ABSTRACT

Title of dissertation: CAPACITY BOUNDS FOR MULTI-USER CHANNELS WITH FEEDBACK, RELAYING AND COOPERATION

Ravi Tandon
Doctor of Philosophy, 2010

Dissertation directed by: Professor Şennur Ulukuş
Department of Electrical and Computer Engineering

Recent developments in communications are driven by the goal of achieving high data rates for wireless communication devices. To achieve this goal, several new phenomena need to be investigated from an information theoretic perspective. In this dissertation, we focus on three of these phenomena: feedback, relaying and cooperation. We study these phenomena for various multi-user channels from an information theoretic point of view.

One of the aims of this dissertation is to study the performance limits of simple wireless networks, for various forms of feedback and cooperation. Consider an uplink communication system, where several users wish to transmit independent data to a base-station. If the base-station can send feedback to the users, one can expect to achieve higher data-rates since feedback can enable cooperation among the users. Another way to improve data-rates is to make use of the broadcast nature of the wireless medium, where the users can overhear each other's transmitted signals. This particular phenomenon has garnered much attention lately, where users can help

in increasing each other's data-rates by utilizing the overheard information. This overheard information can be interpreted as a generalized form of feedback.

To take these several models of feedback and cooperation into account, we study the two-user multiple access channel and the two-user interference channel with generalized feedback. For all these models, we derive new outer bounds on their capacity regions. We specialize these results for noiseless feedback, additive noisy feedback and user-cooperation models and show strict improvements over the previously known bounds.

Next, we study state-dependent channels with rate-limited state information to the receiver or to the transmitter. This state-dependent channel models a practical situation of fading, where the fade information is partially available to the receiver or to the transmitter. We derive new bounds on the capacity of such channels and obtain capacity results for a special sub-class of such channels.

We study the effect of relaying by considering the parallel relay network, also known as the diamond channel. The parallel relay network considered in this dissertation comprises of a cascade of a general broadcast channel to the relays and an orthogonal multiple access channel from the relays to the receiver. We characterize the capacity of the diamond channel, when the broadcast channel is deterministic. We also study the diamond channel with partially separated relays, and obtain capacity results when the broadcast channel is either semi-deterministic or physically degraded. Our results also demonstrate that feedback to the relays can strictly increase the capacity of the diamond channel.

In several sensor network applications, distributed lossless compression of sources

is of considerable interest. The presence of adversarial nodes makes it important to design compression schemes which serve the dual purpose of reliable source transmission to legitimate nodes while minimizing the information leakage to the adversarial nodes. Taking this constraint into account, we consider information theoretic secrecy, where our aim is to limit the information leakage to the eavesdropper. For this purpose, we study a secure source coding problem with coded side information from a helper to the legitimate user. We derive the rate-equivocation region for this problem. We show that the helper node serves the dual purpose of reducing the source transmission rate and increasing the uncertainty at the adversarial node. Next, we considered two different secure source coding models and provide the corresponding rate-equivocation regions.

Capacity Bounds For Multi-user Channels With Feedback, Relaying and Cooperation

by

Ravi Tandon

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2010

Advisory Committee:

Professor Şennur Ulukuş, Chair/Advisor
Professor Prakash Narayan
Professor Alexander Barg
Professor Nuno Martins
Professor Radu Balan

© Copyright by
Ravi Tandon
2010

DEDICATION

To my parents.

ACKNOWLEDGMENTS

I would like to thank my advisor Professor Şennur Ulukuş, without whose constant support this dissertation would not have been possible. Her avid guidance and encouragements to work on meaningful research problems have been of immense help. I am also particularly indebted to her for allowing me ample freedom to work on a variety of research problems which benefitted my learning.

I would like to thank Professors Prakash Narayan, Alexander Barg, Nuno Martins and Radu Balan for serving in my Phd dissertation committee and for their valuable suggestions. I am especially thankful to Professor Prakash Narayan and Professor Alexander Barg for organizing the information theory and coding research seminars and allowing me to present my work. I am also thankful to Professor Kannan Ramchandran for several insightful discussions during my stay at Berkeley.

I also owe a word of thanks to my friends at Communications and Signal Processing Lab (CSPL), Sirin Nitinawarat, Himanshu Tyagi, Ersen Ekrem, Osman Yağan, Beiyu Rong, Nan Liu, Wei Kang and Alkan Soysal for several helpful and cheerful discussions.

