \min_{\mathcal{S}} \left(I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c) | X(\mathcal{S}^c)) - I(\hat{Y}(\mathcal{S}); Y(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c)) \right) - (N-2)\delta(\epsilon') - \delta(\epsilon),$$

which completes the proof of achievability for a single destination node N

In general when $X_N \neq \emptyset$, it can be easily seen by relabeling nodes that the above condition becomes

$$\begin{aligned}
R < \min_{\mathcal{S}} &\left(I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_N | X(\mathcal{S}^c)) \right. \\
&\left. - I(\hat{Y}(\mathcal{S}); Y(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c), Y_N) \right) - (N-2)\delta(\epsilon') - \delta(\epsilon),
\end{aligned}$$

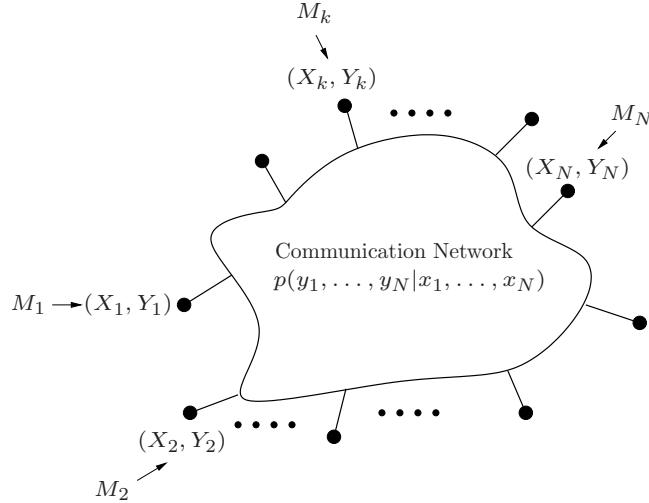
- Now to prove the achievability for a general multicast setup, note that each relay encoder operates in the same manner at the same rate regardless of which node is the destination. Therefore, if each destination node performs the multi-block decoding procedure as in the single-destination case described above, then the probability of decoding error $\rightarrow 0$ as $n \rightarrow 0$, provided that the rate condition for each destination node $k \in \mathcal{D}$ satisfies

$$\begin{aligned}
R < \min_{\mathcal{S}} &\left(I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_j | X(\mathcal{S}^c)) \right. \\
&\left. - I(\hat{Y}(\mathcal{S}); Y(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c), Y_j) \right) - (N-2)\delta(\epsilon') - \delta(\epsilon),
\end{aligned}$$

where the minimum is taken over all cutsets for node j . This completes the proof of achievability

Discrete Memoryless Multiple Source Network

- An N -node *discrete memoryless network* (DMN) $(\mathcal{X}_1 \times \dots \times \mathcal{X}_N, p(y^N|x^N), \mathcal{Y}_1 \times \dots \times \mathcal{Y}_N)$ consists of N sender-receiver alphabet pairs $(\mathcal{X}_k, \mathcal{Y}_k)$, $k \in [1 : N]$, and a collection of conditional pmfs $p(y^N|x^N)$. Each node $k \in [1 : N]$ wishes to send a message M_k to a set $\mathcal{D}_k \subseteq [1 : N] \setminus \{k\}$ of destination nodes



- Formally, a $(2^{nR_1}, 2^{nR_2}, \dots, 2^{nR_N}, n)$ code for a DMN consists of:
 1. Message sets $[1 : 2^{nR_1}], \dots, [1 : 2^{nR_{N-1}}]$
 2. A set of N encoders: Encoder k assigns a symbol $x_{ki}(m_k, y_k^{i-1})$ to each pair (m_k, y_k^{i-1}) for $i \in [1 : n]$
 3. A set of N decoders: Decoder k assigns message estimates $\{\hat{m}_{jk} : j \in [1 : N], k \in \mathcal{D}_j\}$ or an error message to each pair (m_k, y_k^n)
 Note that each node has only one message to send, but can be a destination for zero, one, or more messages. A node can also serve as a relay for messages from other nodes
- Assume that the message tuple (M_1, \dots, M_N) is uniformly distributed over $[1 : 2^{nR_1}] \times \dots \times [1 : 2^{nR_N}]$
- The probability of error is $P_e^{(n)} = \mathbb{P}\{\hat{M}_{jk} \neq M_j \text{ for some } j \in [1 : N], k \in \mathcal{D}_j\}$
- A rate tuple (R_1, \dots, R_N) is said to be achievable if there exists a sequence of codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The capacity region of the DMN is the closure of the set of achievable rates

- Note that this model includes the DM-MAC, DM-IC, DM-RC, and the DM-TWC as special cases
However, it does *not* include broadcast networks with multiple messages sent from a single source. For this case, the outer bound we derive will apply only to the *sum rates* from each sender
 - *Theorem 4 (Cutset Outer Bound):* If a rate tuple (R_1, \dots, R_N) is achievable, then for some $p(x_1, \dots, x_N)$,
- $$\sum_{k \in \mathcal{S}: \mathcal{D}_k \cap \mathcal{S}^c \neq \emptyset} R_k \leq I(X(\mathcal{S}); Y(\mathcal{S}^c) | X(\mathcal{S}^c))$$
- for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D}_k \cap \mathcal{S}^c \neq \emptyset$ for some $k \in [1 : N]$
- The outer bound is not tight in general. Sometimes we can obtain tighter, single letter bounds using tricks (e.g., auxiliary random variables, EPI, Mrs. Gerber's lemma) specific to each channel model
 - Examples where the bound is tight:
 - Noiseless networks with the same set of destinations ($\mathcal{D}_1 = \dots = \mathcal{D}_N = \mathcal{D}$) (cf. Lecture Notes 16)
 - Physically degraded and classes of deterministic relay networks [1, 2, 9]

- Remark: When no cooperation between the nodes is possible (or allowed), i.e., the encoder of each node is a function only of its own message, the outer bound can be tightened by conditioning on a time-sharing random variable Q and replacing $p(x^N)$ by $p(q) \prod_{k=1}^N p(x_k|q)$

With this modification, the bound becomes tight for the N -sender DM-MAC

We also obtain a tighter outer bound on the capacity region of the N sender–receiver pair interference channel

- On the other hand, the message repetition compress–forward coding scheme can be generalized [6] to yield the following inner bound on the capacity region:

Theorem 5 (Noisy Network Coding Inner Bound): Let $\mathcal{D} = \bigcup_{k=1}^N \mathcal{D}_k$. A rate tuple (R_1, \dots, R_N) is achievable for the DMN if for some joint pmf $p(q) \prod_{k=1}^N p(x_k|q)p(\hat{y}_k|y_k, x_k)$ such that

$$\begin{aligned} \sum_{k \in \mathcal{S}} R_k &< \min_{k \in \mathcal{S}^c \cap \mathcal{D}} (I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_k | X(\mathcal{S}^c), Q) \\ &\quad - I(Y(\mathcal{S}); \hat{Y}(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c), Y_k, Q)) \end{aligned}$$

for all $\mathcal{S} \subseteq [1 : N]$ with $\mathcal{S}^c \cap \mathcal{D} \neq \emptyset$

- For the deterministic network $Y_k = y_k(X^N)$, the cutset outer bound simplifies to the set of rate tuples such that for some $p(x_1, \dots, x_N)$

$$\sum_{k \in \mathcal{S}: \mathcal{D}_k \cap \mathcal{S}^c \neq \emptyset} R_k \leq H(Y(\mathcal{S}^c) | X(\mathcal{S}^c))$$

for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D} \cap \mathcal{S}^c \neq \emptyset$, where $\mathcal{D} = \cup_{k=1}^N \mathcal{D}_k$

On the other hand, by taking $\hat{Y}_k = Y_k$ for $k \in [1 : N]$, the noisy network coding inner bound simplifies to the set of rate tuples such that for some $p(x_1) \cdots p(x_N)$

$$\sum_{k \in \mathcal{S}} R_k < H(Y(\mathcal{S}^c) | X(\mathcal{S}^c))$$

for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D} \cap \mathcal{S}^c \neq \emptyset$

In some cases these bounds are tight, establishing the capacity region. For example, if $\mathcal{D}_k = \mathcal{D}$ for all $k \in [1 : N]$ (multi-source multicast) and the cutset bound is achieved by a product pmf (such as noiseless networks [11], deterministic networks with no interference, and linear finite-field deterministic networks), then the network compress-forward coding scheme achieves the capacity region

Key New Ideas and Techniques

- Cutset bound
- Multicast decode-forward
- Network compress-forward: message repetition coding

References

- [1] A. El Gamal, "On information flow in relay networks," in *Proc. IEEE National Telecom Conference*, Nov. 1981, vol. 2, pp. D4.1.1–D4.1.4.
- [2] M. R. Aref, "Information flow in relay networks," Ph.D. Thesis, Stanford University, Stanford, CA, Oct. 1980.
- [3] G. Kramer, M. Gastpar, and P. Gupta, "Cooperative strategies and capacity theorems for relay networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 9, pp. 3037–3063, Sept. 2005.
- [4] A. B. Carleial, "Multiple-access channels with different generalized feedback signals," *IEEE Trans. Inf. Theory*, vol. 28, no. 6, pp. 841–850, Nov. 1982.
- [5] L.-L. Xie and P. R. Kumar, "An achievable rate for the multiple-level relay channel," *IEEE Trans. Inf. Theory*, vol. 51, no. 4, pp. 1348–1358, 2005.
- [6] S. H. Lim, Y.-H. Kim, A. El Gamal, and S.-Y. Chung, "Network compress-forward," 2009.
- [7] T. M. Cover and A. El Gamal, "Capacity theorems for the relay channel," *IEEE Trans. Inf. Theory*, vol. 25, no. 5, pp. 572–584, Sept. 1979.
- [8] A. El Gamal, M. Mohseni, and S. Zahedi, "Bounds on capacity and minimum energy-per-bit for AWGN relay channels," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1545–1561, 2006.
- [9] S. Avestimehr, S. Diggavi, and D. Tse, "Wireless network information flow," 2007, submitted to *IEEE Trans. Inf. Theory*, 2007. [Online]. Available: <http://arxiv.org/abs/0710.3781/>
- [10] N. Ratnakar and G. Kramer, "The multicast capacity of deterministic relay networks with no interference," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2425–2432, 2006.

- [11] A. F. Dana, R. Gowaikar, R. Palanki, B. Hassibi, and M. Effros, "Capacity of wireless erasure networks," *IEEE Trans. Inf. Theory*, vol. 52, no. 3, pp. 789–804, 2006.

Lecture Notes 20

Gaussian Networks

- AWGN Network Model
- Multi-Source Multicast Capacity Region Within Constant Gap
- Capacity Scaling Laws
- Gupta–Kumar Random Network Approach
- Key New Ideas and Techniques
- Appendix: Proof of Lemma 1
- Appendix: Proof of Lemma 2

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

AWGN Network Model

- Motivated by wireless networks, we consider the AWGN network: At time i ,

$$Y^N(i) = GX^N(i) + Z^N(i),$$

where $Y_j(i)$, $j \in [1 : N]$, is the reception at node j , $G \in \mathbb{R}^{N \times N}$ is the channel gain matrix, $X_j(i)$, $j \in [1 : N]$, is the transmission at node j , and $\{Z^N(i)\}$ is a vector of independent WGN(1) processes

- We assume average power constraint P on each sender:

$$\sum_{i=1}^n E(X_j^2(i)) \leq nP \text{ for all } j \in [1 : N]$$

- Given the message requirement (e.g., relay, multicast, multiple unicast), the definitions of codes, probability of error, achievability, and capacity region follow the corresponding DM network
- We consider two channel gain models
 - Constant network: G is an arbitrary constant gain matrix
 - Random network: G is a random gain matrix that depends on the random placement of nodes in the unit area. The path gain G_{jk} between two nodes j

and k with distance r is often modeled by $g(r) = r^{-\nu/2}$ for some $\nu > 2$ (power law) or more generally by $g(r) = e^{-\gamma r/2}r^{-\nu/2}$ for some $\gamma \geq 0$ and $\nu > 2$ (power law with absorption)

- The cutset bounds in Lecture Notes 19 can be easily specialized to the Gaussian network model. For example, if (R_1, \dots, R_N) is achievable for the multi-source Gaussian network with destination sets $(\mathcal{D}_1, \dots, \mathcal{D}_N)$, then for some $X^N \sim N(0, K)$ with $K_{jj} \leq P$, $j \in [1 : N]$,

$$\begin{aligned} \sum_{j \in \mathcal{S}: \mathcal{D}_j \cap \mathcal{S}^c \neq \emptyset} R_j &\leq I(X(\mathcal{S}); Y(\mathcal{S}^c) | X(\mathcal{S}^c)) \\ &\leq h(Y(\mathcal{S}^c) | X(\mathcal{S}^c)) - h(Z(\mathcal{S}^c)) \\ &\leq \frac{1}{2} \log |I + G(\mathcal{S})K(\mathcal{S})G(\mathcal{S})^T| \end{aligned}$$

for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D}_j \cap \mathcal{S}^c \neq \emptyset$ for some $j \in [1 : N]$, where $G(\mathcal{S})$ is defined such that

$$Y(\mathcal{S}^c) = G(\mathcal{S})X(\mathcal{S}) + G'(\mathcal{S}^c)X(\mathcal{S}^c) + Z(\mathcal{S}^c)$$

and $K(\mathcal{S})$ is the conditional covariance matrix of $X(\mathcal{S})$ given $X(\mathcal{S}^c)$

- As in DM networks, when no cooperation between the nodes is possible, the cutset outer bound can be tightened by conditioning on a time-sharing random variable Q and considering $X^N | \{Q = q\} \sim N(0, K(q))$, where $K(q)$ is diagonal and $E_Q(K_{jj}(Q)) \leq P$:

$$\sum_{j \in \mathcal{S}: \mathcal{D}_j \cap \mathcal{S}^c \neq \emptyset} R_j \leq \frac{1}{2} E_Q(\log |I + G(\mathcal{S})K(\mathcal{S}|Q)G(\mathcal{S})^T|)$$

for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D}_j \cap \mathcal{S}^c \neq \emptyset$ for some $j \in [1 : N]$, where $K(\mathcal{S}|Q)$ is the (random) covariance matrix of $X(\mathcal{S})$ given Q

- In general, it is extremely hard to characterize the capacity region in a computable (i.e., single-letter) form, even for simple networks (e.g., relay channel or interference channel). Can we still learn and say something about information flow in a general Gaussian network? We discuss two approaches:
 - Bounds within constant gap: Here we derive bounds on capacity that differ by no more than some constant (cf. the example in Lecture Notes 6 regarding the AWGN-IC capacity within 1/2-bit). Such bounds provide guarantees on the rates of the coding schemes that achieve the inner bounds
 - Scaling laws: Here we investigate how capacity scales with the number of nodes in the network. This approach can shed light on optimal network architecture designs and protocols

Multisource Multicast Capacity Region Within Constant Gap

- Consider the multisource multicast setup $\mathcal{D}_j = \mathcal{D}$, $j \in [1 : N]$, i.e., each destination node wishes to decode all messages
- The cutset bound can be further relaxed to

$$\begin{aligned} \sum_{j \in \mathcal{S}: \mathcal{D} \cap \mathcal{S}^c \neq \emptyset} R_j &\leq \frac{1}{2} \log |I + G(\mathcal{S})K(\mathcal{S})G(\mathcal{S})^T| \\ &\stackrel{(a)}{\leq} \frac{1}{2} \log |I + |\mathcal{S}|P \cdot G(\mathcal{S})G(\mathcal{S})^T| \\ &\leq \frac{1}{2} \log \left| I + \frac{P}{2}G(\mathcal{S})G(\mathcal{S})^T \right| + \frac{|\mathcal{S}^c|}{2} \log(2|\mathcal{S}|) \end{aligned}$$

for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D} \cap \mathcal{S}^c \neq \emptyset$, where (a) follows since $K \preceq \text{tr}(K)I$ for any $K \succeq 0$ and $\text{tr}(K(\mathcal{S})) \leq |\mathcal{S}|P$ from the power constraint

- On the other hand, the multisource multicast noisy network coding inner bound gives the following bound on the capacity region:

Theorem 1: A rate tuple (R_1, \dots, R_N) is achievable for the Gaussian multisource multicast network if

$$\sum_{j \in \mathcal{S}} R_j < \frac{1}{2} \log \left| I + \frac{P}{2}G(\mathcal{S})G(\mathcal{S})^T \right| - \frac{|\mathcal{S}|}{2}$$

for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D} \cap \mathcal{S}^c \neq \emptyset$

- To show this, let $Q \neq \emptyset$ and $X_j \sim \mathcal{N}(0, P)$, $j \in [1 : N]$, be independent of each other. Let $\hat{Y}_j = Y_j + \hat{Z}_j$, where $\hat{Z}_j \sim \mathcal{N}(0, 1)$, $j \in [1 : N]$, are independent of each other and of X^N
- For each $k \in \mathcal{D}$, consider

$$\begin{aligned} I(\hat{Y}(\mathcal{S}); Y(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c), Y_k) &\stackrel{(a)}{\leq} I(\hat{Y}(\mathcal{S}); Y(\mathcal{S}) | X^N) \\ &= h(\hat{Y}(\mathcal{S}) | X^N) - h(\hat{Y}(\mathcal{S}) | Y(\mathcal{S}), X^N) \\ &= \frac{|\mathcal{S}|}{2} \log(2\pi e) - \frac{|\mathcal{S}|}{2} \log(\pi e) = \frac{|\mathcal{S}|}{2} \end{aligned}$$

where (a) follows from the Markovity $(\hat{Y}(\mathcal{S}^c), Y_k) \rightarrow (X^N, Y(\mathcal{S})) \rightarrow \hat{Y}(\mathcal{S})$

- Next consider

$$\begin{aligned}
I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_k | X(\mathcal{S}^c)) &\geq I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c) | X(\mathcal{S}^c)) \\
&= h(\hat{Y}(\mathcal{S}^c) | X(\mathcal{S}^c)) - h(\hat{Y}(\mathcal{S}^c) | X^N) \\
&= \frac{1}{2} \log \left| I + \frac{P}{2} G(\mathcal{S}) G(\mathcal{S})^T \right|
\end{aligned}$$

- Hence by the noisy network coding theorem, the rate tuple (R_1, \dots, R_N) is achievable if

$$\sum_{j \in \mathcal{S}} R_j < I(X(\mathcal{S}); \hat{Y}(\mathcal{S}^c), Y_k | X(\mathcal{S}^c)) - I(\hat{Y}(\mathcal{S}); Y(\mathcal{S}) | X^N, \hat{Y}(\mathcal{S}^c), Y_k)$$

$$\leq \frac{1}{2} \log \left| I + \frac{P}{2} G(\mathcal{S}) G(\mathcal{S})^T \right| - \frac{|\mathcal{S}|}{2}$$

for all $\mathcal{S} \subseteq [1 : N]$ such that $\mathcal{D} \cap \mathcal{S}^c \neq \emptyset$

- Note that the noisy network coding lower bound is interesting in the high SNR regime with the gap of

$$\max_{\mathcal{S}} |\mathcal{S}|/2 + (|\mathcal{S}^c|/2) \log(2|\mathcal{S}|) \leq (N/2) \log(4N)$$

bits from the cutset outer bound. In low and moderate SNR, however, the bound is very loose because the compress-forward scheme results in accumulation of noise that significantly degrades its performance

Capacity Scaling Laws

- We begin with some simple examples where the set \mathcal{S} of *message source nodes* and the set \mathcal{D} of *message destination nodes* are disjoint, i.e., $R_j = 0$, $j \in \mathcal{S}$ and $\mathcal{S} \cap \mathcal{D} = \emptyset$, and the rest of the nodes act as relays to help other nodes communicate their messages
- We then consider a random network model, where the source and destination nodes themselves can also act as relays
- We only consider *network symmetric capacity* $C(N)$, which is the supremum of the set of symmetric rates R such that the rate tuple (R, \dots, R) is achievable
 - In few scenarios we know $C(N)$ exactly
 - In other scenarios we only know its *order*, i.e., how it scales with N
 - But in more general scenarios, we have only loose upper and lower bounds on its order

- Questions we wish to answer using scaling laws:
 - How bad is interference?
 - How does path loss affect network symmetric capacity?
 - How bad is direct communication, i.e., when no cooperation via feedback or relaying is allowed?
 - How useful is relaying?
 - What architectures (transmission schemes) are good for large wireless networks?

N-Sender AWGN Multiple Access Channel

- Consider an N -sender AWGN MAC with associated transmitted random vector $X^N = (X_1, X_2, \dots, X_N)$, received random variable $Y = \sum_{j=1}^N X_j + Z$, where $Z \sim N(0, 1)$, and average power constraint P on each sender
- By the cutset outer bound, the symmetric capacity is upper bounded by

$$C(N) \leq \frac{1}{N} \max_{\prod_{j=1}^N F(x_j)} I(X^N; Y) = C(NP)$$

- We also know that this sum capacity can be achieved using successive cancellation or time-division
- Thus $C(N) = (1/N) C(NP)$
- The order of growth of $C(N) = \Theta(\log N/N)$, which $\rightarrow 0$ as $N \rightarrow \infty$

N S-D pair AWGN Interference Channel Example

- Consider an N source–destination (S-D) pair AWGN interference channel:

$$Y^N = GX^N + Z^N,$$

where G is an $N \times N$ channel gain matrix given by

$$G = \begin{bmatrix} 1 & a & \cdots & a \\ a & 1 & \cdots & a \\ \vdots & \vdots & \ddots & \vdots \\ a & a & \cdots & 1 \end{bmatrix}$$

- Each source X_j wishes to send an independent message M_j to its destination Y_j at rate R_j
- Wish to find the symmetric capacity $C(N)$
- Capacity region for this interference channel is not known, in general
- How does $C(N)$ scale with N ?

- If $a = 0$ (no interference)

$$C(N) = \frac{1}{2} \log(1 + P) = C(P)$$

So for any a , $C(N) = O(1)$

- For $a \neq 0$, a time-division scheme, where each sender transmits $1/N$ fraction of the time at power NP , achieve

$$C(N) = \Omega(\log N/N)$$

- Very large gap between above two bounds

- Let's try to find a tighter upper bound on $C(N)$:

By the cutset bound, the symmetric capacity is upper bounded by

$$\begin{aligned} C(N) &\leq \frac{1}{N} \max_{\prod_{j=1}^N F(x_j): \mathbb{E}(X_j^2) \leq P, j \in [1:N]} I(X^N; Y^N) \\ &= \frac{1}{2N} \log |I + GG^T P| \end{aligned}$$

- The determinant has a simple form:

$$|I + GG^T P| = (1 + (a - 1)^2 P)^{k-1} (1 + (a(N - 1) + 1)^2 P)$$

- Thus

$$C(N) \leq \frac{N-1}{N} C((a-1)^2 P) + \frac{1}{N} C((a(N-1)+1)^2 P)$$

- If $a = 1$, $C(N) \leq (1/N) C(N^2 P) = O(\log N/N)$ —not tight but has the same scaling as achieved by the TDM
- For $a \neq 1$, $C(N) = O(1)$ —bound probably *very* loose

N -Relay AWGN Network

- Consider a single source, single destination, N -relay AWGN network:



- Assume the power law path gain $g(r) = r^{-\nu/2}$, where r is the distance and $\nu > 2$ is the path loss exponent. The received signal at node j is

$$Y_j = \sum_{\substack{k=0 \\ k \neq j}}^N |j-k|^{-\nu/2} X_k + Z_j, \quad j \in [1 : N+1]$$

and the source and relay encoders are given by $X_0^n = x^n(M)$ and $X_{ji} = x_{ji}(Y_j^{i-1})$, $j \in [1 : N]$, $i \in [1 : n]$

- Find the capacity $C(N)$ from source to destination

Achievable Rates

- Capacity of the AWGN relay channel is not known, even for $N = 1$
- How does $C(N)$ scale with N ?
- Without relaying, the maximum rate from the source to the destination is $C(PN^{-\nu}) = \Omega(N^{-\nu})$
- Consider a simple multi-hop scheme, where signals are Gaussian and interference is treated as noise (cf. Lecture Notes 17). In each block:
 - The source transmits a new message to the first relay
 - Relay $j - 1$ transmits its most recently received message to relay j
 - Relay N sends its most recently received message to destination
- The interference power at receiver j is: $I_j = \sum_{\substack{k=0 \\ k \neq j-1, j}}^N |k-j|^{-\nu} P$
- Thus $C(N) \geq \min_j C(P/(I_j + 1))$
- Since $\nu > 1$, $I_j = O(1)$ for all j
Thus $C(N) = \Omega(1)$ —a huge increase from rate without relaying

Upper Bound

- Consider the broadcast bound

$$\begin{aligned} C(N) &\leq \max_{F(x^N): \mathbb{E}(X_j^2) \leq P, j \in [1:N]} I(X_0; Y_1, \dots, Y_{N+1} | X_1, \dots, X_N) \\ &\leq \frac{1}{2} \log |I + AP|, \end{aligned}$$

where

$$A = \begin{bmatrix} 1 \\ \frac{1}{2^{\nu/2}} \\ \frac{1}{3^{\nu/2}} \\ \vdots \\ \frac{1}{(N+1)^{\nu/2}} \end{bmatrix} \begin{bmatrix} 1 & \frac{1}{2^{\nu/2}} & \frac{1}{3^{\nu/2}} & \cdots & \frac{1}{(N+1)^{\nu/2}} \end{bmatrix}$$

This is a rank one matrix with a single nonzero eigenvalue $\lambda = \sum_{j=1}^{k+1} 1/j^\nu$

Hence

$$C(N) \leq C \left(\left(\sum_{j=1}^{N+1} 1/j^\nu \right) P \right),$$

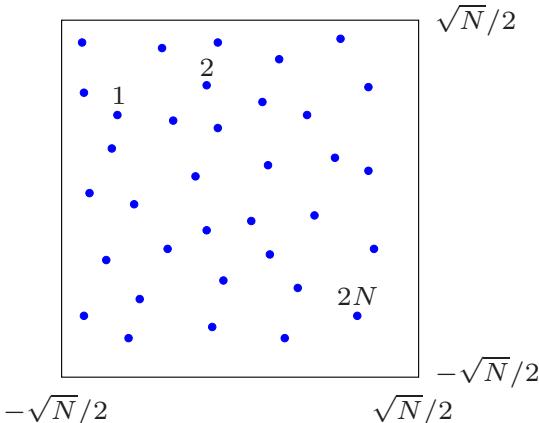
- Since $\nu > 1$, $C(N) = O(1)$ —same scaling as achieved by the simple multi-hop scheme
- Conclusion: Relaying significantly increases rate when path loss is large
- Relaying can also increase the rate in the presence of interference, as we will see shortly

Gupta–Kumar Random Network Approach

- We know that finding capacity for specific networks when broadcasting, interference, and/or relaying are included is in general quite intractable
- The Gupta–Kumar random network approach aims to establish scaling laws for capacity that apply to *most* large networks
- The results can help us better understand the roles of interference and cooperation in large networks, which could lead to better wireless network architectures

Multiple Unicast Network

- Consider a network with $2N$ nodes, each randomly and independently placed according to a uniform pdf over a square of area N (this is referred to as the *constant density model*)
- The nodes are randomly partitioned into N source–destination (S-D) pairs



- 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
- Label the source nodes as $1, 2, \dots, N$ and the destination nodes as $N+1, N+2, \dots, 2N$
- Assume the AWGN channel model with path gain $g(r) = r^{-\nu/2}$, $\nu > 2$, so destination node j , $j \in [N+1 : 2N]$, receives

$$Y_j = \sum_{k=1}^N X_k r_{kj}^{-\nu/2} + Z_j$$

We assume the same average power constraint P on each sender

- Source j wishes to send a message $M_j \in [1 : 2^{nR_j}]$ reliably to destination $j+N$. The messages are assumed to be independent
- We wish to determine the scaling law for the symmetric capacity $C(N)$ that holds *with high probability* (w.h.p.), i.e., with probability $\geq (1 - \epsilon_N)$, where $\epsilon_N \rightarrow 0$ as $N \rightarrow \infty$ (thus holds for most large networks generated in this random manner)

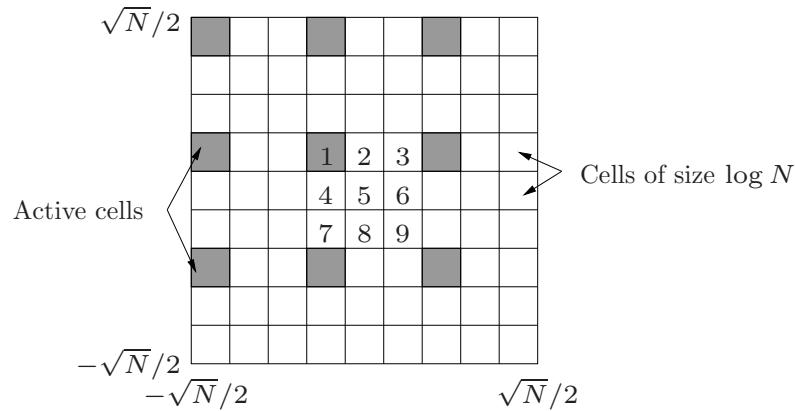
- This problem was first posed and investigated by Gupta and Kumar [1] who assumed a *network theoretic* model:
 - They assumed signal-to-interference *SIR* and *protocol* models for successful transmission
 - They roughly showed that the symmetric capacity under these models scales as $\Theta(N^{-1/2})$
- We assume an information-theoretic model and prove a similar lower bound but only a loose upper bound
- *Theorem 1:* The sum-capacity of the random network model for $\nu > 2$ satisfies the following order bounds
 1. Lower bound [1, 2]: $C(N) = \Omega(N^{-1/2}(\log N)^{-(\nu+1)/2})$ w.h.p.
 2. Upper bound [3]: $C(N) = O(N^{(-1/2+1/\nu)} \log N)$ w.h.p.
- Remark: In [4] the lower bound was improved to $C(N) = \Omega(N^{-1/2})$ w.h.p.

Achievable Rates

- Before proving the upper and lower bounds on symmetric capacity scaling, consider the following simple transmission schemes
- Single randomly chosen S-D pair:
 - Direct transmission achieves $\Omega(N^{-(1+\nu/2)})$
 - Using $\Omega(N^{1/2})$ other nodes as relays (roughly along a straight line from source to destination) and the multi-hop relaying, can show that $\Omega((\log N)^{-\nu/2}/N)$ is achievable w.h.p.—a huge improvement over direct transmission (proved later)
- Lower bound on symmetric capacity for direct transmission: TDM with power control and equal per user pair rate achieves $\Omega(N^{-\nu/2})$
Can do better. Using TDM and multi-hop relaying (no power control), the symmetric capacity $C(N) = \Omega((\log N)^{-\nu/2}/N)$ w.h.p.
- Now we show that much higher symmetric rate can be achieved using a *cellular TDM* scheme

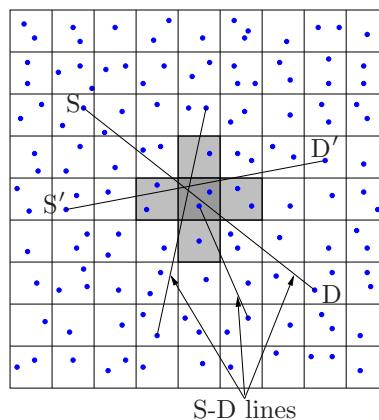
Proof of Lower Bound on $C(N)$ [2]

- Consider a cellular TDM scheme with cells of area $\log N$ (to guarantee that no cell is empty w.h.p.)



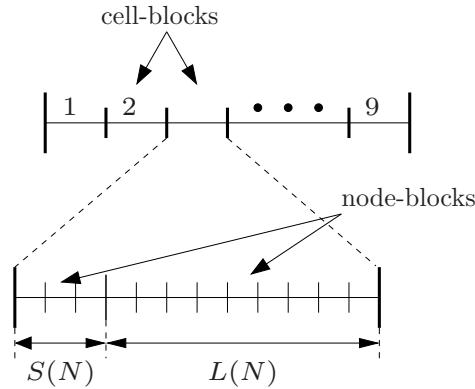
- We assume the same rate for all S-D pairs
- A block Markov transmission scheme is used, where each source sends messages over several transmission blocks
- The cells are divided into 9 groups as shown in the figure, and each transmission block is divided into 9 *cell-blocks*

- A cell is said to be *active* if its nodes are allowed to transmit
- Each cell is active only during one out the 9 cell-blocks. Nodes in non-active cells act as receivers
- Each message is sent from a source to its destination 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 4 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
- Each cell-block is divided into $S(N) + L(N)$ node-blocks for time-division transmission by nodes inside each active cell
 - Each source node in an active cell broadcasts a *new* message during its node-block using Gaussian random codes code with power P
 - One of the nodes in the active cell acts as a relay for the S-D pairs that send their messages through this cell. It relays the messages during the allotted $L(N)$ node-blocks using optimal AWGN channel codes with power P



Analysis of the Probability of Failure

- The cellular TDM scheme we described fails if
 - There is a cell with no nodes in it. Denote this event by \mathcal{E}_1
 - A transmission from a node in a cell to a node in a neighboring cell fails. Denote this event by \mathcal{E}_2
- The total probability that the scheme fails is

$$P(\mathcal{E}) = P(\mathcal{E}_1) + P(\mathcal{E}_2 \cap \mathcal{E}_1^c)$$

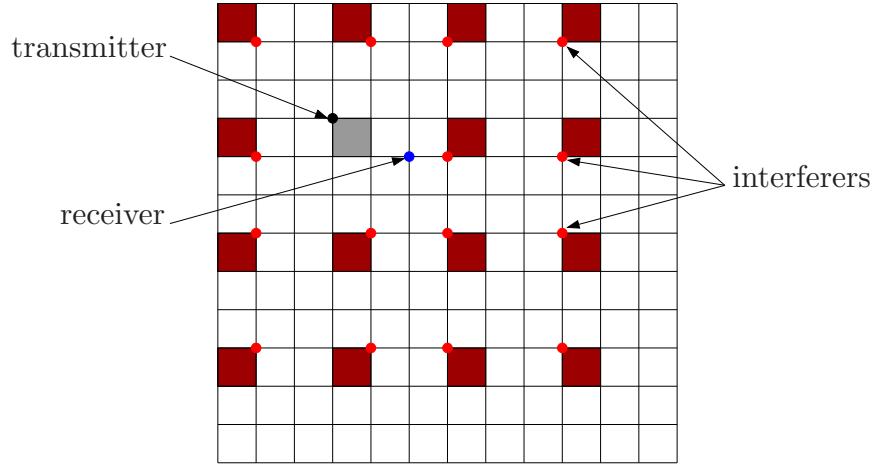
We bound each term as follows:

- It straightforward to show that $P(\mathcal{E}_1) \rightarrow 0$ as $N \rightarrow \infty$
- Consider the event $(\mathcal{E}_2 \cap \mathcal{E}_1^c)$:
 - From the cell geometry, the distance between each transmitting node in a cell and each receiving node in its neighboring cells is always $\leq (5 \log N)^{1/2}$
 - Since each transmitting node uses power P , the received power at a node in a neighboring cell is always $\geq (5 \log N)^{-\nu/2} P$

- From the description of the cellular scheme, we can show (see figure below) that the total average interference power at a receiver from all other transmitting nodes during a cell-block is

$$I \leq \sum_{j=1}^{\infty} \frac{2P}{((3j-2)^2 \log N)^{\nu/2}} + \sum_{j=1}^{\infty} \sum_{k=1}^{\infty} \frac{4P}{(((3j-2)^2 + (3k-1)^2) \log N)^{\nu/2}}$$

Thus if $\nu > 2$, $I \leq a_1(\log N)^{-\nu/2}$, for some constant $a_1 > 0$



Since we are using Gaussian random codes, the probability of error $\rightarrow 0$ as node-block length $n \rightarrow \infty$ if

$$r(N) = C \left(\frac{(5 \log N)^{-\nu/2} P}{1 + a_1(\log N)^{-\nu/2}} \right)$$

Thus for a fixed N and n sufficiently large, $P(\mathcal{E}_3 \cap \mathcal{E}_1^c \cap \mathcal{E}_2^c) \leq 1/N$

- From the above bounds, it follows that a symmetric rate

$$R(N) = \frac{1}{9(L(N) + S(N))} C \left(\frac{(5 \log N)^{-\nu/2} P}{1 + a_1(\log N)^{-\nu/2}} \right) \text{ is achievable w.h.p.}$$

- We can bound $L(N) + S(N)$ as follows:

Lemma 1: $L(N) + S(N) = O((N \log N)^{1/2})$ w.h.p.

The proof is provided in the Appendix

- Thus, we have shown that $C(N) = \Omega(N^{-1/2}(\log N)^{-(\nu+1)/2})$ w.h.p., which completes the proof (check!)

- Remarks:

- Compare this result to $C(N) = \Omega((\log N)^{-\nu/2}/N)$ using TDM and multi-hop

- In [4], the above lower bound was improved to $C(N) = \Omega(N^{-1/2})$ using percolation theory

Upper Bound On $C(N)$

- We show that $C(N) = O(N^{(-1/2+1/\nu)} \log N)$ w.h.p.
- For a given network, denote the source transmissions by X_1, X_2, \dots, X_N and the destination receptions by $Y_{N+1}, Y_{N+2}, \dots, Y_{2N}$, where

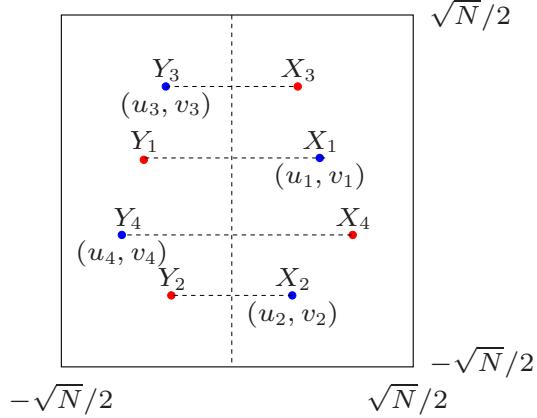
$$Y_k = \sum_{j=1}^N g_{jk} X_j + Z_k, \quad k = N+1, \dots, 2N$$

- Divide the square area of the network into two halves. Assume the case where there are $N/3$ sources on the left half and more than $1/3$ 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 $\rightarrow 0$ as $N \rightarrow \infty$. We relabel the nodes so that these sources are $1, \dots, N'$ and the corresponding destinations are $N+1, \dots, N+N'$
- By the cutset outer bound, the symmetric capacity for these source nodes is upper bounded by

$$\max_{F(x^N)} \frac{1}{N'} I(X^{N'}; Y_{N+1}^{N+N'} | X_{N'+1}^N) \leq \max_{F(x^N)} \frac{1}{N'} I(X^{N'}; \tilde{Y}_{N'+1}^{2N'}),$$

where $\tilde{Y}_k = \sum_{j=1}^{N'} g_{jk-N'+N} X_j + Z_{k-N'+N}$ for $k = N'+1, \dots, 2N'$

- Since the symmetric capacity of the original network is upper bounded by the symmetric capacity of these N' source–destination pairs, we will consider the subnetwork of these source–destination pairs only. We relabel N' as N and \tilde{Y}_k as Y_k for $k = N + 1, \dots, 2N$
- Let node j (source or destination) be at location (u_j, v_j)
- Create an *augmented network* by adding $2N$ mirror nodes as follows:
 - Add destination Y_j at location $(-u_j, v_j)$ for $j \in [1 : N]$
 - Add source X_{N+j} at location $(-u_{N+j}, v_{N+j})$ for $j \in [1 : N]$



We focus on this $N' = N/9$ source–destination pairs and the symmetric capacity $C(N')$ for these nodes

- Consider the augmented $2N$ S-D-pair network

At time i , the received vector at the $2N$ destinations is

$$Y_i^{2N} = GX_i^{2N} + Z_i^{2N},$$

where $\{Z_i^{2N}\}$ is a collection of independent WGN processes each with average 1

- The gain matrix G is symmetric and $G_{jj} = (2|u_j|)^{-\nu/2}$. Furthermore, it can be shown [3] that $G \succeq 0$ (for $\nu > 0$)

- We are now ready to upper bound the symmetric capacity. Consider

$$\begin{aligned}
NC(N) &\leq \sup_{F(x^{2N}): \mathbb{E}|X_j^2| \leq P, j \in [1:2N]} I(X^N; Y_{N+1}^{2N}) \\
&\leq \sup_{F(x^{2N}): \mathbb{E}|X_j^2| \leq P, j \in [1:2N]} I(X^{2N}; Y^{2N}) \\
&\leq \max_{K_X \succeq 0: \text{tr}(K_X) \leq 2NP} \frac{1}{2} \log |I + GK_XG^T| \\
&= \max_{P_j: \sum_{j=1}^{2N} P_j \leq 2NP} \frac{1}{2} \sum_{j=1}^{2N} \log(1 + P_j \lambda_j^2) \\
&\leq \frac{1}{2} \sum_{j=1}^{2N} \log(1 + 2NP \lambda_j^2) \\
&\leq \sum_{j=1}^{2N} \log \left(1 + (2NP)^{1/2} \lambda_j\right) \\
&= \log \left| I_{2N} + (2NP)^{1/2} G \right| \\
&\leq \sum_{j=1}^{2N} \log \left(1 + (2NP)^{1/2} G_{jj}\right),
\end{aligned}$$

where P_j and λ_j , $j \in [1 : 2N]$, are the eigenvalues of the positive semidefinite matrices K_X and G , respectively, and $G_{jj} = (2|U_j|)^{-\nu/2}$

- Define

$$D(N) := \sum_{j=1}^{2N} \log \left(1 + (2|U_j|)^{-\nu/2} (2NP)^{1/2}\right)$$

- *Lemma 2:* $\mathbb{P}\{D(N) = O(N^{(1/2+1/\nu)} \log N)\} > 1 - \epsilon_N$, where $\epsilon_N \rightarrow 0$ as $N \rightarrow \infty$

The proof is given in the Appendix

This establishes the upper bound $C(N) = O(N^{(-1/2+1/\nu)} \log N)$ w.h.p.

- Recall that using the cellular TDM, $C(N) = \Omega(N^{-1/2}(\log N)^{-(\nu+1)/2})$ w.h.p.
- Remark: If we assume the channel path gain to include *absorption*, i.e.,

$$g(r) = e^{-\gamma r/2} \cdot r^{-\nu/2} \text{ for some } \gamma > 0$$

The upper bound on $C(N)$ becomes $O(N^{-1/2}(\log N)^2)$ w.h.p., which has roughly the same order as the lower bound

Key New Ideas and Techniques

- Network sum-capacity $C(N)$ for AWGN networks:
 - We know it exactly for the N -sender MAC
 - We know its order for the N -S-D pair interference network example when $a = 1$
 - We know its order for the N -relay network example
- Random network model (find order capacity for most networks)
- Open problem: How does $C(N)$ grow with N for the symmetric N -S-D pair interference network with $a \neq 1$?