I give a special thanks to my tennis partner, Dr. Manish Shukla and many other friends, Rahul Ratan, Anuj Rawat, Rakesh Panda, Archana Anibha Shukla, Alok Singhal, Vishal Khandelwal, Abhishek Kashyap, Pavan Turaga, Srikanth Vishnubhotla and Abhinav Gupta who made my stay at Maryland wonderful.

Finally, this dissertation would not be possible without the constant unconditional love, support and encouragement of my parents and my wife, Aakriti.

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1

Introduction

Recent surge in research on multi-user information theory can be attributed to the need of understanding performance limits of sophisticated wireless communication systems. As the focus shifts towards deploying ad-hoc and sensor networks, several new issues arise that need to be addressed from an information theoretic perspective. Feedback, relaying and cooperation are among the important aspects which would inevitably arise while characterizing performance limits of such multi-terminal networks. It is, therefore, imperative to study basic building blocks of such multi-terminal networks. Unfortunately, the aspects of feedback, relaying and cooperation are not well understood from an information theory point of view even for three terminal systems. In this dissertation, we study these aspects for simple multi-terminal systems.

Study of multi-user information theory was initiated by Shannon by introducing the two-way channel (TWC) [56] in 1961. The TWC models a bidirectional communication situation where two users wish to communicate to each other. The channel is assumed to be memoryless and the users can use their previously received outputs to construct their next channel inputs. Shannon obtained inner and outer bounds for

the capacity region of a discrete memoryless TWC in [56]. Shannon's inner and outer bounds for the TWC do not match in general and determining the capacity region of the TWC remains an open problem.

One of the objectives of this dissertation is to obtain new outer bounds for multi-user channels with feedback. A general outer bound on the capacity region of multi-user channels with feedback is the cut-set outer bound [14, Theorem 14.10.1]. The cut-set outer bound allows arbitrary correlation between the channel inputs. The cut-set outer bound is not always expected to be tight since it might not always be the case that the set of rates yielded by any achievable scheme could match with the corresponding set of rates of the cut-set outer bound.

For the TWC, Shannon's outer bound and the cut-set outer bound are the same. As Shannon himself pointed out, the simplest example of a TWC for which his inner and outer bounds do not meet is the binary multiplying channel (BMC). The BMC is a single output, deterministic TWC, where, $Y_1 = Y_2 = Y = X_1X_2$. The channel inputs X_1, X_2 and the channel output Y are all binary. For the BMC, Shannon computed his inner and outer bounds for the symmetric rate point as 0.61695 and 0.69424 bits/transmission, respectively. Shannon's outer bound for BMC was improved to 0.64891 bits/transmission by Zhang, Berger and Schalkwijk [71].

The idea of dependence balance was introduced by Hekstra and Willems in [30] to obtain an outer bound for the capacity region of the single-output TWC. The basic idea behind this outer bound is to restrict the set of allowable input distributions, consequently restricting arbitrary correlation between channel inputs. A generalized version of the dependence balance bound resulted in an upper bound of 0.64628

bits/transmission for the BMC. To the best of our knowledge, this is the best known symmetric-rate upper bound for the BMC. Determining the capacity region of the BMC still remains an open problem.

An important class of multi-terminal channels is the multiple access channel (MAC) channel, where several transmitters wish to communicate with a single receiver. The classical MAC models the situation where each transmitter is unaware of the information present at other transmitters. The capacity region of the classical MAC was obtained by Ahlswede [1] and Liao [41] in 1971. In 1975, Gaarder and Wolf showed through a simple example [19] that noiseless feedback can strictly increase the capacity region of MAC. Ozarow showed in [45] that feedback can also increase the capacity region of a two-user Gaussian MAC. A constructive achievability scheme based on the classical Schalkwijk-Kailath [51] feedback scheme was shown to be optimal for the two-user Gaussian MAC. Moreover, the cut-set outer bound was shown to be tight in this case.

Subsequently, Cover and Leung obtained an achievable rate region for the general MAC with feedback (MAC-FB) based on block Markov superposition coding [13]. Even though this region is in general larger than the capacity region of the MAC without feedback, it is not optimal for the two-user Gaussian MAC-FB, as was shown in [45]. Kramer [37] used the notion of directed information to obtain an expression for the capacity region of the discrete memoryless MAC-FB. Unfortunately, this expression is in an incomputable non-single-letter form. Recently, Bross and Lapidoth [6] proposed an achievable rate region for the two-user discrete memoryless MAC-FB and showed that their region includes the Cover-Leung region, the inclusion being

strict for some channels.

For a specific class of MAC-FB, Willems [62] developed an outer bound that equals the Cover-Leung achievable rate region. For this class of MAC-FB, each channel input (say X_1) should be expressible as a deterministic function of the other channel input (X_2) and the channel output (Y). The binary erasure MAC considered by Gaarder and Wolf, where $Y = X_1 + X_2$, falls into this class of channels. Therefore, Cover-Leung region is the feedback capacity region for the binary erasure MAC.

In Chapter 2, we use the idea of dependence balance to obtain new outer bounds for the discrete memoryless MAC-FB. We evaluate our outer bounds for a particular MAC, given as, $Y = X_1 + X_2 + N$, where all X_1, X_2 and N are binary and N is uniform. This is a non-deterministic noisy MAC which does not fall into any class of channels for which the feedback capacity is known. Our outer bounds strictly improve upon the cut-set bound at all points on the boundary where feedback increases capacity. In addition, we explicitly evaluate the Cover-Leung achievable rate region [13] for this channel. The evaluation of these bounds is difficult due to an involved auxiliary random variable, whose large cardinality prohibits an exhaustive search over all input probability distributions. We overcome this difficulty by using a composite function which was first introduced in [63]. As an application of the techniques developed for these evaluations, we explicitly evaluate the capacity region of the MAC studied by Gaarder and Wolf in [19]. This result resolves an open problem mentioned in a survey paper of van der Meulen [58].

In Chapter 3, we study the model of MAC with generalized feedback (MAC-GFB) and the interference channel with generalized feedback (IC-GFB). To motivate the

study of these models, consider the model where the feedback link is noisy, i.e., feedback at the transmitters is a noisy version of Y. As another example, consider a wireless setting, where each transmitter can overhear each other's transmitted information and utilize it for achieving higher rates to the receiver. To take these various forms of feedback into account, we study the model of generalized feedback. In particular, for MAC-GFB, the channel is given by transition probability $p(y, y_{F_1}, y_{F_2}|x_1, x_2)$, where X_1, X_2 are the channel inputs and Y is the channel output at the receiver, Y_{F_1} is the feedback at transmitter 1 and Y_{F_2} is the feedback at transmitter 2. We use the idea of dependence balance to obtain new outer bounds on the capacity regions of the MAC-GFB and the IC-GFB. To show the usefulness of our outer bounds, we will consider three different specific channel models.

We first consider a Gaussian MAC with noisy feedback (MAC-NF), where transmitter k, $k = 1, 2$, receives a feedback Y_{F_k}, which is the channel output Y corrupted with additive white Gaussian noise Z_k. As the feedback noise variances $\sigma^2_{Z_k}$, $k = 1, 2$, become large, one would expect the feedback to become useless. This fact is not reflected by the cut-set outer bound. We demonstrate that our outer bound improves upon the cut-set bound for all non-zero values of the feedback noise variances. Moreover, in the limit as $\sigma^2_{Z_k} \to \infty$, $k = 1, 2$, our outer bound collapses to the capacity region of the Gaussian MAC without feedback. Secondly, we investigate a Gaussian MAC with user-cooperation (MAC-UC), where each transmitter receives an additive white Gaussian noise corrupted version of the channel input of the other transmitter [53]. For this channel model, the cut-set bound is sensitive to the cooperation noises, but not sensitive enough. For all non-zero values of cooperation noise vari-

ances, our outer bound strictly improves upon the cut-set outer bound. Moreover, as the cooperation noises become large, our outer bound collapses to the capacity region of the Gaussian MAC without cooperation. Thirdly, we investigate a Gaussian IC with user-cooperation (IC-UC). For this channel model, the cut-set bound is again sensitive to cooperation noise variances as in the case of MAC-UC channel model, but not sensitive enough. We demonstrate that our outer bound strictly improves upon the cut-set bound for all non-zero values of cooperation noise variances.

In order to evaluate our outer bounds for the Gaussian channel models, we develop a new approach to deal with capacity bounds involving auxiliary random variables. We appropriately tailor this approach according to the channel model in consideration. This allows us to obtain explicit expressions for our outer bounds and hence enables us to compare them with the corresponding cut-set bounds.