Appendix: Proof of Lemma 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. For each S-D pair on the torus, send each packet along 4 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 for considering the torus is that the pmf of the number of lines in each cell is the same

Let H_j be the total number of hops taken by packets travelling along one of 4 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 $(\log N)^{1/2}$,

$$E(H_j) = \Theta\left((N/\log N)^{1/2}\right)$$

Fix a cell $c \in [1 : N/\log N]$ and define I_{jc} to be the indicator of the event that a line between S-D pair j passes through cell c , i.e.,

$$I_{jc} = \begin{cases} 1 & \text{if a hop of S-D pair } j \text{ is in cell } c \\ 0 & \text{otherwise} \end{cases}$$

for $j \in [1 : N]$ and $c \in [1 : N/\log N]$

Summing up the total number of hops in the cells in two different ways, we obtain

$$\sum_{j=1}^N \sum_{c=1}^{N/\log N} I_{jc} = \sum_{j=1}^N H_j$$

Taking expectations on both sides and noting that all the $\mathbb{P}\{I_{jc} = 1\}$ are equal due to symmetry on the torus, we obtain

$$(N^2/\log N) \mathbb{P}\{I_{jc} = 1\}/\log N = N \mathbb{E}(H_j)$$

Thus

$$\mathbb{P}\{I_{jc} = 1\} = \Theta\left((\log N/N)^{1/2}\right)$$

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 given by $L_c = \sum_{j=1}^N I_{jc}$. This is the sum of N i.i.d. Bernoulli random variables since the positions of the nodes are independent and I_{jc} depends only on the positions of the source and destination nodes of S-D pair j . Moreover,

$$\mathbb{E}(L_c) = \sum_{j=1}^N \mathbb{P}\{I_{jc} = 1\} = \Theta\left((N \log N)^{1/2}\right)$$

for every cell c

By the Chernoff bound,

$$\mathbb{P}\{L_c > (1 + \delta) \mathbb{E}(L_c)\} \leq \exp(-\mathbb{E}(L_c)\delta^2/4)$$

Choosing $\delta = 2\sqrt{\log N / \mathbb{E}(L_c)}$ yields

$$\mathbb{P}\{L_c > (1 + \delta) \mathbb{E}(L_c)\} \leq 1/3N^2$$

Since $\delta = o(1)$, $L_c = O(\mathbb{E}(L_c))$ with probability $\geq 1 - 1/N^2$

Finally using the union of events bound over $N/\log N$ cells shows that

$L(N) = \max_{c \in [1:N/\log N]} L_c = O\left((N \log N)^{1/2}\right)$ with probability $\geq 1 - 1/3N$ for sufficiently large N

Appendix: Proof of Lemma 2

- Note that $D(N)$ is the sum of i.i.d. random variables, thus

$$\mathbb{E}(D(N)) = N \mathbb{E} \left(\log \left(1 + (2U)^{-\nu/2} (2NP)^{1/2} \right) \right) := N \mathbb{E}(X(N)),$$

$$\text{Var}(D(N)) = N \text{Var} \left(\log \left(1 + (2U)^{-\nu/2} (2NP)^{1/2} \right) \right) := N \text{Var}(X(N)),$$

where $U \sim \text{Unif}[0, N^{1/2}]$

We find upper and lower bounds on $\mathbb{E}(X(N))$ and an upper bound on $\mathbb{E}(X^2(N))$

For simplicity, we assume the natural logarithm here since we are only interested in order results

Let $a := 2^{-\frac{\nu-1}{2}} P^{1/2}$, $\nu' := \nu/2$, $k := N^{1/2}$, and $u_0 = (ak)^{1/\nu'}$, and consider

$$\begin{aligned} k \mathbb{E}(X(N)) &= \int_0^k \log(1 + au^{-\nu'} k) du \\ &= \int_0^1 \log(1 + au^{-\nu'} k) du + \int_1^{u_0} \log(1 + au^{-\nu'} k) du \\ &\quad + \int_{u_0}^k \log(1 + au^{-\nu'} k) du \end{aligned}$$

$$\begin{aligned} &\leq \int_0^1 \log((1 + ak)u^{-\nu'}) du + \int_1^{u_0} \log(1 + ak) du + \int_{u_0}^k au^{-\nu'} k du \\ &= \log(1 + ak) + \nu' \int_0^1 \log(1/u) du + (u_0 - 1) \log(1 + ak) \\ &\quad + \frac{ak}{\nu' - 1} \left(u_0^{-(\nu'-1)} - k^{-(\nu'-1)} \right) \end{aligned}$$

Thus there exists a constant $b_1 > 0$ such that for N sufficiently large,

$$\mathbb{E}(X(N)) \leq b_1 N^{(-1/2+1/\nu)} \log N$$

- Now we establish a lower bound on $\mathbb{E}(X(N))$

From the second step of the above derivation, we have

$$\begin{aligned} k \mathbb{E}(X(N)) &\geq \int_1^{u_0} \log(1 + au^{-\nu'} k) du \\ &\geq \int_1^{u_0} \log(1 + a) du \\ &= (u_0 - 1) \log(1 + a) \end{aligned}$$

Thus there exists a constant $b_2 > 0$ such that for N sufficiently large,

$$\mathbb{E}(X(N)) \geq b_2 N^{(-1/2+1/\nu)}$$

Next we find an upper bound on $\mathbb{E}(X^2(N))$. Consider

$$\begin{aligned} k \mathbb{E}(X^2(N)) &= \int_0^1 \left(\log(1 + au^{-\nu'} k) \right)^2 du + \int_1^{u_0} \left(\log(1 + au^{-\nu'} k) \right)^2 du \\ &\quad + \int_{u_0}^k \left(\log(1 + au^{-\nu'} k) \right)^2 du \\ &\leq \int_0^1 \left(\log((1 + ak)u^{-\nu'}) \right)^2 du + \int_1^{u_0} (\log(1 + ak))^2 du \\ &\quad + \int_{u_0}^k a^2 u^{-2\nu'} k^2 du \\ &\leq (\log(1 + ak))^2 + (\nu')^2 \int_0^1 (\log(1/u))^2 du \\ &\quad + 2\nu' \log(1 + ak) \int_0^1 \log(1/u) du \\ &\quad + (u_0 - 1) (\log(1 + ak))^2 + \frac{a^2 k^2}{2\nu' - 1} \left(u_0^{-(2\nu' - 1)} - k^{-(2\nu' - 1)} \right) \end{aligned}$$

Thus there exists a constant $b_3 > 0$ such that for N sufficiently large,

$$\mathbb{E}(X^2(N)) \leq b_3 N^{(-1/2+1/\nu)} (\log N)^2$$

Now, using Chebychev inequality for N sufficiently large, we have

$$\begin{aligned} \mathbb{P}\{D(N) \geq 2b_1 N^{(1/2+1/\nu)} \log N\} &\leq \mathbb{P}\{D(N) \geq 2\mathbb{E}(D(N))\} \\ &\leq \mathbb{P}\{|D(N) - \mathbb{E}(D(N))| \geq \mathbb{E}(D(N))\} \\ &\leq \frac{\text{Var}(D(N))}{(\mathbb{E}(D(N)))^2} \\ &\leq \frac{N \mathbb{E}(X^2(N))}{N^2 (\mathbb{E}(X(N)))^2} \\ &\leq \frac{b_3 N^{(-1/2+1/\nu)} (\log N)^2}{b_2^2 N^{2/\nu}} \\ &= (b_3/b_2^2) N^{(-1/2-1/\nu)} (\log N)^2, \end{aligned}$$

which $\rightarrow 0$ as $N \rightarrow \infty$ This completes the proof of the lemma

References

- [1] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 388–404, 2000.
- [2] A. El Gamal, J. Mammen, B. Prabhakar, and D. Shah, "Optimal throughput–delay scaling in wireless networks—I: The fluid model," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2568–2592, June 2006.
- [3] O. Léveque and İ. E. Telatar, "Information-theoretic upper bounds on the capacity of large extended ad hoc wireless networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 3, pp. 858–865, 2005.
- [4] M. Franceschetti, O. Dousse, D. N. C. Tse, and P. Thiran, "Closing the gap in the capacity of wireless networks via percolation theory," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1009–1018, Mar. 2007.

Lecture Notes 21

Source Coding over Noiseless Networks

- Multiple Descriptions Network
- Interactive Lossless Source Coding
- Two-Way Lossy Source Coding
- Two-Way Source Coding Through a Relay
- Key New Ideas and Techniques

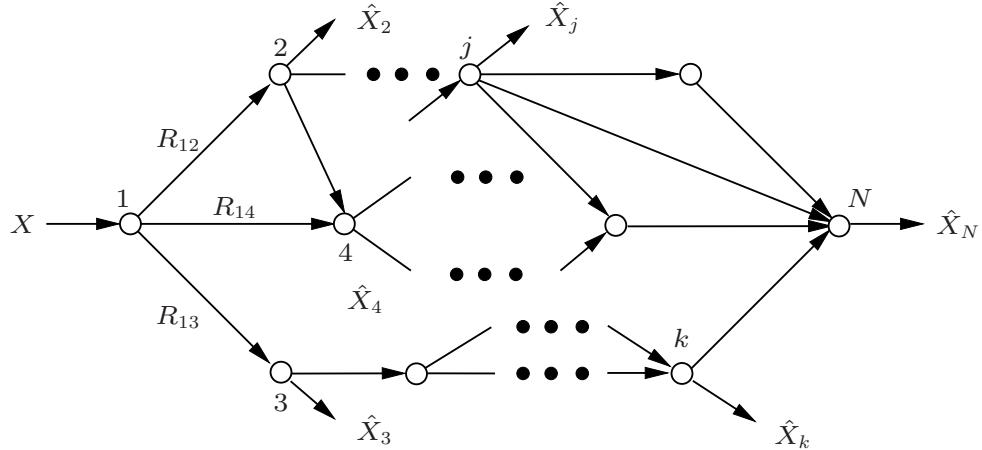
© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Introduction

- In the noiseless networks lecture notes, we assumed that the sources are independent and to be recovered losslessly, and the network is a directed acyclic graph
- In this lecture notes, we generalize this setting in two ways:
 - We first consider single-source multiple descriptions over networks modeled by directed acyclic graphs, and
 - Then, we consider correlated sources over networks with two-way communication and broadcasting

Multiple Descriptions Network

- Consider an N -node communication network modeled by a directed acyclic graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$. Source node 1 observes a DMS X and each node $j \in [2 : N]$ wishes to estimate X with a prescribed distortion D_j under a distortion measure $d_j(x, \hat{x}_j)$. What are the link rates required to achieve the prescribed distortions?



- A $(\{2^{nR_{jk}}\}_{(j,k) \in \mathcal{E}}, n)$ code for the multiple description network $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ consists of
 1. A source encoder that assigns an index $m_{1j}(x^n) \in [1 : 2^{nR_{1j}}]$ to each $x^n \in \mathcal{X}^n$
 2. A set of $N - 1$ relay encoders: For each $(k, l) \in \mathcal{E}$, encoder k assigns an index $m_{kl} \in [1 : 2^{nR_{kl}}]$ to every received index tuple $\{m_{jk} : (j, k) \in \mathcal{E}\}$
 3. A set of $N - 1$ decoders: Decoder k assigns an estimate \hat{x}_j^n to every received index tuple $\{m_{jk} : (j, k) \in \mathcal{E}\}$
- A rate-distortion tuple $(\{R_{jk}\}_{(j,k) \in \mathcal{E}}, D_2, \dots, D_N)$ is achievable if there exists a sequence of $(\{2^{nR_{jk}}\}, n)$ codes such that

$$\limsup_{n \rightarrow \infty} E(d_j(X^n, \hat{X}_j^n)) \leq D_j, \quad j \in [2 : N]$$

- The problem is to find the rate-distortion region $\mathcal{R}(D_2, \dots, D_N)$ for a multiple description network $(\mathcal{N}, \mathcal{E})$, which is the closure of the set of achievable rate tuples $\{R_{jk}\}_{(j,k) \in \mathcal{E}}$ such that $(\{R_{jk}\}_{(j,k) \in \mathcal{E}}, D_2, \dots, D_N)$ is achievable
- Note that without loss of generality we only need to consider the case where the rate on each outgoing edge is less than or equal to the sum of the rates on the incoming edges at its starting node (why?)

- It is easy to show the following cutset outer bound on the rate–distortion region: if $(\{R_{jk}\}_{(j,k) \in \mathcal{E}}, D_2, \dots, D_N)$ is achievable, then for some $p(\hat{x}_2^N | x)$

$$\sum_{j \in \mathcal{S}, k \in \mathcal{S}^c} R_{jk} \geq I(X; \hat{X}(\mathcal{S}^c)) \text{ for all } \mathcal{S} \subseteq [1 : N],$$

where $\hat{X}(\mathcal{S})$ is the ordered vector of $\hat{X}_k, k \in \mathcal{S}$

- If $d_j, j \in [2 : N]$, is a Hamming distortion and $D_j = 0$ or 1 , then the problem reduces to the lossless coding over the noiseless multicast network with the set of destination nodes $\mathcal{D} = \{j \in [2 : N] : D_j = 0\}$. The rate–distortion region is the set of rate tuples such that the resulting min-cut capacity C (minized over all destination nodes) satisfies $H(X) \leq C$
- The rate–distortion region for a multiple description network is not known in general. In the following, we consider a few nontrivial special cases

Special Cases

- Tree network: If the network is a tree, i.e., there is only one incoming edge to each node, then the rate–distortion region is known

Theorem 1: The rate–distortion region for distortion tuple (D_2, D_3, \dots, D_N) is the set of rate tuples $\{R_{jk} : (j, k) \in \mathcal{E}\}$ satisfying

$$R_{jk} \geq I(X; \hat{X}(\mathcal{S}_k^c)),$$

where \mathcal{S}_k^c consists of k and the set of nodes that precedes it (i.e., if node $l \in \mathcal{S}_k^c$, then node k is on the path from node 1 to node l)

- It suffices to consider $p(\hat{x}_2^N | x)$ that satisfy the conditional independence relations induced by the tree structure
- The converse follows immediately from the cutset outer bound by considering the cutset \mathcal{S}_k for each $k \in [2 : N]$

- Outline of the achievability: Without loss of generality, suppose the network is a line, i.e., $\mathcal{E} = \{(j, j+1) : j \in [1 : N-1]\}$

Fix $p(\hat{x}^N|x)$ and consider covering codewords $\hat{x}_k^n(\tilde{m}_k)$, $\tilde{m}_k \in [1 : 2^{n\tilde{R}_k}]$, $k \in [2 : N]$. By the covering lemma, if

$$\tilde{R}_k > I(X; \hat{X}_k | \hat{X}_{k+1}^N) + \delta(\epsilon) \text{ for all } k \in [2 : N]$$

then there exists a tuple $(\hat{x}_2^n(l_2), \dots, \hat{x}_N^n(l_N))$ that satisfy distortion constraints. Letting

$$R_{k-1,k} = \tilde{R}_k + \tilde{R}_{k+1} + \dots + \tilde{R}_N, \quad k \in [2 : N],$$

and using the Fourier–Motzkin elimination, we have the desired inequalities

$$R_{k-1,k} > I(X; \hat{X}_k^N) + \delta(\epsilon), \quad k \in [2 : N]$$

This completes the proof of achievability

- Triangular network: For $N = 3$, the rate–distortion region is known

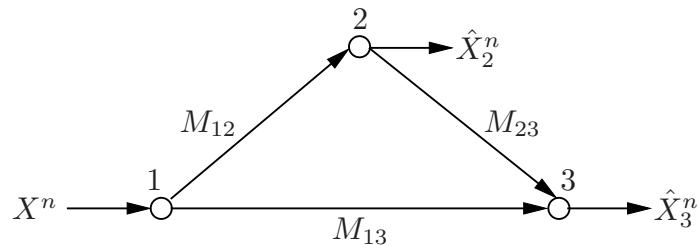
Theorem 2 [1]: The achievable rate–distortion region for distortion pair (D_2, D_3) is the set of rate tuples (R_{12}, R_{13}, R_{23}) satisfying

$$R_{23} \geq I(U; X),$$

$$R_{12} \geq I(U, \hat{X}_2; X),$$

$$R_{13} \geq I(\hat{X}_3; X|U)$$

for some $p(u|x)p(\hat{x}_2|u, x)p(\hat{x}_3|u, x)$ such that $E(d_2(\hat{X}_2; X)) \leq D_2$ and $E(d_3(\hat{X}_3; X)) \leq D_3$



- Outline of the achievability: We first generate a description U of X at rate \tilde{R}_3 . For each description sequence $u^n(\tilde{m}_3)$, we generate a conditional description \hat{X}_2 of X at rate \tilde{R}_2 , and a conditional description \hat{X}_3 of X at rate R_{13} . By letting $R_{12} = \tilde{R}_2 + \tilde{R}_3$ and $R_{23} = \tilde{R}_3$ and applying Fourier–Motzkin elimination, the conditions on the rates given by the theorem guarantee the desired distortions with high probability
- Proof of the converse: We make the auxiliary random variable identification $U_i := (M_{23}, X^{i-1})$. First we can show that

$$\begin{aligned}
nR_{23} &\geq H(M_{23}) \\
&= \sum_{i=1}^n I(M_{23}, X^{i-1}; X_i) \\
&= \sum_{i=1}^n I(U_i; X_i) \\
&= nI(U_Q, Q; X_Q) = nI(U; X),
\end{aligned}$$

where Q is a time-sharing random variable, $U := (U_Q, Q)$, and $X := X_Q$

Next, since M_{23} is a function of M_{12} , we have

$$\begin{aligned}
nR_{12} &\geq H(M_{12}) \\
&= H(M_{12}, M_{23}) \\
&\geq I(M_{12}; X^n | M_{23}) \\
&\geq \sum_{i=1}^n I(\hat{X}_{2i}; X_i | M_{23}, X^{i-1}) \\
&\geq nI(\hat{X}_2; X | U),
\end{aligned}$$

which depends only on $p(x)p(u|x)p(\hat{x}_2|u, x)$

Also

$$\begin{aligned}
nR_{13} &\geq H(M_{13} | M_{23}) \\
&\geq nI(\hat{X}_3; X | U),
\end{aligned}$$

which depends only on $p(x)p(u|x)p(\hat{x}_3|u, x)$

Note that even though as defined, \hat{X}_2 and \hat{X}_3 are not in general conditionally independent given U, X , we can assume without loss of generality that they are because none of the mutual information terms above is a function of the joint pmf of (\hat{X}_2, \hat{X}_3) . This completes the proof of the converse

- Example: Let X be a $\text{WGN}(P)$ source and d_2 and d_3 be mean squared error distortion, then the rate–distortion region for distortion pair (D_2, D_3) is given by the set of rate tuples (R_{12}, R_{13}, R_{23}) satisfying

$$R_{12} \geq R(P/D_2),$$

$$R_{13} + R_{23} \geq R(P/D_3)$$

The converse follows immediately from the cutset outer bound (by considering $\mathcal{S} = \{1, 3\}$ and $\mathcal{S} = \{1, 2\}$ only). The achievability follows from the Gaussian successive refinement coding described in Lecture Notes 14

- Remark: The above results can be extended to the network with edge set $\mathcal{E} = \{(1, 2), (2, 3), \dots, (N - 1, N), (1, N)\}$: The achievable rate–distortion region for distortion tuple (D_2, D_3, \dots, D_N) is the set of rate tuples $(R_{12}, R_{23}, \dots, R_{N-1,N}, R_{1,N})$ satisfying

$$R_{N-1,N} \geq I(U; X),$$

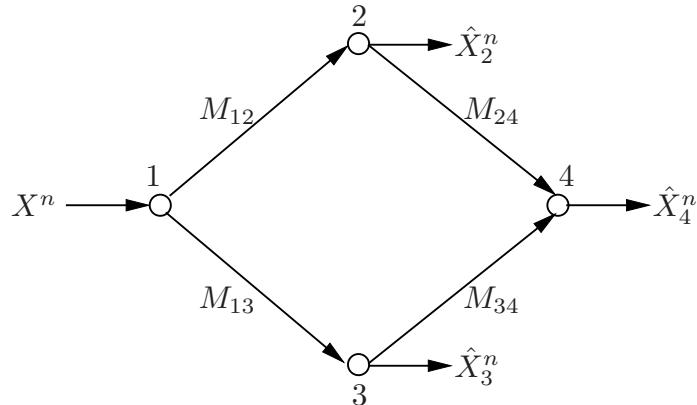
$$R_{N-2,N-1} \geq I(U, \hat{X}_{N-1}; X),$$

$$R_{j-1,j} \geq I(U, \hat{X}_j^{N-1}; X), \quad j \in [2 : N - 1],$$

$$R_{1N} \geq I(\hat{X}_N; X|U)$$

for some $p(u|x)p(\hat{x}_2^{N-1}|u, x)p(\hat{x}_N|u, x)$ such that $E(d_j(\hat{X}_j; X)) \leq D_j$, $j \in [2 : N]$

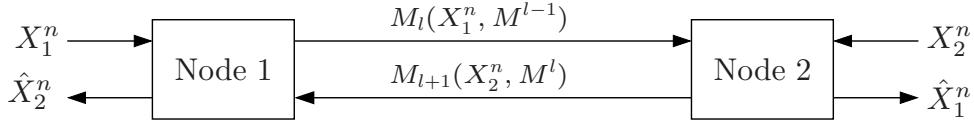
- Diamond network: Consider the following network with $N = 4$



- For $R_{24} = R_{12}$ and $R_{34} = R_{13}$ the problem reduces to the standard multiple description coding problem studied in Lecture Notes 14
- The multiple description network can be generalized by assuming correlated sources, allowing two-way communication, and/or allowing nodes to broadcast to subsets of other nodes, i.e., modeling the network by a *hypergraph*. Such generalizations include all the single-hop multiple user source coding problems we have discussed so far, as well as the interactive source coding problems we discuss in the following

Two-Way Lossless Source Coding

- Let (X_1, X_2) be a 2-DMS and assume a 2-node communication network in which node 1 observes X_1 and node 2 observes X_2 . The nodes communicate over a noiseless two-way channel so that each node losslessly decodes the source of the other node. What are the set of necessary and sufficient communication rates needed?



- Without loss of generality, assume that node 1 sends the first index and that the number of rounds of communication q is even. Note that this assumption does not preclude node 2 from being the first node to send a non-trivial index
- A $(2^{nr_1}, 2^{nr_2}, \dots, 2^{nr_q}, n)$ code for the interactive lossless coding problem consists of:
 - Two encoders, one for each node $j \in [1 : 2]$. At round $l_j \in \{j, j + 2, \dots, q - 2 + j\}$, encoder j sends an index $m_{l_j}(x_1^n, m^{l_j-1}) \in [1 : 2^{nr_{l_j}}]$, i.e., a function of its source vector and all previously transmitted indices

- Two decoders, one for each node $j \in [1 : 2]$. Decoder 1 assigns to each received index sequence m^q an estimate \hat{X}_2^n and Decoder 2 assigns to each received index sequence m^q an estimate \hat{X}_1^n
- The probability of error is defined as

$$P_e^{(n)} = P\{(\hat{X}_1^n, \hat{X}_2^n) \neq (X_1^n, X_2^n)\}$$
- The total transmission rate for node $j \in [1 : 2]$ is $R_j := \sum_{l_j \in \{j, j + 2, \dots, q - 2 + j\}} r_{l_j}$
- A rate pair (R_1, R_2) is said to be achievable if there exists a sequence of $(2^{nr_1}, 2^{nr_2}, \dots, 2^{nr_q}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ such that

$$R_j = \sum_{l_j \in \{j, j + 2, \dots, q - 2 + j\}} r_{l_j}$$
- The problem is to find the rate region, which is the closure of the set of achievable (R_1, R_2) pairs
- The solution to this problem is quite straightforward. By the Slepian-Wolf theorem, $R_1 > H(X_1|X_2)$, $R_2 > H(X_2|X_1)$ are sufficient and can be achieved in two rounds of communication. It is also straightforward to show that this set of rate pairs is necessary
- Remark: For error-free communication, it can be shown that $R_1 \geq H(X_1)$ and $R_2 \geq H(X_2)$ are necessary in some cases, e.g., when $p(x, y) > 0$ for all (x, y) pairs [2]

Multi-Way Lossless Source Coding

- Now, consider a more general setting of a noiseless broadcast network with N -nodes and N -DMS ($\mathcal{X}_1 \times \dots \times \mathcal{X}_N, p(x_1, \dots, x_N)$). Node $j \in [1 : N]$ observes source X_j , and the nodes communicate over a noiseless broadcast channel such that all the nodes in some subset $\mathcal{A} \subseteq [1 : N]$ can losslessly decode all sources. This problem is also known as communication for omniscience (CFO) [3]
- Without loss of generality, assume that the nodes communicate in a round robin fashion in q rounds, where $q \in \mathbb{Z}^+$ is divisible by N and may depend on the code block length, such that node $j \in [1 : N]$ broadcasts in rounds $j, N + j, \dots, q - N + j$. Note that any other node communication order can be achieved using this “protocol” by appropriately having nodes not communicate (or send an agreed upon message) during some of their allotted rounds
- A $(2^{nr_1}, 2^{nr_2}, \dots, 2^{nr_q}, n)$ code for the CFO problem consists of:
 - N encoders, one for each node $j \in [1 : N]$. At round $l_j \in \{j, N + j, \dots, q - N + j\}$, encoder j sends an index $m_{l_j}(x_j^n, m^{l_j-1}) \in [1 : 2^{nr_{l_j}}]$, i.e., a function of its source vector and all previously transmitted indices

- $|\mathcal{A}|$ decoders, one for each node $k \in \mathcal{A}$. Decoder k assigns to each received index sequence m^q an estimate $(\hat{X}_{1k}^n, \hat{X}_{2k}^n, \dots, \hat{X}_{Nk}^n)$
- The probability of error is defined as $P_e^{(n)} = \mathbb{P}\{(\hat{X}_{1k}^n, \hat{X}_{2k}^n, \dots, \hat{X}_{Nk}^n) \neq (X_1^n, X_2^n \dots X_N^n) \text{ for some } k \in \mathcal{A}\}$
- The total transmission rate for node j is $R_j := \sum_{l_j \in \{j, j+N, \dots, q-N+j\}} r_{l_j}$
- A rate tuple (R_1, R_2, \dots, R_N) is said to be achievable if there exists a sequence of $(2^{nr_1}, 2^{nr_2}, \dots, 2^{nr_q}, n)$ codes with $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ such that $R_j = \sum_{l_j \in \{j, j+N, \dots, q-N+j\}} r_{l_j}$
- The optimal rate region $\mathcal{R}(\mathcal{A})$ for the CFO problem is the closure of the set of all achievable rate tuples (R_1, R_2, \dots, R_N)
- In some cases, we are interested in the minimum sum rate for the CFO problem defined as

$$R_{\text{CFO}}(\mathcal{A}) := \inf_{(R_1, R_2, \dots, R_N) \in \mathcal{R}(\mathcal{A})} \sum_{j=1}^N R_j$$

- Theorem 3* [3]: $\mathcal{R}(\mathcal{A})$ is the set of all rate tuples (R_1, R_2, \dots, R_N) satisfying $\sum_{j \in \mathcal{S}} R_j \geq H(X(\mathcal{S})|X(\mathcal{S}^c))$ for all $\mathcal{S} \subseteq [1 : N] \setminus \{k\}$ and all $k \in \mathcal{A}$

- Remark: $\mathcal{R}(\mathcal{A}) = \cap_{k \in \mathcal{A}} \mathcal{R}(\{k\})$
- Examples:
 - 2-nodes, $\mathcal{A} = \{1, 2\}$. Here both nodes wish to know each other's source. The rate region is given by the set of rate pairs (R_1, R_2) such that

$$R_1 \geq H(X_1|X_2), \quad R_2 \geq H(X_2|X_1)$$

and the minimum sum rate $R_{\text{CFO}}(\{1, 2\}) = H(X_1|X_2) + H(X_2|X_1)$

- $N = 3$ and $\mathcal{A} = \{1, 2\}$. The rate region is given by

$$\begin{aligned} R_1 &\geq H(X_1|X_2, X_3), \\ R_2 &\geq H(X_2|X_1, X_3), \\ R_3 &\geq H(X_3|X_1, X_2), \\ R_1 + R_3 &\geq H(X_1, X_3|X_2), \\ R_2 + R_3 &\geq H(X_2, X_3|X_1) \end{aligned}$$

It can be shown (for example, using the Fourier–Motzkin procedure in Appendix D) that

$$R_{\text{CFO}}(\{1, 2\}) = H(X_1|X_2) + H(X_2|X_1) + \max\{H(X_3|X_1), H(X_3|X_2)\}$$

- Remark: $R_{\text{CFO}}(\mathcal{A})$ can be calculated efficiently using duality results from linear programming [3]. In particular, no more than N constraints (as opposed to 2^N) are required
- Proof of achievability: Consider any vector (R_1, \dots, R_N) in the interior of $\mathcal{R}(\mathcal{A})$. We use $q = N$ rounds of communication

Codebook generation: Encoder j randomly and independently assigns each sequence in \mathcal{X}_j^n to one of 2^{nR_j} bins

Encoding: In round j , node j broadcasts the bin index $m_l(x_j^n)$

Decoding: Decoder $k \in \mathcal{A}$ declares that $(\hat{X}_{1k}^n, \dots, \hat{X}_{Nk}^n)$ is the source sequence if $\hat{X}_{jk}^n, j \in [1 : N], j \neq k$ is the unique sequence in bin M_j such that $(\hat{X}_{1k}^n, \dots, \hat{X}_{Nk}^n) \in \mathcal{T}_\epsilon^{(n)}$

Similar to the analysis of the probability of error for the Slepian–Wolf coding, this step succeeds with high probability if $\sum_{j \in \mathcal{S}} R_j \geq H(X(\mathcal{S})|X(\mathcal{S}^c))$ for all $\mathcal{S} \subseteq [1 : N] \setminus \{k\}$. The intersection of the regions for the nodes $k \in \mathcal{A}$ gives the region $\mathcal{R}(\mathcal{A})$. Note that here each receiver also has a source of its own, and hence it is included in the conditioning

- Proof of converse: First assume that $\mathcal{A} = \{N\}$, i.e., only node N wishes to losslessly estimate the N -DMS. Consider the following cutset argument:
 - Partition the nodes of the network into two sets $\mathcal{S} \subseteq \{1, 2, \dots, N-1\}$ and \mathcal{S}^c , the latter of which by definition contains the receiver node N
 - Imagine the nodes on each side of the “cut” to be grouped into a single “super-node”. Super-node \mathcal{S} has the sources $X(\mathcal{S})$ and super-node \mathcal{S}^c has the sources $X(\mathcal{S}^c)$

What is the minimum number of bits that must flow from super-node \mathcal{S} to super-node \mathcal{S}^c in order for the receiver to know all the sources?

 - Clearly, a lower bound on the amount of information that must flow from \mathcal{S} to \mathcal{S}^c is $\sum_{j \in \mathcal{S}} R_j \geq H(X(\mathcal{S})|X(\mathcal{S}^c))$
 - By considering all such node partitions, we obtain an outer bound to the optimal rate region that coincides with the Slepian–Wolf region
- The converse follows by applying the above cutset bound for each node $k \in \mathcal{A}$ as a receiver
- *Remark:* It is indeed surprising that the above simple cutset bound is achievable in this setup and that interactive communication does not enlarge the rate region

Two-Way Lossy Source Coding

- Let (X_1, X_2) be a 2-DMS and d_1, d_2 be two distortion functions. Assume a 2-node communication network in which node 1 observes X_1 and node 2 observes X_2 . The nodes communicate over a two-way noiseless channel so that each node finds an estimate of the source of the other node to within a prescribed distortion. What is the rate–distortion region?
- Again assume that node 1 sends the first index and that the number of rounds of communication q is even
- A $(2^{nr_1}, 2^{nr_2}, \dots, 2^{nr_q}, n)$ is defined as for the lossless case except here a rate–distortion tuple (R_1, R_2, D_1, D_2) is achievable if there exists a sequence of $(2^{nr_1}, 2^{nr_2}, \dots, 2^{nr_q}, n)$ codes such that $R_j = \sum_{l_j \in \{j, j+2, \dots, q-2+j\}} r_{l_j}$ and $\limsup_{n \rightarrow \infty} E(d_j(X_j^n, \hat{X}_j^n)) \leq D_j, j \in [1 : 2]$
- The q -round rate–distortion region $\mathcal{R}_q(D_1, D_2)$ is the closure of the set of achievable rate pairs (R_1, R_2) pairs such that (R_1, R_2, D_1, D_2) is achievable in no more than q rounds
- The rate–distortion region $\mathcal{R}(D_1, D_2)$ is the closure of the union of set of achievable rate pairs (R_1, R_2) pairs such that (R_1, R_2, D_1, D_2) is achievable for some q . Clearly, $\mathcal{R}_q(D_1, D_2) \subseteq \mathcal{R}(D_1, D_2)$

- Inner bound: Each node performs an independent Wyner–Ziv coding on its source considering the other node's source as side information
This scheme, which requires only two rounds of communication yields the inner bound $R_1 > I(X_1; U_1|X_2)$, $R_2 > I(X_2; U_2|X_1)$ for some $p(u_1|x_1)$, $p(u_2|x_2)$, $\hat{x}_1(u_1, x_2)$, and $\hat{x}_2(u_2, x_1)$ such that $E(d_1(X_1, \hat{X}_1)) \leq D_1$, $E(d_2(X_2, \hat{X}_2)) \leq D_2$
- Outer bound: Even if each node knows the other node's source, we must have $R_1 \geq I(X_1; \hat{X}_1|X_2)$, $R_2 \geq I(X_2; \hat{X}_2|X_1)$ for some $p(\hat{x}_1|x_1, x_2)$, $p(\hat{x}_2|x_1, x_2)$ such that $E(d_1(X_1, \hat{X}_1)) \leq D_1$ and $E(d_2(X_2, \hat{X}_2)) \leq D_2$
- The bounds can be tight
Example: Let (X_1, X_2) be 2-WGN sources each with average power P and with correlation coefficient ρ . It can be shown that the rate–distortion region for distortion pair (D_1, D_2) is the set of rate pairs (R_1, R_2) such that $R_1 \geq R((1 - \rho^2)P/D_1)$, $R_2 \geq R((1 - \rho^2)P/D_2)$, and is achieved by two independent rounds of the Wyner–Ziv coding
- In general, the inner and outer bounds are not tight and interactive communication is needed to achieve the rate–distortion region. To reduce the overall rates, the two nodes should interactively build additional correlation between their knowledge of the sources instead of greedily using two independent rounds of Wyner–Ziv coding (cf. the lossless case)

- The q -round rate–distortion region is given by the following
Theorem 4 [4]: The q -round rate–distortion region for the two-way lossy source coding problem with distortion pair (D_1, D_2) is the set of rate pairs (R_1, R_2) satisfying

$$R_1 \geq I(X_1; U^q|X_2),$$

$$R_2 \geq I(X_2; U^q|X_1)$$

for some U^q such that for $p(u^q|x_1, x_2) = \prod_{l=1}^q p(u_l|u^{l-1}, x_{j_l})$, where $j_l = 1$ if l is odd and $j_l = 2$ if l is even, and $\hat{x}_1(u^q, x_2)$, $\hat{x}_2(u^q, x_1)$ such that $E(d_1(X_1, \hat{X}_1)) \leq D_1$, $|U_j| \leq |\mathcal{X}_{j_l}| \cdot |\prod_{l=1}^{j-1} \mathcal{U}_l| + 1$, and $E(d_2(X_2, \hat{X}_2)) \leq D_2$

- Note that the above region is computable for bounded q . However, there is no bound on q that holds in general and therefore the region is not computable in general
- Achievability is proved by using the Wyner–Ziv coding in each round

Fix a joint pmf on U^q given X_1 and X_2 and reconstruction functions of the form specified in the theorem that satisfy the desired distortions

In odd round $l \in [1 : q]$, node 1 sends the bin index of the description U_l of X_1 given U^{l-1} to node 2 at rate $r_{1l} > I(X_1; U_l|U^{l-1}, X_2)$, and in even rounds node 2 sends the index of the description U_l of X_2 at rate $r_{2l} > I(X_2; U_l|U^{l-1}, X_1)$

Summing up the rates for each node establishes the required bounds on $R_1 = \sum_{l \text{ odd}} r_{1l}$ and $R_2 = \sum_{l \text{ even}} r_{2l}$

At the end of the q rounds, node 1 forms the estimate $\hat{x}_1(U^q, X_1)$ and node 2 forms the estimate $\hat{x}_2(U^q, X_2)$ of X_2 and X_1 , respectively. The details follow the proof of achievability of the Wyner–Ziv theorem in Lecture notes 12

Proof of Converse

- Assume q is even and consider

$$\begin{aligned}
nR_1 &\geq \sum_{l \text{ odd}}^{q-1} H(M_l) \\
&\geq H(M_1, M_3, \dots, M_{q-1}) \\
&\geq I(M_1, M_3, \dots, M_{q-1}; X_1^n | X_2^n) \\
&= H(X_1^n | X_2^n) - H(X_1^n | X_2^n, M_1, M_3, \dots, M_{q-1}) \\
&\stackrel{(a)}{=} H(X_1^n | X_2^n) - H(X_1^n | X_2^n, M^q) \\
&\geq \sum_{i=1}^n (H(X_{1i} | X_{2i}) - H(X_{1i} | X_{2i}, X_{2,i+1}^n, X_1^{i-1}, M^q)) \\
&= \sum_{i=1}^n I(X_{1i}; X_{2,i+1}^n, X_1^{i-1}, M^q | X_{2i}) \\
&\stackrel{(b)}{=} \sum_{i=1}^n I(X_{1i}; U^q(i) | X_{2i}),
\end{aligned}$$

where (a) follows since (M_2, M_4, \dots, M_q) is a function of $(M_1, M_3, \dots, M_{q-1}, X_2^n)$ and (b) follows by defining $U_{1i} := (M_1, X_1^{i-1}, X_{2,i+1}^n)$ and $U_{li} = M_l$ for $l \in [2 : q]$. The bound for R_2 can be similarly established with the same U_{li} identifications

- Next, we show that for every $i \in [1 : n]$,
 - (a) $E(d(X_{1i}, \hat{x}_1^*(i, U^q(i), X_{2i}))) \leq E(d(X_{1i}, \hat{x}_{1i}(M^q, X_2^n)))$,
 $E(d(X_{2i}, \hat{x}_2^*(i, U^q(i), X_{1i}))) \leq E(d(X_{2i}, \hat{x}_{2i}(M^q, X_1^n)))$,
for some functions \hat{x}_1^* and \hat{x}_2^* to be specified later
 - (b) $X_{j_{l+1},i} \rightarrow (X_{j_l,i}, U_i^{l-1}) \rightarrow U_{li}$ for every $l \in [1 : q]$

- To prove these claims, we need the following lemma

Lemma 1: Let A_1, A_2, B_1, B_2 be random variables with joint pmf $p(a_1, a_2, b_1, b_2) = p(a_1, b_1)p(a_2, b_2)$ and M_l is a function of (A_1, A_2, M^{l-1}) for l odd and (B_1, B_2, M^{l-1}) for l even. Then,

$$\begin{aligned} I(A_2; B_1 | M^q, A_1, B_2) &= 0 \\ I(B_1; M_l | M^{l-1}, A_1, B_2) &= 0 \text{ for } l \text{ odd} \\ I(A_2; M_l | M^{l-1}, A_1, B_2) &= 0 \text{ for } l \text{ even} \end{aligned}$$

Proof of lemma: Consider

$$\begin{aligned} I(A_2; B_1 | M^q, A_1, B_2) &= H(A_2 | M^q, A_1, B_2) - H(A_2 | M^q, A_1, B_2, B_1) \\ &= H(A_2 | M^{q-1}, A_1, B_2) - I(A_2; M_q | M^{q-1}, A_1, B_2) \\ &\quad - H(A_2 | M^q, A_1, B_2, B_1) \\ &\leq I(A_2; B_1 | M^{q-1}, A_1, B_2) \\ &= H(B_1 | M^{q-1}, A_1, B_2) - H(B_1 | M^{q-1}, A_1, A_2, B_2) \\ &= H(B_1 | M^{q-2}, A_1, B_2) - I(B_1; M_{q-1} | M^{q-2}, A_1, B_2) \\ &\quad - H(B_1 | M^{q-1}, A_1, A_2, B_2) \\ &\leq I(A_2; B_1 | M^{q-2}, A_1, B_2) \end{aligned}$$

Continuing this process gives $I(A_2; B_1 | A_1, B_2) = 0$. Hence, all inequalities hold with equality

- Proof of claim (a): To establish the distortion constraints, we first show that $X_2^{i-1} \rightarrow (U^q(i), X_{2i}) \rightarrow X_{1i}$ form a Markov chain. To see this note that $I(X_{1i}; X_2^{i-1} | M^q, X_{2i}, X_{2,i+1}^n, X_1^{i-1}) \leq I(X_{1i}, X_{1,i+1}^n; X_2^{i-1} | M^q, X_{2i}, X_{2,i+1}^n, X_1^{i-1})$. Setting $A_1 = X_1^{i-1}$, $A_2 = (X_{1,i+1}^n, X_{1i})$, $B_1 = X_2^{i-1}$ and $B_2 = X_{2,i+1}^n, X_{2i}$ in the lemma gives $I(X_{1i}, X_1^{i-1}; X_2^{i-1} | M^q, X_{2i}, X_{2,i+1}^n, X_1^{i-1}) = 0$ as required

Now, consider

$$\begin{aligned} \mathbb{E}(d(X_{1i}, \hat{x}_{1i}(M^q, X_2^n))) &= \sum p(x_1^i, x_2^n, m^q) d(x_{1i}, \hat{x}_{1i}(m^q, x_2^n)) \\ &\stackrel{(a)}{=} \sum p(u^q(i), x_2^i) p(x_{1i}|u^q(i), x_2^i) d(x_{1i}, \hat{x}'_{1i}(u^q(i), x_{2i}, x_2^{i-1})) \\ &= \sum p(u^q(i), x_2^i) p(x_{1i}|u^q(i), x_{2i}) d(x_{1i}, \hat{x}'_{1i}(u^q(i), x_{2i}, x_2^{i-1})), \end{aligned}$$

where in (a) follows by defining $\hat{x}'_{1i}(u^q(i), x_{2i}, x_2^{i-1}) := \hat{x}_{1i}(m^q, x_2^n)$ for all x_1^{i-1} , and the last step follows by the fact that $X_2^{i-1} \rightarrow (U^q(i), X_{2i}) \rightarrow X_{1i}$ form a Markov chain

Defining

$$(x_2^{i-1})^* := \arg \min_{x_2^{i-1}} \sum_{x_{1i}} p(x_{1i}|u^q(i), x_{2i}) d(x_{1i}, \hat{x}'_{1i}(u^q(i), x_{2i}, x_2^{i-1})), \text{ and}$$

$$\hat{x}_1^*(i, u^q(i), x_{2i}) := \hat{x}'_{1i}(u^q(i), x_{2i}, (x_2^{i-1})^*), \text{ then}$$

$$\mathbb{E}(d(X_{1i}, \hat{x}_1^*(i, U^q(i), X_{2i}))) \leq \mathbb{E}(d(X_{1i}, \hat{x}_{1i}(M^q, X_2^n))) \text{ as required}$$

The relationship $\mathbb{E}(d(X_{2i}, \hat{x}_2^*(i, U^q(i), X_{1i}))) \leq \mathbb{E}(d(X_{2i}, \hat{x}_{2i}(M^q, X_1^n)))$ is established by showing that $X_{1,i+1}^n \rightarrow (U^q(i), X_{1i}) \rightarrow X_{2i}$ form a Markov chain and applying similar steps

- Proof of claim (b): Consider the case of odd l . To show that $X_{2i} \rightarrow (X_{1i}, U^{l-1}(i)) \rightarrow U_{li}$ for $l > 1$ note that $U_{li} = M_l$ and hence
- $$I(U_{li}; X_{2i}|X_{1i}, U_i^{l-1}) \leq I(M_l; X_{2i}, X_2^{i-1}|X_{1i}, M^{l-1}, X_1^{i-1}, X_{2,i+1}^n)$$

Setting $A_1 = (X_1^{i-1}, X_{1i})$, $A_2 = X_{1,i+1}^n$, $B_1 = (X_2^{i-1}, X_{2i})$ and $B_2 = X_{2,i+1}^n$ in the lemma gives $I(M_l; X_{2i}, X_2^{i-1}|X_{1i}, M^{l-1}, X_1^{i-1}, X_{2,i+1}^n) = 0$ as required

For $l = 1$, note that

$$\begin{aligned} I(X_{2i}; M_1, X_1^{i-1}, X_{2,i+1}^n|X_{1i}) &\leq I(X_{2i}; M_1, X_1^{i-1}, X_{2,i+1}^n, X_{1,i+1}^n|X_{1i}) \\ &= I(X_{2i}; X_1^{i-1}, X_{2,i+1}^n, X_{1,i+1}^n|X_{1i}) = 0 \end{aligned}$$

The case of even l can be similarly proved

- Using a time sharing random variable T , setting $U_1 := (T, U_{1T})$ and $U_l := U_{lT}$ for $l \in [2 : q]$, and noting that (X_{1T}, X_{2T}) has the same pmf as (X_1, X_2) , we have

$$\begin{aligned} R_1 &\geq \frac{1}{n} \sum_{i=1}^n I(X_{1i}; U^q(i)|X_{2i}) \\ &= I(X_{1T}; U^q(T)|X_{2T}, T) \\ &= I(X_1; U^q|X_2), \text{ and} \end{aligned}$$

$$R_2 \geq I(X_2; U^q|X_1)$$

Using claim (b) and the definition of the U^q , it can be verified that $p(u^q|x_1, x_2) = \prod_{l=1}^q p(u_l|u^{l-1}, x_{j_l})$ as desired

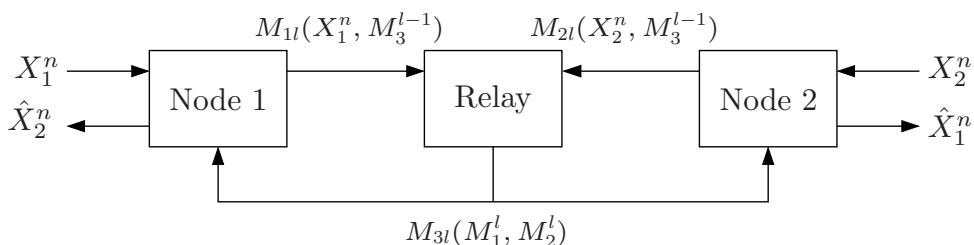
- To verify the distortion constraints, consider

$$\begin{aligned}\mathbb{E}(d(X_1, \hat{x}_1^*(U^q, X_2))) &= \frac{1}{n} \sum_{i=1}^n \mathbb{E}(d(X_{1i}, \hat{x}_1^*(i, U^q(i), X_{2i})) | T = i) \\ &\leq \frac{1}{n} \sum_{i=1}^n \mathbb{E}(d(X_{1i}, \hat{x}_{1i}(M^q, X_2^n))) \leq D_1\end{aligned}$$

The other distortion constraint can be verified similarly

Two-Way Source Coding Through a Relay

- Consider the following communication setting motivated by wireless mesh networks. Two nodes wish to communicate through a relay. Communication is performed in rounds, where at each round each node sends a codeword to the relay that depends on its information source and past received sequences and the relay broadcasts a codeword to the two nodes that depends on its received sequences. What are the necessary and sufficient conditions for reliable communication between the two nodes?