In Chapter 4, we consider state dependent channels with rate-limited channel state information (CSI) at the receiver and at the transmitter, respectively. We first consider state-dependent channels where the receiver is supplied CSI at a rate R_d. We note that this model falls in the class of relay channels [12] since the state encoder can be regarded as a relay. Also note that this problem is one of the simplest channel coding problems with a source coding constraint. Secondly, we consider the case when the transmitter is supplied CSI at a rate R_e. This model can be regarded as a generalization of the Gelfand-Pinsker problem of coding for channels with random parameters [23]. For both of these channel models, we develop new upper bounds on their capacities, $\mathcal{C}(R_d)$ and $\mathcal{C}(R_e)$, respectively. Although the problems of characterizing the capacities, $\mathcal{C}(R_d)$ and $\mathcal{C}(R_e)$ still remain open, we show that our

upper bounds are tight for all the cases where these capacities have been characterized. Furthermore, we show that our upper bound for $\mathcal{C}(R_d)$ yields a new capacity result for a particular class of state-dependent channels when the receiver is supplied CSI at a rate R_d. This result validates a conjecture due to Ahlswede and Han [2] for this class of channels. We also investigate a rate-limited version of the dirty-paper-coding (DPC) problem and show that a modified version of our upper bound for $\mathcal{C}(R_e)$ strictly improves upon Costa's DPC upper bound [9] for certain values of R_e.

In several communication scenarios, it is possible that the source and destination are not connected through a direct link and the communication must take place by the help of intermediate relay nodes. This scenario is modelled by the parallel relay network, which is also commonly referred to as the diamond channel [52]. The diamond channel comprises of a broadcast channel (BC) followed by a MAC. Even though the two ingredients of the diamond channel, i.e., the BC and the MAC have been studied intensively in the information theory literature, little is known about the resulting channel when these two channels are combined. One of the challenges in understanding this channel lies in the distributed information processing at the relays and subsequent coordination to achieve high data-rates at the destination. In Chapter 5, we consider diamond channels with a general BC $p(y, z|x)$, with outputs Z and Y at relays 1 and 2, respectively, and where the relays 1 and 2 have noiseless links of capacities R_z and R_y, respectively, to the decoder. For the case when Y and Z are deterministic functions of X, we establish the capacity. We next give an upper bound for the capacity of the class of diamond channels with a physically degraded broadcast channel, i.e., when $X \to Y \to Z$ forms a Markov chain. We show that

this upper bound is tight, if in addition to $X \to Y \to Z$, the output of relay 2, i.e., Y, is a deterministic function of X. We finally consider the diamond channel with partially separated relays, i.e., when the output of relay 2 is available at relay 1. We establish the capacity for this model in two cases, first, when the broadcast channel is physically degraded, i.e., when $X \to Y \to Z$ forms a Markov chain, and second, when the broadcast channel is semi-deterministic, i.e, when $Y = f(X)$. For both of these cases, we show that the capacity is equal to the cut-set bound. This final result shows that even partial feedback from the decoder to relays strictly increases the capacity of the diamond channel.

In Chapter 6, we shift our focus to information theoretic secrecy. We consider a secure lossless source coding problem with a rate-limited helper. In particular, Alice observes an i.i.d. source X^n and wishes to transmit this source losslessly to Bob at a rate R_x. A helper, say Helen, observes a correlated source Y^n and transmits at a rate R_y to Bob. A passive eavesdropper can observe the coded output of Alice. The equivocation Δ is measured by the conditional entropy $H(X^n|J_x)/n$, where J_x is the coded output of Alice. In this problem, the goal is to losslessly transmit the source X^n to Bob, while minimizing the information leakage to Eve. We first completely characterize the rate-equivocation region for this secure source coding model, where we show that Slepian-Wolf binning of X is optimal.

We next study two generalizations of this model and provide single-letter characterizations for the respective rate-equivocation regions. In particular, we first consider the case of a two-sided helper where Alice also has access to the coded output of Helen. We show that for this case, Slepian-Wolf binning of X is suboptimal and one

can further decrease the information leakage to the eavesdropper by utilizing the side information at Alice. In this problem, Helen can also be interpreted as a relay serving a dual purpose. Firstly, due to the presence of correlated side information at Helen, she helps in reducing the rate of transmission of Alice. Secondly, due to the secure common link from Helen to Alice and Bob, she also helps in reducing the information leakage to Eve. We finally generalize this result to the case when there are both secure and insecure rate-limited links from Helen and additional uncoded side informations W^n and Z^n are available at Bob and Eve, respectively. For this model, we provide a complete characterization of the rate-equivocation region when $Y^n \to X^n \to (W^n, Z^n)$ forms a Markov chain.

Chapter 2

Outer Bounds for Multiple Access Channels with Feedback using Dependence Balance

2.1 Introduction

Noiseless feedback can increase the capacity region of the discrete memoryless MAC, unlike for the single-user discrete memoryless channel. This was shown by Gaarder and Wolf in [19] for the binary erasure MAC, which is defined as $Y = X_1 + X_2$. Ozarow showed in [45] that feedback can also increase the capacity region of a two-user Gaussian MAC-FB. A constructive achievability scheme based on the classical Schalkwijk-Kailath [51] feedback scheme was shown to be optimal for the two-user Gaussian MAC-FB. Moreover, the cut-set outer bound was shown to be tight in this case.

Subsequently, Cover and Leung obtained an achievable rate region for the general MAC-FB based on block Markov superposition coding [13]. Even though this region is in general larger than the capacity region of the MAC without feedback, it is not optimal for the two-user Gaussian MAC-FB, as was shown in [45]. Kramer [37] used the notion of directed information to obtain an expression for the capacity

region of the discrete memoryless MAC-FB. Unfortunately, this expression is in an incomputable non-single-letter form. Recently, Bross and Lapidoth [6] proposed an achievable rate region for the two-user discrete memoryless MAC-FB and showed that their region includes the Cover-Leung region, the inclusion being strict for some channels.

For a specific class of MAC-FB, Willems [62] developed an outer bound that equals the Cover-Leung achievable rate region. For this class of MAC-FB, each channel input (say X_1) should be expressible as a deterministic function of the other channel input (X_2) and the channel output (Y). The binary erasure MAC considered by Gaarder and Wolf, where $Y = X_1 + X_2$, falls into this class of channels. Therefore, Cover-Leung region is the feedback capacity region for the binary erasure MAC.

A general outer bound for MAC-FB is the cut-set bound. Although the cut-set bound was shown to be tight for the two-user Gaussian MAC-FB, it is in general loose. An intuitive reason for the cut-set bound to be loose for the general MAC-FB is its permissibility of arbitrary input distributions, some of which yielding rates which may not be achievable. For instance, even though Cover-Leung achievability scheme introduces correlation between X_1 and X_2, it is a limited form of correlation, as the channel inputs are conditionally independent given an auxiliary random variable, whereas the cut-set bound allows all possible correlations.

The idea of dependence balance was introduced by Hekstra and Willems in [30] to obtain an outer bound on the capacity region of the single-output two-way channel. The basic idea behind this outer bound is to restrict the set of allowable input distributions, consequently restricting arbitrary correlation between channel inputs.

The authors also developed a parallel channel extension for the dependence balance bound. The parallel channel extension can be interpreted as follows: the parallel channel output can be considered as a genie aided information which is made available at both transmitters and the receiver and it also effects the set of allowable input distributions through the dependence balance bound. Depending on the choice of the genie information (which is equivalent to choosing a parallel channel), there is an inherent tradeoff between the set of allowable input distributions and the excessive mutual information rate terms which appear in the rate expressions as a consequence of the parallel channel output. We will exploit this tradeoff provided by the parallel channel extension of the dependence balance bound to obtain a strict improvement over the cut-set bound for a particular MAC whose feedback capacity is not known.

To motivate the choice of our MAC, consider the binary erasure MAC used by Gaarder and Wolf given by $Y = X_1 + X_2$. If we introduce binary additive noise at the channel output, then the channel becomes $Y = X_1 + X_2 + N$, where all X_1, X_2 and N are binary and N has a uniform distribution. This is a non-deterministic noisy MAC which does not fall into any class of channels for which the feedback capacity is known. We should mention that this particular MAC was extensively studied by Kramer in [37,39], where the first improvement over the Cover-Leung achievable rate region was obtained.

We extend the idea of dependence balance to obtain an outer bound for the entire capacity region of this binary additive noisy MAC-FB. Direct evaluation of the parallel channel based dependence balance bound is intractable due to an involved auxiliary random variable whose large cardinality prohibits an exhaustive search. We

use composite functions and their properties to obtain a simple characterization for our bound. Our outer bound strictly improves upon the cut-set bound at all points on the boundary where feedback increases capacity. In addition, we explicitly evaluate the Cover-Leung achievable rate region for our binary additive noisy MAC-FB.