- Let's first consider a lossless source coding version of this problem. Let (X_1, X_2) be 2-DMS. Node 1 observes X_1 and node 2 observes X_2 . What is the minimum achievable sum-rate $R_{\text{sum}}(D_1, D_2)$, which is the minimum number of bits/symbol-pair that need to be communicated so that each node can losslessly estimate the other node's source

- A simple upper bound on R_{sum}^* can be achieved by having each node perform Slepian-Wolf coding on its source and sending its index to the relay. The relay then simply broadcasts these two indices to both nodes. This yields the upper bound $R_{\text{sum}}^* \leq 2(H(X_1|X_2) + H(X_2|X_1))$
- Using a cutset argument, we can show that $R_{\text{sum}}^* \geq H(X_1|X_2) + H(X_2|X_1) + \max\{H(X_1|X_2), H(X_2|X_1)\}$ (Why?)
- Now we show that the lower bound is achievable via Slepian-Wolf coding and “network coding” (see Lecture 16 for more on network coding)

We use Slepian-Wolf coding. Node 1 sends a k_1 -bit bin index sequence $U_1^{k_1}$ and node 2 sends a k_2 -bit bin index sequence $U_2^{k_2}$. Without loss of generality, assume that $k_1 \geq k_2$. The relay pads $U_2^{k_2}$ by zeros to obtain the k_1 -bit sequence $\tilde{U}_2^{k_1}$. It then adds the two sequences mod 2 and broadcasts the index $V^{k_1} = U_1^{k_1} \oplus \tilde{U}_2^{k_1}$. Upon receiving V^{k_1} , each node recovers the other node's index and decodes its message using joint typicality. Following the achievability proof of the Slepian-Wolf theorem if $k_1 > H(X_1|X_2) + \delta(\epsilon)$ and $k_2 > H(X_2|X_1) + \delta(\epsilon)$, the probability of decoding error $\rightarrow 0$ as $n \rightarrow \infty$, and any sum rate $R > 2H(X_1|X_2) + H(X_2|X_1) + 3\delta(\epsilon)$ is achievable

- Now, consider the lossy coding formulation of the above problem. Assume that each node wishes to estimate the other node's source to some prescribed distortion. Following two-way lossy source coding and using network coding at the relay, we can obtain an upper bound on the sum rate for q rounds. Is this upper bound optimal?
- Channel coding model for the above setting is studied in [5]

Key New Ideas and Techniques

- Cutset bounds for source coding networks
- Interactive source coding
- Open problems:
 - Generalize the lossless two-way source coding with relay to lossy source coding
 - Generalize two-way lossy source coding to more than 2 sources

References

- [1] H. Yamamoto, "Source coding theory for a triangular communication systems," *IEEE Trans. Inf. Theory*, vol. 42, no. 3, pp. 848–853, May 1996.
- [2] A. El Gamal and A. Orlitsky, "Interactive data compression," in *Proceedings of the 25th Annual Symposium on Foundations of Computer Science*, Washington, DC, Oct. 1984, pp. 100–108.
- [3] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.
- [4] A. H. Kaspi, "Two-way source coding with a fidelity criterion," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 735–740, 1985.
- [5] S. Katti, I. Maric, A. Goldsmith, D. Katabi, and M. Médard, "Joint relaying and network coding in wireless networks," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 1101–1105.

Part IV. Extensions

Lecture Notes 22

Communication for Computing

- Coding for Computing with Side Information
- Distributed Coding for Computing
- Two-Way Coding for Computing
- Cascade Coding for Computing
- Distributed Lossy Averaging
- Computing over a MAC
- Key New Ideas and Techniques
- Appendix: Proof of Orlitsky–Roche Theorem
- Appendix: Proof of Bounds on $R(D)$

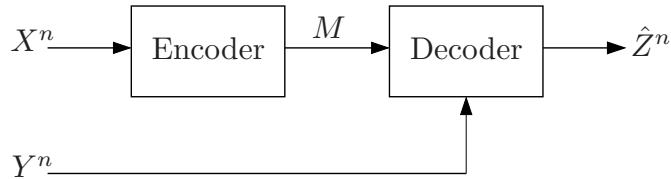
© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Introduction

- In many distributed systems, such as multiprocessors, peer-to-peer networks, networked agents, and sensor networks, the purpose of communication is not to communicate or store data, but rather to compute a function, make a decision, or coordinate an action based on distributed information. How much communication is needed to perform such a task?
- This problem has been studied in computer science (communication complexity, gossip), control and optimization (distributed consensus), and information theory (coding for computing, μ -sum problem)
- We present some of the information theoretic work on this problem and briefly discuss connections to related work in computer science and control

Coding for Lossy Computing with Side Information

- Consider a lossy source coding with side information setting for a 2-DMS (X, Y) (cf. Lecture Notes 12) and distortion measure $d(z, \hat{z})$. Suppose that the receiver wishes to estimate a function $Z = g(X, Y)$ of the 2-DMS with distortion D . What is the set of necessary and sufficient rates, i.e., the rate-distortion region for computing g with distortion D ?



- We define a $(2^{nR}, n)$ code, achievability, and the rate distortion function $R_g(D)$ as in Lecture Notes 12

- Following the proof steps of the Wyner-Ziv theorem, we can determine the rate-distortion function

Theorem 1 [1]: The rate-distortion function for computing $Z = g(X, Y)$ is

$$R_g(D) = \min_{p(u|x), \hat{z}(u,y)} I(X; U|Y),$$

where the minimum is over $p(u|x)$ with $|\mathcal{U}| \leq |\mathcal{X}| + 1$ and $\hat{z}(u,y)$ such that $E(d(Z, \hat{Z})) \leq D$

- Example: Let (X, Y) be 2-WGN(P, ρ) sources and d be the squared error distortion. If $g(X, Y) = (X + Y)/2$, then $R_g(D) = R((1 - \rho^2)P/4D)$

Coding for Lossless Computing with Side Information

- Now suppose the receiver wishes to estimate the function $Z = g(X, Y)$ losslessly. What is the optimal rate R_g^* ?
- Clearly,

$$H(Z|Y) \leq R_g^* \leq H(X|Y)$$

- The bounds sometimes coincide, e.g., when $Z = X$, or when (X, Y) are DSBS(p) and $g(X, Y) = X \oplus Y$
- The bounds do not coincide in general, however

Example [2]: Let $X = (V_1, V_2, \dots, V_{10})$, where the V_j , $j \in [1 : 10]$, are i.i.d. $\text{Bern}(1/2)$, and $Y \sim \text{Unif}[1 : 10]$. Suppose $g(X, Y) = V_Y$

The lower bound gives $H(V_Y|Y) = 1$ bit and the upper bound gives $H(X|Y) = 10$ bits

It can be shown that $R_g^* = 10$ bits

- Following arguments from the proof of the optimal rate for the causal lossless source coding with side information (cf. Lecture Notes 12), we can consider the lossy setting with Hamming distortion measure when $D = 0$, and show that

$$R_g^* = R_g(0) = \min_{p(u|x)} I(X; U|Y),$$

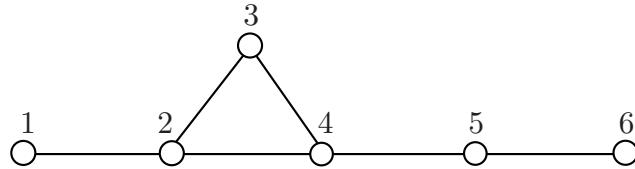
where the minimum is over $p(u|x)$ such that $H(Z|U, Y) = 0$

- Orlitsky and Roche [2] obtained a refined expression for R_g^* . To describe their result, we need the following definitions:

A set of nodes of a graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$ is *independent* if no two nodes are connected to each other through an edge. An independent set is *maximally independent* if it is not a subset of another independent set. Let $\Gamma(\mathcal{G})$ be the collection of maximally independent sets of \mathcal{G}

Example: Consider the graph in the figure.

$$\Gamma(\mathcal{G}) = \{\{1, 3, 5\}, \{1, 3, 6\}, \{1, 4, 6\}, \{2, 5\}, \{2, 6\}\} \text{ (check)}$$



Let X be a random variable over the nodes of the graph \mathcal{G} . Define the random variable $W \in \Gamma(\mathcal{G})$ with conditional pmf $p(w|x)$ such that $p(w|x) = 0$ if $x \notin w$, and hence for every x , $\sum_{w:x \in w} p(w|x) = 1$. The *graph entropy* of X [3] is defined as

$$H_{\mathcal{G}}(X) := \min_{p(w|x)} I(X; W)$$

Examples:

- o Graph with no edges, i.e., $\mathcal{E} = \emptyset$: Here $H_{\mathcal{G}}(X) = 0$ ($\Gamma(\mathcal{G}) = \{\mathcal{N}\}$ has a single element)
- o Complete graph: Here $H_{\mathcal{G}}(X) = H(X)$ (take $W = \{X\}$)
- o Let X be uniformly distributed over $\{1, 2, 3\}$ and \mathcal{G} has a single edge $\{1, 3\}$. $\Gamma(\mathcal{G}) = \{\{1, 2\}, \{2, 3\}\}$. By convexity of mutual information, $I(X; W)$ is

minimized when $p(\{1, 2\}|2) = p(\{2, 3\}|2) = 1/2$. Thus,

$$H_{\mathcal{G}}(X) = H(W) - H(W|X) = 1 - \frac{1}{3} = \frac{2}{3}$$

Now, let (X, Y) be two random variables and let the nodes of the graph \mathcal{G} be the support set of X . The graph entropy of X given Y is defined as

$$H_{\mathcal{G}}(X|Y) := \min_{p(w|x)} I(X; W|Y),$$

where the minimum is over $p(w|x)$ such that $W \in \Gamma(\mathcal{G})$ and $p(w|x) = 0$ if $x \notin w$

Examples:

- o Graph with no edges, i.e., $\mathcal{E} = \emptyset$: Here $H_{\mathcal{G}}(X|Y) = 0$
- o Complete graph: Here $H_{\mathcal{G}}(X|Y) = H(X|Y)$
- o Let (X, Y) be uniformly distributed over $\{(x, y) : x, y \in \{1, 2, 3\}, x \neq y\}$ and \mathcal{G} has a single edge $\{1, 3\}$. $\Gamma(\mathcal{G}) = \{\{1, 2\}, \{2, 3\}\}$. By convexity, $I(X; W|Y)$ is minimized when $p(\{1, 2\}|2) = p(\{2, 3\}|2) = 1/2$. Thus,

$$H_{\mathcal{G}}(X|Y) = H(W|Y) - H(W|X, Y) = \frac{1}{3} + \frac{2}{3} \cdot H(1/4) - \frac{1}{3} = \frac{2}{3} \cdot H(1/4)$$

Finally, define the *characteristic graph* \mathcal{G} of the (X, Y, g) tuple [4] with nodes

over the support set of X such that distinct nodes x, x' are connected if there is an y such that $p(x, y), p(x', y) > 0$ and $g(x, y) \neq g(x', y)$

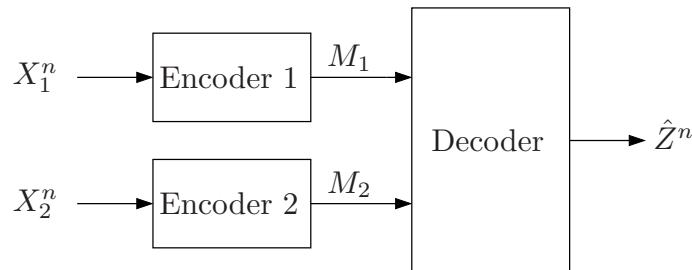
- *Orlitsky–Roche Theorem* [2]: The optimal rate for losslessly computing of function g is

$$R_g^* = H_{\mathcal{G}}(X | Y)$$

The proof is in the Appendix

Distributed Coding for Lossless Computing

- Consider a distributed lossless source coding setting for a 2-DMS (X_1, X_2) (cf. Lecture Notes 11). Suppose that the receiver wishes to losslessly compute a function $Z = g(X_1, X_2)$ of the 2-DMS. What is the set of necessary and sufficient rate pairs, i.e., the optimal rate region for computing g ?



- This problem is in general open

- Simple inner and outer bounds

- Inner bound: Clearly, the Slepian–Wolf region

$$\begin{aligned} R_1 &\geq H(X_1|X_2), \\ R_2 &\geq H(X_2|X_1), \\ R_1 + R_2 &\geq H(X_1, X_2) \end{aligned}$$

constitutes an inner bound to the rate region for any function $g(X_1, X_2)$

- Outer bound: Even when the receiver knows X_1 , $R_2 \geq H(Z|X_1)$ is still necessary. Similarly, we must have $R_1 \geq H(Z|X_2)$. These constraints constitute the following outer bound on the rate region for any function $Z = g(X_1, X_2)$,

$$\begin{aligned} R_1 &\geq H(Z|X_2), \\ R_2 &\geq H(Z|X_1) \end{aligned}$$

- The inner bound is sometimes tight, e.g., when $Z = (X_1, X_2)$. In [5], necessary and sufficient conditions are given for the inner bound to be tight

- The outer bound is sometimes tight. Consider the following:

Example [6]: Let (X_1, X_2) be DSBS(p), thus $X_1 \sim \text{Bern}(1/2)$ and $Z \sim \text{Bern}(p)$ are independent and $X_2 = X_1 \oplus Z$. Let $g(X_1, X_2) = X_1 \oplus X_2 = Z$

The inner bound reduces to $R_1 \geq H(p)$, $R_2 \geq H(p)$, $R_1 + R_2 \geq 1 + H(p)$, while the outer bound reduces to $R_1 \geq H(p)$ and $R_2 \geq H(p)$

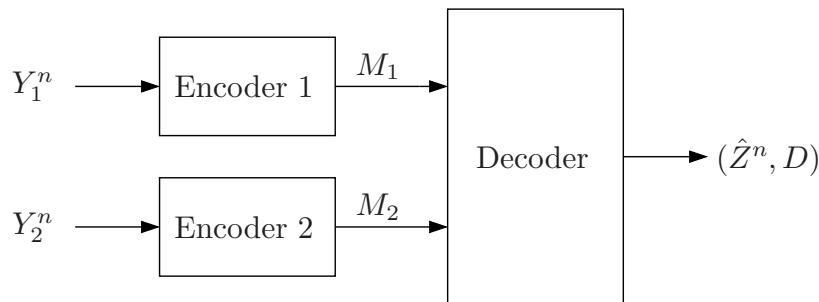
We now show that the outer bound is achievable using random linear codes!

- Codebook generation: Randomly generate $k \times n$ binary matrix A with i.i.d. $\text{Bern}(1/2)$ entries
- Encoding: Sender 1 sends the binary k -vector $A X_1^n$ and Sender 2 sends the binary k -vector $A X_2^n$
- Decoding: The receiver adds the two binary k -vectors to obtain $A X_1^n \oplus A X_2^n = A Z^n$
- It can be shown that if $k/n > H(p) + \delta(\epsilon)$, then the probability of decoding error averaged over the choice of the encoding matrix $\rightarrow 0$ as $n \rightarrow \infty$ (why?)

- Remark: The above simple outer bound can be improved using the Orlitsky–Roche Theorem twice, once when the receiver knows X_1 and a second time when it knows X_2 . Defining the characteristic graphs \mathcal{G}_1 for (X_1, X_2, g) and \mathcal{G}_2 for (X_2, X_1, g) as before, we obtain the outer bound $R_1 \geq H_{\mathcal{G}_1}(X_1|X_2)$, $R_2 \geq H_{\mathcal{G}_2}(X_2|X_1)$

μ -Sum Problem

- The above lossless setting can be extended to a lossy setting where the receiver wishes to estimate Z with respect to a distortion measure $d(z, \hat{z})$. We consider an example where the sum rate distortion function is known
- Let (Y_1, Y_2) be 2-WGN($1, \rho$) sources with $\rho \geq 0$ and $\mu = [\mu_1 \mu_2]^T$. The sources are separately encoded with the objective of computing $Z = \mu^T \mathbf{Y}$ at the decoder to within a prescribed average squared error distortion



- A $(2^{nR_1}, 2^{nR_2}, n)$ code can be defined as usual

- A rate pair (R_1, R_2) is said to be *achievable* with distortion D if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, n)$ codes with

$$\limsup_{n \rightarrow \infty} E \left(\frac{1}{n} \sum_{i=1}^n (\mu_1 Y_{1i} + \mu_2 Y_{2i} - \hat{Z}_i)^2 \right) \leq D$$

- The μ -sum rate-distortion region $\mathcal{R}_\mu(D)$ is the set of rate pairs (R_1, R_2) that are achievable with distortion D
- *Theorem 3 [7]:* Let $\mu_1 \mu_2 = \delta^2 s_1 s_2 / \rho > 0$, where $s_1 = \rho(\rho + \mu_1/\mu_2)/(1 - \rho^2)$, $s_2 = \rho(\rho + \mu_2/\mu_1)/(1 - \rho^2)$, and $\delta = 1/(1 + s_1 + s_2)$. The μ -sum rate-distortion region is the set of rate pairs (R_1, R_2) satisfying

$$\begin{aligned} R_1 &\geq r_1 + \frac{1}{2} \log \left(\frac{1}{D + \delta} \right) - \frac{1}{2} \log (1 + s_2(1 - 2^{-2r_2})) \\ R_2 &\geq r_2 + \frac{1}{2} \log \left(\frac{1}{D + \delta} \right) - \frac{1}{2} \log (1 + s_1(1 - 2^{-2r_1})) \\ R_1 + R_2 &\geq r_1 + r_2 + \frac{1}{2} \log \left(\frac{1}{D + \delta} \right) \end{aligned}$$

for some $r_1, r_2 \geq 0$ such that $(D + \delta)^{-1} \leq 1 + s_1(1 - 2^{-2r_1}) + s_2(1 - 2^{-2r_2})$

- Note that if (R_1, R_2) is achievable with distortion D for μ , then for any $b > 0$, (R_1, R_2) is also achievable with distortion $b^2 D$ for $b\mu$ since if

$$E[(\mu_1 Y_1 + \mu_2 Y_2 - \hat{Z})^2] \leq D$$

then

$$E[(b\mu_1 Y_1 + b\mu_2 Y_2 - \tilde{Z})^2] \leq b^2 D$$

where $\tilde{Z} = b\hat{Z}$ is the estimate for $b\mu$. Thus, the theorem characterizes the rate-distortion region for any μ with $\mu_1 \mu_2 > 0$

- Proof: We show that the μ -sum problem is equivalent to a CEO problem (cf. Lecture Notes 13) and use this equivalence to find $\mathcal{R}_\mu(D)$

Since Y_1 and Y_2 are jointly Gaussian, they can be expressed as

$$Y_1 = a_1 X + Z_1, \quad Y_2 = a_2 X + Z_2$$

for some $a_1 a_2 = \rho$, and independent random variables $X \sim N(0, 1)$, $Z_1 \sim N(0, 1 - a_1^2)$, and $Z_2 \sim N(0, 1 - a_2^2)$

We consider the MMSE estimate \tilde{X} of X given (Y_1, Y_2)

$$\begin{aligned} \tilde{X} &= E(X | Y_1, Y_2) = [a_1 \ a_2] K_Y^{-1} \mathbf{Y} \\ &= \left[\frac{a_1 - \rho a_2}{1 - \rho^2} \ \frac{a_2 - \rho a_1}{1 - \rho^2} \right] \mathbf{Y} \end{aligned}$$

We now choose a_j , $j = 1, 2$, such that $\tilde{X} = \boldsymbol{\mu}^T \mathbf{Y}$, that is,

$$\frac{a_1 - \rho a_2}{1 - \rho^2} = \mu_1, \quad \frac{a_2 - \rho a_1}{1 - \rho^2} = \mu_2$$

Solving for a_1, a_2 , we have

$$a_1^2 = \rho \frac{\rho + \mu_1/\mu_2}{1 + \rho\mu_1/\mu_2} = \frac{s_1}{1 + s_1}, \quad a_2^2 = \rho \frac{\rho + \mu_2/\mu_1}{1 + \rho\mu_2/\mu_1} = \frac{s_2}{1 + s_2}$$

It can be readily checked that the constraint $\rho = a_1 a_2$ is equivalent to the normalization

$$\mu_1 \mu_2 = \frac{\rho}{(\rho + \mu_1/\mu_2)(\rho + \mu_2/\mu_1)},$$

and that the corresponding mean squared error is

$$\mathbb{E} \left((X - \tilde{X})^2 \right) = 1 - \left(\frac{a_1 - \rho a_2}{1 - \rho^2} a_1 + \frac{a_2 - \rho a_1}{1 - \rho^2} a_2 \right) = 1 - \frac{a_1^2 + a_2^2 - 2\rho^2}{1 - \rho^2} = \delta$$

- Now, for any U satisfying the Markov chain $X \rightarrow (Y_1, Y_2) \rightarrow U$,

$$\begin{aligned} \mathbb{E} \left[(X - \mathbb{E}(X|U))^2 \right] &= \mathbb{E} \left[(\boldsymbol{\mu}^T \mathbf{Y} + \tilde{Z} - \mathbb{E}(\boldsymbol{\mu}^T \mathbf{Y} + \tilde{Z}|U))^2 \right] \\ &= \delta + \mathbb{E} \left[(\boldsymbol{\mu}^T \mathbf{Y} - \mathbb{E}(\boldsymbol{\mu}^T \mathbf{Y}|U))^2 \right] \end{aligned}$$

Therefore, any code that achieves distortion D for the $\boldsymbol{\mu}$ -sum problem can be used to achieve distortion $D + \delta$ for a CEO problem and vice versa

The observations for the corresponding CEO problem are $Y_j/a_j = X + \tilde{Z}_j$, $j = 1, 2$, where $\tilde{Z}_j = Z_j/a_j \sim N(0, 1/s_j)$ since $s_j = a_j^2/(1 - a_j^2)$

- Thus the rate region is as specified in the theorem, since the rate region of the CEO problem with distortion $D + \delta$ is the set of rate pairs (R_1, R_2) satisfying

$$\begin{aligned} R_1 &\geq r_1 + \frac{1}{2} \log \left(\frac{1}{D + \delta} \right) - \frac{1}{2} \log \left(1 + s_2(1 - 2^{-2r_2}) \right), \\ R_2 &\geq r_2 + \frac{1}{2} \log \left(\frac{1}{D + \delta} \right) - \frac{1}{2} \log \left(1 + s_1(1 - 2^{-2r_1}) \right), \\ R_1 + R_2 &\geq r_1 + r_2 + \frac{1}{2} \log \left(\frac{1}{D + \delta} \right) \end{aligned}$$

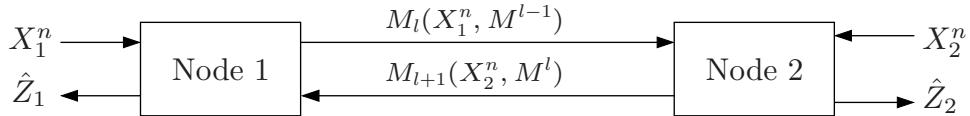
for some $r_1, r_2 \geq 0$ such that $(D + \delta)^{-1} \leq 1 + s_1(1 - 2^{-2r_1}) + s_2(1 - 2^{-2r_2})$

- Remarks

- When $\mu_1 \mu_2 = 0$, then the $\boldsymbol{\mu}$ -sum problem is equivalent to the quadratic Gaussian distributed source coding (Lecture Notes 13) with $D_1 \geq 1$ or $D_2 \geq 1$. The rate distortion region is given by Oohama [8] with proper normalization. Thus, for $\mu_1 \mu_2 \geq 0$, the Berger–Tung inner bound is tight
- On the other hand, when $\mu_1 \mu_2 < 0$, it can be shown that the Berger–Tung inner bound is not tight in general [9]

Two-Way Coding for Lossy Computing

- Consider a two-way lossy source coding setting for 2-DMS (cf. Lecture Notes 21), where node 1 wishes to estimate a function $Z_1 = g_1(X_1, X_2)$ and node 2 wishes to estimate a function $Z_2 = g_2(X_1, X_2)$ with respect to distortion measures d_1 and d_2 , respectively. What is the rate–distortion region for this scenario?



- Simple inner and outer bounds:

- Inner bound: Using two independent rounds of Wyner-Ziv coding, we obtain the inner bound $R_1 > I(X_1; U_1|X_2)$, $R_2 > I(X_2; U_1|X_1)$ for some $p(u_1|x_1)$, $p(u_2|x_2)$, $\hat{z}_1(u_1, x_2)$, and $\hat{z}_2(u_2, x_1)$ such that $E(d_1(Z_1, \hat{Z}_1)) \leq D_1$, $E(d_2(Z_2, \hat{Z}_2)) \leq D_2$
- Outer bound: Even if each encoder knows the other node's source, we must have $R_1 \geq I(Z_2; \hat{Z}_2|X_2)$, $R_2 \geq I(Z_1; \hat{Z}_1|X_1)$ for some $p(\hat{z}_1|x_1, x_2)$, $p(\hat{z}_2|x_1, x_2)$ such that $E(d_1(Z_1, \hat{Z}_1)) \leq D_1$ and $E(d_2(Z_2, \hat{Z}_2)) \leq D_2$

- The bounds can be tight

Example [10]: Let (X, Y) be a 2-WGN(P, ρ) source let $Z_1 = Z_2 = Z = (X_1 + X_2)/2$. The rate–distortion region for distortion D is the set of of rate pairs (R_1, R_2) such that $R_1 \geq R((1 - \rho^2)P/4D)$, $R_2 \geq R((1 - \rho^2)P/4D)$. It is easy to see that this region coincides with the inner bound. It can also be shown that it coincides with the outer bound (why?)

- The bounds are not tight in general. Following the two-way lossy source coding theorem (cf. Lecture Notes 21), we can readily establish the following rate–distortion region for q rounds of communication

Theorem 4: The q -round rate–distortion region for computing functions Z_1 and Z_2 with distortion pair (D_1, D_2) is the set of rate pairs (R_1, R_2) satisfying

$$R_1 \geq I(X_1; U^q|X_2),$$

$$R_2 \geq I(X_2; U^q|X_1)$$

for some $p(u^q|x_1, x_2) = \prod_{l=1}^q p(u_l|u^{l-1}, x_{j_l})$, $j_l = 1$ if l is odd and $j_l = 2$ if l is even, $\hat{z}_1(u^q, x_1)$ and $\hat{z}_2(u^q, x_2)$ such that $E(d_1(Z_1, \hat{Z}_1)) \leq D_1$ and $E(d_2(Z_2, \hat{Z}_2)) \leq D_2$

- Note that the above region is computable for bounded q . However, there is no bound on the cardinality of q in general

Two-Way Coding for Lossless Computing

- Consider the two-way lossless source coding setting in Lecture Notes 21, where node 1 wishes to losslessly estimate $Z_1 = g_1(X_1, X_2)$ and node 2 wishes to losslessly estimate $Z_2 = g_2(X_1, X_2)$. What is the optimal rate region for this setting?
- The theorem for the lossy setting can be specialized to yield the following characterization of the optimal rate region for q rounds

Theorem 5 [2, 11]: The optimal q -round rate region for lossless computing of the functions Z_1 and Z_2 is the set of rate pairs (R_1, R_2) satisfying

$$R_1 \geq I(X_1; U^q | X_2),$$

$$R_2 \geq I(X_2; U^q | X_1)$$

for some $p(u^q | x_1, x_2) = \prod_{l=1}^q p(u_l | u^{l-1}, x_{j_l})$, $j_l = 1$ if l is odd and $j_l = 2$ if l is even, such that $H(g_1(X_1, X_2) | X_1, U^q) = 0$ and $H(g_2(X_1, X_2) | X_2, U^q) = 0$

- In some cases, 2 independent rounds is sufficient, e.g., if $Z_1 = X_2$ and $Z_2 = X_1$, or when (X_1, X_2) is a DSBS and $Z_1 = Z_2 = X_1 \oplus X_2$ (Why?)

- In general, interactivity can reduce transmission

Assume $Z_1 = Z$ and $Z_2 = \emptyset$ and consider 2 rounds of communication; in round 1, node 1 sends a message to node 2 that depends on X_1 and in round 2, node 2 sends a second message to node 1 that depends on X_2 and the first message

By Theorem 5, the optimal rate region for 2 rounds of communication is the set of rate pairs (R_1, R_2) such that

$$R_1 \geq I(U_1; X_1 | X_2),$$

$$R_2 \geq I(U_2; X_2 | U_1, X_1)$$

for some $p(u_1 | x_1)p(u_2 | u_1, x_2)$ satisfying $H(Z | U_1, U_2, X_1) = 0$

The following example shows that 2 rounds can be better than one round

Example [2]: Let X_1 be a $\text{Bern}(p)$ source for $p \ll 1/2$, X_2 be $\text{Bern}(1/2)$, and $Z = X_1 \cdot X_2$. The minimum rate for one round of communication from node 2 to node 1 is $R_2 = 1$ bit/ symbol

Consider the following 2-round coding scheme. In the first round, node 1 uses Slepian–Wolf coding to send X_1 losslessly to node 2. This succeeds provided $R_1 > H(p)$. In the second round, node 2 sets $Y = X_2$ if $X_1 = 1$ and $Y = e$ if $X_1 = 0$. It then uses Slepian–Wolf coding to send Y losslessly to node 1. This succeeds provided $R_2 > H(Y | X_1) = p$. Thus the sum rate for the two rounds is $R_1 + R_2 = H(p) + p < 1$ for sufficiently small p

- More than 2 rounds may reduce transmission further

Example [11]: Let (X_1, X_2) be DSBS(p) and $g_1(X_1, X_2) = g_2(X_1, X_2) = X_1 \cdot X_2$. For two rounds of communication, $R_1 > H_G(X_1|X_2) = H(X_1|X_2) = H(p)$ and $R_2 > H(g_1(X_1, X_2)|X_1) = (1/2)H(p)$ are achievable. Optimality follows by the Orlitsky–Roche Theorem for the R_1 bound and by the cutset bound for the R_2 bound

Consider the following 3-round coding scheme. Set the auxiliary random variables in the above theorem as $U_1 = (1 - X_1) \cdot W$, where $W \sim \text{Bern}(1/2)$ is independent of X_1 , $U_2 = X_2 \cdot (1 - U_1)$, and $U_3 = X_1 \cdot U_2$. Since $U_3 = X_1 \cdot X_2$, both nodes can compute the product noiselessly. This gives the upper bound on the sum rate

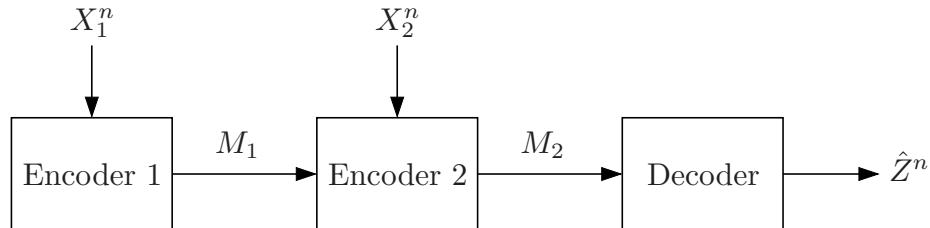
$$R_1 + R_2 < \frac{5}{4}H(p) + \frac{1}{2}H\left(\frac{1-p}{2}\right) - \frac{1-p}{2} < \frac{3}{2}H(p)$$

In [11] it is shown that more rounds improve the sum rate further and an upper bound on the sum rate is provided for an infinite number of rounds

- The two-way coding for computing problem is closely related to *communication complexity* introduced in [12]. In this setup both nodes wish to compute the same function with no errors. Work in this area is described in [13]

Cascade Coding for Computing

- Consider the following lossy source coding for computing problem for 2-DMS (X_1, X_2) [14]. The decoder wishes to reconstruct the function $Z = g(X_1, X_2)$ with respect to distortion measure $d(z, \hat{z})$. What is the rate–distortion region?



- The rate–distortion region is not known in general, even when X_1 and X_2 are independent! We discuss inner and outer bounds
- Cutset outer bound: If a rate pair (R_1, R_2) is achievable at distortion D , then it must satisfy the conditions

$$R_1 \geq I(X_1; U|X_2),$$

$$R_2 \geq I(Z; \hat{Z})$$

for some $p(u|x_1)p(\hat{z}|x_2, u)$ such that $E(d(Z, \hat{Z})) \leq D$

- Local computing inner bound: Encoder 1 uses Wyner-Ziv coding to send a description U of its source X_1 to encoder 2 at rate $R_1 > I(X_1; U|X_2)$. Encoder 2 sends the estimate \hat{Z} based on (U, X_2) at rate $R_2 > I(X_2, U; \hat{Z})$ to the decoder. This gives the *local computing* inner bound for distortion D that consists of all rate pairs (R_1, R_2) satisfying

$$R_1 > I(X_1; U|X_2),$$

$$R_2 > I(X_2, U; \hat{Z})$$

for some $p(u|x_1)p(\hat{z}|x_2, u)$ such that $E(d(Z, \hat{Z})) \leq D$

- The local computing bound coincides with the cutset bound for the special case of lossless computing of Z . To show this, let d be the Hamming distortion measure and consider the case of $D = 0$. This yields

$$R_1 > I(X_1; U|X_2),$$

$$R_2 > H(Z)$$

for some $p(u|x_1)$ such that $H(Z|U, X_2) = 0$. Now, consider the cutset bound and set $\hat{Z} = Z$. Since $\hat{Z} \rightarrow (X_2, U) \rightarrow X_1$ form a Markov chain and Z is a function of (X_1, X_2) , we must have the condition $H(Z|U, X_2) = 0$

As in the Orlitsky–Roche Theorem, the condition $R_1 > I(X_1; U|X_2)$ can be further simplified to a graph entropy

- Forwarding inner bound: Consider the following alternative coding scheme. Encoder 1 again sends a description U_1 of its source X_1 at rate $R_1 > I(X_1; U_1|X_2)$. Encoder 2 forwards the description from encoder 1 together with a description U_2 of its source X_2 given U_1 at total rate $R_2 > I(X_1; U_1) + I(X_2; U_2|U_1)$. The decoder then computes the estimate $\hat{Z}(U_1, U_2)$. This yields the *forwarding* inner bound for distortion D consisting of all rate pairs (R_1, R_2) satisfying

$$R_1 > I(X_1; U_1|X_2),$$

$$R_2 > I(U_1; X_1) + I(U_2; X_2|U_1)$$

for some $p(u_1|x_1)p(u_2|x_2, u_1)$ and $\hat{z}(u_1, u_2)$ such that $E(d(Z, \hat{Z})) \leq D$

- Forwarding is optimal when X_1 and X_2 are independent and $Z = (X_1, X_2)$
- The lossless computing example shows that local computing can outperform forwarding (check). We give another example where this is the case

Example [14]: Let X_1, X_2 be independent WGN(1) sources, d be squared error distortion, and $Z = X_1 + X_2$

Consider the sum rate for the forwarding inner bound. It can be shown that it is optimized when we set $U_1 = \hat{X}_1$ and $U_2 = \hat{X}_2$ are independently encode the two sources using Gaussian codes. This gives

$$R_f := R_1 + R_2 = 2R\left(\frac{1}{D_1}\right) + R\left(\frac{1}{D_2}\right) = R\left(\frac{1}{D_1^2 D_2}\right)$$

such that $D_1 + D_2 \leq D$. Optimizing over D_1, D_2 gives the minimum sum rate

$$R_f^* = R\left(\frac{27}{4D^3}\right),$$

which is achieved when $D_1 = 2D_2 = 2D/3$

Next, consider the sum rate using local computing. Let

$$U = X_1 + W_1, V = E(X_1|U) + X_2 + W_2, \text{ and } \hat{Z} = E(Z|V),$$

where

$$W_1 \sim N\left(0, \frac{D_1}{1 - D_1}\right), W_2 \sim N\left(0, \frac{(2 - D_1)D_2}{(2 - D_1) - D_2}\right)$$

are independent of each other and of (X_1, X_2)

The sum rate for this test channel choice is

$$R_l := R_1 + R_2 = R\left(\frac{1}{D_1}\right) + R\left(\frac{2 - D_1}{D_2}\right)$$

subject to the distortion constraint $D_1 + D_2 \leq D$. Optimizing over D_1, D_2 , we obtain

$$R_l^* = R\left(\frac{1}{2\left(1 - \sqrt{1 - D/2}\right)^2}\right) < R_f^*$$

for all $D \in (0, 1]$. Thus local computing can outperform forwarding for this example

- Combined inner bound: Local computing and forwarding can be combined as follows. Encoder 1 uses Wyner-Ziv coding to send the description pair (U, V) of X_1 to encoder 2. Encoder 2 forwards the description V to the decoder and the estimate \hat{Z} based on U, V, X_2 . This yields the inner bound for distortion D consisting of all rate pairs (R_1, R_2) satisfying

$$R_1 > I(X_1; U, V | X_2),$$

$$R_2 > I(X_1; V) + I(X_2, U; \hat{Z} | V)$$

for some $p(u, v|x_1)p(\hat{z}|x_2, u, v)$ such that $E(d(Z, \hat{Z})) \leq D$

- This general inner bound does not coincide with the cutset bound in general

- Cascade source coding versus distributed source coding for computing:
 - The lossless computing rate region is known for the cascade case but is not known in general for the distributed source coding setting. This apparently suggests that the cascade problem is in general more tractable than distributed source coding for computing
 - This is not the case, however. Consider the μ -sum problem. While the rate–distortion region for WGN sources is known for the distributed source coding setting (see Lecture Notes 13), it is not known for the cascade case, even when X_1 and X_2 are independent

Distributed Lossy Averaging

- The distributed averaging problem is a canonical example of distributed consensus studied in control and computer science [15, 16, 17]. We consider the following lossy source coding formulation for this problem
- Consider a noiseless network modeled by a graph with N nodes and a set of undirected edges representing two-way communication links
- Node $j \in [1 : N]$ observes an independent WGN(1) source X_j
- Each node wishes to estimate the average $Z := (1/N) \sum_{j=1}^N X_j$ to a prescribed MSE distortion D
- Communication is performed in q rounds. In each round an edge (node-pair) is selected and the two nodes communicate over the selected noiseless two-way link (using two-way coding for lossy computing with subrounds of block codes as detailed previously)
- Let r_l be the total communication rate in round $l \in [1 : q]$ and define the network *sum rate* as $R = \sum_{l=1}^q r_l$

- A rate–distortion pair (R, D) is achievable if there exists a number of rounds q and associated sequence of edge selections and codes such that

$$\limsup_{n \rightarrow \infty} \frac{1}{N} \sum_{j=1}^N \frac{1}{n} \sum_{i=1}^n \mathbb{E} [(\hat{Z}_{ji} - Z_i)^2] \leq D,$$

where $Z_i = (1/N) \sum_{j=1}^N X_{ji}$ and \hat{Z}_{ji} is the estimate of node j of Z_i

- The *network rate–distortion function* $R(D)$ is the infimum of sum rates R such that (R, D) is achievable
- $R(D) = 0$ for $D \geq (N - 1)/N^2$, which is achieved by taking $\hat{Z}_{ji} = X_{ji}/N$ for each $j \in [1 : N]$ and $i \in [1 : n]$
- $R(D)$ is known completely for $N = 2$ (see the example in two-way lossy computing). It is not known in general for $N > 2$
- Cutset lower bound on $R(D)$:

Theorem 6 [10]: The network rate–distortion function for the lossy averaging problem is lower bounded by

$$R(D) \geq N R \left(\frac{N - 1}{N^2 D} \right)$$

This result is proved by considering information flow into each node from the rest of the nodes when they are combined into a single “super node.” Details of the proof are given in the Appendix

- Remark: The cutset bound holds for any connected network. The bound can be improved for tree networks by considering the number of bits flowing through each edge in both directions
- Upper bound on $R(D)$: We can show that the cutset bound is achievable within a factor of 2 for any network that contains a star network as a subnetwork

Theorem 7 [10]: The network rate–distortion function for a network with star subnetwork is upper bounded by

$$R(D) \leq 2(N - 1) R \left(\frac{2(N - 1)^2}{N^3 D} \right) \leq 2N R \left(\frac{N - 1}{N^2 D} \right)$$

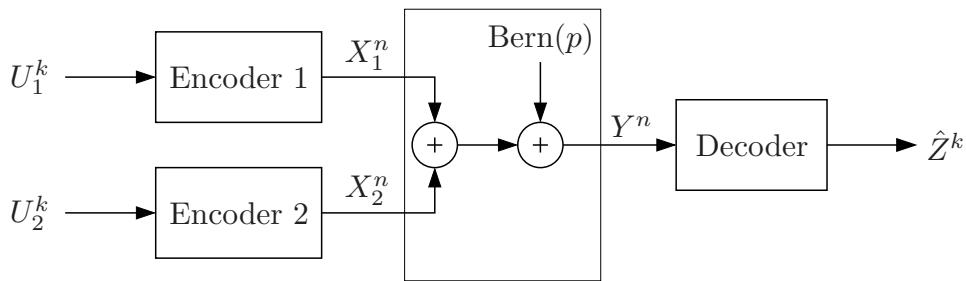
for $D < (N - 1)/N^2$

The proof is given in the Appendix

Computing over a MAC

- As we have discussed in Lecture Notes 15, source–channel separation holds when sending independent sources over a DM-MAC, but does not necessarily hold when the sources are correlated. We show through an example that even when the sources are independent, separation does not necessarily hold when the goal is to compute a function of the sources over a DM-MAC
- Example [18]: Let (U_1, U_2) be a pair of independent Bern(1/2) sources and suppose we wish to compute $Z = U_1 \oplus U_2$ over a modulo-2 sum DM-MAC followed by a BSC(p)

What are the sufficient and necessary conditions to compute Z^k losslessly by using the MAC n times (i.e., the transmission rate is $r = k/n$)?