We particularly focus on the symmetric-rate[1] point on the feedback capacity region of this channel. Cover-Leung's achievable symmetric-rate for this channel was obtained in [39] as 0.43621 bits/transmission. In [39], Kramer obtained an improved symmetric-rate inner bound as 0.43879 bits/transmission by using superposition coding and binning with code trees. The cut-set upper bound on the symmetric-rate was obtained in [39] as 0.45915 bits/transmission. We obtain a symmetric-rate upper bound of 0.45330 bits/transmission which strictly improves upon the cut-set bound. Furthermore, we also show that a binary and uniform selection of the involved auxiliary random variable is sufficient to obtain our symmetric-rate upper bound.

It should be remarked that the channel we consider in this chapter can be thought of as the discrete counterpart of the channel considered by Ozarow [45]. Although the cut-set bound was shown to be tight for the two-user Gaussian MAC-FB, our result shows that the cut-set bound is not tight for the discrete version of the additive noisy MAC-FB.

As an application of the properties of the composite functions developed in this chapter, we are able to obtain the entire boundary of the capacity region of the binary erasure MAC-FB. The evaluation of the asymmetric rate pairs on the boundary of

[1]By symmetric-rate point, we refer to the maximum rate R such that the rate pair (R, R) lies in the capacity region of MAC-FB.

the feedback capacity region of the binary erasure MAC was mentioned as an open problem in [61]. It was shown in [63] that a binary and uniform auxiliary random variable T is sufficient to attain the sum-rate point on the capacity region of the binary erasure MAC-FB. We show here that this is also the case for any asymmetric rate point on the boundary of the feedback capacity region. This result also complements the work of Kramer [38], where feedback strategies were developed for the binary erasure MAC-FB and it was shown that these strategies achieve all rates yielded by a binary selection of the auxiliary random variable T in the capacity region. Our result hence shows in effect that the feedback strategies developed in [38] for binary erasure MAC are optimal and capacity achieving.

2.2 System Model

A discrete memoryless two-user MAC-FB (see Figure 2.1) is defined by the following: two input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, an output alphabet $\mathcal{Y}$, and the channel defined by a probability transition function $p(y|x_1, x_2)$ for all $(x_1, x_2, y) \in \mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y}$. A (n, M_1, M_2, P_e) code for the MAC-FB consists of two sets of encoding functions f_{1i}, f_{2i} for $i = 1, \ldots, n$ and a decoding function g

$$f_{1i} : \mathcal{M}_1 \times \mathcal{Y}^{i-1} \to \mathcal{X}_1, \quad i = 1, \ldots, n$$

$$f_{2i} : \mathcal{M}_2 \times \mathcal{Y}^{i-1} \to \mathcal{X}_2, \quad i = 1, \ldots, n$$

$$g : \mathcal{Y}^n \to \mathcal{M}_1 \times \mathcal{M}_2$$

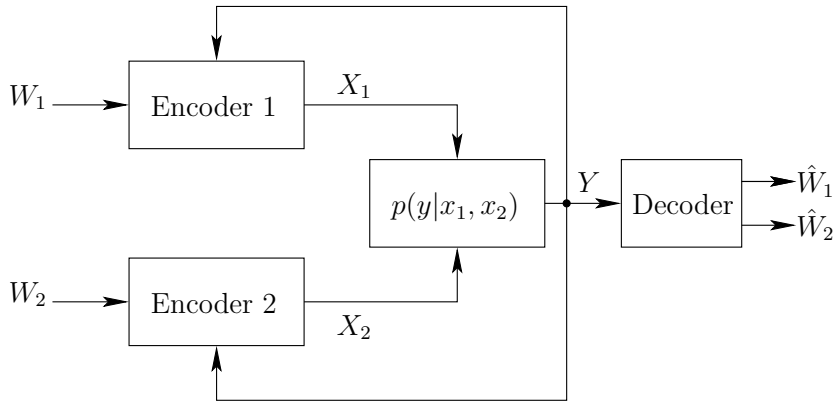

Figure 2.1: The multiple access channel with noiseless feedback (MAC-FB).

The two transmitters produce independent and uniformly distributed messages $W_1 \in \{1, \ldots, M_1\}$ and $W_2 \in \{1, \ldots, M_2\}$, respectively, and transmit them through n channel uses. The average error probability is defined as $P_e = Pr(g(Y^n) \neq (W_1, W_2))$. A rate pair (R_1, R_2) is said to be achievable for MAC-FB if for any $\epsilon \geq 0$, there exists a pair of n encoding functions $\{f_{1i}\}_{i=1}^n$, $\{f_{2i}\}_{i=1}^n$, and a decoding function g such that $R_1 \leq \log(M_1)/n$, $R_2 \leq \log(M_2)/n$ and $P_e \leq \epsilon$ for sufficiently large n. The capacity region of MAC-FB is the closure of the set of all achievable rate pairs (R_1, R_2).