- With separate source–channel coding, $Z = U_1 \oplus U_2$ can be computed losslessly over the DM-MAC at rate r if and only if

$$\begin{aligned} rH(Z|U_2) &= rH(U_1) \leq I(X_1; Y|X_2, Q), \\ rH(U_2) &\leq I(X_2; Y|X_1, Q), \\ r(H(U_1) + H(U_2)) &\leq I(X_1, X_2; Y|Q) \end{aligned}$$

for some $p(q)p(x_1|q)p(x_2|q)$

This reduces to $r(H(U_1) + H(U_2)) = 2r \leq 1 - H(p)$. Thus, r is achievable via separate source–channel coding if and only if $r \leq (1 - H(p))/2$

On the other hand, considering the cutset at the input of the BSC part of the channel gives the upper bound

$$rH(U_1 \oplus U_2) \leq 1 - H(p)$$

We now show that the upper bound is achievable using random linear codes:

- Codebook generation: Randomly and independently generate a $l \times k$ binary matrix A and an $n \times l$ binary matrix B each with i.i.d. Bern(1/2) entries
- Encoding: Encoder 1 sends $X_1^n = BAU_1^k$ and Encoder 2 sends $X_2^n = BAU_2^k$

- Decoding: The receiver first decodes $A(U_1^k \oplus U_2^k)$ and then decodes $Z^k = U_1^k \oplus U_2^k$
 If $l < n(1 - H(p) - \delta(\epsilon))$, the receiver can decode $A(U_1^k \oplus U_2^k)$ with probability of error (averaged over the random matrix B) $\rightarrow 0$ as $n \rightarrow \infty$ (cf. channel coding with linear codes in Lecture Notes 3)
 If $l > k(1 + \delta(\epsilon))$, the receiver can decode Z^k with probability of error (averaged over the random matrix A) $\rightarrow 0$ as $n \rightarrow \infty$. Therefore, $r < 1 - H(p)$ is achievable using joint source–channel coding

Key New Ideas and Techniques

- Information theoretic framework for distributed computing
- Graph entropy and conditional graph entropy
- Interaction reduces communication requirement for computing
- Source–channel separation is suboptimal even when computing from independent sources
- Open problem: What is the optimal rate region for distributed computing?

References

- [1] H. Yamamoto, "Wyner-Ziv theory for a general function of the correlated sources," *IEEE Trans. Inf. Theory*, vol. 28, no. 5, pp. 803–807, Sept. 1982.
- [2] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, 2001.
- [3] J. Körner, "Coding of an information source having ambiguous alphabet and the entropy of graphs," in *Transactions of the Sixth Prague Conference on Information Theory, Statistical Decision Functions, Random Processes (Tech Univ., Prague, 1971; dedicated to the memory of Antonín Špaček)*. Prague: Academia, 1973, pp. 411–425.
- [4] H. S. Witsenhausen, "The zero-error side information problem and chromatic numbers," *IEEE Trans. Inf. Theory*, vol. 22, no. 5, pp. 592–593, 1976.
- [5] T. S. Han and K. Kobayashi, "A dichotomy of functions $F(X, Y)$ of correlated sources (X, Y) from the viewpoint of the achievable rate region," *IEEE Trans. Inf. Theory*, vol. 33, no. 1, pp. 69–76, 1987.
- [6] J. Körner and K. Marton, "How to encode the modulo-two sum of binary sources," *IEEE Trans. Inf. Theory*, vol. 25, no. 2, pp. 219–221, 1979.
- [7] A. B. Wagner, S. Tavildar, and P. Viswanath, "Rate region of the quadratic Gaussian two-encoder source-coding problem," *IEEE Trans. Inf. Theory*, vol. 54, no. 5, pp. 1938–1961, May 2008.
- [8] Y. Oohama, "Rate-distortion theory for Gaussian multiterminal source coding systems with

- several side informations at the decoder," *IEEE Trans. Inf. Theory*, vol. 51, no. 7, pp. 2577–2593, July 2005.
- [9] D. Krishivasan and S. S. Pradhan, "Lattices for distributed source coding: Jointly gaussian sources and reconstruction of a linear function," 2007, submitted to *IEEE Trans. Inf. Theory*, 2007. [Online]. Available: <http://arxiv.org/abs/0707.3461/>
- [10] H.-I. Su and A. El Gamal, "Distributed lossy averaging," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009.
- [11] N. Ma and P. Ishwar, "Two-terminal distributed source coding with alternating messages for function computation," in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 51–55.
- [12] A. C.-C. Yao, "Some complexity questions related to distributive computing," in *Proc. the 11th Annual ACM Symposium on Theory of Computing*. New York: ACM, 1979, pp. 209–213.
- [13] E. Kushilevitz and N. Nisan, *Communication Complexity*. Cambridge: Cambridge University Press, 1997.
- [14] P. Cuff, H.-I. Su, and A. El Gamal, "Cascade multiterminal source coding," in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 1199–1203.
- [15] J. N. Tsitsiklis, "Problems in decentralized decision making and computation," Ph.D. Thesis, Massachusetts Institute of Technology, Cambridge, MA, Nov. 1984.
- [16] L. Xiao and S. Boyd, "Fast linear iterations for distributed averaging," *Systems Control Letters*, vol. 53, no. 1, pp. 65–78, 2004.
- [17] S. Boyd, A. Ghosh, B. Prabhakar, and D. Shah, "Randomized gossip algorithms," *IEEE Trans. Inf. Theory*, vol. 52, no. 6, pp. 2508–2530, 2006.

- [18] B. Nazer and M. Gastpar, "Computation over multiple-access channels," *IEEE Trans. Inf. Theory*, vol. 53, no. 10, pp. 3498–3516, Oct. 2007.

Appendix: Proof of Orlitsky–Roche Theorem

- We prove that

$$\min_{p(u|x)} I(U; X|Y) = \min_{p(w|x)} I(W; X|Y),$$

where the first minimum is over all $p(u|x)$ with $H(Z|U, Y) = 0$ and the second minimum is over all $p(w|x)$ such that $W \in \Gamma(\mathcal{G})$ and $X \in W$

- Consider $p(w|x)$ that achieves the second minimum. Since w is a maximally independent set with respect to the characteristic graph of (X, Y, g) , for each $y \in \mathcal{Y}$, $g(x, y)$ is constant for all $x \in w$ with $p(x, y) > 0$. Hence, $g(x, y)$ can be uniquely determined from (w, y) whenever $p(w, x, y) > 0$, or equivalently, $H(g(X, Y)|W, Y) = 0$. By identifying $U = W$, it follows that $\min_{p(u|x)} I(U; X|Y) \leq \min_{p(w|x)} I(W; X|Y)$
- To show the other direction of inequality, let $p(u|x)$ achieve the first minimum and define

$$w(u) := \{x : p(u, x) > 0\}$$

- If $p(w, x) > 0$, then there exists a u such that $w(u) = w$ and $p(u, x) > 0$. By definition, $x \in w$

- Also $W \rightarrow X \rightarrow Y$ form a Markov chain, since $U \rightarrow X \rightarrow Y$ form a Markov chain and W is a function of U
- Furthermore, suppose $p(w) > 0$, i.e., there exists a u such that $p(u) > 0$ and $w(u) = w$. Now if $x \in w$, then $p(u, x) > 0$. Hence by Markovity $p(x, y) > 0$ implies $p(u, x, y) > 0$. But since $H(g(X, Y)|U, Y) = 0$, (u, y) should determine $g(x, y)$ uniquely. It follows that if $x, x' \in w$ and $p(x, y), p(x', y) > 0$, then $g(x, y) = g(x', y)$, which means that W is maximally independent
- Finally, since $I(W; X|Y) \leq I(W, U; X|Y) \leq I(U; X|Y)$, we have $\min_{p(u|x)} I(U; X|Y) \geq \min_{p(w|x)} I(W; X|Y)$, which completes the proof

Appendix: Proof of Bounds on $R(D)$

- Proof of the cutset bound lower bound: Let R_j be the total receiving rate of node j . Since only pairwise communications are allowed, the sum-rate $R = \sum_{j=1}^N R_j$

Let M_j be the index received by node j , and $U_{ji} := Z_i - (1/N)X_{ji}$. We can bound the receiving rate as follows

$$\begin{aligned}
nR_j &\geq H(M_j) \geq H(M_j | X_j^n) \geq I(U_j^n; M_j | X_j^n) \\
&= \sum_{i=1}^n (h(U_{ji} | U_j^{k-1}, X_j^n) - h(U_{ji} | U_j^{k-1}, X_j^n, M_j)) \\
&= \sum_{i=1}^n (h(U_{ji}) - h(U_{ji} | U_j^{k-1}, X_j^n, M_j, \hat{Z}_j^n)) \\
&\geq \sum_{i=1}^n (h(U_{ji}) - h(U_{ji} | X_{ji}, \hat{Z}_{ji})) \\
&\geq \frac{n}{2} \log \left(\frac{N-1}{N^2} \right) - \sum_{i=1}^n h \left(U_{ji} + \frac{1}{N} X_{ji} - \hat{Z}_{ji} \middle| X_{ji}, \hat{Z}_{ji} \right)
\end{aligned}$$

$$\begin{aligned} &\geq \frac{n}{2} \log \left(\frac{(2\pi e)(N-1)}{N^2} \right) - \sum_{i=1}^n h(Z_i - \hat{Z}_{ji}) \\ &\geq \frac{n}{2} \log \left(\frac{N-1}{N^2 D_j} \right), \end{aligned}$$

where $D_j = (1/n) \sum_{i=1}^n \mathbb{E}((Z_i - \hat{Z}_{ji})^2)$

Thus, the network rate-distortion function is lower bounded by

$$R(D) \geq \min_{(1/N) \sum_{j=1}^N D_j \leq D} \sum_{j=1}^N R\left(\frac{N-1}{N^2 D_j}\right) = R\left(\frac{N-1}{N^2 D}\right),$$

where the equality follows from Jensen's inequality and the distortion constraint $(1/N) \sum_{j=1}^N D_j \leq D$

- Proof of the upper bound: Distortion $D \geq (N-1)/N^2$ is achievable with zero rate by choosing $\hat{Z}_j = (1/N)X_j$. Consider distortion $D < (N-1)/N^2$

Suppose that there are $(N-1)$ edges between node 1 and nodes $2, \dots, N$.
Nodes $j > 1$ sends Gaussian description \hat{X}_j of its source X_j to node 1 at rate

$$I(X_j; \hat{X}_j) = R(D')$$

where $0 < D' < 1$ will be determined later

Node 1 computes the estimates

$$\begin{aligned} \hat{Z}_1 &= \frac{1}{N} X_1 + \frac{1}{N} \sum_{j=2}^N \hat{X}_j, \\ U_j &= \hat{Z}_1 - \frac{1}{N} \hat{X}_j \end{aligned}$$

and sends the Gaussian description \hat{U}_j to node $j > 1$ at rate

$$I(U_j; \hat{U}_j) = R(D')$$

Then node $j > 1$ computes the estimate $\hat{Z}_j = (1/N)X_j + \hat{U}_j$

Next we consider distortion

$$D_1 := \mathbb{E}((\hat{Z}_1 - Z)^2) = \mathbb{E}\left(\left(\frac{1}{N} \sum_{j=2}^N (X_j - \hat{X}_j)\right)^2\right) = \frac{N-1}{N^2} D'$$

and for $j > 1$

$$\begin{aligned} D_j &:= \mathsf{E} \left((\hat{Z}_j - Z)^2 \right) = \mathsf{E} \left(\left((\hat{U}_j - U_j) + \frac{1}{N} \sum_{k \neq 1, j} (\hat{X}_k - X_k) \right)^2 \right) \\ &= \left(\frac{1}{N^2} + \frac{N-2}{N^2} (1 - D') \right) D' + \frac{N-2}{N^2} D' \leq \frac{2N-3}{N^2} D' \end{aligned}$$

The average distortion

$$\frac{1}{N} \sum_{j=1}^N D_j \leq \frac{2(N-1)^2}{N^3} D'$$

Choose $D' = N^3 D / 2(N-1)^2$ satisfying the distortion constraint. Then the sum rate

$$R = 2(N-1) \mathsf{R}(D') \leq 2(N-1) \mathsf{R} \left(\frac{2(N-1)^2}{N^3 D} \right)$$

Note that the upper bound on $R(D)$ is not convex and therefore can be improved by time-sharing

Lecture Notes 23

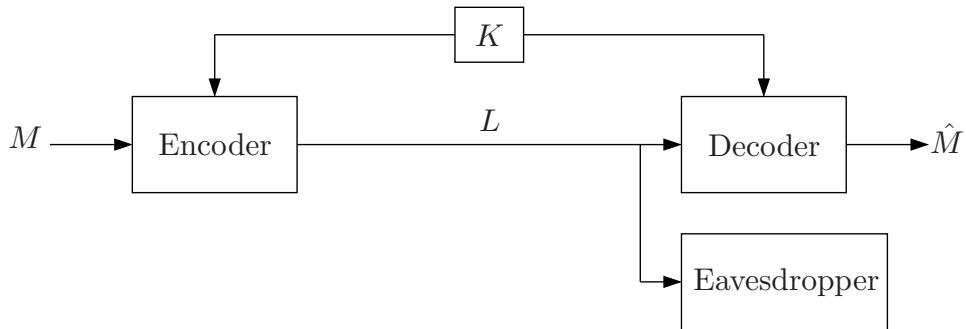
Information Theoretic Secrecy

- Shannon's Secrecy System
- Secure Communication over a DMC
- The Wiretap Channel
- Secret Key Agreement: The Source Model
- Secret Key Agreement: The Channel Model
- Key New Ideas and Techniques
- Proof of Lemmas

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Shannon's Secrecy System

- A sender (Alice) wishes to communicate a message $M \in [1 : 2^{nR}]$ to a receiver (Bob) over a public channel in the presence of an eavesdropper (Eve) who observes the channel output. Alice and Bob share a key $K \in \mathbb{Z}^+$, which is unknown to Eve. How many key bits ($H(K)$) are needed so that Eve cannot obtain any information about the message ?



- The message $M \sim \text{Unif}[1 : 2^{nR}]$
- The encoder (encryption function) assigns a ciphertext $l(m, k)$ to each message $m \in [1 : 2^{nR}]$ and key k , and the decoder (decryption function) assigns a message $\hat{m}(l, k)$ to each ciphertext l and key k

- The communication system is said to have *perfect secrecy* if
 - $P\{M \neq \hat{M}(L(M, K), K)\} = 0$, i.e., the message is decoded correctly, and
 - The *information leakage* $I(L; M) = 0$, i.e., the ciphertext reveals no information about the message
- *Theorem 1* (Shannon's Perfect Secrecy Theorem) [1]: The sufficient and necessary condition for perfect secrecy is $H(K) \geq H(M)$
- Proof: To prove necessity, consider

$$\begin{aligned} H(M) &\stackrel{(a)}{=} H(M|L) \\ &\leq H(M, K|L) \\ &\stackrel{(b)}{=} H(K|L) \\ &\leq H(K), \end{aligned}$$

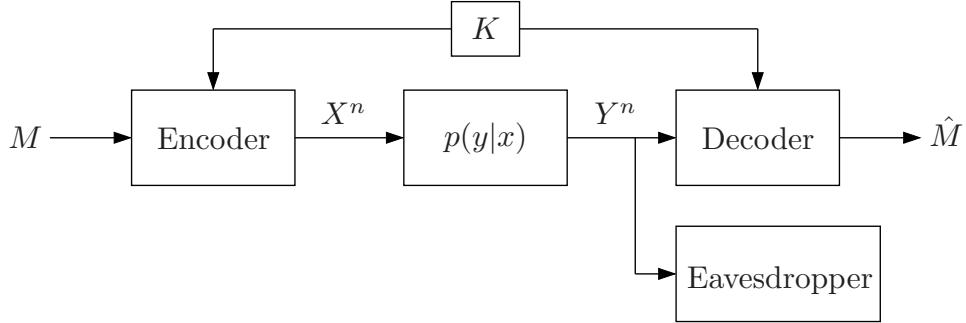
where (a) follows by the secrecy constraint $I(M; L) = 0$ and (b) follows from the communication constraint $P\{M \neq \hat{M}\} = 0$

To prove sufficiency, let the key K be uniformly distributed over $[1 : 2^{nR}]$ and take $L = M + K \pmod{2^{\lfloor nR \rfloor}}$, or equivalently, take the bitwise XOR of the binary expansions of M and K (so called *one-time pad*). It can be readily checked that M and L are independent. To recover the message M from the ciphertext L , the receiver simply subtract the key from the ciphertext to recover $M = L - K \pmod{2^{\lfloor nR \rfloor}}$

- So this is bad news! Alice and Bob need to share a key as long as the message itself
How do they share the long key to begin with?
- Several directions to avoid this limitation of Shannon's secrecy system
 - Computational security: how to exploit the computational hardness of recovering the message from the ciphertext without knowing the key (assuming $P \neq NP$) [2, 3]?
 - Wiretap channel: how to use the better quality of Alice–Bob channel to outdo eves
 - Secret key generation: how to agree upon a secret key (common randomness) from correlated random variables?

Secure Communication over a DMC

- Consider the following extension of the Shannon secrecy system to DMC



- Formally, A $(2^{nR}, 2^{nR_K}, n)$ secrecy code for the Shannon system consists of:
 - A message set $[1 : 2^{nR}]$ and a key set $[1 : 2^{nR_K}]$
 - A *randomized* encoder that generates codeword $X^n(m, k) \in \mathcal{X}^n$ according to the conditional pmf $p(x^n|m, k)$ for each message–key pair $(m, k) \in [1 : 2^{nR}] \times [1 : 2^{nR_K}]$
 - A decoder that assigns a message $\hat{M}(y^n, k)$ or an error message e to each received sequence $y^n \in \mathcal{Y}^n$ and key $k \in [1 : 2^{nR_K}]$

- We assume that the message–key pair (M, K) is uniformly distributed over $[1 : 2^{nR}] \times [1 : 2^{nR_K}]$
- The *information leakage rate* associated with the $(2^{nR}, 2^{nR_K}, n)$ secrecy code is defined as

$$R_l^{(n)} = \frac{1}{n} I(M; Y^n)$$

- The average probability of error for the secrecy code is defined as

$$P_e^{(n)} = P\{M \neq \hat{M}(Y^n, K)\}$$

- A rate R is achievable at key rate R_K if there exists a sequence of $(2^{nR}, 2^{nR_K}, n)$ codes with $R_l^{(n)} \rightarrow 0$ and $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The *secrecy capacity* $C(R_K)$ of the DMC is the supremum of all achievable rates at key rate R_K
- This asymptotic notion of secrecy is weaker than Shannon's original notion of perfect secrecy. Can we send at a higher rate?
- Theorem 2 [1]:* The secrecy capacity is

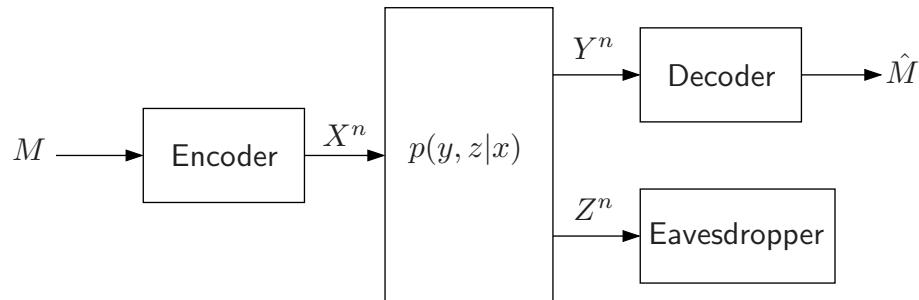
$$C(R_K) = \min\{R_K, \max_{p(x)} I(X; Y)\}$$

Thus secure communication is still limited by the key rate until saturated by the channel capacity

- What will happen if the enemy does not receive the same channel output but listens through another channel? Can we achieve a positive rate without a shared key?

The Wiretap Channel

- A *discrete-memoryless wiretap channel* (DM-WTC) $(\mathcal{X}, p(y, z|x), \mathcal{Y} \times \mathcal{Z})$ is a DM-BC with sender X , legitimate receiver Y and eavesdropper Z
- The sender X wishes to send a message $M \in [1 : 2^{nR}]$ reliably to the receiver Y while keeping it secret from the eavesdropper Z



- A $(2^{nR}, n)$ secrecy code for the DM-WTC consists of:
 1. A message set $[1 : 2^{nR}]$
 2. A randomized encoder that generates a codeword $X^n(m)$, $m \in [1 : 2^{nR}]$, according to $p(x^n|m)$

3. A decoder that assigns a message $\hat{m}(y^n)$ or an error message e to each received sequence $y^n \in \mathcal{Y}^n$
- The message $M \sim \text{Unif}[1 : 2^{nR}]$
- The *information leakage rate* is defined as $R_l^{(n)} := (1/n)I(M; Z^n)$
- The probability of error, achievability, and the secrecy capacity C_S are defined as for the problem of secure communication over DMC
- *Theorem 3 [4]:* The secrecy capacity of the DM-WTC $(\mathcal{X}, p(y, z|x), \mathcal{Y} \times \mathcal{Z})$ is given by

$$C_S = \max_{p(u,x)} (I(U; Y) - I(U; Z))$$

for $|\mathcal{U}| \leq |\mathcal{X}|$

- Special cases:
 - The wiretap channel was first introduced by Wyner [5], who assumed that the channel to the eavesdropper is a physically degraded version of the channel to the receiver, i.e. $p(y, z|x) = p(y|x)p(z|y)$, Under this assumption,

$$\begin{aligned} I(U; Y) - I(U; Z) &= I(U; Y|Z) \\ &\leq I(X; Y|Z) \\ &= I(X; Y) - I(X; Z) \end{aligned}$$

Hence, the secrecy capacity in this case is

$$C_S = \max_{p(x)} (I(X; Y) - I(X; Z))$$

It can be shown that the secrecy capacity depends only on the marginal pmfs $p(y|x)$ and $p(z|x)$. Hence, the above result generalizes to stochastically degraded DM-WTC

- The above result holds if Y is more capable than Z . To show this consider

$$\begin{aligned} I(U; Y) - I(U; Z) &= I(X; Y) - I(X; Z) - (I(X; Y|U) - I(X; Z|U)) \\ &\leq I(X; Y) - I(X; Z), \end{aligned}$$

since the more capable condition implies that $I(X; Y|U) - I(X; Z|U) \geq 0$ for all $p(u, x)$

Examples

- *Binary symmetric wiretap channel* [6]: Consider the BS-WTC: $Y_i = X_i \oplus Z_{1i}$, and $Z_i = X_i \oplus Z_{2i}$, where $\{Z_{1i}\}$ and $\{Z_{2i}\}$ are independent $\text{Bern}(p_1)$ and $\text{Bern}(p_2)$ processes, respectively

The secrecy capacity for this channel is

$$C_S = \begin{cases} H(p_2) - H(p_1) & \text{for } p_2 \geq p_1, \\ 0 & \text{otherwise} \end{cases}$$

Proof: When $p_1 > p_2$, The eavesdropper can decode any message that the receiver can decode, thus $C_S = 0$

When $p_2 \geq p_1$, capacity can be achieved using binary-symmetric random codes

To prove the converse, let $X \sim \text{Bern}(p)$ and consider

$$I(X; Y) - I(X; Z) = H(p_2) - H(p_1) - (H(p * p_2) - H(p * p_1))$$

For $p < 1/2$, $p * \epsilon$ is monotonically increasing in ϵ . This implies that $H(p * p_2) - H(p * p_1) \geq 0$. Thus setting $p = 1/2$ optimizes the above expression

- *Gaussian wiretap channel* [7]: Consider an AWGN-WTC: $Y_i = X_i + Z_{1i}$ and $Z_i = X_i + Z_{2i}$, where $\{Z_{1i}\}$ and $\{Z_{2i}\}$ are $\text{WGN}(N_1)$ and $\text{WGN}(N_2)$ processes, respectively, and an input power constraint $\sum_{i=1}^n X_i^2(m) \leq nP$ is satisfied (surely) for each $m \in [1 : 2^{nR}]$

The secrecy capacity of this channel is

$$C_S = \begin{cases} C(P/N_1) - C(P/N_2) & \text{for } N_1 \leq N_2, \\ 0 & \text{otherwise} \end{cases}$$

Proof: Capacity is achieved using Gaussian random codes

To prove the converse, assume without loss of generality that the channel is physically degraded and $Z_2 = Z_1 + Z'_2$ where $Z'_2 \sim \mathcal{N}(0, N_2 - N_1)$. Consider

$$I(X; Y) - I(X; Z) = \frac{1}{2} \log \left(\frac{N_2}{N_1} \right) - (h(Z) - h(Y))$$

By the EPI,

$$\begin{aligned} h(Z) - h(Y) &= h(Y + Z'_2) - h(Y) \\ &\geq \frac{1}{2} \log(2^{2h(Z'_2)} + 2^{2h(Y)}) - h(Y) \\ &= \frac{1}{2} \log(2\pi e(N_2 - N_1) + 2^{h(Y)}) - h(Y) \end{aligned}$$

Now since $(1/2) \log(2\pi e(N_2 - N_1) + 2^\nu) - \nu$ is an increasing function in ν , and $h(Y) \leq (1/2) \log(2\pi e(P + N_1))$,

$$\begin{aligned} h(Z) - h(Y) &\geq \frac{1}{2} \log(2\pi e(N_2 - N_1) + 2\pi e(P + N_1)) - \frac{1}{2} \log(2\pi e(P + N_1)) \\ &= \frac{1}{2} \log \left(\frac{P + N_2}{P + N_1} \right) \end{aligned}$$

Hence,

$$C_S \leq \frac{1}{2} \log \left(\frac{N_2}{N_1} \right) - \frac{1}{2} \log \left(\frac{P + N_2}{P + N_1} \right) = C(P/N_1) - C(P/N_2)$$

- *Gaussian vector (MIMO) wiretap channel* [8]: Consider a Gaussian vector WTC:

$$\begin{aligned} \mathbf{Y}(i) &= G_1 \mathbf{X}(i) + \mathbf{Z}_1(i), \\ \mathbf{Z}(i) &= G_2 \mathbf{X}(i) + \mathbf{Z}_2(i) \end{aligned}$$

with $K_{Z_1} = K_{Z_2} = I$ and power constraint P

The secrecy capacity [8] is

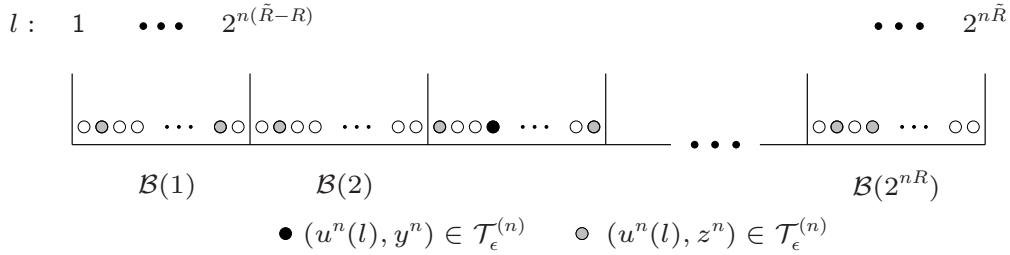
$$C_S = \max_{\text{tr}(K_X) \leq P} \log |I + G_1 K_X G_1^T| - \log |I + G_2 K_X G_2^T|$$

Addition of the spatial dimension allows the possibility of beamforming the signal away from eavesdropper

Proof of Achievability

-
- **Codebook generation:** Assume $C_S > 0$, and fix $p(u, x)$ that achieves it. Thus $I(U; Y) - I(U; Z) > 0$.
Randomly and independently generate $2^{n\tilde{R}}$ sequences $u^n(l)$, $l \in [1 : 2^{n\tilde{R}}]$, each according to $\prod_{i=1}^n p(u_i)$. Partition the set of indices $[1 : 2^{n\tilde{R}}]$ into 2^{nR} bins
 $\mathcal{B}(m) = [(m-1)2^{n(\tilde{R}-R)} + 1 : m2^{n(\tilde{R}-R)}]$
The chosen $u^n(l)$ codebook is revealed to the encoder, decoder, and eavesdropper
 - **Encoding:** To send message $m \in [1 : 2^{nR}]$, the encoder picks an index $l \in \mathcal{B}(m)$ uniformly at random. It then generates $X^n \sim \prod_{i=1}^n p_{X|U}(x_i|u_i(l))$ and transmits it. This randomization step aims to introduce more uncertainty about the message to the eavesdropper than to the intended receiver
 - **Decoding and analysis of the probability of error:** The decoder declares that \hat{l} is sent if it is the unique index such that $(u^n(\hat{l}), y^n) \in \mathcal{T}_\epsilon^{(n)}$ and declares that the message sent is the bin index \hat{m} of \hat{l}

By the LLN and the packing lemma, if $\tilde{R} < I(U; Y) - \delta(\epsilon)$, the probability of error $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$



- Analysis of the information leakage rate: For each bin $\mathcal{C}(m)$, the eavesdropper (on average) has $\doteq 2^{n(\tilde{R} - R - I(U;Z))}$ indices such that $(u^n(i), z^n) \in \mathcal{T}_\epsilon^{(n)}$. Thus if we take $\tilde{R} - R > I(U;Z)$, the eavesdropper would have roughly equal number of indices (in the exponent) in each bin, providing it with almost no information about the message sent.

For each message m , let $L(m)$ be the randomly selected index by the encoder.

Any codebook c induces a joint pmf on (M, L, U^n, Z^n) of the form

$$p(m, l, u^n, z^n | c) = 2^{-nR} 2^{-n(\tilde{R}-R)} p(u^n | l, c) \prod_{i=1}^n p_{Z|U}(z_i | u_i)$$

Now consider the eavesdropper message rate averaged over the randomly chosen codebook \mathcal{C}

$$\begin{aligned}
I(M; Z^n | \mathcal{C}) &= I(M, L; Z^n | \mathcal{C}) - I(L; Z^n | M, \mathcal{C}) \\
&= I(L; Z^n | \mathcal{C}) - H(L | M, \mathcal{C}) + H(L | Z^n, M, \mathcal{C}) \\
&= I(L; Z^n | \mathcal{C}) - n(\tilde{R} - R) + H(L | Z^n, M, \mathcal{C}) \\
&\leq I(U^n; Z^n | \mathcal{C}) - n(\tilde{R} - R) + H(L | Z^n, M, \mathcal{C}) \\
&= H(Z^n | \mathcal{C}) - \sum_{i=1}^n H(Z_i | U^n, Z^{i-1}, \mathcal{C}) - n(\tilde{R} - R) + H(L | Z^n, M, \mathcal{C}) \\
&\stackrel{(a)}{\leq} \sum_{i=1}^n H(Z_i | \mathcal{C}) - \sum_{i=1}^n H(Z_i | U_i, \mathcal{C}) - n(\tilde{R} - R) + H(L | Z^n, M, \mathcal{C}) \\
&\stackrel{(b)}{\leq} nH(Z) - nH(Z | U) - n(\tilde{R} - R) + H(L | Z^n, M, \mathcal{C}) \\
&\leq nI(U; Z) - n(\tilde{R} - R) + H(L | Z^n, M),
\end{aligned}$$

where (a) follows by convexity of the entropy function and the fact that $(U^n, Z^{i-1}, \mathcal{C}) \rightarrow (U_i, \mathcal{C}) \rightarrow Z_i$ form a Markov chain, (b) follows by the fact that $H(Z_i|\mathcal{C}) \leq H(Z_i) = H(Z)$ and $H(Z_i|U_i, \mathcal{C}) = \sum_{\mathcal{C}} p(\mathcal{C})p(u_i|\mathcal{C})H(Z|u_i, \mathcal{C}) = \sum_{\mathcal{C}} p(\mathcal{C})p(u_i|\mathcal{C})H(Z|u_i) = H(Z|U)$

- The equivocation term in the last step is bounded as follows

Lemma 1: If $R < I(U; Y) - I(U; Z) - 4\delta(\epsilon)$, then

$$\lim_{n \rightarrow \infty} H(L|Z^n, M)/n \leq \tilde{R} - R - I(U; Z) + \delta(\epsilon)$$

The proof of the lemma is in the Appendix

Substituting, we have shown that if $R < I(U; Y) - I(U; Z) - 4\delta(\epsilon)$, then

$$\lim_{n \rightarrow \infty} \frac{1}{n} I(M; Z^n | \mathcal{C}) \leq \delta(\epsilon)$$

- From the above, it follows that there must exist a sequence of codes with $P_e^{(n)} \rightarrow 0$ and $R_l^{(n)} \rightarrow 0$, which completes the proof of achievability

- Remark: Instead of sending a random X^n , we can randomly generate a subcodebook consisting of $2^{nR'}$ codewords $x^n(l, l')$ for each $u^n(l)$, reveal them to all parties, and randomly choose one of them for transmission. To achieve secrecy, we must have $R' > I(X; Z|U) + \delta(\epsilon)$ in addition to $\tilde{R} - R > I(U; Z)$. As we discuss below, this approach is useful for establishing lower bounds on the secrecy capacity of wiretap channels with more than one legitimate receiver

Proof of Converse

- Consider any sequence of $(2^{nR}, n)$ codes with $P_e^{(n)} \rightarrow 0$ and $R_l^{(n)} \rightarrow 0$ as $n \rightarrow \infty$. Then, by the assumption, $R_l^{(n)} \leq \epsilon_n$ and by Fano's inequality, $H(M|Y^n) \leq n\epsilon_n$, where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$. Thus, we have

$$\begin{aligned}
nR &\leq I(M; Y^n) + n\epsilon_n \\
&= I(M; Y^n) - I(M; Z^n) + nR_l^{(n)} + n\epsilon_n \\
&\leq \sum_{i=1}^n (I(M; Y_i | Y^{i-1}) - I(M; Z_i | Z_{i+1}^n)) + 2n\epsilon_n \\
&\stackrel{(a)}{=} \sum_{i=1}^n (I(M, Z_{i+1}^n; Y_i | Y^{i-1}) - I(M, Y^{i-1}; Z_i | Z_{i+1}^n)) + 2n\epsilon_n \\
&\stackrel{(b)}{=} \sum_{i=1}^n (I(M; Y_i | Y^{i-1}, Z_{i+1}^n) - I(M; Z_i | Y^{i-1}, Z_{i+1}^n)) + 2n\epsilon_n \\
&\stackrel{(c)}{=} \sum_{i=1}^n (I(U_i; Y_i | V_i) - I(U_i; Z_i | V_i)) + 2n\epsilon_n
\end{aligned}$$

$$\begin{aligned}
&\stackrel{(d)}{=} I(U; Y | V) - I(U; Z | V) + n\epsilon_n \\
&\leq \max_v (I(U; Y | V = v) - I(U; Z | V = v)) + n\epsilon_n \\
&\leq C_S + 2n\epsilon_n,
\end{aligned}$$

where (a) and (b) follow by the Csiszár sum identity, (c) follows by defining $V_i := (Y^{i-1}, Z_{i+1}^n)$ and $U_i := (M, V_i)$, (d) follows by introducing a time-sharing random variable Q and defining $U := (U_Q, Q)$, $V := (V_Q, Q)$, $Y := Y_Q$, and $Z := Z_Q$, and (e) follows since $U \rightarrow X \rightarrow (Y, Z)$ form a Markov chain given $\{V = v\}$. The bound on cardinality can be proved using the first method in Appendix C

Extensions

- A secret key between the sender and receiver can be used to further increase the secrecy capacity. If R_K is the rate of the secret key, then the secrecy capacity of a wiretap channel $p(y, z|x)$ is

$$C_S(R_K) = \max_{p(u,x)} \min\{I(U;Y) - I(U;Z) + R_K, I(U;Y)\}$$

Sometimes interaction between the sender and receiver can generate a shared key. Ahlswede and Cai [9] and Ardestanizadeh et al. [10] studied a secure feedback coding scheme to generate a shared key, which is optimal when the wiretap channel is physically degraded. We will soon see that even *nonsecure* interaction can provide a secret key

- The secrecy capacity for more than 2 receivers is not known. In [11], a lower bound on the secrecy capacity for a 2-receivers, 1-eavesdropper wiretap channel is established. We briefly discuss this result as it involves several ideas beyond wiretap channel coding

Consider a general 3-receiver DM-BC with sender X , two legitimate receivers Y_1, Y_2 and an eavesdropper Z . The sender wishes to send a message $M \in [1 : 2^{nR}]$ reliably to Y_1 and Y_2 while keeping it asymptotically secret from Z , i.e., $\lim_{n \rightarrow \infty} I(M; Z^n)/n = 0$

A straightforward extension of the wiretap result to 3-receivers yields the lower bound

$$C_S \geq \max_{p(u,x)} \min\{I(U;Y_1) - I(U;Z), I(U;Y_2) - I(U;Z)\}$$

Now, suppose Z is a degraded version of Y_1 , then from the wiretap result, $I(U;Y_1) - I(U;Y_3) \leq I(X;Y_1) - I(X;Z)$ for all $p(u,x)$. However, no such inequality holds in general for the second term. Using indirect decoding [12], we can replace U with X in the first term while keeping U in the second term.

This can increase the rate (see example in Lecture notes 5). To prove achievability of this rate, we randomly and independently generate sequences $u^n(l_0)$, $l_0 \in [1 : 2^{n\tilde{R}}]$, each generated according to $\prod_{i=1}^n p(u_i)$. Partition the set $[1 : 2^{n\tilde{R}}]$ into 2^{nR} bins $\mathcal{B}(m)$ $m \in [1 : 2^{nR}]$. For each $u^n(l_0)$, conditionally independently generate 2^{nR_1} sequences $x^n(l_0, l_1)$, $l_1 \in [1 : 2^{nR_1}]$, each according to $\prod_{i=1}^n p(x_i|u_i)$. To send a message $m \in [1 : 2^{nR}]$, choose an index pair (L_0, L_1) uniformly at random from $\mathcal{B}(m) \times [1 : 2^{nR_1}]$, and transmit $x^n(L_0, L_1)$. Receiver Y_2 decodes m directly through U and receiver Y_1 decodes m indirectly through X . It can be shown that the probability of error $\rightarrow 0$ as $n \rightarrow \infty$ if

$$\tilde{R} < I(U;Y_2) - \delta(\epsilon), \quad \tilde{R} + R_1 < I(X;Y_1) - \delta(\epsilon)$$

Further, it can be shown that M is kept asymptotically secret from the eavesdropper Z if

$$\tilde{R} - R > I(U; Z) + \delta(\epsilon), R_1 > I(X; Z|U) + \delta(\epsilon)$$

Eliminating \tilde{R} and R_1 using the Fourier-Motzkin procedure, we obtain the lower bound

$$C_S \geq \max_{p(u,x)} \min\{I(X; Y_1) - I(X; Z), I(U; Y_2) - I(U; Z)\}$$

This bound can be shown to be tight for the BEC example in Lecture notes 5 and is strictly larger than the straightforward extension of the Csiszár–Körner–Marton secrecy capacity result

The above bound can be improved via Marton coding and time-sharing to obtain the following lower bound:

Theorem 4:

$$C_S \geq \min\{I(U_1; Y_1|Q) - I(U_1; Z|Q), I(U_2; Y_2|Q) - I(U_2; Z|Q), \frac{1}{2}(I(U_1; Y_1|Q) + I(U_2; Y_2|Q) - 2I(U_0; Z|Q) - I(U_1; U_2|U_0))\}$$

for some $p(q, u_0)p(u_1|u_0)p(x, u_2|u_0, u_1) = p(q, u_0)p(u_2|u_0)p(x, u_1|u_0, u_2)$ such that $I(U_1, U_2; Z|U_0) \leq I(U_1; Z|U_0) + I(U_2; Z|U_0) - I(U_1; U_2|U_0)$. This bound was shown to be optimal for reversely degraded BC with an arbitrarily number of sub-channels and when both Y_1 and Y_2 are less noisy than Z [11]

- Broadcast channel with common and confidential messages: In [4], it is assumed that there is a common message M_0 that needs to be sent reliably to both the receiver Y and eavesdropper Z in addition to a confidential message M_1 that needs to be sent to Y and kept partially secret from Z

Formally, a $(2^{nR_0}, 2^{nR_1}, 2^{nR_l}, n)$ code for the DM-BC with common and confidential messages consists of: (i) two message sets $[1 : 2^{nR_0}]$ and $[1 : 2^{nR_1}]$; (ii) an encoder that randomly assigns a codeword $X^n(m_0, m_1)$ to each (m_0, m_1) according to $p(x^n|m_0, m_1)$; and (iii) two decoders; decoder Y assigns to each sequence y^n an estimate $(\hat{M}_{01}, \hat{M}_{11}) \in [1 : 2^{nR_0}] \times [1 : 2^{nR_1}]$ or an error message, and decoder Z assigns to each sequence z^n an estimate $\hat{M}_{02} \in [1 : 2^{nR_0}]$ or an error message. The message pair (M_0, M_1) are assumed to be uniformly distributed over the message sets. The probability of error is

$$P_e^{(n)} = P\{\hat{M}_{0j} \neq M_0 \text{ for } j = 1, 2 \text{ or } \hat{M}_1 \neq M_1\}$$

The information leakage rate at receiver Z is $I(M_1; Z^n)/n$

A secrecy rate tuple (R_0, R_1, R_l) is said to be achievable if there exists a sequence of codes such that $P_e^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ and $\limsup_{n \rightarrow \infty} \frac{1}{n} I(M_1; Z^n) \leq R_l$. The *secrecy capacity region* is the closure of the set of achievable rate tuples (R_0, R_1, R_l)

Theorem 5 [4]: The secrecy capacity region of the 2-receiver DM-BC with common and confidential messages is the set of rate tuples (R_0, R_1, R_l) such that

$$\begin{aligned} R_0 &\leq I(U; Z), \\ R_1 &\leq I(V; Y|U), \\ R_0 + R_1 &\leq I(V; Y), \\ R_l &\geq \max\{0, R_1 - [I(V; Y|U) - I(V; Z|U)]^+\} \end{aligned}$$

for some $p(u, v, x) = p(u)p(v|u)p(x|v)$, where $[a]^+ := \max\{a, 0\}$

In [11], inner bounds on the secrecy capacity regions for 2-receiver and 1-eavesdropper and 1-receiver and 2-eavesdroppers are given. The secrecy capacity regions for these scenarios are known only for some special cases

- The work on wiretap channel has been extended to other multiple user channels (see survey paper [13]):
 - BC channels: In [14] inner and outer bounds for the DM-BC with independent confidential messages is established. Broadcast fading channels and product channels are considered in [15]
 - Relay channels: In [16] the DM-RC with eavesdropper at the relay is studied, and in [17], results for DM-RC with eavesdropper at the receiver is studied

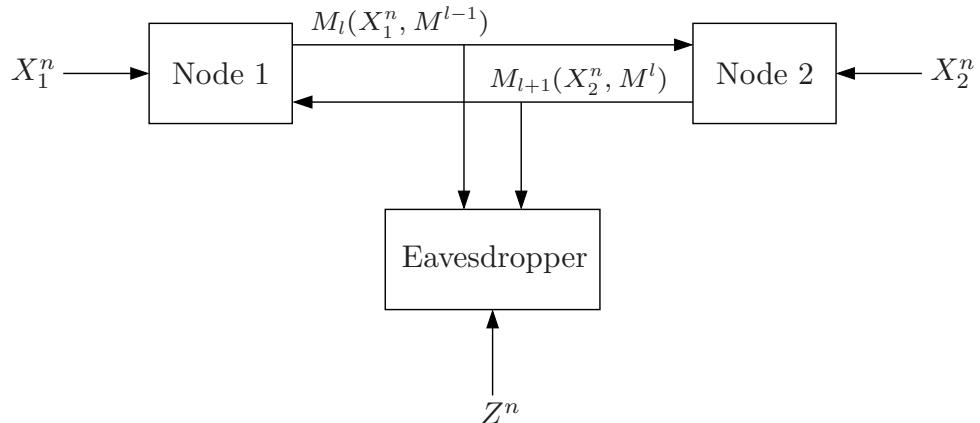
- MAC: In [18], it is assumed that both transmitters are broadcasting to a common receiver. Each transmitter can eavesdrop on the other transmitter's signal. Transmission of independent confidential messages to the common receiver is considered. In [19], the Gaussian MAC in which an eavesdropper is treated as another MAC receiver is considered
- Interference Channels: Inner and outer bounds for the interference channel with confidential messages in which each message is to be kept secret from the unintended receiver is considered in [14]. A model of the interference channel with secrecy constraint in which a common message is available at both encoders and a confidential message is available at encoder 2 only, which is to be kept secret from receiver 1 is studied in [20]
- Compound channels and channels with state/side information: Results for the compound wiretap channel are reported in [21]. Achievable rate-information leakage regions for channels with state or side information available at encoder or decoder are studied in [22] and [23]
- Source coding: In [24, 25] the source coding problem when an eavesdropper observes the output of the encoder, but does not observe the side information (or the key) is considered. The secrecy measure in this case is the equivocation the eavesdropper has about the source without knowing the key. A tradeoff exists between the key rate and equivocation at the eavesdropper

Secret Key Agreement: The Source Model

- Motivation: If the channel to the eavesdropper is less noisy than the channel to the receiver, then $C_S = 0$. Thus no secret communication can take place at a positive rate without a secret key shared between the sender and receiver. It turned out, however, that it is possible to agree on a secret key over a public channel if the sender and receiver have access to correlated random variables work on secret key agreement
- We discuss the secret key agreement under the source model in some detail. We then briefly discuss the problem under the channel model

Problem Setup

- Consider a system with two nodes, a single eavesdropper, and 3-DMS $(\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Z}, p(x_1, x_2, z))$. Node 1 observes a DMS X_1 , node 2 observes a DMS X_2 , and the eavesdropper observes a DMS Z . The nodes communicate over a public, noiseless broadcast channel with the goal of agreeing on a secret key that the eavesdropper is ignorant of. What is the maximum achievable secret key rate?