2.3 Cut-Set Outer Bound for MAC-FB

By applying Theorem 14.10.1 in [14], the cut-set outer bound on the capacity region of MAC-FB can be obtained as:

$$\mathcal{CS} = \Big\{(R_1, R_2) : R_1 \leq I(X_1; Y|X_2) \tag{2.1}$$

$$R_2 \leq I(X_2; Y|X_1) \tag{2.2}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\Big\} \tag{2.3}$$

where the random variables (X_1, X_2, Y) have the joint distribution

$$p(x_1, x_2, y) = p(x_1, x_2)p(y|x_1, x_2) \tag{2.4}$$

The cut-set outer bound allows all input distributions $p(x_1, x_2)$, which makes it seemingly loose since an achievable scheme might not achieve arbitrary correlation and rates given by the cut-set bound. Our aim is to restrict the set of allowable input distributions by using a dependence balance approach.

2.4 Dependence Balance Outer Bound for MAC-FB

Hekstra and Willems [30] showed that the capacity region of MAC-FB is contained within $\mathcal{DB}$, where

$$\mathcal{DB} = \Big\{(R_1, R_2) : R_1 \leq I(X_1; Y|X_2, T) \tag{2.5}$$

$$R_2 \leq I(X_2; Y|X_1, T) \tag{2.6}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y|T)\Big\} \tag{2.7}$$

where the random variables (X_1, X_2, Y, T) have the joint distribution

$$p(t, x_1, x_2, y) = p(t)p(x_1, x_2|t)p(y|x_1, x_2) \tag{2.8}$$

and also satisfy the following dependence balance bound

$$I(X_1; X_2|T) \leq I(X_1; X_2|Y, T) \tag{2.9}$$

where T is subject to a cardinality constraint of $|\mathcal{T}| \leq |\mathcal{X}_1||\mathcal{X}_2| + 2$. The dependence balance bound restricts the set of input distributions in the sense that it allows only those input distributions $p(t, x_1, x_2)$ which satisfy (2.9). It should be noted that by ignoring the constraint in (2.9), one obtains the cut-set bound.

2.5 Adaptive Parallel Channel Extension of the Dependence Balance Bound

In [30], Hekstra and Willems also developed an adaptive parallel channel extension for the dependence balance bound which is given as follows: Let $\Delta(\mathcal{U})$ denote the set of all distributions of U and $\Delta(\mathcal{U}|\mathcal{V})$ denote the set of all conditional distributions of U given V. Then for any mapping $F : \Delta(\mathcal{X}_1 \times \mathcal{X}_2) \to \Delta(\mathcal{Z}|\mathcal{X}_1 \times \mathcal{X}_2 \times \mathcal{Y})$, the capacity

region of the MAC-FB is contained in

$$\mathcal{DB}_{PC} = \Big\{(R_1, R_2) : R_1 \leq I(X_1; Y, Z|X_2, T) \tag{2.10}$$

$$R_2 \leq I(X_2; Y, Z|X_1, T) \tag{2.11}$$

$$R_1 \leq I(X_1; Y|X_2) \tag{2.12}$$

$$R_2 \leq I(X_2; Y|X_1) \tag{2.13}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y) \tag{2.14}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, Z|T)\Big\} \tag{2.15}$$

where the random variables (X_1, X_2, Y, Z, T) have the joint distribution

$$p(t, x_1, x_2, y, z) = p(t)p(x_1, x_2|t)p(y|x_1x_2)p^+(z|x_1, x_2, y, t) \tag{2.16}$$

such that for all t

$$p^+(z|x_1, x_2, y, t) = F(p_{X_1X_2}(x_1, x_2|t)) \tag{2.17}$$

and such that

$$I(X_1; X_2|T) \leq I(X_1; X_2|Y, Z, T) \tag{2.18}$$

where T is subject to a cardinality bound of $|\mathcal{T}| \leq |\mathcal{X}_1||\mathcal{X}_2| + 3$.