- We assume without loss of generality that the nodes communicate in a round robin fashion over q rounds, where q is even and may depend on n . Thus Node 1 transmits during rounds $l = 1, 3, \dots, q - 1$, and Node 2 transmits during the rest of the rounds
- A $(2^{nR_1}, \dots, 2^{nR_q}, n)$ code for the secret key agreement problem consists of:
 1. Two randomized encoders, one for each node. In odd rounds $l = 1, 3, \dots, q - 1$, encoder 1 generates an index $M_l \in [1 : 2^{nR_l}]$ according to $p(m_l | x_1^n, m^{l-1})$, i.e., a random assignment given its source vector and all previously transmitted indices. Similarly, in even rounds $l = 2, 4, \dots, q$, encoder 2, generates an index $M_l \in [1 : 2^{R_l}]$ according to $p(m_l | x_2^n, m^{l-1})$
 2. Two decoders, one for each node. Decoder $j = 1, 2$ generates a key $K_j \in \mathbb{Z}^+$ according to $p(k_j | m^q, x_l^n)$, i.e., a random assignment given its source sequence and all received sequence of indices
- The probability of error for the code is defined as

$$P_e^{(n)} = \mathbb{P}\{K_1 \neq K_2\}$$

- The *key leakage rate* is defined as $R_l^{(n)} := (1/n) \max_{j \in [1:2]} I(K_j; Z^n, M^q)$

- A *secret key rate* R is achievable if there exists a sequence of $(2^{nR_1}, 2^{nR_2}, \dots, 2^{nR_q}, n)$ codes such that $P_e^{(n)} \rightarrow 0$, $R_l^{(n)} \rightarrow 0$ as $n \rightarrow \infty$, and
- $$\liminf_{n \rightarrow \infty} \frac{1}{n} H(K_j) \geq R \text{ for } j \in [1 : 2]$$
- The *secret key capacity* $C_K(X_1; X_2 || Z)$ (or in short when there is no ambiguity C_K) is the supremum of all achievable rates R

We denote the secret key capacity with deterministic encoding and key generation as $C_K^{(d)}$

Secret Key Capacity from One-Way Communication

- We consider the case of one-way communication, where the public communications is either from node 1 to node 2 or visa versa, that is, $M^q = (M_1, 0)$ or $(0, M_2)$, and denote the one-way secret key capacity by C_{K-1}
- Clearly $C_{K-1} \leq C_K$
- *Theorem 6 [26]:* The one-way secret key capacity for sources (X_1, X_2, Z) is

$$C_{K-1}(X_1; X_2 || Z) = \max \left\{ \begin{aligned} & \max_{p(v|x_1)p(u|v)} (I(V; X_2 | U) - I(V; Z | U)), \\ & \max_{p(v|x_2)p(u|v)} (I(V; X_1 | U) - I(V; Z | U)) \end{aligned} \right\},$$

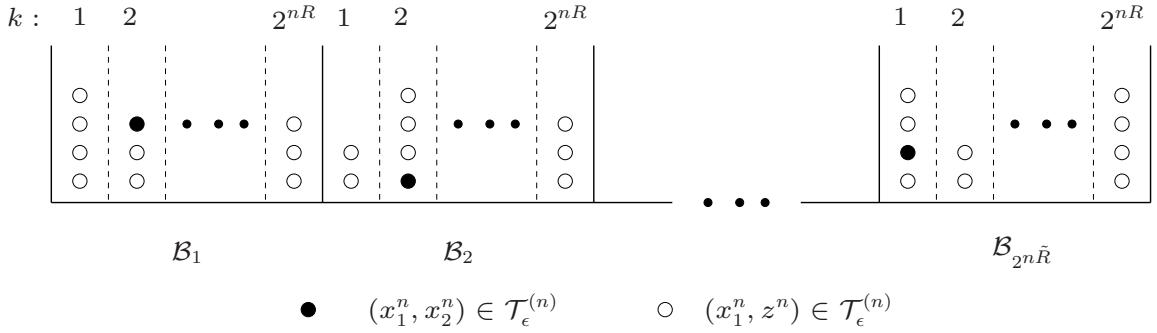
- Notation:
 - When there is no confusion, we use C_{K-1}
 - $C_{K-1}(X_1; X_2^{(s)} || Z) := \max_{p(v|x_1)p(u|v)} (I(V; X_2 | U) - I(V; Z | U))$, where (s) stands for “silent”
 - Similarly, $C_{K-1}(X_1^{(s)}; X_2 || Z) := \max_{p(v|x_2)p(u|v)} (I(V; X_1 | U) - I(V; Z | U))$

Proof of Achievability

- We first prove achievability for the special case of $U = \emptyset$, $V = X_1$ (or $V = X_2$) and then generalize the result. Assume that $I(X_1; X_2) - I(X_1; Z) = H(X_1|Z) - H(X_1|X_2) > 0$. The case of $I(X_2; X_1) - I(X_2; Z) > 0$ can be proved similarly
- Codebook generation: Randomly and independently partition the set of sequences \mathcal{X}_1^n into $2^{n\tilde{R}}$ bins \mathcal{B}_m , $m \in [1 : 2^{n\tilde{R}}]$. Randomly and independently partition the sequences in each non-empty bin \mathcal{B}_m into 2^{nR} sub-bins, $\mathcal{B}_m(k)$, $k \in [1 : 2^{nR}]$

The binning assignments are revealed to all parties (including the eavesdropper)

- Encoding: Given a sequence $x_1^n \in \mathcal{T}_\epsilon^{(n)}(X_1)$, node 1 finds the index pair (m, k) such that $x_1^n \in \mathcal{B}_m(k)$. If $x_1^n \notin \mathcal{T}_\epsilon^{(n)}(X_1)$, it generates an index pair (m, k) uniformly at random. It then sends out the index m to both node 2 and the eavesdropper



- Decoding and key generation: Node 1 sets its key $K_1 = k$. Upon receiving m , node 2 finds the unique sequence $\hat{x}_1^n \in \mathcal{B}_m$ that is jointly typical with its sequence x_2^n . If such a unique sequence exists, then it sets $K_2 = \hat{k}$ such that $\hat{x}_1^n \in \mathcal{B}_m(\hat{k})$. If there is no such sequence or there is more than one sequence, it sets K_2 to a randomly generated sub-bin index

- Analysis of the probability of error: We analyze the average probability that $K_1 \neq K_2$ averaged over bin assignments. Without loss of generality assume that $M = 1$. Define the following events:

$$\mathcal{E}_1 := \{(X_1^n, X_2^n) \notin \mathcal{T}_\epsilon^{(n)}\},$$

$$\mathcal{E}_2 := \{(\tilde{x}_1^n, X_2^n) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{x}_1^n \neq X_1^n, \tilde{x}_1^n \in \mathcal{B}_1\}$$

The average probability of error

$$P(\mathcal{E}) = P(\mathcal{E}|M=1) \leq P(\mathcal{E}_1) + P(\mathcal{E}_2|X_1^n \in \mathcal{B}_1)$$

By the LLN, $P(\mathcal{E}_1) \rightarrow 0$ as $n \rightarrow \infty$

By the Slepian–Wolf theorem, if $\tilde{R} > H(X_1|X_2) + \delta(\epsilon)$, $P(\mathcal{E}_2|X_1^n \in \mathcal{B}_1) \rightarrow 0$ as $n \rightarrow \infty$

Thus $P(\mathcal{E}) \rightarrow 0$ as $n \rightarrow \infty$

- Analysis of the key rate: We first establish the following bound on key rate

Lemma 2: If $R < H(X_1) - 4\delta(\epsilon)$, then $\lim_{n \rightarrow \infty} H(K_1|\mathcal{C})/n \geq R - \delta(\epsilon)$

The proof of this lemma is in the Appendix

Next we show that $H(K_2|\mathcal{C})$ is close to $H(K_1|\mathcal{C})$. By Fano's inequality,

$$H(K_2|\mathcal{C}) = H(K_1|\mathcal{C}) + H(K_2|K_1, \mathcal{C}) - H(K_1|K_2, \mathcal{C}) \leq H(K_1|\mathcal{C}) + 1 + nR P(\mathcal{E}),$$

$$H(K_2|\mathcal{C}) \geq H(K_1|\mathcal{C}) - H(K_1|K_2, \mathcal{C}) \geq H(K_1|\mathcal{C}) - 1 - nR P(\mathcal{E})$$

Thus, if $\tilde{R} > H(X_1|X_2) + \delta(\epsilon)$, $(1/n)(H(K_2|\mathcal{C}) - H(K_1|\mathcal{C})) \rightarrow 0$ as $n \rightarrow \infty$

- Analysis of key leakage rate: Consider the eavesdropper key rate averaged over \mathcal{C} . By symmetry, we only need to consider the K_1 term

$$\begin{aligned} I(K_1; Z^n, M|\mathcal{C}) &= I(K_1, X_1^n; Z^n, M|\mathcal{C}) - I(X_1^n; Z^n, M|K_1, \mathcal{C}) \\ &= I(X_1^n; Z^n, M|\mathcal{C}) - H(X_1^n|K_1, \mathcal{C}) + H(X_1^n|Z^n, M, K_1, \mathcal{C}) \\ &= H(X_1^n) - H(X_1^n|Z^n, M, \mathcal{C}) - H(X_1^n|K_1, \mathcal{C}) + H(X_1^n|Z^n, M, K_1, \mathcal{C}) \end{aligned}$$

Now,

$$\begin{aligned} H(X_1^n|Z^n, M, \mathcal{C}) &= H(X_1^n|Z^n) + H(M|Z^n, X_1^n, \mathcal{C}) - H(M|Z^n, \mathcal{C}) \\ &= H(X_1^n|Z^n) - H(M|Z^n, \mathcal{C}) \\ &\geq H(X_1^n|Z^n) - H(M) = n(H(X_1|Z) - \tilde{R}), \text{ and} \\ H(X_1^n|K_1, \mathcal{C}) &= H(X_1^n) + H(K_1|X_1^n, \mathcal{C}) - H(K_1|\mathcal{C}) \\ &= H(X_1^n) - H(K_1|\mathcal{C}) \geq n(H(X_1) - R) \end{aligned}$$

Substituting, we have

$$I(K_1; Z^n, M|\mathcal{C}) \leq n(\tilde{R} + R - H(X_1|Z)) + H(X_1^n|Z^n, M, K_1, \mathcal{C})$$

We bound the remaining term in the following

Lemma 3: if $R < H(X_1|Z) - H(X_1|X_2) - 2\delta(\epsilon)$, then

$$\lim_{n \rightarrow \infty} H(X_1^n|Z^n, M, K_1, \mathcal{C})/n \leq H(X_1|Z) - \tilde{R} - R + \delta(\epsilon)$$

Substituting in the bound on $I(K_1; Z^n, M|\mathcal{C})$, and taking limits shows that if $R < H(X_1|Z) - H(X_1|X_2) - 2\delta(\epsilon)$, then $(1/n)I(K_1; Z^n, M|\mathcal{C}) \leq \delta(\epsilon)$ as $n \rightarrow \infty$

- To summarize, we have shown that if $R < H(X_1|Z) - H(X_1|X_2) - 2\delta(\epsilon)$, then as $n \rightarrow \infty$
 - $H(K_j|\mathcal{C}) \geq R - \delta(\epsilon)$ for $j = 1, 2$,
 - $P(\mathcal{E}_1) \rightarrow 0$, and
 - $(1/n)I(K_j; Z^n, M|\mathcal{C}) \leq \delta(\epsilon)$ for $j = 1, 2$

Therefore, there exists a sequence of codes such that $P_e^{(n)} \rightarrow 0$, $\liminf_{n \rightarrow \infty} H(K_j) \geq R$, and $R_l^{(n)} \leq \delta(\epsilon)$

- To complete the proof of achievability, we modify code generation as follows. Node 1 generate (U^n, V^n) according to $\prod_{i=1}^n p(v_i|x_{1i})p(u_i|v_i)$, By the LLN, $P\{(U^n, V^n, X_1^n, X_2^n, Z^n) \notin \mathcal{T}_\epsilon^{(n)}\} \rightarrow 0$ as $n \rightarrow \infty$. Node 1 then sends U^n over the public channel. Following the previous proof with V (instead of X_1) at node 1, (U, X_2) at node 2, and (U, Z) at the eavesdropper proves the achievability of $R < I(V; X_2|U) - I(V; Z|U)$

Proof of Converse

- Restricted to one-way communication, the achievability bound is tight [26]. To prove this, consider

$$\begin{aligned}
 nR &\leq H(K_1) \\
 &\stackrel{(a)}{=} H(K_1) - H(K_1 | X_2^n, M) + n\epsilon_n \\
 &\leq I(K_1; X_2^n, M) + n\epsilon_n \\
 &\stackrel{(b)}{\leq} I(K_1; X_2^n, M) - I(K_1; Z^n, M) + n\epsilon_n \\
 &= I(K_1; X_2^n | M) - I(K_1; Z^n | M) + n\epsilon_n \\
 &\stackrel{(c)}{=} \sum_{i=1}^n (I(K_1; X_{2i} | M, X_2^{i-1}, Z_{i+1}^n) - I(K_1; Z_i | M, X_2^{i-1}, Z_{i+1}^n)) + n\epsilon_n \\
 &\stackrel{(d)}{=} \sum_{i=1}^n (I(V_i; X_{2i} | U_i) - I(V_i; Z_i | U_i)) + n\epsilon_n \\
 &\stackrel{(e)}{=} n(I(V; X_2 | U) - I(V; Z | U)) + n\epsilon_n
 \end{aligned}$$

where (a) follows by Fano's inequality, (b) follows from the eavesdropper key rate condition, (c) follows from the converse proof for the wiretap secrecy capacity theorem, (d) follows by defining $U_i = (M, X_2^{i-1}, Z_{i+1}^n)$ and $V_i = (K_1, U_i)$, and (e) follows by introducing a time-sharing random variable Q , defining $U = (U_Q, Q)$, $V = (U, K_1)$, and the fact that $X_{2Q} = X_2$, $Z_Q = Z$. Finally, observing that $p(u, v | x_1, x_2, z) = p(u, v | x_1) = p(v | x_1)p(u | v)$ completes the proof

- One-way key generation with rate constraint: Consider one-way communication with only node 1 transmitting and a rate constraint R on the public discussion link. The one-way key capacity [27] is

$$C_{K-1} = \max_{p(v|x_1)p(u|v)} (I(V; X_2 | U) - I(V; Z | U))$$

subject to $R \geq I(V; X_1) - I(V; X_2)$

Secret Key Agreement from Interactive Communication

- The secret key capacity for general interactive communication is not known. We establish lower and upper bounds
- *Theorem 7 [28]:* The following is a lower bound on the secret key capacity for the sources (X_1, X_2, Z)

$$\begin{aligned} C_K &\geq \sum_{l=1}^q (I(U_l; X_{j_l}|U^{l-1}) - I(U_l; Z|U^{l-1})) \\ &= H(U^q|Z) - \sum_{l=1}^q H(U_l|U^{l-1}, X_{j_l}) \end{aligned}$$

for $q \geq 1$, where $j_l = 1$ if l is even and 2 if l is odd, and (U_1, U_2, \dots, U_q) have finite alphabets and conditional pmf of the form

$$p(u_1, u_2, \dots, u_q | x_1, x_2, z) = \prod_{l=1}^q p(u_l | u^{l-1}, x_{j_l})$$

- Outline of achievability:
 - Fix a joint pmf that satisfies the condition of the theorem

- Codebook generation: For each $l \in [1 : q]$, randomly and independently assign each sequence in \mathcal{U}_l^n to one of $2^{n\tilde{R}_l}$ bins $\mathcal{B}_l(m_l)$, $m_l \in [1 : 2^{n\tilde{R}_l}]$. For each message sequence $(m_1, \dots, m_q) \in \prod_{l=1}^q [1 : 2^{n\tilde{R}_l}]$, randomly and independently assign each sequence $(u_1^n, u_2^n, \dots, u_q^n) \in \prod_{l=1}^q \mathcal{B}_l(m_l)$ to one of 2^{nR} sub product bins $\mathcal{B}_{m_1, \dots, m_q}(k)$, $k \in [1 : 2^{nR}]$
- Encoding: Assume l is odd. A similar procedure applies for even rounds with nodes 1 and 2 interchanged. Assuming $(\hat{u}_2^n, \hat{u}_4^n, \dots, \hat{u}_{l-1}^n)$ to be node 1's estimate of the sequences generated by node 2, node 1 generates a sequence u_l^n according to $\prod_{i=1}^n p(u_{li} | u_{1i}, \hat{u}_{2i}, u_{3i}, \dots, \hat{u}_{l-1,i}, x_{1i})$. Node 1 sends the index m_l such that $u_l^n \in \mathcal{B}_l(m_l)$ to node 2
- Decoding: Again assume that l is odd. Assuming $(u_1, u_2^n, \dots, u_{l-1}^n, x_1^n) \in \mathcal{T}_\epsilon^{(n)}$ and that node 1 knows these sequences, then upon receiving m_l , it finds the unique sequence $\hat{u}_l^n \in \mathcal{B}_l(m_l)$ such that $(u_1^n, u_2^n, \dots, \hat{u}_l^n, x_1^n) \in \mathcal{T}_\epsilon^{(n)}$. Otherwise, it picks a random sequence from \mathcal{U}_l^n
- Key generation: At the end of round q , if all sequences are known to node 1, it finds the sub product bin index \hat{k} to which the set of sequences belongs and sets $K_1 = \hat{k}$. Otherwise it sets K_1 to a random index in $[1 : 2^{nR}]$

- Analysis of the probability of error: We bound the probability that $K_1 \neq K_2$ averaged over bin assignments. Assume without loss of generality that $M_1 = M_2 = \dots = M_q = 1$. Define the following events:

For $l \in [1 : q]$,

$$\mathcal{E}_{0l} := \{(U_1^n, U_2^n, \dots, U_l^n, X_1^n, X_2^n) \notin \mathcal{T}_\epsilon^{(n)}\}$$

$$\mathcal{E}_{1l} := \{\tilde{u}_l^n \in \mathcal{B}_l(1) \cap \mathcal{T}_\epsilon^{(n)}(U^{l-1}, X_{j_l}) \text{ for some } \tilde{u}_l^n \neq U_l^n\}$$

Then, the probability of error

$$P(\mathcal{E} | U_l^n \in \mathcal{B}_l(1), l \in [1 : q]) \leq \sum_{l=1}^q P(\mathcal{E}_{0l} \cap \mathcal{E}_{0,l-1}^c) + \sum_{l=1}^q P(\mathcal{E}_{1l} | U_l^n \in \mathcal{B}_l(1))$$

By the LLN, each term in the first sum $\rightarrow 0$ as $n \rightarrow \infty$

If $\tilde{R}_l > H(U_l | U^{l-1}, X_{j_l}) + \delta(\epsilon)$, the l th term in the second sum $\rightarrow 0$ as $n \rightarrow \infty$

- Analysis of the nodes key rates and the eavesdropper's key leakage rate follow the same steps as for the one-way case. If $\tilde{R}_l > H(U_l | U^{l-1}, X_{j_l}) + \delta(\epsilon)$ and $R + \sum_{l=1}^q \tilde{R}_l < H(U^q | Z)$, then $H(K_1 | \mathcal{C}), H(K_2 | \mathcal{C}) \geq n(R - \epsilon_n)$ and $(1/n)I(K_1; Z^n, M^q | \mathcal{C}) \rightarrow 0$ as $n \rightarrow \infty$

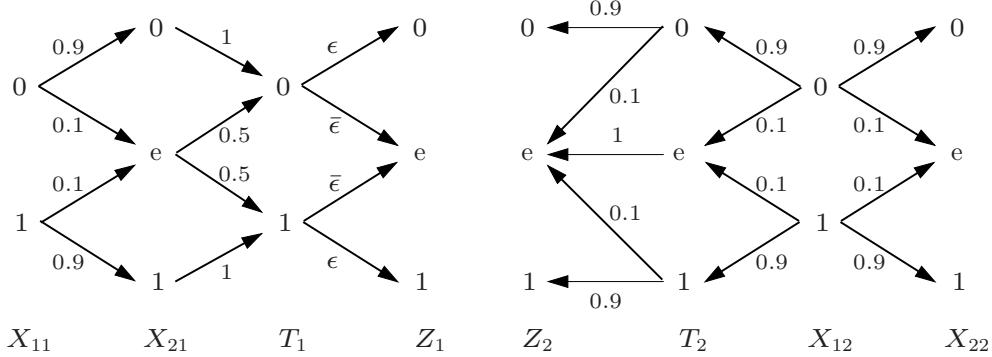
This completes the proof of achievability

- Remark: As in the one-way communication case, the key rate may improve by first exchanging U_1, U_2, \dots, U_{p-1} for some $p < q$ and then conditionally double binning U_p, U_{p-1}, \dots, U_q to generate the key. This gives the lower bound

$$C_K \geq \sum_{l=p}^q (I(U_l; X_{j_l} | U^{l-1}) - I(U_l; Z | U^{l-1}))$$

- It is not difficult to see that the above lower bound is at least as large as the one-way key capacity. To show that it can be strictly larger, consider the following example

Example [28]: Let $X_1 = (X_{11}, X_{12})$, where X_{11} and X_{12} are $\text{Bern}(1/2)$ random variables. The joint conditional pmf for $X_2 = (X_{21}, X_{22})$ and $Z = (Z_1, Z_2)$ is defined in the figure below



As will be seen shortly, an upper bound on the key rate is given by $I(X_1; X_2|Z) = I(X_{11}; X_{21}|Z_1) + I(X_{12}; X_{22}|Z_2)$. Note that this is achievable using the interactive communication achievability bound by setting $U_1 = X_{11}$ and $U_2 = X_{21}$. This, however, is larger than the one-way secrecy key rate C_{K-1} .

To show this, first note that the one-way rate from X_1 to X_2 depends only on the marginals $p(x_1, x_2)$ and $p(x_1, z)$. From the figure, $(X_{11}, X_{12}, X_{21}, X_{22})$ has the same joint pmf as $(X_{11}, X_{12}, X_{21}, T_2)$

Further, $(X_{11}, X_{12}) \rightarrow (X_{21}, T_2) \rightarrow (Z_1, Z_2)$ form a Markov chain. This gives

$$\begin{aligned} C_{K-1}(X_1; X_2^{(s)} || Z) &= C_{K-1}(X_1; (X_{21}, T_2)^{(s)} || Z) \\ &\stackrel{(a)}{=} I(X_1; X_{21}, T_2 | Z) \\ &= I(X_{11}; X_{21} | Z_1) + I(X_{12}; T_2 | Z_2), \end{aligned}$$

where (a) follows from the bound

$$C_{K-1}(X_1; (X_{21}, T_2)^{(s)} || Z) \geq I(X_1; X_{21}, T_2) - I(X_1; Z) = I(X_1; X_{21}, T_2 | Z).$$

But since the key capacity for $(X_{11}, X_{12}) \rightarrow (X_{21}, T_2) \rightarrow (Z_1, Z_2)$ is upper bounded by $I(X_1; X_{21}, T_2 | Z)$, we have

$C_{K-1}(X_1; (X_{21}, T_2)^{(s)} || Z) = I(X_1; X_{21}, T_2 | Z)$. This key rate is less than the upper bound for the original system since

$$\begin{aligned} I(X_{12}; T_2 | Z_2) &= I(X_{12}; T_2) - I(X_{12}; Z_2) \\ &= I(X_{12}; T_2) - I(X_{22}; Z_2)/0.9 \\ &< I(X_{12}; T_2) - I(X_{22}; Z_2) \\ &= I(X_{12}; X_{22}) - I(X_{22}; Z_2) = I(X_{12}; X_{22} | Z_2) \end{aligned}$$

- Since X_{11} has a uniform pmf, $p((x_{11}, x_{12}), (x_{21}, x_{22})) = p((t_1, x_{12}), (x_{21}, x_{22}))$. A similar argument shows that $C_{K-1}(X_1^{(s)}; X_2 || Z) < I(X_1; X_2 | Z)$, since $I(X_{11}; Z_1) < I(X_{21}; Z_1)$

Upper Bound on 2-Node Secret Key Capacity

- *Theorem 8* [29]: The following is an upper bound on the 2-node secret key capacity for the source (X_1, X_2, Z)

$$C_K \leq \min_{p(\bar{Z}|z)} I(X_1; X_2 | \bar{Z}),$$

where $(X_1, X_2) \rightarrow Z \rightarrow \bar{Z}$ form a Markov chain

- The above bound is tight If $X_1 \rightarrow X_2 \rightarrow Z$ or $X_2 \rightarrow X_1 \rightarrow Z$. This follows immediately from the achievability bound in one way key rate and Markovity

- Proof:

- We first consider the case where the encoding and key generation functions are *deterministic* and establish an upper bound on $C_K^{(d)}$

Given a sequence of deterministic codes with $P_e^{(n)} \rightarrow 0$ and

$(1/n) \max_{j \in [1:2]} I(K_j; Z^n, M^q) \rightarrow 0$, we establish an upper bound on the key rate R

By definition, we require bounds on both $H(K_1)/n$ and $H(K_2)/n$. However, using Fano's inequality it suffices to provide a bound only on $H(K_1)/n$. First, we show that $H(K_1) \leq I(X_1^n; X_2^n | M^q, Z^n) + n\epsilon_n$

The expression $I(X_1^n; X_2^n | M^q, Z^n)$ is then reduced to a single letter form using the conditions for interactive communications [6]

$H(K_1) = I(K_1; M^q, Z^n) + H(K_1 | M^q, Z^n)$, where $I(K_1; M^q, Z^n) \leq n\epsilon_n$ by the secrecy condition and $H(K_1 | M^q, Z^n)$ can be upper bounded as follows

$$\begin{aligned} H(K_1 | M^q, Z^n) &= H(K_1, X_1^n | M^q, Z^n) - H(X_1^n | M^q, K_1, Z^n) \\ &= H(X_1^n | M^q, Z^n) + H(K_1 | X_1^n, M^q, Z^n) - H(X_1^n | M^q, K_1, Z^n) \\ &\stackrel{(a)}{\leq} H(X_1^n | M^q, Z^n) - H(X_1^n | M^q, K_1, X_2^n, Z^n) \\ &= H(X_1^n | M^q, Z^n) - H(X_1^n, K_1 | M^q, X_2^n, Z^n) + H(K_1 | M^q, X_2^n, Z^n) \\ &\stackrel{(b)}{=} H(X_1^n | M^q, Z^n) - H(X_1^n | M^q, X_2^n, Z^n) + H(K_1 | M^q, X_2^n, Z^n) \\ &\stackrel{(c)}{\leq} I(X_1^n; X_2^n | M^q, Z^n) + H(K_1 | K_2), \end{aligned}$$

where (a) and (b) follow from $H(K_1 | M^q, X_1) = 0$ and (c) follows from the inequality $H(K_1 | M^q, X_2, Z) = H(K_1 | M^q, K_2, X_2, Z) \leq H(K_1 | K_2)$. By the condition that $P\{K_1 \neq K_2\} \leq \epsilon_n$ and Fano's inequality, we have

$$H(K_1 | K_2) \leq n\epsilon_n$$

Next assume without loss of generality that q is odd. Then,
 $H(M_l|X_1^n, M^{l-1}) = 0$ if l is odd and $H(M_l|X_2^n, M^{l-1}) = 0$ if l is even

$$\begin{aligned} I(X_1^n; X_2^n | M^q, Z^n) &= H(X_2^n | M^q, Z^n) - H(X_2^n | M^q, X_1^n, Z^n) \\ &= H(X_2^n | M^q, Z^n) - H(X_2^n | M^{q-1}, X_1^n, Z^n) \\ &\leq H(X_2^n | M^{q-1}, Z^n) - H(X_2^n | M^{q-1}, X_1^n, Z^n) \\ &= I(X_1^n; X_2^n | Z^n, M^{q-1}) \end{aligned}$$

Using the same procedure, we expand $I(X_1^n; X_2^n | M^{q-1}, Z^n)$ in the other direction to obtain

$$\begin{aligned} I(X_1^n; X_2^n | M^{q-1}, Z^n) &= H(X_1^n | M^{q-1}, Z^n) - H(X_1^n | M^q, X_2^n, Z^n) \\ &\leq I(X_1^n; X_2^n | M^{q-2}, Z^n) \end{aligned}$$

Repeating the procedure q times gives $I(X_1^n; X_2^n | Z^n, M^q) \leq I(X_1^n; X_2^n | Z^n)$. Using the fact that the sources are i.i.d. yields the upper bound

$$C_K^{(d)} \leq I(X_1; X_2 | Z)$$

- We can readily improve the bound by allowing the eavesdropper to pass Z through an arbitrary channel $p(\bar{z}|z)$ to generate a new random variable \bar{Z}

However, any secrecy protocol for the original system with (X_1, X_2, Z) is also a secrecy protocol for (X_1, X_2, \bar{Z}) , since

$$\begin{aligned} I(K_1; \bar{Z}, M^q) &= H(K_1) - H(K_1 | \bar{Z}, M^q) \\ &\leq H(K_1) - H(K_1 | \bar{Z}, Z, M^q) \\ &= I(K_1; M^q, Z) \end{aligned}$$

This gives the bound

$$C_K^{(d)}(X_1; X_2 | | Z) \leq C_K^{(d)}(X_1; X_2 | | \bar{Z}) \leq I(X_1; X_2 | \bar{Z})$$

Since this holds for any \bar{Z} generated through an arbitrary channel, taking the infimum over $p(\bar{z}|z)$ gives the desired bound

- Clearly the improved bound is at least as tight as $I(X_1; X_2 | Z)$. We show that it is can be strictly tighter

Example: [29] Let $X_1, X_2, Z \in \{0, 1, 2, 3\}$ with the following joint distribution

$$\begin{aligned} p_{X_1, X_2, Z}(0, 0, 0) &= p_{X_1, X_2, Z}(0, 1, 1) = p_{X_1, X_2, Z}(1, 0, 1) = p_{X_1, X_2, Z}(1, 1, 0) = \frac{1}{8} \\ p_{X_1, X_2, Z}(2, 2, 2) &= p_{X_1, X_2, Z}(3, 3, 3) = \frac{1}{4} \end{aligned}$$

Then, $I(X_1; X_2|Z) = 1/2$. Define \bar{Z} using the channel

$$\begin{aligned} p_{\bar{Z}|Z}(0|0) &= p_{\bar{Z}|Z}(1|0) = p_{\bar{Z}|Z}(0|1) = p_{\bar{Z}|Z}(1|1) = \frac{1}{2} \\ p_{\bar{Z}|Z}(2|2) &= p_{\bar{Z}|Z}(3|3) = 1 \end{aligned}$$

Then, $I(X_1; X_2|\bar{Z}) = 0$, which shows that the improved bound is strictly tighter

- The case with randomized encoding and key generation can be dealt with as follows. Note that randomization is equivalent to having random variables W_1 at node 1 and W_2 at node 2 that are independent of each other and of (X_1^n, X_2^n, Z^n) and performing the encoding and key generation using deterministic functions of the source sequence, messages, and the random variable at each node

Considering this equivalence, we can show that the upper bound on C_K holds with randomization as follows

$$\begin{aligned} C_K(X_1; X_2||Z) &= \sup_{p(w_1)p(w_2)} C_K^{(d)}((X_1, W_1); (X_2, W_2)||Z) \\ &\leq \sup_{p(w_1)p(w_2)} I(X_1, W_1; X_2, W_2|\bar{Z}) \\ &= \sup_{p(w_1)p(w_2)} (I(X_1, W_1; W_2|\bar{Z}) + I(X_1, W_1; X_2|\bar{Z}, W_2)) \\ &= \sup_{p(w_1)p(w_2)} I(X_1, W_1; X_2|\bar{Z}) \\ &= \sup_{p(w_1)p(w_2)} I(X_1; X_2|\bar{Z}) \\ &= I(X_1; X_2|\bar{Z}) \end{aligned}$$

Special Cases

- Consider the secret key agreement problem when nodes 1 and 2 know the eavesdropper's sequence Z^n , and we wish to find the secret key capacity defined as before. This models a scenario where we know which nodes are eavesdropping and have the ability to force these nodes to broadcast their information to all nodes

For this case the secrecy capacity is

$$C_K(\tilde{X}_1; \tilde{X}_2 || Z) = I(X_1; X_2 | Z)$$

Achievability follows by defining $\tilde{X}_1 := (X_1, Z)$, $\tilde{X}_2 := (X_2, Z)$, and $\tilde{Z} = Z$, and using the one-way achievability scheme (setting $U = \emptyset$ and $V = \tilde{X}_1$). The converse follows from the above upper bound

- The case where $Z = \emptyset$ (or Z is independent of (X_1, X_2)) corresponds to the case where the eavesdropper listens to the public communication but has no prior correlated information. This secrecy capacity for this case is $I(X_1; X_2)$

Extension to Multiple Nodes

- Consider a network with N nodes, an eavesdropper , and an $(N + 1)$ -DMS $(\mathcal{X}_1 \times \mathcal{X}_2 \times \dots \times \mathcal{X}_N \times \mathcal{Z}, p(x_1, \dots, x_N, Z))$. Node $j \in [1 : N]$ observes source X_j and the eavesdropper observes Z . The nodes communicate in a round robin fashion over q rounds, where q is divisible by N , such that node j communicates in times $j, N + j, 2N + j, \dots, q - N + j$
- A $(2^{nR_1}, 2^{nR_2}, \dots, 2^{nR_q}, n)$ code for the N -source secret key agreement consists of:
 - N encoders. In time $l_j \in \{j, N + j, 2N + j, \dots, q - N + j\}$, encoder j generates an index $M_{l_j} \in [1 : 2^{nR_{l_j}}]$ according to $p(m_{l_j} | x_j^n, m^{l_j-1})$
 - N -decoders. At the end of communication, decoder j generates a key $K_j \in \mathbb{Z}^+$ according to $p(k_j | m^q, x_j^n)$
- The probability of error for the code is defined as

$$P_e^{(n)} = 1 - P\{K_1 = K_2 = \dots = K_N\}$$

- The eavesdropper key rate rate is defined as

$$R_l^{(n)} := \frac{1}{n} \max_{j \in [1:N]} I(K_j; Z^n, M^q)$$

- A secret key rate R is achievable if there exists a sequence of codes such that $P_e^{(n)} \rightarrow 0$, $R_l^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ and

$$\liminf_{n \rightarrow \infty} \frac{1}{n} H(K_j) \geq R \text{ for } j \in [1 : N]$$

- The secret key capacity, $C_K(X_1; X_2; \dots; X_N | Z)$, is the supremum of all achievable rates R

Special Case: All Nodes Know Z

- Consider the case where the eavesdropper observes Z and node $j \in [1 : N]$ observes (X_j, Z) , which is a generalization of the special case for the 2-node setup discussed earlier
- *Theorem 9* [30]: The secret key capacity when all the nodes know Z is

$$C_K = H(X^N | Z) - R_{\text{CFO}}([1 : N] | Z),$$

where $R_{\text{CFO}}([1 : N] | Z)$ is the CFO rate (see Lecture notes 21) conditioned on all nodes knowing Z

- Achievability: The codebook generation for the public communications between nodes follows that of the CFO problem. For the secret key codebook, for each $z^n \in \mathcal{T}_\epsilon^{(n)}$, we randomly and independently partition the set of conditionally typical $X^n([1 : N])$ sequences to 2^{nR} bins. The index of the bin is the key to be agreed upon

The nodes communicate to achieve omniscience using the protocol described in the CFO achievability proof. That is, node j sends the bin index M_j of its source sequence. For decoding, every node first reconstructs $\hat{X}^n([1 : N])$ and then sets the secret key equal to the bin index of $\hat{X}^n([1 : N])$

Analysis of probability of error: An error occurs if

$(\hat{X}_{1j}^n, \hat{X}_{2j}^n, \dots, \hat{X}_{Nj}^n) \neq (X_1^n, X_2^n, \dots, X_N^n)$ for some $j \in [1 : N]$. The analysis follows that of the CFO problem with side information Z

Analysis of key rate: Analysis of key rate is similar to that for the 2 nodes case

Analysis of eavesdropper key rate: We consider the eavesdropper key rate only with respect to node 1 key K_1 . Other cases follow by Fano's inequality as in the 2 nodes case. Denote $\mathbf{X}^n := X^n([1 : N])$ and consider

$$\begin{aligned} I(K_1; M^N, Z^n) &= I(K_1, \mathbf{X}^n; M^N, Z^n) - I(\mathbf{X}^n; M^N, Z^n | K_1) \\ &= I(\mathbf{X}^n; M^N, Z^n) - I(\mathbf{X}^n; M^N, Z^n | K_1) \\ &= H(M^N, Z^n) - H(M^N, Z^n | \mathbf{X}^n) - I(\mathbf{X}^n; M^N, Z^n | K_1) \\ &\leq H(M^N) + I(Z^n; \mathbf{X}^n) - H(\mathbf{X}^n | K_1) + H(\mathbf{X}^n | M^N, K_1, Z^n) \\ &\stackrel{(a)}{\leq} nR_{\text{CFO}}([1 : N] | Z) + H(Z^n) - (H(\mathbf{X}^n | Z^n) + H(Z^n) - H(\mathbf{X}^n)) \\ &\quad - (H(\mathbf{X}^n) + H(K_1 | \mathbf{X}^n) - H(K_1)) + H(\mathbf{X}^n | M^N, K_1, Z^n) + n\delta(\epsilon) \\ &= n(R_{\text{CFO}}([1 : N] | Z) - H(\mathbf{X}^n | Z) + R + \delta(\epsilon)) + H(\mathbf{X}^n | M^N, K_1, Z^n) \end{aligned}$$

where (a) follows by the fact that $H(M^N) \leq R_{\text{CFO}} + \delta(\epsilon)$ in the CFO protocol.

Using a similar approach to the 2-node case, it can be shown that if

$R < H(X^N | Z) - R_{\text{CFO}}([1 : N] | Z) - \delta(\epsilon)$, then

$H(\mathbf{X}^n | M^N, K_1, Z^n) < n(H(\mathbf{X}^n | Z) - R - R_{\text{CFO}}([1 : N] | Z)) + n\delta(\epsilon)$.

Combining bounds gives $I(K_1; M^N, Z^n) \leq n\delta(\epsilon)$, which completes the achievability proof

- Converse: It suffices to bound $H(K_1)/n$, which will result in an upper bound on the achievable key rate. As for the 2-node case, we first assume the case with no randomization. Consider

$$\begin{aligned} \frac{1}{n}H(K_1) &= \frac{1}{n}(H(K_1) - I(K_1; Z^n, M^q) + I(K_1; Z^n, M^q)) \\ &\leq \frac{1}{n}H(K_1 | Z^n, M^q) + \epsilon_n, \end{aligned}$$

where the second step follows from the fact that by assumption eavesdropper key rate $\rightarrow 0$ as $n \rightarrow \infty$

To bound $H(K_1 | Z^n, M^q)$, note that both M^q and K_1 are functions of \mathbf{X}^n, Z^n , thus

$$\begin{aligned} H(\mathbf{X}^n | Z^n) &= H(M^q, K_1, \mathbf{X}^n | Z^n) \\ &= H(M^q | Z^n) + H(K_1 | Z^n, M^q) + H(\mathbf{X}^n | Z^n, K_1, M^q) \end{aligned}$$

Now,

$$\begin{aligned} & H(M^q|Z^n) + H(\mathbf{X}^n|Z^n, K_1, M^q) \\ &= \sum_{l=1}^q H(M_l|M^{l-1}, Z^n) + \sum_{j=1}^N H(X_j^n|X^n([1:j-1]), Z^n, K_1, M^q) \end{aligned}$$

Defining R'_j as

$$R'_j := \frac{1}{n} \sum_{l_j} H(M_{l_j}|M^{l_j-1}, Z^n) + \frac{1}{n} H(X_j^n|X^n([1:j-1]), Z^n, K_1, M^q) + \epsilon_n$$

We see that

$$\frac{1}{n} H(K_1|Z^n, M^q) = \frac{1}{n} H(\mathbf{X}^n|Z^n) - \sum_{j=1}^N R'_j + \epsilon_n$$

Thus

$$\begin{aligned} \frac{1}{n} H(K_1) &\leq \frac{1}{n} H(K_1|Z^n, M^q) + \epsilon_n \\ &\leq H(X([1:N])|Z) - \sum_{j=1}^N R'_j + 2\epsilon_n \end{aligned}$$

Next, we show that $(R'_1, R'_2, \dots, R'_N) \in \mathcal{R}_{\text{CFO}}([1:N]|Z)$, which implies that $\sum_{j=1}^N R'_j \geq R_{\text{CFO}}([1:N]|Z)$. Consider a set $\mathcal{J} \subset [1:N]$, then

$$\begin{aligned} & H(X^n(\mathcal{J})|X^n(\mathcal{J}^c), Z^n) \\ &= H(M^q, K_1, X^n(\mathcal{J})|X^n(\mathcal{J}^c), Z^n) \\ &= \sum_{j=1}^N \sum_{l_j} H(M_{l_j}|M^{l_j-1}, X^n(\mathcal{J}^c), Z^n) + H(K_1|M^q, X^n(\mathcal{J}^c), Z^n) \\ &\quad + \sum_{j \in \mathcal{J}} H(X_j^n|M^q, K_1, X^n([1:j-1]), X^n(\mathcal{J}^c \cap [j+1:N]), Z^n) \end{aligned}$$

Since \mathcal{J} is a strict subset of $[1:N]$, $H(K_1|M^q, X^n(\mathcal{J}^c), Z^n) \leq n\epsilon_n$ by Fano's inequality. Since M_{l_j} is a function of (M^{l_j-1}, X_j^n) , the first term is non-zero only for $j \in \mathcal{J}$. Hence,

$$\begin{aligned} H(X(\mathcal{J})|X(\mathcal{J}^c), Z) &= \frac{1}{n} H(X^n(\mathcal{J})|X^n(\mathcal{J}^c), Z^n) \\ &\leq \frac{1}{n} \sum_{j \in \mathcal{J}} \sum_{l_j} H(M_{l_j}|M^{l_j-1}, Z^n) \\ &\quad + \frac{1}{n} \sum_{j \in \mathcal{J}} H(X_j^n|M^q, K_1, X^n([1:j-1]), Z^n) + \epsilon_n = \sum_{j \in \mathcal{J}} R'_j \end{aligned}$$

Hence, $(1/n)H(K_1) \leq H(X([1 : N])|Z) - R_{\text{CFO}}([1 : N]|Z) + 2\epsilon_n$, which completes the proof of the converse for no randomization.

- The case with randomization follows the same steps of the converse proof with X_j^n, W_j as the random variables available at node j , where W_j is the private, independent random variable at node j
 - Remarks:
 - Consider the case where only a subset of the nodes $\mathcal{A} \subseteq [1 : N]$ wish to agree on a secret key, and the rest of the nodes act as “helpers” to achieve higher secret key rate. As before, all nodes observe the random variable at the wiretapper, Z^n . In this case, it can be shown that [30]
- $$C_K(\mathcal{A}) = H(X^N|Z) - R_{\text{CFO}}(\mathcal{A}|Z)$$
- Note that this key capacity can be larger than when no helper nodes are present
- The above secrecy capacity can be efficiently computed because $R_{\text{CFO}}(\mathcal{A}|Z)$ can be efficiently computed

Upper and Lower Bounds for N Nodes

- The interactive communication lower bound for 2-nodes discussed earlier can be extended to N nodes [28], and we obtain the best known lower bound

$$C_K(X_1; X_2; \dots; X_N || Z) \geq \sum_{l=1}^q \min_{j \in [1:N]} (I(U_l; X_j | U^{l-1}) - I(U_l; Z | U^{l-1}))$$

for (U_1, U_2, \dots, U_q) satisfying the following constraint

$$p(u^q | x_1, x_2, \dots, x_N, z) = \prod_{j=1}^N \prod_{l_j} p(u_{l_j} | u^{l_j-1}, x_j)$$

- The best known upper bound on the secret key agreement for multiple nodes [28] is

$$\begin{aligned} C_K(X_1; X_2; \dots; X_N || Z) &\leq \inf_{p(u|x^N)} \{H(X([1 : N])|U) - R_{\text{CFO}}(X([1 : N])|U) \\ &\quad + I(X([1 : N]); U|Z)\} \end{aligned}$$

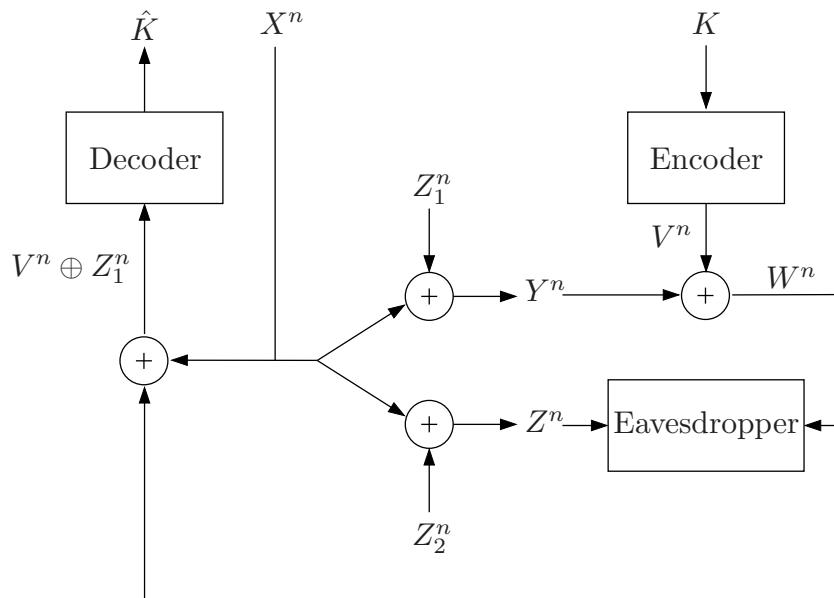
- For the case of $N = 2$, the bound reduces to $\inf_U (I(X_1; X_2|U) + I(X_1, X_2; U|Z))$. It can be shown that this bound is tighter than the upper bound of $\min_{p(\bar{z}|z)} I(X_1; X_2|\bar{Z})$

Secret Key Agreement: The Channel Model

- In the source model, it is assumed that nodes have access to correlated sources. Where do these correlated sources come from?
- The channel model generalizes the source model by including a DM-WTC from one of the nodes to the rest of the nodes (including the eavesdropper) in addition to the noiseless public broadcast channel. The noisy channel channel is used to generate the correlated sources at the nodes, which is used to generate the secret key
- Communication in the channel model is performed in multiple rounds. Each round consists of a number of transmissions over the DM-WTC followed by rounds of interactive communication over the public channel. The definitions of the secret key rate and achievability are similar to those of the source model
- Example [6]: Consider the BS-WTC(p_1, p_2) as defined before. Assume that the Bob is allowed to feed back information to Alice through a public noiseless link of unlimited capacity. This information is also available to Eve. Alice and Bob wish to agree on a key for secure communication that the eavesdropper is ignorant of. What is secret key capacity?

Maurer established the secrecy capacity using a wiretap channel coding scheme

over a virtual degraded BC from Bob to Alice Eve. Alice first sends a random sequence X^n . Bob then randomly picks a key $K \in [1 : 2^{nR}]$, adds its codeword V^n to the received sequence Y^n , and sends the sum W^n over the public channel. Alice uses her knowledge of X^n to obtain a better version of V^n than Eve's and proceeds to decode it to find \hat{K}



- Now, to the details:
 - Codebook generation: Let X and V be independent $\text{Bern}(1/2)$ random variables. Randomly and independently generate $2^{n\tilde{R}}$ sequences $v^n(l)$, $l \in [1 : 2^{n\tilde{R}}]$, each according to $\prod_{i=1}^n p_V(v_i)$ and partition them into 2^{nR} equal size bins $\mathcal{B}(k)$, $k \in [1 : 2^{nR}]$. This codebook is revealed to everyone
 - Alice sends $X^n \sim \prod_{i=1}^n p_X(x_i)$ over the BS-WTC
 - Bob randomly picks an index l according a uniform pmf over $[1 : 2^{n\tilde{R}}]$. The secret key k is the index of the bin that $v^n(l)$ belongs to. He sends $W^n = v^n(l) \oplus Y^n$ over the public channel
 - Upon receiving W^n , Alice adds it to X^n to obtain $v^n(l) \oplus Z_1^n$. Thus in effect Alice receives $v^n(l)$ over a $\text{BSC}(p_1)$. She declares \hat{l} is sent by Bob if it is the unique index such that $(v^n(\hat{l}), v^n(l) \oplus Z_1^n) \in \mathcal{T}_\epsilon^{(n)}$ and then declares the bin index \hat{k} of $v^n(\hat{l})$ as the key estimate. By the packing lemma, her probability of decoding error $\rightarrow 0$ if $\tilde{R} < I(V; V \oplus Z_1) - \delta(\epsilon) = 1 - h(p_1) - \delta(\epsilon)$
 - We now show that K satisfies the secrecy requirement. First we show that $H(K|Z^n, W^n) = H(K|Z^n \oplus W^n)$, i.e., $Z^n \oplus W^n = Z_1^n \oplus Z_2^n \oplus V^n$ is a “sufficient statistic” for K given (W^n, Z^n) . To prove this, note that

$$\begin{aligned}
 W^n &= X^n \oplus V^n \oplus Z_1^n \text{ is independent of } K, V^n, Z_1^n, \text{ and } Z_2^n. \text{ Thus} \\
 H(K|Z^n, W^n) &= H(K|W^n, W^n \oplus Z^n) \\
 &= H(K, W^n|Z^n \oplus W^n) - H(W^n|Z^n \oplus W^n) \\
 &= H(K|Z^n \oplus W^n) + H(W^n|K, Z^n \oplus W^n) - H(W^n|Z^n \oplus W^n) \\
 &= H(K|Z^n \oplus W^n)
 \end{aligned}$$

- This yields $I(K; W^n, Z^n) = I(K; W^n \oplus Z^n)$
- Thus, we can assume that Eve has $Z^n \oplus W^n = V^n \oplus Z_1^n \oplus Z_2^n$, i.e., she receives $v^n(l)$ over a $\text{BSC}(p_1 * p_2)$. From the analysis of the wiretap channel, a key rate of $R < I(V; V \oplus Z_1) - I(V; V \oplus Z_1 \oplus Z_2) - 2\delta = H(p_1 * p_2) - H(p_1) - 2\delta$ is achievable
 - The optimality of the above coding scheme is proved using the general upper bound on the secrecy capacity for channel model in [6]

$$C_{\text{K-channel}} \leq \min \left\{ \max_{p(x_1)} I(X_1; X_2), \max_{p(x_1)} I(X_1; X_2|Z) \right\}$$

It can be readily verified that this upper bound is tight for Maurer's example. The proof of the upper bound follows similar steps to the upper bound on the key capacity for the source model

- Lower bounds for the source model can be readily extended to the channel model by restricting communication to one round consisting of n i.i.d. transmissions over the DM-WTC to generate the correlated sources, followed by interactive public communication to generate the key

This restriction turns the problem into an *equivalent* source model with sources $(X_1, X_2, \dots, X_N, Z) \sim p(x_1)p(x_2, \dots, x_N, z|x_1)$, where $p(x_2, \dots, x_N, z|x_1)$ is the DM-WTC from X_1 to (X_2, \dots, X_N, Z) . Thus, if $R_K(X_1; \dots; X_N|Z)$ is a lower bound on the key capacity for the source model with sources $(X_1, X_2, \dots, X_N, Z)$, then

$$C_{\text{K-channel}} \geq \max_{p(x_1)} R_K(X_1; \dots; X_N|Z)$$

- Connection between Source Model and WTC [6]: Note that in Maurer's example we generated a key by constructing a *virtual* degraded wiretap channel from X_2 to (X, Z) . This observation can be generalized to obtain the one-way key rate for the source model from the wiretap channel result. We now show achievability of the one-way key rate for the source model by converting it into a WTC. For simplicity, we show the achievability of $R_{K-1} = I(X_1; X_2) - I(X_1; Z)$. The general one-way key rate result can be obtained as discussed in the section on one-way key rate

Fix $V \sim \text{Unif}(\mathcal{X}_1)$ independent of (X_1, X_2, Z) . For $i \in [1 : n]$, node 1 turns the public discussion channel into a wiretap channel by sending $V_i \oplus X_{1i}$ over it. The equivalent WTC is then $V \rightarrow ((X_2, V \oplus X_1), (Z, V \oplus X_1))$. From the WTC result, we transmit a confidential message at a rate of

$$\begin{aligned} R_{K-1} &= I(V; X_2, V \oplus X_1) - I(V; Z, V \oplus X_1) \\ &= I(V; X_2|V \oplus X_1) - I(V; Z|V \oplus X_1) \\ &= H(X_2|V \oplus X_1) - H(X_2|V \oplus X_1, V) - H(Z|V \oplus X_1) + H(Z|V \oplus X_1, V) \\ &\stackrel{(a)}{=} H(X_2) - H(X_2|X_1, V) - H(Z) + H(Z|X_1, V) \\ &= H(X_2) - H(X_2|X_1) - H(Z) + H(Z|X_1) = I(X_1; X_2) - I(X_1; Z), \end{aligned}$$

where (a) follows since $V \oplus X_1$ is independent of X_1 and hence (X_2, Z) by Markovity

- In [31] it is shown that if the eavesdropper's sequence Z^n is known to all nodes (through the public channel), then

$$C_{\text{K-channel}} = \max_{p(x_1)} (H(X^N|Z) - R_{\text{CFO}}([1:N]|Z))$$

Note that this is an upper bound on the key capacity when the nodes do not know Z . Generally tighter upper bounds are reported in [31, 32]

Key New Ideas and Techniques

- Information theoretic notion of secrecy
- Randomized encoding
- Key generation from common randomness via public communication

References

- [1] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Tech. J.*, vol. 28, pp. 656–715, 1949.
- [2] W. Diffie and M. E. Hellman, "New directions in cryptography," *IEEE Trans. Inf. Theory*, vol. 22, no. 6, pp. 644–654, 1976.
- [3] A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL: CRC Press, 1997.
- [4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [5] A. D. Wyner, "The wire-tap channel," *Bell System Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.
- [6] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [7] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, 1978.
- [8] F. Oggier and B. Hassibi, "The secrecy capacity of the MIMO wiretap channel," in *Proc. the 3rd International Symposium on Communications, Control and Signal Processing*, Mar. 2008, pp. 213–218.
- [9] R. Ahlswede and N. Cai, "Transmission, identification, and common randomness capacities for wire-tap channels with secure feedback from the decoder," in *General Theory of Information*

Transfer and Combinatorics, R. Ahlswede, L. Bäumer, N. Cai, H. Aydinian, V. Blinovsky, C. Deppe, and H. Mashurian, Eds. Berlin: Springer, 2007, pp. 258–275.

- [10] E. Ardestanizadeh, M. Franceschetti, T. Javidi, and Y.-H. Kim, “Wiretap channel with rate-limited feedback,” in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 101–105.
- [11] Y.-K. Chia and A. El Gamal, “3-receiver broadcast channels with common and confidential messages,” in *Proc. IEEE International Symposium on Information Theory*, Seoul, Korea, June/July 2009, pp. 1849–1853.
- [12] C. Nair and A. El Gamal, “The capacity region of a class of three-receiver broadcast channels with degraded message sets,” *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.
- [13] Y. Liang, H. V. Poor, and S. Shamai, “Information theoretic security,” *Foundations and Trends in Communications and Information Theory*, vol. 5, no. 4–5, pp. 355–580, 2009.
- [14] R. Liu, I. Marić, P. Spasojević, and R. D. Yates, “Discrete memoryless inference and broadcast channels with confidential messages: Secrecy rate regions,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2493–2507, 2008.
- [15] A. Khisti, A. Tchamkerten, and G. W. Wornell, “Secure broadcasting over fading channels,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2453–2469, 2008.
- [16] Y. Oohama, “Coding for relay channels with confidential messages,” in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sept. 2001, pp. 87–89.
- [17] L. Lai and H. El Gamal, “Cooperative secrecy: The relay-eavesdropper channel,” in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 931–935.

- [18] Y. Liang and H. V. Poor, “Multiple-access channels with confidential messages,” *IEEE Trans. Inf. Theory*, vol. 54, no. 3, pp. 976–1002, 2008.
- [19] E. Tekin and Y. Aylin, “The general Gaussian multiple-access and two-way wire-tap channels: Achievable rates and cooperative jamming,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2735–2751, June 2008.
- [20] Y. Liang, A. Somekh-Baruch, H. V. Poor, and S. Shamai, “Capacity of cognitive interference channels with and without secrecy,” *IEEE Trans. Inf. Theory*, vol. 55, no. 2, pp. 604–619, 2009.
- [21] Y. Liang, G. Kramer, P. H. V., and S. Shamai, “Recent results on compound wire-tap channels,” in *Proc. IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC)*, Cannes, France, Sept. 2008, pp. 1–5.
- [22] Y. Chen and A. J. Han Vinck, “Wiretap channel with side information,” *IEEE Trans. Inf. Theory*, vol. 54, no. 1, pp. 395–402, 2008.
- [23] W. Liu and B. Chen, “Wiretap channel with two-sided state information,” in *Proc. 41st Asilomar Conf. Signals, Systems and Comp.*, Pacific Grove, CA, Nov. 2007, pp. 893–897.
- [24] D. Gunduz, E. Erkip, and H. V. Poor, “Lossless compression with security constraints,” in *Proc. IEEE International Symposium on Information Theory*, Toronto, Canada, July 2008, pp. 111–115.
- [25] H. Yamamoto, “Rate-distortion theory for the Shannon cipher system,” *IEEE Trans. Inf. Theory*, vol. 43, no. 3, pp. 827–835, 1997.
- [26] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography—I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [27] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” *IEEE Trans. Inf. Theory*, vol. 46, no. 2, pp. 344–366, 2000.

- [28] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—I: Source model," 2008, submitted to *IEEE Trans. Inf. Theory*, 2008.
- [29] U. M. Maurer and S. Wolf, "Unconditionally secure key agreement and the intrinsic conditional information," *IEEE Trans. Inf. Theory*, vol. 45, no. 2, pp. 499–514, 1999.
- [30] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminals," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, 2004.
- [31] ———, "Secrecy capacities for multiterminal channel models," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2437–2452, 2008.
- [32] A. A. Gohari and V. Anantharam, "Information-theoretic key agreement of multiple terminals—II: Channel model," 2008, submitted to *IEEE Trans. Inf. Theory*, 2008.

Appendix: Proof of Lemma 1

- We bound $H(L|Z^n, m)/n$ for every m
- We first bound the probabilities of the following events:

Fix $L = l$ and a sequence $z^n \in \mathcal{T}_\epsilon^{(n)}$. Let $N(m, l, z^n) := |\{\tilde{l} \in \mathcal{B}(m) : (U^n(\tilde{l}), z^n) \in \mathcal{T}_\epsilon^{(n)} \tilde{l} \neq l\}|$. It is not difficult to show that

$$2^{n(\tilde{R}-R-I(U;Z)-\delta(\epsilon)-\epsilon_n)} \leq \mathbb{E}(N(m, l, z^n)) \leq 2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n)},$$

$$\text{Var}(N(m, l, z^n)) \leq 2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n)},$$

where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$

Define the random event

$\mathcal{E}_2(m, l, z^n) := \{N(m, l, z^n) \geq 2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n/2)+1}\}$. Using Chebyshev's inequality, it is easy to show that the probability of $\mathcal{E}_2(m, l, z^n)$ is

$$\begin{aligned} \mathbb{P}(\mathcal{E}_2(m, l, z^n)) &= \mathbb{P}(N(m, l, z^n) \geq 2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n/2)+1}) \\ &\leq \mathbb{P}(N(m, l, z^n) \geq \mathbb{E}(N(m, l, z^n)) + 2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n/2)}) \\ &\leq \mathbb{P}(|N(m, l, z^n) - \mathbb{E}(N(m, l, z^n))| \geq 2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n/2)}) \\ &\leq \frac{\text{Var}(N(m, l, z^n))}{2^{2n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n/2)}} \end{aligned}$$

Thus if $\tilde{R} - R - I(U; Z) \geq 0$, i.e., $R < I(U; Y) - I(U; Z) - \delta(\epsilon)$, $\mathbb{P}(\mathcal{E}_2(m, l, z^n)) \rightarrow 0$ as $n \rightarrow \infty$ for every m

- Next for each message m , define

$$\begin{aligned} N(m) &:= |\{\tilde{l} \in \mathcal{B}(m) : (U^n(\tilde{l}), Z^n) \in \mathcal{T}_\epsilon^{(n)} \tilde{l} \neq L\}| \text{ and} \\ \mathcal{E}_2(m) &:= \{N(m) \geq 2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n/2)+1}\} \end{aligned}$$

- Finally, define the indicator random variable $E(m) := 0$ if $(U^n(L), Z^n) \in \mathcal{T}_\epsilon^{(n)}$ and the event $\mathcal{E}_2(m)^c$ occurs, and $E(m) := 1$, otherwise

Clearly,

$$\mathbb{P}(E(m) = 1) \leq \mathbb{P}\{(U^n(L), Z^n) \notin \mathcal{T}_\epsilon^{(n)}\} + \mathbb{P}(\mathcal{E}_2(m))$$

The first term $\rightarrow 0$ as $n \rightarrow \infty$ by the LLN. For $\mathbb{P}(\mathcal{E}_2(m))$,

$$\begin{aligned} \mathbb{P}(\mathcal{E}_2(m)) &\leq \sum_{z^n \in \mathcal{T}_\epsilon^{(n)}} p(z^n) \mathbb{P}\{\mathcal{E}_2(m) | Z^n = z^n\} + \mathbb{P}\{Z^n \notin \mathcal{T}_\epsilon^{(n)}\} \\ &= \sum_{z^n \in \mathcal{T}_\epsilon^{(n)}} \sum_l p(z^n) p(l | z^n) \mathbb{P}\{\mathcal{E}_2(m) | Z^n = z^n, L = l\} + \mathbb{P}\{Z^n \notin \mathcal{T}_\epsilon^{(n)}\} \\ &= \sum_{z^n \in \mathcal{T}_\epsilon^{(n)}} \sum_l p(z^n) p(l | z^n) \mathbb{P}\{\mathcal{E}_2(m, z^n, l)\} + \mathbb{P}\{Z^n \notin \mathcal{T}_\epsilon^{(n)}\} \end{aligned}$$

By the argument above, the first term $\rightarrow 0$ as $n \rightarrow \infty$ if $R < I(U; Y) - I(U; Z) - \delta(\epsilon)$ and the second term $\rightarrow 0$ as $n \rightarrow \infty$ since $\mathbb{P}\{(U^n, Z^n) \notin \mathcal{T}_\epsilon^{(n)}\} \rightarrow 0$.

- We are now ready to bound the last eavesdropper message rate term. Consider

$$\begin{aligned} H(L | Z^n, m) &\leq 1 + P\{E(m) = 1\}H(L | Z^n, m, E(m) = 1) + H(L | Z^n, m, E(m) = 0) \\ &\leq 1 + n(\tilde{R} - R) \mathbb{P}\{E(m) = 1\} + H(L | Z^n, m, E(m) = 0) \\ &\leq 1 + n(\tilde{R} - R) \mathbb{P}\{E(m) = 1\} + \log(2^{n(\tilde{R}-R-I(U;Z)+\delta(\epsilon)-\epsilon_n/2)+1} + 1) \end{aligned}$$

Now since $\mathbb{P}\{E(m) = 1\} \rightarrow 0$ as $n \rightarrow \infty$ if $R < I(U;Y) - I(U;Z) - \delta(\epsilon)$, then for every m ,

$$\lim_{n \rightarrow \infty} H(L|Z^n, m)/n \leq \tilde{R} - R - I(U;Z) + \delta'(\epsilon)$$

- This completes the proof of the lemma

Proof of Lemma 2

- Consider

$$\begin{aligned} H(K_1|\mathcal{C}) &\geq \mathbb{P}\left\{X^n \in \mathcal{T}_\epsilon^{(n)}\right\} H\left(K_1|\mathcal{C}, X^n \in \mathcal{T}_\epsilon^{(n)}\right) \\ &\geq (1 - \epsilon'_n) H\left(K_1|\mathcal{C}, X^n \in \mathcal{T}_\epsilon^{(n)}\right) \end{aligned}$$

- Let $P(k_1)$ be the random pmf of K_1 given $\{X^n \in \mathcal{T}_\epsilon^{(n)}\}$, where the randomness is induced by the random bin assignment (codebook) \mathcal{C}

By symmetry, $P(k_1)$, $k_1 \in [1 : 2^{nR}]$, are identically distributed. Let $\mathcal{B}(1) = \bigcup_m \mathcal{B}_m(1)$ and express $P(1)$ in terms of a weighted sum of indicator functions as

$$P(1) = \sum_{x^n \in \mathcal{T}_\epsilon^{(n)}} \frac{p(x^n)}{\mathbb{P}\{X^n \in \mathcal{T}_\epsilon^{(n)}\}} \cdot I_{\{x^n \in \mathcal{B}(1)\}}$$

It can be easily shown that

$$\mathbb{E}_{\mathcal{C}}(P(1)) = 2^{-nR},$$

$$\begin{aligned} \text{Var}(P(1)) &= 2^{-nR}(1 - 2^{-nR}) \sum_{x^n \in \mathcal{T}_\epsilon^{(n)}} \left(\frac{p(x^n)}{\mathbb{P}\{X^n \in \mathcal{T}_\epsilon^{(n)}\}} \right)^2 \\ &\leq 2^{-nR} 2^{n(H(X) + \delta(\epsilon))} \frac{2^{-2n(H(X) - \delta(\epsilon))}}{(1 - \epsilon'_n)^2} \\ &\leq 2^{-n(R + H(X) - 4\delta(\epsilon))} \end{aligned}$$

for sufficiently large n

By the Chebychev inequality,

$$\begin{aligned} \mathbb{P}\{|P(1) - \mathbb{E}(P(1))| \geq \epsilon \mathbb{E}(P(1))\} &\leq \frac{\text{Var}(P(1))}{(\epsilon \mathbb{E}(P(1)))^2} \\ &\leq \frac{2^{-n(H(X) - R - 4\delta(\epsilon))}}{\epsilon^2} \end{aligned}$$

Note that if $R < H(X) - 4\delta(\epsilon)$, this probability $\rightarrow 0$ as $n \rightarrow \infty$

- Now, by symmetry

$$\begin{aligned} H(K_1 | \mathcal{C}, X^n \in \mathcal{T}_\epsilon^{(n)}) &= 2^{nR} \mathbb{E}(P(1)) \log(1/P(1)) \\ &\geq 2^{nR} \mathbb{P}\{|P(1) - \mathbb{E}(P(1))| < \epsilon 2^{-nR}\} \mathbb{E}(P(1) \log(1/P(1)) \mid |P(1) - \mathbb{E}(P(1))| < \epsilon 2^{-nR}) \\ &\geq \left(1 - \frac{2^{-n(H(X) - R - 4\delta(\epsilon))}}{\epsilon^2}\right) \cdot (nR(1 - \epsilon) - (1 - \epsilon) \log(1 + \epsilon)) \\ &\geq n(R - \delta(\epsilon)) \end{aligned}$$

for sufficiently large n and $R < H(X) - 4\delta(\epsilon)$

- Thus, we have shown that if $R < H(X) - 4\delta(\epsilon)$, $\lim_{n \rightarrow \infty} H(K_1 | \mathcal{C}) \geq R - \delta(\epsilon)$. This completes the proof of the lemma

Proof Lemma 3

- Let $I_1 := 1$ if $(X_1^n, Z^n) \notin \mathcal{T}_\epsilon^{(n)}$ and $I_1 := 0$, otherwise. Note that by the LLN, $\mathbb{P}\{I_1 = 1\} \rightarrow 0$ as $n \rightarrow \infty$. Consider

$$\begin{aligned} H(X_1^n | Z^n, M, K_1, \mathcal{C}) &\leq H(X_1^n, I_1 | Z^n, M, K_1, \mathcal{C}) \\ &\leq 1 + n \mathbb{P}\{I_1 = 1\} \log |\mathcal{X}_1| + \sum_{(z^n, m_1, k_1)} p(z^n, m_1, k_1 | I_1 = 0) \\ &\quad \cdot H(X_1^n | z^n, m_1, k_1, I_1 = 0, \mathcal{C}) \end{aligned}$$

- Now, for codebook \mathcal{C} and $z^n \in \mathcal{T}_\epsilon^{(n)}$, let $N(z^n, \mathcal{C})$ be the number of sequences $x_1^n \in \mathcal{B}_{m_1}(k_1) \cap \mathcal{T}_\epsilon^{(n)}(X_1 | z^n)$, and define $I_2(z^n, \mathcal{C}) := 1$ if $N(z^n, \mathcal{C}) \geq 2 \mathbb{E}(N(z^n, \mathcal{C}))$ and $I_2(z^n, \mathcal{C}) := 0$, otherwise. It is easy to show that

$$\mathbb{E}(N(z^n, \mathcal{C})) = 2^{-n(\tilde{R}+R)} |\mathcal{T}_\epsilon^{(n)}(X_1 | z^n)|$$

and

$$\text{Var}(N(z^n, \mathcal{C})) \leq 2^{-n(\tilde{R}+R)} |\mathcal{T}_\epsilon^{(n)}(X_1 | z^n)|$$

Then, by the Chebyshev inequality

$$\mathbb{P}\{I_2(z^n, \mathcal{C}) = 1\} \leq \frac{\text{Var}(N(z^n, \mathcal{C}))}{(\mathbb{E}(N(z^n, \mathcal{C})))^2} \leq 2^{-n(H(X_1 | Z) - \tilde{R} - R - \delta(\epsilon))}$$

- Thus if $\tilde{R} + R < H(X_1 | Z) - \delta(\epsilon)$, i.e., $R < H(X_1 | Z) - H(X_1 | X_2) - 2\delta(\epsilon)$, $\mathbb{P}\{I_2(z^n, \mathcal{C}) = 1\} \rightarrow 0$ as $n \rightarrow \infty$. Now,

$$\begin{aligned} H(X_1^n | z^n, m_1, k_1, I_1 = 0, \mathcal{C}) &\leq H(X_1^n, I_2 | z^n, m_1, k_1, I_1 = 0, \mathcal{C}) \\ &\leq 1 + n \mathbb{P}\{I_2 = 1\} \log |\mathcal{X}_1| + H(X_1^n | z^n, m_1, k_1, I_1 = 0, I_2 = 0, \mathcal{C}) \\ &\leq 1 + n \mathbb{P}\{I_2 = 1\} \log |\mathcal{X}_1| + n(H(X_1 | Z) - \tilde{R} - R + \delta(\epsilon)) \end{aligned}$$

- Thus, if $R < H(X_1 | Z) - H(X_1 | X_2) - 2\delta(\epsilon)$, $H(X_1^n | Z^n, M, K_1, \mathcal{C})/n \leq H(X_1 | Z) - \tilde{R} - R + \delta(\epsilon)$ as $n \rightarrow \infty$

Lecture Notes 24

Information Theory and Networking

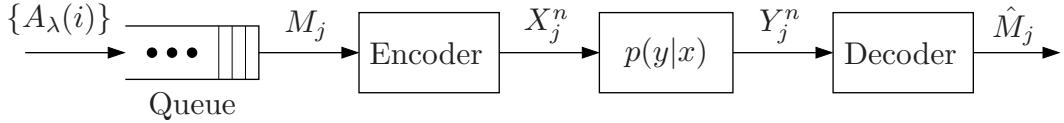
- Random Data Arrival at a DMC
- Asynchronous MAC
- Random Access Channel [3]
- Key New Ideas and Techniques
- Appendix: Proof of Lemma 1
- Appendix: Proof of Lemma 2

© Copyright 2002–10 Abbas El Gamal and Young-Han Kim

Random Data Arrival at a DMC

- In the definitions of the channel coding problems, we assumed that data is always available at the encoder. In many network applications, data is bursty and it may or may not be available at the sender when the channel is free. Moreover, the amount of data at the sender may exceed its finite queue size resulting in data loss even before transmission
- 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, the data can be sent reliably to the receiver, while if $\lambda \geq C$, data cannot be reliably sent either because the incoming data exceeds the sender's queue size or because transmission rate exceeds capacity
- We illustrate this general result using the following simple random data arrival process. Assume data packets arrive at the sender according to an i.i.d. process $\{A_\lambda(i)\}$, where the arrival rate λ is the product of the packet arrival rate $p \in (0, 1]$ and packet size k bits. At the “end” of transmission time $i = 1, 2, \dots$, $A(i) = k$ bits, i.e., a packet arrives at the sender, with probability p (the packet bits are modeled by k i.i.d. $\text{Bern}(1/2)$ random variables), and $A(i) = 0$, i.e., no packet arrives, with probability \bar{p} . The packets arriving at different transmission times are assumed to be independent

- Define an *augmented* $(2^{nR}, n)$ block code for the DMC to consist of:
 1. An augmented message set $[1 : 2^{nR}] \cup \{0\}$,
 2. an encoder that assigns a codeword $x^n(m)$ to each $m \in [1 : 2^{nR}] \cup \{0\}$, and
 3. 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 time $i = 1, 2, \dots$. At the beginning of time jn , $j = 1, 2, \dots$, i.e., 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, by the definition of the arrival time process,
 $M_j | \{M_j \neq 0\} \sim \text{Unif}[1 : 2^{nR}]$
- The queue is said to be *stable* if $\sup_i E(Q(i)) \leq B$ for some constant $B < \infty$

- Lemma 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 the Appendix
- Queue stability implies that we can make the probability of data loss as small as desired with a finite buffer size (why?)
- Let p_j be the probability that the sender queue has less than nR bits at the beginning of transmission block j
- Define the probability of error in transmission block j as

$$\begin{aligned} P_{ej}^{(n)} &:= P\{\hat{M}_j \neq M_j\} \\ &= p_j P\{\hat{M}_j \neq 0 | M_j = 0\} + \frac{(1 - p_j)}{2^{nR}} \sum_{m=1}^{2^{nR}} P\{\hat{M}_j \neq m | M_j \neq 0\} \end{aligned}$$

- A rate R is said to be achievable if there exists a sequence of codes with $\sup_j P_{ej}^{(n)} \rightarrow 0$ as $n \rightarrow \infty$
- The data arriving at the encoder according to the process $\{A_\lambda(i)\}$ can be reliably communicated at rate R over the DMC if (i) the queue is stable, and (ii) there exists a sequence of $(2^{nR}, n)$ codes with $\sup_j P_{ej}^{(n)} \rightarrow 0$ as $n \rightarrow \infty$

- We wish to find necessary and sufficient conditions for reliable communication of the data over the DMC
- *Theorem 1:* The random data arrival process $\{A_\lambda(i)\}$ can be reliably communicated over a DMC $(\mathcal{X}, p(y|x), \mathcal{Y})$ with capacity C if $\lambda < C$. Conversely, given any sequence of $(2^{nR}, n)$ codes with $\sup_j P_{ej}^{(n)} \rightarrow 0$ as $n \rightarrow \infty$ such that the queue is stable, then $\lambda < R \leq C$
- Achievability: If $R < C$, there exists a sequence of augmented $(2^{nR}, n)$ codes with maximal probability of error $\rightarrow 0$ as $n \rightarrow \infty$. Using this sequence of codes guarantees that $P_{ej}^{(n)} \rightarrow 0$ for every j
- Converse: We already know that we must have $R > \lambda$. Now, for each j ,

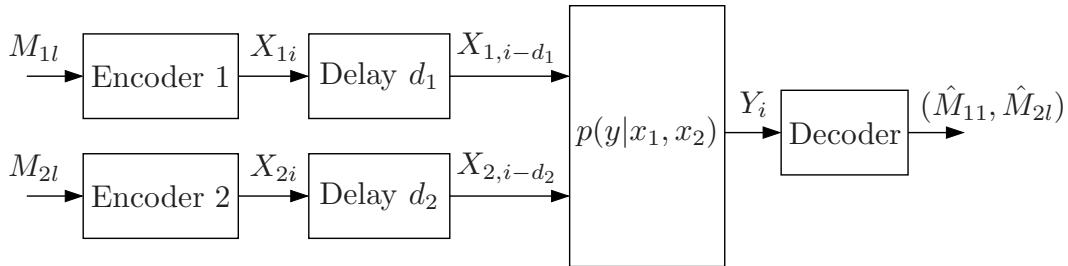
$$\begin{aligned} nR &= H(M_j | M_j \neq 0) \\ &\leq I(M_j; Y^n | M_j \neq 0) + n\epsilon_n \\ &\leq n(C + \epsilon_n) \end{aligned}$$

- The above result can be extended to multiple user 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 $\{A_{\lambda_1}(i)\}$ and $\{A_{\lambda_2}(i)\}$. The *stability region* \mathcal{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 DMC case
- Let \mathcal{C} be the capacity of region for the DM-MAC, then it can be readily shown that $\mathcal{S} = \mathcal{C}$
- Remark: The same result holds when the packets arrivals (but not the packet contents) are correlated

Asynchronous MAC

- In the single-hop channel models we discussed in Part II, we assumed that the transmissions from the senders to the receivers are synchronized (both at the symbol and block levels). In practice achieving such complete synchronization may not be feasible. How does the lack of synchronization affect the capacity region of the channel?
- We consider this question for the DM-MAC



- We assume that the senders wish to send a sequence of i.i.d. messages $(M_{1l}, M_{2l}) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}], l = 1, 2, \dots$ (as before, the messages from the two senders are assumed to be independent) and that the same codebook is used in each transmission block

- We further assume that symbols are synchronized, but that the blocks sent by the two encoders incur delays $d_1, d_2 \in [0 : d]$, respectively, for some $d \leq n - 1$. Assume the delays to be unknown a priori to the encoders and decoder. The received sequence is generated according to

$$p(y^n | x_{1,1-d}^n, x_{2,1-d}^n) = \prod_{i=1}^n p_{Y|X_1, X_2}(y_i | x_{1,i-d_1}, x_{2,i-d_2}),$$

where the symbols with negative indices are from the previous transmission block

- A $(2^{nR_2}, 2^{nR_2}, n, d)$ code for the asynchronous DM-MAC consists of:
 1. two encoders: encoder 1 assigns a sequence of codewords $x_1^n(m_{1l})$ to each message sequence $m_{1l} \in [1 : 2^{nR_1}], l = 1, 2, \dots$. Similarly, encoder 2 assigns a sequence of codewords $x_2^n(m_{2l})$ to each message sequence $m_{2l} \in [1 : 2^{nR_2}], l = 1, 2, \dots$
 2. 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 $l = 1, 2, \dots$ (the received sequence $y_{(l-1)n+1}^{ln+d}$ can include parts of the previous and next blocks)

- The 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 $P_{el}^{(n)}(d_1, d_2) := \mathbb{P}\{(\hat{M}_{1l}, \hat{M}_{2l}) \neq (M_{1l}, M_{2l}) | d_1, d_2\}$

- Note that by assumption, $\sup_l P_{el}^{(n)}(d_1, d_2) = P_{el}^{(n)}(d_1, d_2)$ 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
- Consider two scenarios:
 - *Slightly asynchronous* [1]: Here $d/n \rightarrow 0$ as $n \rightarrow \infty$. In this case, the capacity region is the same as for the synchronous case even when the receiver does not know the delays
 - *Totally asynchronous* [2]: $d = n - 1$, i.e., d_1, d_2 can vary from 0 to $n - 1$. In this case time-sharing becomes infeasible and the capacity region reduces to the following:

Theorem 2 [2]: The capacity region for the asynchronous DM-MAC is the set of all rate pairs (R_1, R_2) such that

$$R_1 \leq I(X_1; Y | X_2),$$

$$R_2 \leq I(X_2; Y | X_1),$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)$$

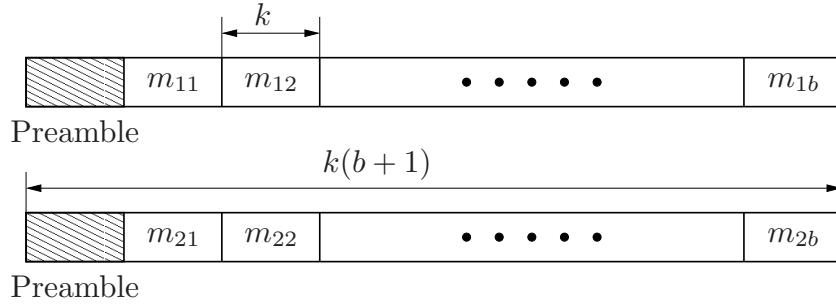
for some $p(x_1)p(x_2)$

- Remark: The capacity region for the AWGN-MAC does not change with asynchrony. However, one needs joint decoding to achieve all the points in the capacity region

Achievability

- We divide each n -transmission block into $b + 1$ subblocks each consisting of k symbols (thus the delays range from 0 to $(b + 1)k - 1$). The first block labeled $j = 0$ is a *preamble* block. We divide the message pair (M_1, M_2) into b independent sub-message 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

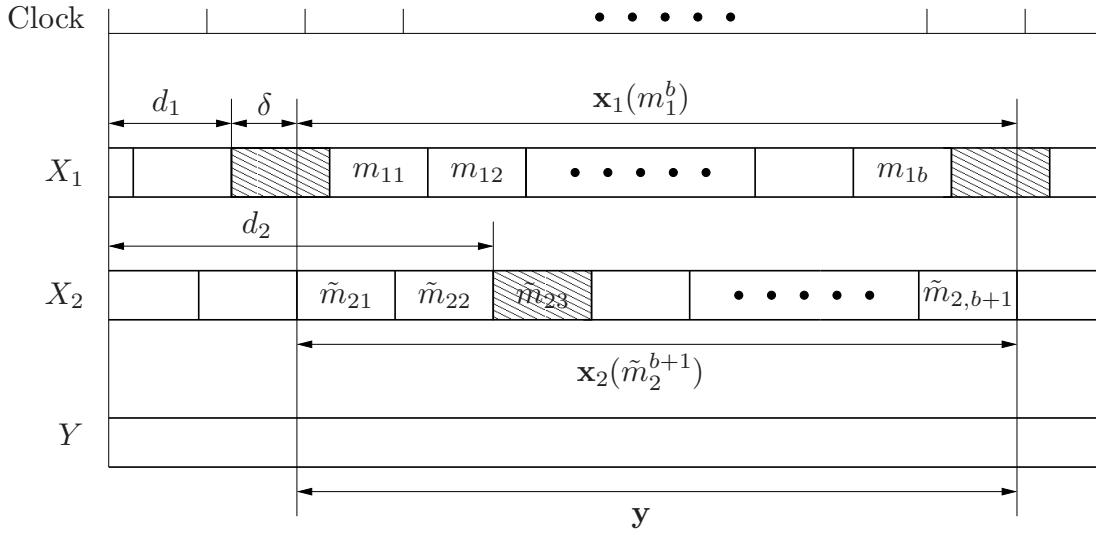
Note that the resulting rate pair for this code, $(bR_1/(b + 1), bR_2/(b + 1))$, can be made arbitrarily close to (R_1, R_2) as $b \rightarrow \infty$



- Codebook generation:** Fix $p(x_1)p(x_2)$ and randomly and independently generate 2^{kR_1} codewords $x_1^k(m_1)$, $m_1 \in [1 : 2^{kR_1}]$, and a preamble codeword $x_1^k(0)$, each according to $\prod_{i=1}^k p_X(x_i)$. Similarly generate 2^{kR_2} codewords $x_2^k(m_2)$, $m_2 \in [1 : 2^{kR_2}]$, and a preamble codeword $x_2^k(0)$
- Encoding:** To send the sub-messages $\{m_{1j}, j \in [1 : b]\}$, encoder 1 first sends its preamble codeword $x_1^k(0)$ followed by $x_1^k(m_{1j})$ for each $j \in [1 : b]$. Similarly, encoder 2 sends its preamble codeword followed by $x_2^k(m_{2j})$ for each $j \in [1 : b]$
- Decoding:** Without loss of generality, assume that $d_1 \leq d_2$. Define (see the figure below)

$$\begin{aligned}\mathbf{x}_1(m_1^b) &:= (x_{1,\delta+1}^k(0), x_1^k(m_{11}), x_1^k(m_{12}), \dots, x_1^k(m_{1b}), x_1^{k-\delta}(0)), \\ \mathbf{x}_2(\tilde{m}_2^{b+1}) &:= (x_2^k(\tilde{m}_{21}), x_2^k(\tilde{m}_{22}), \dots, x_2^k(\tilde{m}_{2,b+1})), \\ \mathbf{y} &:= y_{d_1+\delta+1}^{(b+1)k+d_1+\delta},\end{aligned}$$

where $\delta = (d_2 - d_1) \bmod k$



1. Preamble decoding: The receiver declares \hat{d}_1 as the estimate for d_1 if it is the unique index in $[0 : (b + 1)k - 1]$ such that $(x_1^k(0), y_{\hat{d}_1+1}^{d_1+k}) \in \mathcal{T}_\epsilon^{(n)}$. Similarly, the receiver declares \hat{d}_2 as the estimate for d_2 if it is the unique index in $[0 : (b + 1)k - 1]$ such that $(x_2^k(0), y_{\hat{d}_2+1}^{d_2+k}) \in \mathcal{T}_\epsilon^{(n)}$. An error is declared if no such unique delay pair (\hat{d}_1, \hat{d}_2) exist

2. Decoding of message sequence m_1^b : The receiver declares that \hat{m}_1^b is the sequence of sub-messages sent by sender 1 if it is the unique sub-message sequence such that $(\mathbf{x}_1(\hat{m}_1^b), \mathbf{x}_2(\hat{m}_2^{b+1}), \mathbf{y}) \in \mathcal{T}_\epsilon^{(n)}$ for some \hat{m}_2^{b+1}
3. Decoding of 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 error averaged over codes

First we bound the probability of preamble decoding error. Define the error events

$$\begin{aligned}\mathcal{E}_{p10} &:= \left\{ \left(X_1^k(0), Y_{d_1+1}^{d_1+k} \right) \notin \mathcal{T}_\epsilon^{(n)} \right\}, \\ \mathcal{E}_{p11} &:= \left\{ \left(X_1^k(0), Y_{\tilde{d}+1}^{\tilde{d}+k} \right) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{d} \neq d_1, \tilde{d} \in [0 : (b + 1)k - 1] \right\}, \\ \mathcal{E}_{p20} &:= \left\{ \left(X_2^k(0), Y_{d_2+1}^{d_2+k} \right) \notin \mathcal{T}_\epsilon^{(n)} \right\}, \\ \mathcal{E}_{p21} &:= \left\{ \left(X_2^k(0), Y_{\tilde{d}+1}^{\tilde{d}+k} \right) \in \mathcal{T}_\epsilon^{(n)} \text{ for some } \tilde{d} \neq d_2, \tilde{d} \in [0 : (b + 1)k - 1] \right\}\end{aligned}$$

The average probability of preamble decoding error is

$$P(\mathcal{E}_p) \leq P(\mathcal{E}_{p10}) + P(\mathcal{E}_{p20}) + P(\mathcal{E}_{p11}) + P(\mathcal{E}_{p21})$$

The first and third terms $\rightarrow 0$ as $k \rightarrow \infty$ by the LLN. To bound the other two terms, we use the following:

Lemma 2: Suppose $p(x, y) \neq p(x)p(y)$. If ϵ is sufficiently small, then there exists $\gamma > 0$ that depends only on $p(x, y)$ such that

$$\mathbb{P} \left\{ \left(X_1^k(0), Y_{\tilde{d}+1}^{\tilde{d}+k} \right) \in \mathcal{T}_\epsilon^{(n)} \right\} \leq 2^{-k\gamma}$$

for all $\tilde{d} \neq d_1$

The proof is provided in the Appendix

Then by the union of events bound, we have

$$\mathbb{P}(\mathcal{E}_{p11}) \leq (b+1)k2^{-k\gamma}$$

Thus the second and fourth error probability terms $\rightarrow 0$ as $n \rightarrow \infty$

Next we bound the probability of decoding error for message sequence m_1^b assuming the preambles are correctly decoded. Define the error events:

$$\begin{aligned} \mathcal{E}_0 &:= \left\{ (\mathbf{X}_1(m_1^b), \mathbf{X}_2(\tilde{m}_2^{b+1}), \mathbf{Y}) \notin \mathcal{T}_\epsilon^{(n)} \right\}, \\ \mathcal{E}(\mathcal{J}_1, \mathcal{J}_2) &:= \left\{ \hat{m}_{1j_1} \neq m_{1j_1} \text{ for } j_1 \in \mathcal{J}_1, \hat{m}_{2j_2} \neq \tilde{m}_{2j_2} \text{ for } j_2 \in \mathcal{J}_2, \right. \\ &\quad \left. \hat{m}_{1j_1} = m_{1j_1} \text{ for } j_1 \notin \mathcal{J}_1, \hat{m}_{2j_2} = \tilde{m}_{2j_2} \text{ for } j_2 \notin \mathcal{J}_2 \right\} \end{aligned}$$

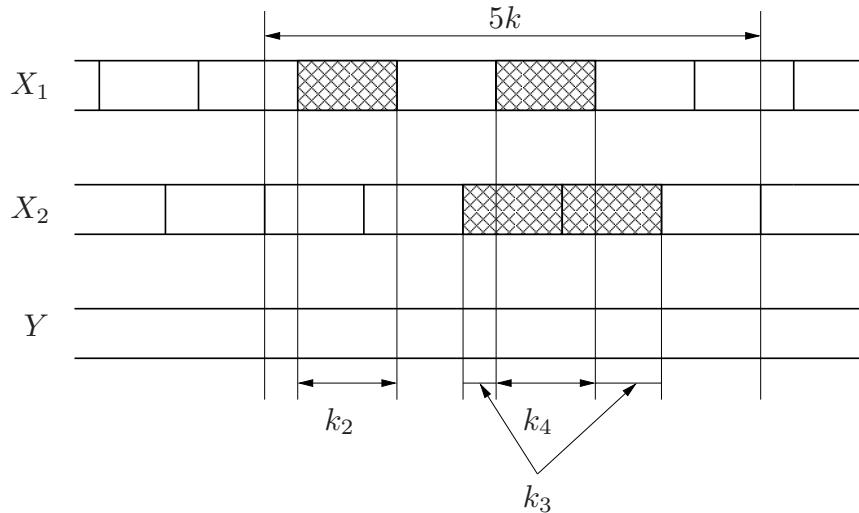
for every $\mathcal{J}_1 \subseteq [1 : b]$ and $\mathcal{J}_2 \subseteq [1 : b+1]$

The probability of decoding error for message sequence m_1^b averaged over codebooks is

$$\mathbb{P}(\mathcal{E}_1) \leq \mathbb{P}(\mathcal{E}_0) + \sum_{\emptyset \neq \mathcal{J}_1 \subseteq [1:b], \mathcal{J}_2 \subseteq [1:b+1]} \mathbb{P}(\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2))$$

The first term $\rightarrow 0$ as $k \rightarrow \infty$ by the LLN

Now consider the error event $\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2)$ illustrated for $b = 4$,
 $\mathcal{J}_1 = \{1, 3\}$, $\mathcal{J}_2 = \{3, 4\}$



The $(b + 1)k$ transmissions are divided into 4 groups:

- Transmissions where both sender 1 messages and sender 2 messages are correct. Each symbol in this group is generated according to $p(x_1)p(x_2)p(y|x_1, x_2)$. Assume there are $k_1 \in [0 : (b + 1)k - 1]$ such symbols

- Transmissions where sender 1's messages are in error but sender 2's messages are correct. Each symbol in this group is generated according to $p(x_1)p(x_2)p(y|x_2)$. Assume there are k_2 such symbols
- Transmissions where sender 2's messages are in error but sender 1's messages are correct. Each symbol in this group is generated according to $p(x_1)p(x_2)p(y|x_1)$. Assume there are k_3 such symbols
- Transmissions where both sender 1 messages and sender 2 messages are in error. Each symbol in this group is generated according to $p(x_1)p(x_2)p(y)$. Assume there are k_4 such symbols

It is not difficult to see that $k_1 + k_2 + k_3 + k_4 = (b + 1)k$, $k_2 + k_4 = k|\mathcal{J}_1|$, and $k_3 + k_4 = k|\mathcal{J}_2|$

To simplify the analysis of the probability of the event $\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2)$, define the event that no message is repeated in the block as

$$\begin{aligned}\mathcal{A} := & \{m_{1j} \neq m_{1j'} \text{ for all } j, j' \in [1 : b], j \neq j', \\ & \text{and } \tilde{m}_{2j} \neq \tilde{m}_{2j'} \text{ for all } j, j' \in [1 : b + 1], j \neq j'\}\end{aligned}$$

Thus $P(\mathcal{A}) \rightarrow 1$ as $k \rightarrow \infty$. We now bound $P(\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2) \cap \mathcal{A})$

Since all messages sent in the block are different, all erroneous messages must be different (otherwise they would be detected and treated as part of event $\mathcal{E}_0 \cap \mathcal{A}$). Thus the symbol triples (X_{1i}, X_{2i}, Y_i) are mutually independent for all $i \in [d_1 + \delta + 1 : (b + 1)k + d_1 + \delta]$. Using this independence and the joint typicality lemma for each term, the probability of each erroneous message pattern in subblocks $\mathcal{J}_1, \mathcal{J}_2$ is upper bounded by

$$2^{-k_2(I(X_1;Y|X_2)-\delta(\epsilon))} \cdot 2^{-k_3(I(X_2;Y|X_1)-\delta(\epsilon))} \cdot 2^{-k_4(I(X_1,X_2;Y)-\delta(\epsilon))}$$

The number of symbol patterns in the error locations is upper bounded by $2^{k(|\mathcal{J}_1|R_1+|\mathcal{J}_2|R_2)}$. Thus, using the union of events bound, we obtain

$$\begin{aligned} & P(\mathcal{E}(\mathcal{J}_1, \mathcal{J}_2) \cap \mathcal{A}) \\ & \leq 2^{k(|\mathcal{J}_1|R_1+|\mathcal{J}_2|R_2)} \cdot 2^{-k_2(I(X_1;Y|X_2)-\delta(\epsilon))-k_3(I(X_2;Y|X_1)-\delta(\epsilon))-k_4(I(X_1,X_2;Y)-\delta(\epsilon))} \\ & = 2^{-k_2(I(X_1;Y|X_2)-R_1-\delta(\epsilon))} \cdot 2^{-k_3(I(X_2;Y|X_1)-R_2-\delta(\epsilon))} \cdot 2^{-k_4(I(X_1,X_2;Y)-R_1-R_2-\delta(\epsilon))}, \end{aligned}$$

which $\rightarrow 0$ as $k \rightarrow \infty$ if $R_1 < I(X_1;Y|X_2) - \delta(\epsilon)$, $R_2 < I(X_2;Y|X_1) - \delta(\epsilon)$, $R_1 + R_2 < I(X_1, X_2; Y) - \delta(\epsilon)$

Bounding the probability of decoding error for m_2^b follows similarly. This completes the proof of achievability

Converse

- Given a sequence of $(2^{nR_1}, 2^{nR_2}, n, d = n - 1)$ codes with $P_e^{(n)} = \max_{d_1, d_2 \in [0:n-1]} \sup_l P_{el}^{(n)}(d_1, d_2) \rightarrow 0$, we wish to show that (R_1, R_2) satisfy the conditions of the theorem for some $p(x_1)p(x_2)$
- 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 $\max_{d_2 \in [0:n-1]} \sup_l P_{el}^{(n)}(0, d_2) \leq P_e^{(n)}$. Further, assume that $D_2 \sim \text{Unif}[0 : n - 1]$, then the expected probability of error $E_{D_2}(\sup_l P_{el}^{(n)}(0, D_2)) \leq P_e^{(n)}$. 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 remote 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 sequence of κ message pairs $(M_{1l}, M_{2l}) \in [1 : 2^{nR_1}] \times [1 : 2^{nR_2}]$, $l \in [1 : \kappa]$, from the received sequence $Y^{(\kappa+1)n-1}$

- By Fano's inequality,

$$H(M_{1l}, M_{2l} | Y^{(\kappa+1)n}, D_2) \leq H(M_{1l}, M_{2l} | Y^{(\kappa+1)n-1}) \leq n\epsilon_n$$

for $l \in [1 : \kappa]$, where $\epsilon_n \rightarrow 0$ as $n \rightarrow \infty$

- Following the converse proof for the synchronous DM-MAC in Lecture Notes 4, it is straightforward to show that

$$\begin{aligned}\kappa n R_1 &\leq \sum_{i=1}^{(\kappa+1)n} I(X_{1i}; Y_i | X_{2,i-D_2}, D_2) + \kappa n \epsilon_n, \\ \kappa n R_2 &\leq \sum_{i=1}^{(\kappa+1)n} I(X_{2,i-D_2}; Y_i | X_{1i}, D_2) + \kappa n \epsilon_n, \\ \kappa n (R_1 + R_2) &\leq \sum_{i=1}^{(\kappa+1)n} I(X_{1i}, X_{2,i-D_2}; Y_i | D_2) + \kappa n \epsilon_n\end{aligned}$$

- Now let $Q \sim \text{Unif}[1 : n]$ (not $[1 : (\kappa+1)n - 1]$) be the time-sharing random variable independent of $(X_1^{\kappa n}, X_2^{\kappa n}, Y^{(\kappa+1)n}, D_2)$. Then

$$\begin{aligned}\kappa n R_1 &\leq \sum_{l=1}^{(\kappa+1)} n I(X_{1,Q+(l-1)n}; Y_{Q+(l-1)n} | X_{2,Q+(l-1)n-D_2}, D_2, Q) + \kappa n \epsilon_n \\ &\stackrel{(a)}{=} (\kappa+1) n I(X_{1Q}; Y_Q | X_{2,Q-D_2}, Q, D_2) + \kappa n \epsilon_n \\ &= (\kappa+1) n I(X_1; Y | X_2, Q, D_2) + \kappa n \epsilon_n \\ &\stackrel{(b)}{\leq} (\kappa+1) n I(X_1; Y | X_2) + \kappa n \epsilon_n,\end{aligned}$$

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 $(Q, D_2) \rightarrow (X_1, X_2) \rightarrow Y$ form a Markov chain. Similarly,

$$\begin{aligned}\kappa n R_2 &\leq (\kappa+1) n I(X_2; Y | X_1) + \kappa n \epsilon_n, \\ \kappa n (R_1 + R_2) &\leq (\kappa+1) n I(X_1, X_2; Y) + \kappa n \epsilon_n\end{aligned}$$

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 noting that κ can be made as large as desired (after taking $n \rightarrow \infty$) completes the proof of the converse

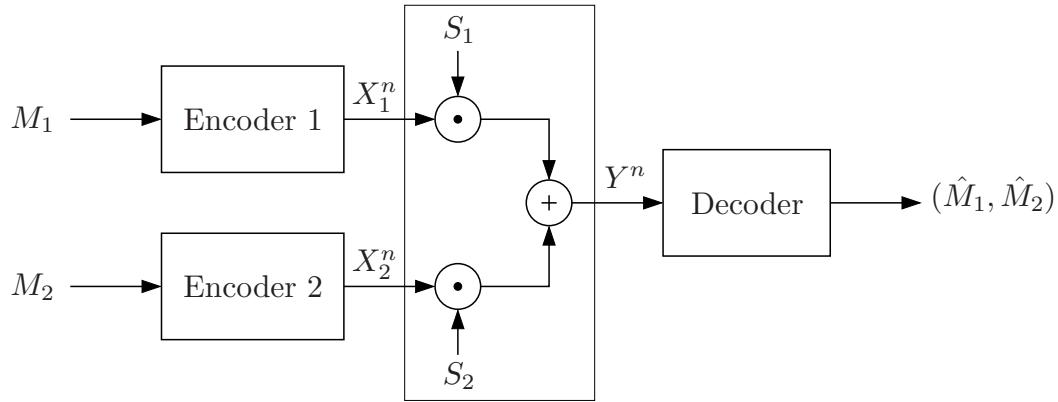
Random Access Channel [3]

- The random access channel (RAC) is a DM-MAC with state defined as

$$Y_i = S_{1i} \cdot X_{1i} \oplus S_{2i} \cdot X_{2i},$$

where $\{S_{1i}\}$ and $\{S_{2i}\}$ are independent Bern(p) processes

- This channel models packet collision in wireless multi-access network (Aloha []). Sender $j = 1, 2$ has a packet to transmit (is active) when $S_j = 1$ and is inactive when $S_j = 0$. The receiver knows which senders are active, but each sender does not know whether the other sender is active



This model can be viewed as a special case of the fading DM-MAC [4] where the receiver knows the complete channel state but each sender knows its own state only. We consider the slow fading scenario

- The compound channel capacity region is $R_1 = R_2 = 0$
- The adaptive capacity region is the set of rate quadruples $(R_{10}, R_{11}, R_{20}, R_{21})$ such that

$$R_{10} = \min_{s_2} I(X_1; Y | X_2, s_1 = 0, s_2) = 0,$$

$$R_{20} = \min_{s_1} I(X_1; Y | X_2, s_1, s_2 = 0) = 0,$$

$$R_{11} \leq \min_{s_2} I(X_1; Y | X_2, s_1 = 1, s_2) \leq 1,$$

$$R_{21} \leq \min_{s_1} I(X_1; Y | X_2, s_1, s_2 = 1) \leq 1,$$

$$R_{10} + R_{20} \leq I(X_1, X_2; Y | s_1 = 0, s_2 = 0) = 0,$$

$$R_{10} + R_{21} \leq I(X_1, X_2; Y | s_1 = 0, s_2 = 1) \leq 1,$$

$$R_{11} + R_{20} \leq I(X_1, X_2; Y | s_1 = 1, s_2 = 0) \leq 1,$$

$$R_{11} + R_{21} \leq I(X_1, X_2; Y | s_1 = 1, s_2 = 1) \leq 1$$

for some $p(x_1)p(x_2)$

It is straightforward to see that $X_1 \sim \text{Bern}(1/2)$ and $X_2 \sim \text{Bern}(1/2)$ achieve the upper bounds, and hence the adaptive capacity region reduces to the set of rate quadruples $(R_{10}, R_{11}, R_{20}, R_{21})$ satisfying

$$R_{10} = R_{20} = 0, R_{11} \leq 1, R_{21} \leq 1$$

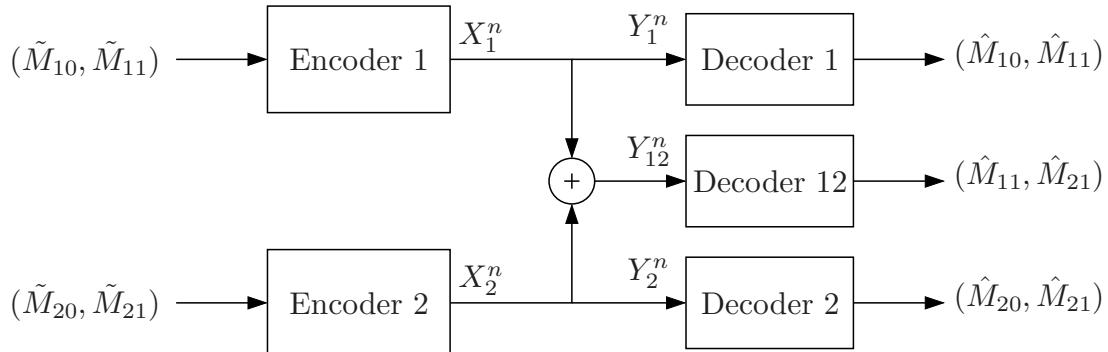
$$R_{10} + R_{20} = 0, R_{10} + R_{21} \leq 1, R_{11} + R_{20} \leq 1,$$

$$R_{11} + R_{21} \leq 1$$

Since $R_{10} = R_{20} = 0$ and $R_{11} = 1 - R_{21}$, the average adaptive sum-capacity is $p(1-p)(R_{10} + R_{21}) + p(1-p)(R_{11} + R_{20}) + p^2(R_{11} + R_{21}) = p(R_{11} + R_{21}) = p$

Therefore, allowing rate adaptation can greatly increase the average sum-rate

- Broadcast channel approach: As in the single-user Gaussian fading channel, each sender can superimpose additional information to be decoded when the channel condition is more favorable. As depicted in the following figure, the message pair $(\tilde{M}_{j0}, \tilde{M}_{j1})$ from the active sender j is to be decoded when there is no collision, while the message pair $(\tilde{M}_{11}, \tilde{M}_{21})$, one from each sender is to be decoded when there is collision



It can be shown that the capacity region of this 2-sender 3-receiver channel is the set of rate quadruples $(\tilde{R}_{10}, \tilde{R}_{11}, \tilde{R}_{20}, \tilde{R}_{21})$ such that

$$\tilde{R}_{10} + \tilde{R}_{11} \leq 1,$$

$$\tilde{R}_{20} + \tilde{R}_{21} \leq 1,$$

$$\tilde{R}_{10} + \tilde{R}_{11} + \tilde{R}_{21} \leq 1,$$

$$\tilde{R}_{20} + \tilde{R}_{11} + \tilde{R}_{21} \leq 1$$

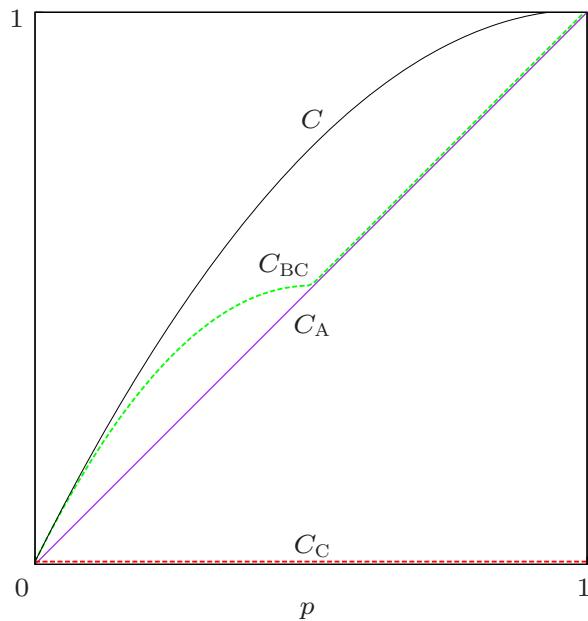
Hence, the average sum capacity is

$$C_{\text{sp}} = \max(p(1-p)(\tilde{R}_{10} + \tilde{R}_{11}) + p(1-p)(\tilde{R}_{20} + \tilde{R}_{21}) + p^2(\tilde{R}_{11} + \tilde{R}_{21})),$$

where the maximum is over rate quadruples in the capacity region. By symmetry, it can be readily checked that

$$C_{\text{sp}} = \max\{2p(1-p), p\}$$

- Note that the ergodic sum capacity for this channel is $1 - (1-p)^2$ for both the case when the encoders know both states and the case when each encoder knows its own state only
- The following figure compares the sum capacities C_C (compound channel capacity), C_A (adaptive coding capacity), C_{BC} (broadcasting capacity), and C (ergodic capacity) for different values of $p \in (0, 1)$



The broadcast channel approach is better than the adaptive coding approach when the senders are active less often

Key New Ideas and Techniques

- Asynchronous communication model
- Capacity region without synchronization
- Open problem: What is the capacity region of the asynchronous DM-MAC when $d = \alpha n$ for $\alpha \in (0, 1)$

References

- [1] T. M. Cover, R. J. McEliece, and E. C. Posner, "Asynchronous multiple-access channel capacity," *IEEE Trans. Inf. Theory*, vol. 27, no. 4, pp. 409–413, 1981.
- [2] J. Y. N. Hui and P. A. Humblet, "The capacity region of the totally asynchronous multiple-access channel," *IEEE Trans. Inf. Theory*, vol. 31, no. 2, pp. 207–216, Mar. 1985.
- [3] P. Minero, M. Franceschetti, and D. N. C. Tse, "Random access: An information-theoretic perspective," 2009.
- [4] C.-S. Hwang, M. Malkin, A. El Gamal, and J. M. Cioffi, "Multiple-access channels with distributed channel state information," in *Proc. IEEE International Symposium on Information Theory*, Nice, France, June 2007, pp. 1561–1565.
- [5] S. Meyn and R. L. Tweedie, *Markov Chains and Stochastic Stability*, 2nd ed. Cambridge: Cambridge University Press, 2009.
- [6] G. H. Hardy, *Divergent Series*, 2nd ed. New York: American Mathematical Society, 1992.

Appendix: Proof of Lemma 1

- The backlog $Q(i)$ is a time-variant Markov process with the following transition law:

$$Q(i+1) = \begin{cases} Q(i) - nR + A(i) & \text{if } i = jn \text{ and } Q(i) \geq nR, \\ Q(i) + A(i) & \text{otherwise} \end{cases}$$

- We first prove the converse (necessity of $\lambda \leq R$). From the above transition law,

$$Q(i+1) \geq \begin{cases} Q(i) - nR + A(i) & \text{if } i = jn, \\ Q(i) + A(i) & \text{otherwise} \end{cases}$$

Hence, by summing over i , we have

$$Q(jn+1) \geq \sum_{i=1}^{jn} A(i) - jnR$$

By taking expectation on both sides and using the stability condition,

$$\infty > B \geq E(Q(jn+1)) \geq jn(\lambda - R)$$

for $j = 1, 2, \dots$, which implies that $R \geq \lambda$

- Next, we prove the sufficiency of $\lambda < R$ using an elementary form of Foster–Lyapunov techniques [5]

- Let $\tilde{Q}_j = Q((j-1)n+1)$ for $j = 1, 2, \dots$ and $\tilde{A}_j = \sum_{i=(j-1)n+1}^{jn} A(i)$. Then, from the queue transition law,

$$\begin{aligned} \tilde{Q}_{j+1} &= \begin{cases} \tilde{Q}_j - nR + \tilde{A}_j & \text{if } \tilde{Q}_j \geq nR, \\ \tilde{Q}_j + \tilde{A}_j & \text{otherwise} \end{cases} \\ &\leq \max\{\tilde{Q}_j - nR, nR\} + \tilde{A}_j \\ &= \max\{\tilde{Q}_j - 2nR, 0\} + \tilde{A}_j + nR \end{aligned}$$

Since $(\max\{\tilde{Q}_j - 2nR, 0\})^2 \leq (\tilde{Q}_j - 2nR)^2$,

$$\tilde{Q}_{j+1}^2 \leq \tilde{Q}_j^2 + (2nR)^2 + (\tilde{A}_j + nR)^2 - 2\tilde{Q}_j(nR - \tilde{A}_j)$$

By taking expectation on both sides and noting the independence of \tilde{Q}_j and \tilde{A}_j , that $E(\tilde{A}_j) = n\lambda$, and that $E((\tilde{A}_j + nR)^2) \leq n^2(k + R)^2$,

$$E(\tilde{Q}_{j+1}^2) \leq E(\tilde{Q}_j^2) + n^2((k + R)^2 + 4R^2) - 2n(R - \lambda) E(\tilde{Q}_j),$$

or equivalently,

$$E(\tilde{Q}_j) \leq \frac{n((k + R)^2 + 4R^2)}{2(R - \lambda)} + \frac{E(\tilde{Q}_j^2) - E(\tilde{Q}_{j+1}^2)}{2n(R - \lambda)}$$

Summing over j and telescoping, we have

$$\begin{aligned}\frac{1}{b} \sum_{j=1}^b \mathbb{E}(\tilde{Q}_j) &\leq \frac{n((k+R)^2 + 4R^2)}{2(R-\lambda)} + \frac{\mathbb{E}(\tilde{Q}_1^2) - \mathbb{E}(\tilde{Q}_{b+1}^2)}{2nb(R-\lambda)} \\ &\leq \frac{n((k+R)^2 + 4R^2)}{2(R-\lambda)},\end{aligned}$$

since $\tilde{Q}_1 = 0$

Recall the definition of $\tilde{Q}_j = Q((j-1)n+1)$ and note that $Q(i) \leq Q((j-1)n+1) + kn$ for $i \in [(j-1)n+1 : jn]$. Therefore, we have the *stability in the mean*, that is,

$$\sup_l \frac{1}{l} \sum_{i=1}^l \mathbb{E}(Q(i)) \leq B < \infty$$

- To prove the stability $\sup_i \mathbb{E}(Q(i)) < \infty$ (which is a stronger notion than the stability in the mean), 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 (why?). Hence, the chain has a unique limiting distribution and $\mathbb{E}(\tilde{Q}_j)$ converges to a limit [5]

But by the Cesaro mean lemma [6], $(1/b) \sum_{j=1}^b \mathbb{E}(\tilde{Q}_j) < \infty$ for all b implies that $\lim_j \mathbb{E}(\tilde{Q}_j) < \infty$. Thus, $\sup \mathbb{E}(\tilde{Q}_j) < \infty$ (since $\mathbb{E}(\tilde{Q}_j) < \infty$ for all j)

Finally, using the same argument as before, we can conclude that $\sup_i \mathbb{E}(Q(i)) < \infty$, establishing the stability

Appendix: Proof of Lemma 2

- Without loss of generality, assume that $d_1 = 0$. First consider the case $\tilde{d} \geq k$ (indices for the underlying k -sequences do not overlap). Then $(X_1, Y_{\tilde{d}+1}), (X_2, Y_{\tilde{d}+2}), \dots$ are i.i.d. with $(X_i, Y_{\tilde{d}+i}) \sim p_X(x_i)p_Y(y_{\tilde{d}+i})$. Hence, by the joint typicality lemma,

$$\mathbb{P}\{(X^k(0), \tilde{Y}_{\tilde{d}+1}^{\tilde{d}+k}) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\} \leq 2^{-k(I(X;Y) - \delta(\epsilon))}$$

- Next consider the case $\tilde{d} \in [1, k-1]$. Then $X^k(0)$ and $\tilde{Y}_{\tilde{d}+1}^{\tilde{d}+k}$ have overlapping indices and are no longer independent of each other

Let (x, y) be such that $(1 - \epsilon)p_{X,Y}(x, y) = (1 + \delta)p_X(x)p_Y(y)$ for some $\epsilon, \delta > 0$. For such (x, y) , let $p := p_X(x)p_Y(y)$ and $q := p_{X,Y}(x, y)$

Consider

$$\pi(x, y | X^k, Y_{\tilde{d}+1}^{\tilde{d}+k}) = \frac{|\{i : (X_i, \tilde{Y}_i) = (x, y)\}|}{k} = \sum_{i=1}^k I_{\{(X_i, \tilde{Y}_i) = (x, y)\}}$$

Since $\{(X_i, \tilde{Y}_i)\}$ is stationary ergodic with $p_{X_i, \tilde{Y}_i}(x, y) = p$ for all $i \in [1 : k]$, by

the ergodic theorem

$$\begin{aligned} \mathbb{P}\{(X^k, Y_{\tilde{d}+1}^{\tilde{d}+k}) \in \mathcal{T}_\epsilon^{(n)}(X, Y)\} &\leq \mathbb{P}\{\pi(x, y | X^k, Y_{\tilde{d}+1}^{\tilde{d}+k}) \geq (1 - \epsilon)q\} \\ &= \mathbb{P}\{\pi(x, y | X^k, Y_{\tilde{d}+1}^{\tilde{d}+k}) \geq (1 + \delta)p\} \rightarrow 0 \end{aligned}$$

as $n \rightarrow \infty$, where

To show the exponential tail probability, however, we should bound

$\mathbb{P}\{\pi(x, y | X^k, \tilde{Y}_{\tilde{d}+1}^{\tilde{d}+k}) \geq (1 + \delta)p\}$ more carefully. We consider two cases:

- Suppose \tilde{d} is odd. Let $U^{k/2} := \{(X_{2i-1}, \tilde{Y}_{\tilde{d}+2i-1})\}_{i=1}^{k/2}$ 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,

$$\mathbb{P}\{\pi(x, y | U^{k/2}) \geq (1 + \delta)p\} \leq e^{-kp\delta^2/8}$$

Similarly, let $V^{k/2} := \{(X_{2i}, \tilde{Y}_{2i})\}_{i=1}^{k/2}$ be the subsequence of even indices. Then

$$\mathbb{P}\{\pi(x, y | V^{k/2}) \geq (1 + \delta)p\} \leq e^{-kp\delta^2/8}$$

Now by the union bound,

$$\begin{aligned}
& \mathsf{P}\{\pi(x, y|X^k, Y_{\tilde{d}+1}^{\tilde{d}+k}) \geq (1 + \delta)p\} \\
&= \mathsf{P}\{\pi(x, y|U^{k/2}, V^{k/2}) \geq (1 + \delta)p\} \\
&\leq \mathsf{P}\{\pi(x, y|U^{k/2}) \geq (1 + \delta)p \text{ or } \pi(x, y|V^{k/2}) \geq (1 + \delta)p\} \\
&\leq 2e^{-kp\delta^2/8}
\end{aligned}$$

- Suppose \tilde{d} is even. We can construct two i.i.d. subsequences by alternating even indices and odd indices for every \tilde{d} indices:

$$U^{k/2} = \{(X_i, Y_{\tilde{d}+i}) : i \text{ odd } \in [(2l-1)\tilde{d}+1 : 2l\tilde{d}], i \text{ even } \in [2l\tilde{d}+1 : 2(l+1)\tilde{d}]\}$$

For example, if $\tilde{d} = 2$, then

$$U^{k/2} = \{(X_i, Y_{\tilde{d}+i}) : i = 1, 4, 5, 8, 9, 12, \dots\}$$

The rest of the analysis is the same as before

Appendices

Appendix A

Convex Sets and Functions

- Recall that a set $\mathcal{R} \subseteq \mathbb{R}^d$ is called *convex* if $\mathbf{x}, \mathbf{y} \in \mathcal{R}$ implies that $\alpha\mathbf{x} + \bar{\alpha}\mathbf{y} \in \mathcal{R}$ for all $\alpha \in [0, 1]$. Thus, a convex set includes a line segment between any pair of two points in the set. Consequently, a convex set includes every *convex combination* \mathbf{x} of any finite number of elements $\mathbf{x}_1, \dots, \mathbf{x}_k$, that is,

$$\mathbf{x} = \sum_{j=1}^k \alpha_j \mathbf{x}_j$$

for some $(\alpha_1, \dots, \alpha_k)$ such that $\alpha_j \geq 0$, $j \in [1 : k]$, and $\sum_{j=1}^k \alpha_j = 1$. Thus, a convex set includes every possible “average” among any tuple of points in the set

- The convex hull of a set $\mathcal{R} \subseteq \mathbb{R}^d$ is the union of all finite convex combinations of elements in \mathcal{R} . Equivalently, the convex hull of \mathcal{R} is the smallest convex set containing \mathcal{R}

The convex closure of \mathcal{R} is the closure of the convex hull of \mathcal{R} , or equivalently, the smallest closed convex set containing \mathcal{R}

- Fenchel–Eggleston–Carathéodory Theorem* [1]: Any point in the convex closure of a connected compact set $\mathcal{R} \in \mathbb{R}^d$ can be represented as a convex combination of at most d points in \mathcal{R}
- Let \mathcal{R} be a convex set and \mathbf{x}_0 be a point on its boundary. Suppose $\mathbf{a}^T \mathbf{x} \leq \mathbf{a}^T \mathbf{x}_0$ for all $\mathbf{x} \in \mathcal{R}$ for some $\mathbf{a} \neq 0$. Then the hyperplane $\{\mathbf{y} : \mathbf{a}^T(\mathbf{y} - \mathbf{x}_0) = 0\}$ is referred to as a *supporting hyperplane* to \mathcal{R} at the point \mathbf{x}_0 . The *supporting hyperplane theorem* [1] states that at least one such hyperplane exists
- Any closed bounded convex set \mathcal{R} can be described as the intersection of closed half spaces characterized by supporting hyperplanes. This provides a condition to check if two convex sets are identical

Lemma A.1 [2]: Let $\mathcal{R} \subseteq \mathbb{R}^d$ be convex. Let $\mathcal{R}_1 \subseteq \mathcal{R}_2$ be two bounded convex subsets of \mathcal{R} , closed relative to \mathcal{R} . If every supporting hyperplane of \mathcal{R}_2 intersects with \mathcal{R}_1 , then $\mathcal{R}_1 = \mathcal{R}_2$

- Sometimes it is easier to consider supporting hyperplanes of the smaller set

Lemma A.2: Let $\mathcal{R} \subseteq \mathbb{R}^d$ be convex. Let $\mathcal{R}_1 \subseteq \mathcal{R}_2$ be two bounded convex subsets of \mathcal{R} , closed relative to \mathcal{R} . Let \mathcal{A} be a subset of boundary points of \mathcal{R}_1 such that the convex hull of \mathcal{A} includes all boundary points. If each $\mathbf{x}_0 \in \mathcal{A}$ has a unique supporting hyperplane and lies on the boundary of \mathcal{R}_2 , then $\mathcal{R}_1 = \mathcal{R}_2$

- Convex function: A real-valued function $g(\mathbf{x})$ is called *convex* if the epigraph $\{(\mathbf{x}, a) : g(\mathbf{x}) \leq a\}$ is convex for all a . If $g(\mathbf{x})$ is twice differentiable, it is convex iff

$$\nabla^2 g(\mathbf{x}) = \left(\frac{\partial^2 g(\mathbf{x})}{\partial x_i \partial x_j} \right)_{ij}$$

is positive semidefinite for all \mathbf{x}

If $-g(\mathbf{x})$ is convex, then $g(\mathbf{x})$ is called *concave*

- Examples

- Entropy: $g(\mathbf{x}) = -\sum_j x_j \log x_j$ is concave
- Log determinant: $\log |X|$ is concave on the positive definite matrices X
- Maximum: $\sup\{g_\theta\}$ of any collection of convex functions is convex

References

-
- [1] H. G. Eggleston, *Convexity*. Cambridge: Cambridge University Press, 1958.
 - [2] R. T. Rockafellar, *Convex Analysis*. Princeton, NJ: Princeton University Press, 1970.

Appendix B

Probability and Estimation

- Probability Bounds and Limits
- Functional Representation Lemma
- Mean Squared Error Estimation
- Gaussian Random Vectors

Probability Bounds and Limits

- Union of Events Bound: Let $\mathcal{E}_1, \mathcal{E}_2, \dots, \mathcal{E}_k$ be events. Then

$$P\left(\bigcup_{j=1}^k \mathcal{E}_j\right) \leq \sum_{j=1}^k P(\mathcal{E}_j)$$

- Jensen's Inequality [1]: Let $X \in \mathcal{X}$ (or \mathbb{R}) be a random variable with finite mean $E(X)$ and g be a real-valued convex function over \mathcal{X} (or \mathbb{R}) with finite expectation $E(g(X))$. Then

$$E(g(X)) \geq g(E(X))$$

- We use the following variant of the standard Chebyshev inequality [2]

Chebyshev Lemma: Let X be a random variables with finite mean $E(X)$ and variance $\text{Var}(X)$, and let $\delta > 0$. Then

$$P\{|X - E(X)| \geq \delta E(X)\} \leq \frac{\text{Var}(X)}{(\delta E(X))^2}$$

This implies that

$$\mathbb{P}\{X \leq (1 - \delta) \mathbb{E}(X)\} \leq \frac{\text{Var}(X)}{(\delta \mathbb{E}(X))^2},$$

$$\mathbb{P}\{X \geq (1 + \delta) \mathbb{E}(X)\} \leq \frac{\text{Var}(X)}{(\delta \mathbb{E}(X))^2}$$

- Chernoff Bound [3, 4]: Let X_1, X_2, \dots be a sequence of independent identically distributed (i.i.d.) $\text{Bern}(p)$ random variables and $Y_n := \sum_{i=1}^n X_i$. For $\delta > 0$,

$$\mathbb{P}\{Y_n \geq n(1 + \delta)p\} \leq e^{-np\delta^2/4}$$

- Weak Law of Large Numbers (LLN): Let X_1, X_2, \dots be a sequence of i.i.d. random variables with finite mean $\mathbb{E}(X)$ and variance, then for every $\epsilon > 0$,

$$\lim_{n \rightarrow \infty} \mathbb{P}\left\{ \left| \frac{1}{n} \sum_{i=1}^n X_i - \mathbb{E}(X) \right| \geq \epsilon \right\} = 0$$

- Dominated Convergence Theorem: Let $\{g_n(x)\}$ be a sequence of real-valued functions such that $|g_n(x)| \leq \phi(x)$ for some integrable function $\phi(x)$ (i.e., $\int \phi(x)dx < \infty$). Then

$$\int \lim_{n \rightarrow \infty} g_n(x) dx = \lim_{n \rightarrow \infty} \int g_n(x) dx$$

Functional Representation Lemma

- The following lemma shows that any conditional pmf can be represented as a function of the input and an independent random variable
- *Functional Representation Lemma* [5]: Let $(X, Y, Z) \sim p(x, y, z)$. Then, we can represent Z as a function of (Y, W) for some random variable W of cardinality $|\mathcal{W}| \leq |\mathcal{Y}|(|\mathcal{Z}| - 1) + 1$ such that W is independent of Y and $X \rightarrow (Y, Z) \rightarrow W$ form a Markov chain
- Proof:
 - It suffices to show that Z can be represented as a function of (Y, W) for some W independent of Y with $|\mathcal{W}| \leq |\mathcal{Y}|(|\mathcal{Z}| - 1) + 1$. The Markovity $X \rightarrow (Y, Z) \rightarrow W$ is guaranteed by generating X according to the conditional pmf $p(x|y, z)$, which results in the desired joint pmf $p(x, y, z)$ on (X, Y, Z)
 - We first illustrate the proof through the following example

Suppose (Y, Z) is a DBSP(p) for some $p < 1/2$, i.e., $p_{Z|Y}(0|0) = p_{Z|Y}(1|1) = 1 - p$ and $p_{Z|Y}(0|1) = p_{Z|Y}(1|0) = p$

Let $\mathcal{P} := \{F(z|y) : (y, z) \in \mathcal{Y} \times \mathcal{Z}\}$ be the set of all values the conditional cdf $F(z|y)$ takes and let W be a random variable independent of Y with cdf

$F(w)$ such that $\{F(w) : w \in \mathcal{W}\} = \mathcal{P}$ as shown in the figure below

$Z = 0$	$Z = 0$	$Z = 1$	$F_{Z Y}(z 0)$
$Z = 0$	$Z = 1$	$Z = 1$	$F_{Z Y}(z 1)$
$W = 1$	$W = 2$	$W = 3$	$F(w)$

0 p $1 - p$ 1

In this example, $\mathcal{P} = \{0, p, 1 - p, 0\}$ and W is ternary with pmf

$$p(w) = \begin{cases} p, & w = 1, \\ 1 - 2p, & w = 2, \\ p, & w = 3 \end{cases}$$

Now we can write $Z = g(Y, W)$ with

$$g(y, w) = \begin{cases} 0, & (y, w) = (0, 1) \text{ or } (0, 2) \text{ or } (1, 1), \\ 1, & (y, w) = (0, 3) \text{ or } (1, 2) \text{ or } (1, 3) \end{cases}$$

It is straightforward to see that for each $y \in \mathcal{Y}$, $Z = g(y, W) \sim F(z|y)$

- o We can easily generalize the above example to an arbitrary $p(y, z)$. Without loss of generality, assume that $\mathcal{Y} = \{1, 2, \dots, |\mathcal{Y}|\}$ and $\mathcal{Z} = \{1, 2, \dots, |\mathcal{Z}|\}$

Let $\mathcal{P} = \{F(z|y) : (y, z) \in \mathcal{Y} \times \mathcal{Z}\}$ be the set of all values $F(z|y)$ takes and define W to be a random variable independent of Y with cdf $F(w)$ taking the values in \mathcal{P} . It is easy to see that $|\mathcal{W}| = |\mathcal{P}| - 1 \leq |\mathcal{Y}|(|\mathcal{Z}| - 1) + 1$

Now consider the function

$$g(y, w) = \min\{z \in \mathcal{Z} : F(w) \leq F(z|y)\}$$

Then

$$\begin{aligned} \mathbb{P}\{g(Y, W) \leq z | Y = y\} &= \mathbb{P}\{g(y, W) \leq z | Y = y\} \\ &\stackrel{(a)}{=} \mathbb{P}\{F(W) \leq F(z|y) | Y = y\} \\ &\stackrel{(b)}{=} \mathbb{P}\{F(W) \leq F(z|y)\} \\ &\stackrel{(c)}{=} F(z|y), \end{aligned}$$

where (a) follows since $g(y, w) \leq z$ if and only if $F(w) \leq F(z|y)$, (b) follow from independence of Y and W , and (c) follows since $F(w)$ takes values in $\mathcal{P} = \{F(z|y)\}$

Hence we can write $Z = g(Y, W)$

Mean Squared Error Estimation

- Let $(X, \mathbf{Y}) \sim F(x, \mathbf{y})$. The minimum mean squared error (MMSE) estimate of X given \mathbf{Y} is a (measurable) function $\hat{x}(\mathbf{Y})$ of \mathbf{Y} that minimizes the mean squared error (MSE) $E((X - \hat{X})^2)$
- To find the MMSE estimate, note that $E(Xg(\mathbf{Y})) = E(E(X|\mathbf{Y})g(\mathbf{Y}))$ for every $g(\mathbf{Y})$. Hence, the MSE is lower bounded by

$$\begin{aligned} E((X - \hat{X})^2) &= E((X - E(X|\mathbf{Y}) + E(X|\mathbf{Y}) - \hat{X})^2) \\ &= E((X - E(X|\mathbf{Y}))^2) + E((E(X|\mathbf{Y}) - \hat{X})^2) \\ &\geq E((X - E(X|\mathbf{Y}))^2) \end{aligned}$$

Thus, the MMSE estimate of X given \mathbf{Y} is the conditional expectation $E(X|\mathbf{Y})$ and the corresponding MSE is

$$E(X - E(X|\mathbf{Y}))^2 = E(X^2) - E((E(X|\mathbf{Y}))^2) = E(\text{Var}(X|\mathbf{Y}))$$

Note that

$$\text{Var}(X) = E(\text{Var}(X|\mathbf{Y})) + \text{Var}(E(X|\mathbf{Y})),$$

- The linear MMSE estimate of X given $\mathbf{Y} = (Y_1, \dots, Y_n)$ is a linear (or affine) function $\hat{X} = \mathbf{a}^T \mathbf{Y} + b$ that minimizes the MSE

- For simplicity we first consider the case $E(X) = 0$ and $E(\mathbf{Y}) = 0$

Orthogonality Principle: The linear MMSE estimate of X given \mathbf{Y} is

$$\hat{X} = \mathbf{a}^T \mathbf{Y},$$

where \mathbf{a} is such that the estimation error $(X - \hat{X})$ is orthogonal to \mathbf{Y} , that is,

$$E((X - \mathbf{a}^T \mathbf{Y}) Y_i) = 0 \text{ for every } i \in [1 : n],$$

or equivalently,

$$\mathbf{a}^T K_{\mathbf{Y}} = K_{X\mathbf{Y}}$$

If $K_{\mathbf{Y}}$ is nonsingular, then the linear MMSE estimate is

$$\hat{X} = K_{X\mathbf{Y}} K_{\mathbf{Y}}^{-1} \mathbf{Y}$$

with corresponding MSE

$$\begin{aligned} E((X - \hat{X})^2) &\stackrel{(a)}{=} E((X - \hat{X}) X) \\ &= E(X^2) - E(K_{X\mathbf{Y}} K_{\mathbf{Y}}^{-1} \mathbf{Y} X) \\ &= K_X - K_{X\mathbf{Y}} K_{\mathbf{Y}}^{-1} K_{\mathbf{Y}X}, \end{aligned}$$

where (a) follows since $E((X - \hat{X}) \hat{X}) = 0$ by the orthogonality

- When X or \mathbf{Y} has a nonzero mean, the linear MMSE estimate is determined by finding the MMSE estimate of $X' = X - \mathbb{E}(X)$ given $\mathbf{Y}' = \mathbf{Y} - \mathbb{E}(\mathbf{Y})$ and setting $\hat{X} = \hat{X}' + \mathbb{E}(X)$. Thus, if $K_{\mathbf{Y}}$ is nonsingular, then the linear MMSE estimate of X given \mathbf{Y} is

$$\hat{X} = K_{X\mathbf{Y}}K_{\mathbf{Y}}^{-1}(\mathbf{Y} - \mathbb{E}(\mathbf{Y})) + \mathbb{E}(X)$$

with corresponding MSE

$$K_X - K_{X\mathbf{Y}}K_{\mathbf{Y}}^{-1}K_{\mathbf{Y}X}$$

- Thus, unlike the (nonlinear) MMSE estimate, the linear MMSE estimate is a function only of $\mathbb{E}(X), \mathbb{E}(\mathbf{Y}), \text{Var}(X), K_{\mathbf{Y}}, K_{X\mathbf{Y}}$
- Since the linear MMSE is in general not optimal,

$$\mathbb{E}(\text{Var}(X|\mathbf{Y})) \leq K_X - K_{X\mathbf{Y}}K_{\mathbf{Y}}^{-1}K_{\mathbf{Y}X}$$

- The following fact on matrix inversion is often useful in calculating the linear MMSE estimate:

Matrix Inversion Lemma:

$$(K_{11} - K_{12}K_{22}^{-1}K_{21})^{-1} = K_{11}^{-1} + K_{11}^{-1}K_{12}(K_{22} - K_{21}K_{11}^{-1}K_{12})^{-1}K_{21}K_{11}^{-1}$$

- Example: Let X be a signal with mean μ and variance P , which is sent over an additive noise channel as $Y_i = X + Z_i$, for $i = [1 : n]$, where the Z_i are zero mean noise with variance N uncorrelated with each other and with X . We wish to find the linear MMSE estimate \hat{X} of X given $\mathbf{Y} = (Y_1, \dots, Y_n)$. Since $K_{\mathbf{Y}} = P\mathbf{1}\mathbf{1}^T + NI$, by the matrix inversion lemma (with $K_{11} = NI$, $K_{12} = \mathbf{1}$, $K_{21} = \mathbf{1}^T$, $K_{22} = -1/P$),

$$K_{\mathbf{Y}}^{-1} = \frac{1}{N}I - \frac{P}{N(nP + N)}\mathbf{1}\mathbf{1}^T$$

Also note that $\mathbb{E}(\mathbf{Y}) = \mu\mathbf{1}$ and $K_{X\mathbf{Y}} = P\mathbf{1}^T$. Hence, the MMSE estimate is

$$\begin{aligned}\hat{X} &= K_{X\mathbf{Y}}K_{\mathbf{Y}}^{-1}(\mathbf{Y} - \mathbb{E}(\mathbf{Y})) + \mathbb{E}(X) \\ &= \frac{P}{nP + N} \sum_{i=1}^n (Y_i - \mu) + \mu \\ &= \frac{P}{nP + N} \sum_{i=1}^n Y_i + \frac{N}{nP + N}\mu\end{aligned}$$

and the MMSE is

$$\mathbb{E}((X - \hat{X})^2) = P - K_{X\mathbf{Y}}K_{\mathbf{Y}}^{-1}K_{\mathbf{Y}X} = \frac{PN}{nP + N}$$

Gaussian Random Vectors

- Let $\mathbf{X} = (X_1, \dots, X_n)$ be a random vector with mean $\boldsymbol{\mu}$ and covariance matrix $K \succeq 0$. We say that (X_1, \dots, X_n) is *jointly Gaussian* and \mathbf{X} is a *Gaussian random vector* if every linear combination $\mathbf{a}^T \mathbf{X}$ is a Gaussian random variable. If $K \succ 0$, then the joint pdf is well-defined as

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

- A Gaussian random vector $\mathbf{X} = (X_1, \dots, X_n)$ satisfies the following properties:

- If X_1, \dots, X_n are uncorrelated (i.e., K is diagonal), then X_1, \dots, X_n are independent
This can be verified by substituting $K_{ij} = 0$ for all $i \neq j$ in the joint pdf
- Linear transformation of a GRV yields a GRV, i.e., given any $m \times n$ matrix A , then

$$\mathbf{Y} = A\mathbf{X} \sim N(A\boldsymbol{\mu}, AKA^T)$$

This can be verified from the characteristic function of \mathbf{Y}

- Marginals of \mathbf{X} are Gaussian, i.e., $X(\mathcal{S})$ is jointly Gaussian for any subset $\mathcal{S} \subseteq [1 : n]$

This follows from the second property

- Conditionals of \mathbf{X} are Gaussian, more specifically, if

$$\mathbf{X} = \begin{bmatrix} \mathbf{X}_1 \\ \mathbf{X}_2 \end{bmatrix} \sim N \left(\begin{bmatrix} \boldsymbol{\mu}_1 \\ \boldsymbol{\mu}_2 \end{bmatrix}, \begin{bmatrix} K_{11} & K_{12} \\ K_{21} & K_{22} \end{bmatrix} \right),$$

where $\mathbf{X}_1 = (X_1, \dots, X_k)$ and $\mathbf{X}_2 = (X_{k+1}, \dots, X_n)$, then

$$\mathbf{X}_2 \mid \{\mathbf{X}_1 = \mathbf{x}\} \sim N(K_{21}K_{11}^{-1}(\mathbf{x} - \boldsymbol{\mu}_1) + \boldsymbol{\mu}_2, K_{22} - K_{21}K_{11}^{-1}K_{12})$$

This follows from the above properties of Gaussian random vectors

- Remark: The last property implies that if (X, \mathbf{Y}) are jointly Gaussian, then the MMSE estimate of X given \mathbf{Y} is linear

Since uncorrelation implies independence for Gaussian random vectors, the error $(X - \hat{X})$ of the MMSE estimate and the observation \hat{Y} are independent

References

- [1] J. L. W. V. Jensen, "Sur les fonctions convexes et les inégalités entre les valeurs moyennes," *Acta Math.*, vol. 30, no. 1, pp. 175–193, 1906.
- [2] G. H. Hardy, J. E. Littlewood, and G. Pólya, *Inequalities*, 2nd ed. Cambridge: Cambridge University Press, 1952.
- [3] H. Chernoff, "A measure of asymptotic efficiency for tests of a hypothesis based on the sum of observations," *Ann. Math. Statistics*, vol. 23, pp. 493–507, 1952.
- [4] W. Hoeffding, "Probability inequalities for sums of bounded random variables," *J. Amer. Statist. Assoc.*, vol. 58, pp. 13–30, 1963.
- [5] F. M. J. Willems and E. C. van der Meulen, "The discrete memoryless multiple-access channel with cribbing encoders," *IEEE Trans. Inf. Theory*, vol. 31, no. 3, pp. 313–327, 1985.

Appendix C

Cardinality Bounding Techniques

- Here we introduce a general technique [1] for bounding the cardinalities of auxiliary random variables.
- We use the following lemma, which is a direct consequence of Fenchel–Eggleston–Carathéodory Theorem in Appendix A:

Lemma: Let \mathcal{X} be a finite set and \mathcal{U} be an arbitrary set. Let $\mathcal{P}(\mathcal{X})$ be the set of pmfs on \mathcal{X} and $p(x|u)$ be a collection of conditional pmfs on \mathcal{X} for every $u \in \mathcal{U}$. Let g_j , $j = 1, \dots, d$, be real-valued continuous functions on $\mathcal{P}(\mathcal{X})$. Then for every $U \sim F(u)$ defined on \mathcal{U} , there exist a random variable $U' \sim p(u')$ with cardinality $|\mathcal{U}'| \leq d$ and a collection of conditional pmfs $p(x|u')$ on \mathcal{X} for every $u' \in \mathcal{U}'$ such that for $j = 1, \dots, d$,

$$\int_{\mathcal{U}} g_j(p_{X|U}(x|u)) dF(u) = \sum_{u'} g_j(p_{X|U'}(x|u')) p(u')$$

- To be concrete, we focus on bounding the cardinality of the auxiliary random

variable U in the characterization of the capacity region of the degraded DM-BC $(\mathcal{X}, p(y_1, y_2|x), \mathcal{Y}_1 \times \mathcal{Y}_2)$

Let $\mathcal{R}(U, X)$ be the set of rate pairs (R_1, R_2) such that $R_1 \leq I(X; Y_1|U)$, $R_2 \leq I(U; Y_2)$ for some $(U, X) \sim p(u, x)$, with U taking values in an arbitrary finite set \mathcal{U} . Recall that the capacity region is the union of $\mathcal{R}(U, X)$ over all (U, X)

We use the above lemma to show that given any (U, X) there exists (U', X) with $|\mathcal{U}'| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\} + 1$ such that $\mathcal{R}(U, X) = \mathcal{R}(U', X)$, which implies that it suffices to consider the auxiliary random variable U with the same cardinality bound

- We first show that it suffices to take $|\mathcal{U}| \leq |\mathcal{X}| + 1$. Without loss of generality, assume that $\mathcal{X} = \{1, 2, \dots, |\mathcal{X}|\}$

Given $(U, X) \sim p(u)p(x|u)$, consider the following $|\mathcal{X}| + 1$ continuous functions of $p(x|u)$:

$$g_j(p_{X|U}(x|u)) = \begin{cases} p_{X|U}(j|u), & j = 1, \dots, |\mathcal{X}| - 1, \\ H(Y_1|U = u), & j = |\mathcal{X}|, \\ H(Y_2|U = u), & j = |\mathcal{X}| + 1 \end{cases}$$

The first $|\mathcal{X}| - 1$ functions are conditional probabilities $\mathbb{P}\{X = j|U = u\}$, each of which is a continuous function of the conditional pmf $p(x|u)$. The last two functions are also continuous in $p(x|u)$ by continuity of entropy function and linearity of $p(y_1|u) = \sum_x p(y_1|x)p(x|u)$ and $p(y_2|u) = \sum_x p(y_2|x)p(x|u)$ in $p(x|u)$

Now from the lemma, we can find a random variable U' taking at most $|\mathcal{X}| + 1$ values such that

$$H(Y_1|U) = \int_{\mathcal{U}} H(Y_1|U = u)dF(u) = \sum_{u'} H(Y_1|U' = u')p(u') = H(Y_1|U'),$$

$$H(Y_2|U) = \int_{\mathcal{U}} H(Y_2|U = u)dF(u) = \sum_{u'} H(Y_2|U' = u')p(u') = H(Y_2|U'),$$

$$\int_{\mathcal{U}} p_{X|U}(x|u)dF(u) = p(x) = \sum_{u'} [p_{X|U'}(x|u')]$$

for $x = 1, 2, \dots, |\mathcal{X}| - 1$, and hence for $x = |\mathcal{X}|$

Since $p(x)$ determines $p(x, y_1) = p(x)p(y_1|x)$ and $p(y_2) = \sum_x p(x)p(y_2|x)$, and hence $H(Y_1|X_1)$ and $H(Y_2)$, we have

$$I(X; Y_1|U) = H(Y_1|U) - H(Y_1|X) = H(Y_1|U') - H(Y_1|X) = I(X; Y_1|U')$$

$$I(U; Y_2) = H(Y_2) - H(Y_2|U) = H(Y_2) - H(Y_2|U') = I(U'; Y_2)$$

Thus we have shown that $\mathcal{R}(U, X) = \mathcal{R}(U', X)$ for some U' with $|\mathcal{U}'| \leq |\mathcal{X}| + 1$

- o Now we derive the bound $|\mathcal{U}'| \leq |\mathcal{Y}_2| + 1$. Again assume that $\mathcal{Y}_2 = \{1, 2, \dots, |\mathcal{Y}_2|\}$

Consider the following $|\mathcal{Y}_2|$ continuous functions of $p(x|u)$:

$$g_j(p(x|u)) = \begin{cases} p_{Y_2|U}(j|u), & j = 1, \dots, |\mathcal{Y}_2| - 1, \\ H(Y_2|U = u), & j = |\mathcal{Y}_2|, \\ I(X; Y_1|U = u), & j = |\mathcal{Y}_2| + 1 \end{cases}$$

Again from the lemma, there exists U' (in general different from the one above) with $|\mathcal{U}'| \leq |\mathcal{Y}_2| + 1$ such that $p(y_2) = \mathbb{E}_{U'}[p_{Y_2|U}(y_2|U')]$, and $H(Y_2|U')$, $I(X; Y_1|U')$, and $H(Y_2)$ stay the same as with the original U . Hence $\mathcal{R}(U, X) = \mathcal{R}(U', X)$

- o We can show that $\mathcal{R}(U, X) = \mathcal{R}(U', X)$ for some U' with $|\mathcal{U}'| \leq |\mathcal{Y}_1| + 1$ in the exactly same manner, but by fixing $p(y_1)$ instead of $p(y_2)$. The physical degradedness of the channel guarantees that $p(y_1)$ determines $H(Y_2)$
- o Combining the above three steps, we have shown that for every U there exists a U' with $|\mathcal{U}'| \leq \min\{|\mathcal{X}|, |\mathcal{Y}_1|, |\mathcal{Y}_2|\} + 1$ and $\mathcal{R}(U, X) = \mathcal{R}(U', X)$. This establishes the desired cardinality bound on U

- This technique can be extended to give cardinality bounds for capacity regions with two or more auxiliary random variables [2, 3]

As an example, consider the 3-receiver degraded DM-BC $p(y_1, y_2, y_3|x)$. The capacity region is the set of rate triples (R_1, R_2, R_3) such that

$$R_1 \leq I(X; Y_1|V),$$

$$R_2 \leq I(V; Y_2|U),$$

$$R_3 \leq I(U; Y_3)$$

for some $p(u)p(v|u)p(x|v)$

We show that it suffices to take $|\mathcal{U}| \leq |\mathcal{X}| + 2$ and $|\mathcal{V}| \leq (|\mathcal{X}| + 1)(|\mathcal{X}| + 2)$

- First consider the $|\mathcal{X}| + 2$ continuous functions of $p(v|u)$:

$$p(x|u),$$

$$I(X; Y_1|V, U = u) = I(X; Y_1|U = u) - I(V; Y_1|U = u),$$

$$I(V; Y_2|U = u),$$

$$H(Y_3|U = u)$$

As in the 2-receiver DM-BC example (the bound $|\mathcal{U}| \leq |\mathcal{Y}_2| + 1$), there exists U' with $|\mathcal{U}'| \leq |\mathcal{X}| + 2$ such that $p(x)$, $I(X; Y_1|V) = I(X; Y_1|V, U)$,

$I(V; Y_2|U)$, $I(U; Y_3)$ are preserved. Let V' denote the corresponding random variable

- Now for each $u' \in |\mathcal{U}'|$, consider $|\mathcal{X}| + 1$ continuous functions of $p(x|v', u')$: $p(x|v', u')$, $I(V'; Y_1|U' = u')$, $H(Y_2|V = v', U' = u')$. Then as in the 2-receiver DM-BC example (the bound $|\mathcal{U}| \leq |\mathcal{X}| + 1$), for each u' , there exists $V''|\{U' = u'\} \sim p(v''|u')$ such that the support of $p(v''|u')$ is $\leq |\mathcal{X}| + 1$ and that $p(x|u')$, $I(X; Y_1|V', U' = u')$, $I(V'; Y_2|U' = u')$ are preserved
- By relabeling the support of $p(v''|u')$ for each $u' \in \mathcal{U}'$ and redefining $p(x|v'', u')$ accordingly, we can construct (U', V'') with $|\mathcal{U}'| \leq |\mathcal{X}| + 2$ and $|\mathcal{V}''| \leq |\mathcal{X}| + 1$ with all three mutual information terms same as before
However, this choice does not satisfy the Markov condition $U' \rightarrow V'' \rightarrow X$ in general!
- Instead, we use $V''' = (U', V'')$ (without relabeling). Then $|\mathcal{V}'''| \leq |\mathcal{U}'| \cdot |\mathcal{V}''| \leq (|\mathcal{X}| + 1)(|\mathcal{X}| + 2)$ and $U' \rightarrow V''' \rightarrow X \rightarrow (Y_1, Y_2, Y_3)$

form a Markov chain. Furthermore,

$$\begin{aligned}
I(X; Y_1 | V''') &= I(X; Y_1 | U') - I(V'''; Y_1 | U') \\
&= I(X; Y_1 | U') - I(V''; Y_1 | U') \\
&= I(X; Y_1 | U') - I(V'; Y_1 | U') \\
&= I(X; Y_1 | U) - I(V; Y_1 | U) \\
&= I(X; Y_1 | V)
\end{aligned}$$

Similarly

$$\begin{aligned}
I(V''; Y_2 | U') &= I(V''; Y_2 | U') = I(V'; Y_2 | U') = I(V; Y_2 | U), \\
I(U'; Y_3) &= I(U; Y_3)
\end{aligned}$$

This completes the proof of cardinality bound

- Remarks:

- We can apply the same technique to bound the cardinality of the time-sharing random variable Q appearing in the characterization of the DM-MAC capacity region. Recall that the capacity region of the DM-MAC is the set of rate pairs

(R_1, R_2) such that

$$\begin{aligned}
R_1 &\leq I(X_1; Y | X_2, Q), \\
R_2 &\leq I(X_2; Y | X_1, Q), \\
R_1 + R_2 &\leq I(X_1, X_2; Y | Q)
\end{aligned}$$

for some $p(q)p(x_1|q)p(x_2|q)$

By considering the three continuous functions of $p(x_1|q)p(x_2|q)$:

$$\begin{aligned}
g_1(p(x_1|q)p(x_2|q)) &= I(X_1; Y | X_2, Q = q), \\
g_2(p(x_1|q)p(x_2|q)) &= I(X_2; Y | X_1, Q = q), \\
g_3(p(x_1|q)p(x_2|q)) &= I(X_1, X_2; Y | Q = q),
\end{aligned}$$

we can easily establish the cardinality bound $|Q| \leq 3$. Although this is weaker than the bound $|Q| \leq 2$ given in Lecture Notes 4, the technique described here can be easily extended to other scenarios we encounter throughout the course

- This technique, however, does not provide cardinality bounds for all capacity/rate-distortion regions. Most notably, cardinality bounds for U_0, U_1, U_2 in the Marton inner bound have been recently proved based on a perturbation method

- Perturbation method [4, 5]: To be concrete, we consider the maximum sum rate for the Marton inner bound (Lecture Notes 9)

$$\max_{p(u_1, u_2), x(u_1, u_2)} I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2)$$

and show that it suffices to take $|\mathcal{U}_1|, |\mathcal{U}_2| \leq |\mathcal{X}|$

- Let $(U_1, U_2, X) \sim p(u_1, u_2, x)$ achieve the maximum above and let $(U'_1, U'_2, X') \sim p_\epsilon(u'_1, u'_2, x') = p_{U_1, U_2, X}(u'_1, u'_2, x')(1 + \epsilon\phi(u'_1))$ be its perturbed version. We assume that $1 + \epsilon\phi(u_1) \geq 0$ for all u_1 and $E(\phi(U_1)) = \sum_{u_1} p(u_1)\phi(u_1) = 0$, so that $p_\epsilon(u'_1, u'_2, x')$ is a valid pmf
- We further assume that

$$E(\phi(U_1)|X = x) = \sum_{u_1, u_2} p(u_1, u_2|x)\phi(u_1) = 0$$

for all $x \in \mathcal{X}$, which implies that $p(x') = p_X(x')$. In other words, the perturbation keeps the pmf of X and hence that of (Y_1, Y_2) unchanged. Observe that this condition can be satisfied with a nonzero $\phi(u_1)$ as long as $|\mathcal{U}_1| \geq |\mathcal{X}| + 1$ (why?)

Note that X' continues to be a function of U'_1, U'_2 since $p_{U_1, U_2, X}(u'_1, u'_2, x') = 0$ implies $p_\epsilon(u'_1, u'_2, x') = 0$

- Now consider

$$\begin{aligned} & I(U'_1; Y'_1) + I(U'_2; Y'_2) - I(U'_1; U'_2) \\ &= H(Y'_1) + H(Y'_2) + H(U'_1, U'_2) - H(U'_1, Y'_1) - H(U'_2, Y'_2) \\ &= H(Y_1) + H(Y_2) + H(U'_1, U'_2) - H(U'_1, Y'_1) - H(U'_2, Y'_2) \\ &= H(Y_1) + H(Y_2) + H(U_1, U_2) - H(U_1, Y_1) \\ &\quad + \epsilon H_\phi(U_1, U_2) - \epsilon H_\phi(U_1, Y_1) - H(U'_2, Y'_2), \end{aligned}$$

where $H_\phi(U_1, U_2) = -\sum_{u_1, u_2} p(u_1, u_2)\phi(u_1) \log p(u_1, u_2)$ and $H_\phi(U_1, Y_1) = -\sum_{u_1, y_1} p(u_1, y_1)\phi(u_1) \log p(u_1, y_1)$. Since $p(u_1, u_2, x)$ achieves the maximum,

$$\frac{\partial^2}{\partial \epsilon^2} I(U'_1; Y'_1) + I(U'_2; Y'_2) - I(U'_1; U'_2) = -\frac{\partial^2}{\partial \epsilon^2} I(U'_2; Y'_2) \leq 0,$$

which implies that $E[E(\phi(U_1)|U_2, Y_2)^2] \leq 0$. In particular, $E(\phi(U_1)|U_2, Y_2) = 0$ whenever $p(u_2, y_2) > 0$. Hence $H(U_2, Y_2) = H(U'_2, Y'_2)$

- Using this, we have

$$\begin{aligned} & I(U'_1; Y'_1) + I(U'_2; Y'_2) - I(U'_1; U'_2) \\ &= H(Y_1) + H(Y_2) + H(U_1, U_2) - H(U_1, Y_1) - H(U_2, Y_2) \\ &\quad + \epsilon H_\phi(U_1, U_2) - \epsilon H_\phi(U_1, Y_1) \end{aligned}$$

Once again from the optimality of $p(u_1, u_2)$, we have

$$\frac{\partial}{\partial \epsilon} I(U'_1; Y'_1) + I(U'_2; Y'_2) - I(U'_1; U'_2) = H_\phi(U_1, U_2) - H_\phi(U_1, Y_1) = 0,$$

which, in turn, implies that

$$I(U'_1; Y'_1) + I(U'_2; Y'_2) - I(U'_1; U'_2) = I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2),$$

that is, $(U'_1, U'_2, X') \sim p_\epsilon(u'_1, u'_2, x')$ also achieves the maximum

- o Finally, we choose the largest $\epsilon > 0$ such that $1 + \epsilon\phi(u_1) \geq 0$, i.e., $1 + \epsilon\phi(u_1^*) = 0$ for some $u_1^* \in \mathcal{U}_1$. Then $p_\epsilon(u_1^*) = 0$, i.e., $|\mathcal{U}'_1| \leq |\mathcal{U}_1| - 1$ and the maximum is still achieved

We can repeat the same argument as long as $E(\phi(U_1)|X) = 0$. Hence by induction, we can take $|\mathcal{U}'_1| \leq |\mathcal{X}|$ while preserving
 $I(U_1; Y_1) + I(U_2; Y_2) - I(U_1; U_2)$

- o Using the same argument for U_2 , we can take $|\mathcal{U}'_2| \leq |\mathcal{X}|$ as well

References

- [1] R. F. Ahlswede and J. Körner, "Source coding with side information and a converse for degraded broadcast channels," *IEEE Trans. Inf. Theory*, vol. 21, no. 6, pp. 629–637, 1975.
- [2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
- [3] C. Nair and A. El Gamal, "The capacity region of a class of three-receiver broadcast channels with degraded message sets," *IEEE Trans. Inf. Theory*, vol. 55, no. 10, pp. 4479–4493, Oct. 2009.
- [4] A. A. Gohari and V. Anantharam, "Evaluation of Marton's inner bound for the general broadcast channel," 2009, submitted to *IEEE Trans. Inf. Theory*, 2009.
- [5] V. Jog and C. Nair, "An information inequality for the BSSC channel," 2009. [Online]. Available: <http://arxiv.org/abs/0901.1492>

Appendix D

Fourier–Motzkin Elimination

- Suppose $\mathcal{R} \subseteq \mathbb{R}^d$ is the set of tuples (r_1, r_2, \dots, r_d) satisfying a finite system of linear inequalities $Ar^d \leq b^k$:

$$\begin{aligned} a_{11}r_1 + a_{12}r_2 + \dots + a_{1d}r_d &\leq b_1 \\ a_{21}r_1 + a_{22}r_2 + \dots + a_{2d}r_d &\leq b_2 \\ &\vdots \quad \leq \quad \vdots \\ a_{k1}r_1 + a_{k2}r_2 + \dots + a_{kd}r_d &\leq b_k \end{aligned}$$

Such \mathcal{R} is called a *polyhedron* (or a *polytope* if it is bounded)

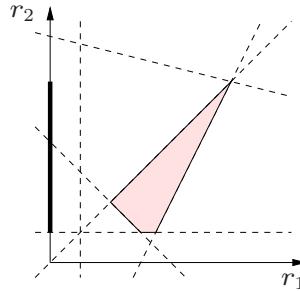
- Let $\mathcal{R}' \subseteq \mathbb{R}^{d-1}$ be the projection of \mathcal{R} on the hyperplane $\{r_1 = 0\}$ (or any hyperplane parallel to it). In other words:

1. If $(r_1, r_2, \dots, r_d) \in \mathcal{R}$, then $(r_2, \dots, r_d) \in \mathcal{R}'$
2. If $(r_2, \dots, r_d) \in \mathcal{R}'$, then there exists an r_1 such that $(r_1, r_2, \dots, r_d) \in \mathcal{R}$

Thus \mathcal{R}' captures the exact collection of inequalities satisfied by (r_2, \dots, r_d)

- Question:* How can we find the system of linear inequalities that characterize \mathcal{R}' from the original system of k inequalities for \mathcal{R} ?
- The Fourier–Motzkin elimination (see, e.g., [1]) gives a systematic procedure to finding the system of linear inequalities in (r_2, \dots, r_d)
- As an example, consider the system of inequalities given by

$$\begin{aligned} -r_1 &\leq -1 \\ -2r_2 &\leq -1 \\ -r_1 + r_2 &\leq 0 \\ -r_1 - r_2 &\leq -2 \\ +r_1 + 4r_2 &\leq 15 \\ +2r_1 - r_2 &\leq 3 \end{aligned}$$



Note that $r_2 \in \mathcal{R}'$ if and only if there exists r_1 (for given r_2) that satisfies all inequalities, which in turn happens if and only if every lower bound on r_1 is \leq every upper bound on r_1 . Hence, the sufficient and necessary condition for $r_2 \in \mathcal{R}'$ becomes

$$\max\{1, r_2, 2 - r_2\} \leq \min\{(r_2 + 3)/2, 15 - 4r_2\}$$

(6 inequalities total) as well as the inequality $-2r_2 \leq -1$ in the original system that does not involve r_1

Solving for r_2 and removing redundant inequalities, it can be easily checked that $\mathcal{R}' = \{r_2 : 1/2 \leq r_2 \leq 3\}$

- Now the extension of this method to the d -dimensional case is straightforward:
 - Write the system of inequalities into three categories: 1) the ones without r_1 , i.e., $a_{j1} = 0$, 2) upper bounds on r_1 , i.e., $a_{j1} > 0$, 3) lower bounds on r_1 , i.e., $a_{j1} < 0$. Here each upper or lower bound is an affine equation in (r_2, \dots, r_d)
 - The first category is copied verbatim for \mathcal{R}' as inequalities in (r_2, \dots, r_d)
 - Then we generate a new system of inequalities by writing each lower bound \leq each upper bound

Thus we have a new system of inequalities in (r_2, \dots, r_d)

- Remarks:
 - The number of inequalities can increase rapidly—in the worst case, there can be $k^2/4$ inequalities generated from original k inequalities. Some inequalities can be inactive (i.e., redundant)
 - We can project to an arbitrary hyperplane by taking an affine transformation of variables
 - We can eliminate multiple variables by applying the method successively
 - This method can be applied to “symbolic” inequalities as well. In this case, we can consider $(r_1, \dots, r_d, b_1, \dots, b_k)$ as the set of variables and eliminate unnecessary variables among r_1, \dots, r_d . In particular, if the constants b_1, \dots, b_k are information quantities, inequality relations among them can be further incorporated to remove inactive inequalities (see [2] for an example)
 - The Fourier–Motzkin procedure can be performed easily by computer programs such as PORTA [3]

Example: Han–Kobayashi Inner Bound

- Suppose we wish to eliminate R_{01} and R_{02} in the system of inequalities:

$$\begin{aligned} R_1 - R_{01} &\leq I_1, \\ R_1 &\leq I_2, \\ R_1 - R_{01} + R_{02} &\leq I_3, \\ R_1 + R_{02} &\leq I_4, \\ R_2 - R_{02} &\leq I_5, \\ R_2 &\leq I_6, \\ R_2 - R_{02} + R_{01} &\leq I_7, \\ R_2 + R_{01} &\leq I_8, \end{aligned}$$

- Step 1 (elimination of R_{01})

We have two upper bounds on R_{01} :

$$\begin{aligned} R_{01} &\leq I_7 - R_2 + R_{02}, \\ R_{01} &\leq I_8 - R_2 \end{aligned}$$

and two lower bounds on R_{01} :

$$\begin{aligned} R_{01} &\geq R_1 - I_1, \\ R_{01} &\geq R_1 + R_{02} - I_3 \end{aligned}$$

Comparing upper and lower bounds, and copying four inequalities in the original system that do not involve R_{01} , we obtain a new system of inequalities in (R_{02}, R_1, R_2) given by

$$\begin{aligned} R_1 &\leq I_2, \\ R_1 + R_{02} &\leq I_4, \\ R_2 - R_{02} &\leq I_5, \\ R_2 &\leq I_6, \\ R_1 + R_2 - R_{02} &\leq I_1 + I_7, \\ R_1 + R_2 &\leq I_1 + I_8, \\ R_1 + R_2 &\leq I_3 + I_7, \\ R_1 + R_2 + R_{02} &\leq I_3 + I_8 \end{aligned}$$

Noting that none of these 8 inequalities is redundant, we move on to eliminate R_{02} from them

- Step 2 (elimination of R_{02})

Comparing upper bounds on R_{02}

$$R_{02} \leq I_4 - R_1, \quad R_{02} \leq I_3 + I_8 - R_1 - R_2$$

with lower bounds

$$R_{02} \geq R_2 - I_5, \quad R_{02} \geq R_1 + R_2 - I_1 - I_7,$$

and copying inequalities that do not involve R_{20} , we obtain

$$R_1 \leq I_2,$$

$$R_2 \leq I_6,$$

$$R_1 + R_2 \leq I_1 + I_8,$$

$$R_1 + R_2 \leq I_3 + I_7,$$

$$R_1 + R_2 \leq I_4 + I_5,$$

$$2R_1 + R_2 \leq I_1 + I_4 + I_7,$$

$$R_1 + 2R_2 \leq I_3 + I_5 + I_8,$$

$$2R_1 + 2R_2 \leq I_1 + I_3 + I_7 + I_8$$

Finally we note that the last inequality is redundant since it is implied by the third and fourth inequalities; thus we have 7 inequalities on (R_1, R_2)

References

- [1] G. M. Ziegler, *Lectures on Polytopes*. New York: Springer-Verlag, 1995.
- [2] P. Minero and Y.-H. Kim, “Correlated sources over broadcast channels,” 2009.
- [3] T. Christof and A. Löbel, “PORTA: Polyhedron representation transformation algorithm,” 2009.
[Online]. Available: <http://www.zib.de/Optimization/Software/Porta/>

Appendix E

Convex Optimization

- We review basic results in convex optimization. For details, please refer to [1]
- An optimization problem

$$\begin{aligned} & \text{minimize } g_0(\mathbf{x}) \\ & \text{subject to } g_j(\mathbf{x}) \leq 0, j \in [1 : k], \\ & \quad A\mathbf{x} = \mathbf{b} \end{aligned}$$

is *convex* if $g_j, j \in [0 : k]$ are convex. We denote by $\mathcal{D} = \{\mathbf{x} : g_j(\mathbf{x}) \leq 0, j \in [1 : k], A\mathbf{x} = \mathbf{b}\}$ the set of feasible points (domain of the optimization problem). The convex optimization problem is *feasible* if $\mathcal{D} \neq \emptyset$. The optimal value of the problem is denoted by $p^* = \inf\{g_0(\mathbf{x}) : \mathbf{x} \in \mathcal{D}\}$ (or $-\infty$ if the problem is infeasible). Any \mathbf{x} that attains the infimum is *optimal* and denoted by \mathbf{x}^*

- Examples

- Linear programming (LP):

$$\begin{aligned} & \text{minimize } \mathbf{c}^T \mathbf{x} \\ & \text{subject to } A\mathbf{x} = \mathbf{b}, \\ & \quad x_j \geq 0 \text{ for all } j \end{aligned}$$

See, for example, [2] for more details

- Differential entropy maximization under correlation constraint [3, 4]:

$$\begin{aligned} & \text{maximize } \log |K| \\ & \text{subject to } K_{j,j+k} = a_k, k \in [0 : l] \end{aligned}$$

Note that this problem is a special case of matrix determinant maximization with linear matrix inequalities (max-det) [5]

- Lagrangian dual problem: We define the *Lagrangian* associated with a feasible optimization problem

$$\begin{aligned} & \text{minimize } g_0(\mathbf{x}) \\ & \text{subject to } g_j(\mathbf{x}) \leq 0, j \in [1 : k], \\ & \quad A\mathbf{x} = \mathbf{b} \end{aligned}$$

as

$$L(\mathbf{x}, \boldsymbol{\lambda}, \boldsymbol{\nu}) = g_0(\mathbf{x}) + \sum_{j=1}^k \lambda_j g_j(\mathbf{x}) + \boldsymbol{\nu}^T (\mathbf{A}\mathbf{x} - \mathbf{b})$$

We further define the *Lagrangian dual function* (or *dual function* in short) as

$$\phi(\boldsymbol{\lambda}, \boldsymbol{\nu}) = \inf_{\mathbf{x}} L(\mathbf{x}, \boldsymbol{\lambda}, \boldsymbol{\nu})$$

It can be easily seen that for any $(\boldsymbol{\lambda}, \boldsymbol{\nu})$ with $\lambda_j \geq 0$ for all j and any feasible \mathbf{x} ,

$$\phi(\boldsymbol{\lambda}, \boldsymbol{\nu}) \leq g_0(\mathbf{x})$$

This leads to the following (Lagrange) *dual problem*:

$$\text{maximize } \phi(\boldsymbol{\lambda}, \boldsymbol{\nu})$$

$$\text{subject to } \lambda_j \geq 0, j \in [1 : k]$$

Note that $\phi(\boldsymbol{\lambda}, \boldsymbol{\nu})$ is concave, hence the dual problem is convex (regardless of whether the primal problem is convex or not). The optimal value of the dual problem is denoted by d^* and the dual optimal point is denoted by $(\boldsymbol{\lambda}^*, \boldsymbol{\nu}^*)$

The original optimization problem and its feasible set and optimal value are sometimes referred to as the primal problem, primal feasible set, and primal optimal value

- Example: Consider the LP discussed above with $\mathbf{x} = x^n$. The Lagrangian is

$$L(\mathbf{x}, \boldsymbol{\lambda}, \boldsymbol{\nu}) = \mathbf{c}^T \mathbf{x} - \sum_{j=1}^n \lambda_j x_j + \boldsymbol{\nu}^T (\mathbf{A}\mathbf{x} - \mathbf{b}) = -\mathbf{b}^T \boldsymbol{\nu} + (\mathbf{c} + \mathbf{A}^T \boldsymbol{\nu} - \boldsymbol{\lambda})^T \mathbf{x}$$

and the dual function is

$$\begin{aligned} \phi(\boldsymbol{\lambda}, \boldsymbol{\nu}) &= -\mathbf{b}^T \boldsymbol{\nu} + \inf_{\mathbf{x} \in \mathcal{D}} (\mathbf{c} + \mathbf{A}^T \boldsymbol{\nu} - \boldsymbol{\lambda})^T \mathbf{x} \\ &= \begin{cases} -\mathbf{b}^T \boldsymbol{\nu} & \text{if } \mathbf{A}^T \boldsymbol{\nu} - \boldsymbol{\lambda} + \mathbf{c} = 0, \\ -\infty & \text{otherwise} \end{cases} \end{aligned}$$

Hence, the dual problem is

$$\text{maximize } -\mathbf{b}^T \boldsymbol{\nu}$$

$$\text{subject to } \mathbf{A}^T \boldsymbol{\nu} - \boldsymbol{\lambda} + \mathbf{c} = 0,$$

$$\lambda_j \geq 0 \text{ for all } j,$$

which is another LP

- Strong duality: From the definition of the dual function and dual problem, we already know the following lower bound on the primal optimal value:

$$d^* \leq p^*$$

When the bound is tight (i.e., $d^* = p^*$), we say that *strong duality* holds. One simple condition for strong duality is as follows:

Slater's condition: If the primal problem is convex and there exists a feasible \mathbf{x} in the relative interior of \mathcal{D} , that is, $g_j(\mathbf{x}) < 0$, $j \in [1 : k]$ and $A\mathbf{x} = \mathbf{b}$, then strong duality holds

- KKT condition: If the strong duality holds (say, Slater's condition holds), then

$$\begin{aligned} g_0(\mathbf{x}^*) &= \phi(\boldsymbol{\lambda}^*, \boldsymbol{\nu}^*) \\ &\leq \inf_{\mathbf{x}} g_0(\mathbf{x}) + \sum_{j=1}^k \lambda_j^* g_j(\mathbf{x}) + (\boldsymbol{\nu}^*)^T (A\mathbf{x} - \mathbf{b}) \\ &\leq g_0(\mathbf{x}^*) + \sum_{j=1}^k \lambda_j^* g_j(\mathbf{x}^*) + (\boldsymbol{\nu}^*)^T (A\mathbf{x}^* - \mathbf{b}) \\ &\leq g_0(\mathbf{x}^*) \end{aligned}$$

Following equality conditions, we obtain the following sufficient and necessary condition (commonly referred to as the *KKT condition*) for the primal optimal point \mathbf{x}^* and dual optimal point $(\boldsymbol{\lambda}^*, \boldsymbol{\nu}^*)$:

- \mathbf{x}^* minimizes $L(\mathbf{x}, \boldsymbol{\lambda}^*, \boldsymbol{\nu}^*)$. This condition can be easily checked if $L(\mathbf{x}, \boldsymbol{\lambda}^*, \boldsymbol{\nu}^*)$ is differentiable
- Complementary slackness: $\lambda_j^* g_j(\mathbf{x}^*) = 0$, $j \in [1 : k]$
- Example: Consider the following determinant maximization problem in X :

$$\text{maximize } \log |X + K|$$

$$\text{subject to } X \succeq 0,$$

$$\text{tr}(X) \leq P,$$

where K is a given positive definite matrix

Noting that $X \succeq 0$ iff $\text{tr}(\Upsilon X) \geq 0$ for every $\Upsilon \succeq 0$, we form the Lagrangian

$$L(X, \Upsilon, \lambda) = \log |X + K| + \text{tr}(\Upsilon X) - \lambda(\text{tr}(X) - P)$$

Since the domain \mathcal{D} has nonempty interior (for example, $X = (P/2)I$ is feasible), Slater's condition is satisfied and strong duality holds. Hence the KKT condition characterizes the optimal X^* and (Υ^*, λ^*)

- X^* maximizes the Lagrangian. Since $(d/dY) \log |Y| = Y^{-1}$ for $Y \succ 0$ and $(d/dY) \text{tr}(AY) = A$ (see [1] for more details of matrix differentiation),

$$\frac{\partial}{\partial X} L(X, \Upsilon^*, \lambda^*) = (X + K)^{-1} + \Upsilon^* - \lambda I = 0$$

- Complementary slackness:

$$\begin{aligned}\text{tr}(\Upsilon^* X^*) &= 0 \\ \lambda^*(\text{tr}(X^*) - P) &= 0\end{aligned}$$

References

- [1] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge: Cambridge University Press, 2004.
- [2] D. G. Luenberger and Y. Ye, *Linear and Nonlinear Programming*, 3rd ed. New York: Springer, 2008.
- [3] J. P. Burg, "Maximum entropy spectral analysis," in *Proc. 37th Meet. Society Exploration Geophysicists*, Oklahoma City, OK, 1967, reprinted in *Modern Spectral Analysis*, D. G. Childers, Ed. New York: IEEE Press, 1978, pp. 34–41.
- [4] B. S. Choi and T. M. Cover, "An information-theoretic proof of Burg's maximum entropy spectrum," *Proc. IEEE*, vol. 72, no. 8, pp. 1094–1096, Aug. 1984.
- [5] L. Vandenberghe, S. Boyd, and S.-P. Wu, "Determinant maximization with linear matrix inequality constraints," *SIAM J. Matrix Anal. Appl.*, vol. 19, no. 2, pp. 499–533, 1998.