We should remark that the parallel channel (defined by $p^+(z|x_1, x_2, y, t)$) is se-

lected apriori, and for every choice of the parallel channel, one obtains an outer bound on the capacity region of MAC-FB, which is in general tighter than the cut-set bound. The set of allowable input distributions $p(t, x_1, x_2)$ are those which satisfy the constraint in (2.18). Also note that only the right hand side of (2.18), i.e., only $I(X_1; X_2|Y, Z, T)$, depends on the choice of the parallel channel. By carefully selecting $p^+(z|x_1, x_2, y, t)$, one can reduce $I(X_1; X_2|Y, Z, T)$, thereby making the constraint in (2.18) more stringent, consequently reducing the set of allowable input distributions. To obtain an improvement over the cut-set bound, we need to select a "good" parallel channel such that it restricts the input distributions to a small allowable set and yields small values of $I(X_1; Z|Y, X_2, T)$ and $I(X_2; Z|Y, X_1, T)$ at the same time. These two mutual information "leak" terms are the extra terms that appear in (2.10) and (2.11) relative to the rates appearing in (2.5) and (2.6), respectively.

To motivate the choice of our particular parallel channel, first consider a trivial choice of Z: $Z = \phi$ (a constant). For this choice of Z, (2.18) reduces to (2.9) and we are not restricting the set of allowable input distributions any more than the $\mathcal{DB}$ bound. Moreover, for a constant selection of Z, (2.10) and (2.11) reduce to (2.5) and (2.6), respectively. Thus, a constant selection of Z for $\mathcal{DB}_{PC}$ is equivalent to $\mathcal{DB}$ itself.

Also note that the smallest value of $I(X_1; X_2|Y, Z, T)$ is zero. Thus, it follows that if we select a parallel channel such that $I(X_1; X_2|Y, Z, T) = 0$ for every input distribution $p(t, x_1, x_2)$, then $I(X_1; X_2|T) = 0$ by (2.18). Hence, the smallest set of input distributions permissable by $\mathcal{DB}_{PC}$ consists of those $p(t, x_1, x_2)$ for which X_1 and X_2 are conditionally independent given T. Furthermore, for a parallel channel

such that $I(X_1; X_2|Y, Z, T) = 0$, the bound in (2.15) is redundant. This can be seen from:

$$\begin{aligned} 0 &= I(X_1; X_2|T) - I(X_1; X_2|Y, Z, T) \\ &= I(X_1; Y, Z|T) - I(X_1; Y, Z|X_2, T) \\ &= I(X_1, X_2; Y, Z|T) - I(X_1; Y, Z|X_2, T) - I(X_2; Y, Z|X_1, T) \end{aligned} \tag{2.19}$$

Using (2.19), it is clear that the sum of constraints (2.10) and (2.11) is at least as strong as the constraint (2.15). This shows that (2.15) is redundant for the class of parallel channels where $I(X_1; X_2|Y, Z, T) = 0$.

2.6 Binary Additive Noisy MAC-FB

In this section, we will consider a binary-input additive noisy MAC given by

$$Y = X_1 + X_2 + N \tag{2.20}$$

where N is binary, uniform over $\{0, 1\}$ and is independent of X_1 and X_2. The channel output Y takes values from the set $\mathcal{Y} = \{0, 1, 2, 3\}$. This channel does not fall into any class of MAC for which the feedback capacity region is known. This channel was also considered by Kramer in [37, 39] where it was shown that the Cover-Leung achievable rate is strictly sub-optimal for the sum-rate.

We select a parallel channel $p^+(z|x_1, x_2, y)$ such that $I(X_1; X_2|Y, Z, T) = 0$. By (2.18), this will imply $I(X_1; X_2|T) = 0$, and hence only distributions of the type

$p(t, x_1, x_2) = p(t)p(x_1|t)p(x_2|t)$ will be allowed. By doing so, we restrict the set of allowable input distributions to be the smallest permitted by $\mathcal{DB}_{PC}$, although we pay a penalty due to the positive "leak" terms $I(X_1; Z|Y, X_2, T)$ and $I(X_2; Z|Y, X_1, T)$.

Two simple choices of Z which yield $I(X_1; X_2|Y, Z, T) = 0$ are $Z = X_1$ and $Z = X_2$. For each of these choices, the corresponding outer bounds are,

$$\mathcal{DB}_{PC}^{(1)} = \Big\{(R_1, R_2) : R_1 \leq I(X_1; Y|X_2, T) + H(X_1|Y, X_2, T) \tag{2.21}$$

$$R_2 \leq I(X_2; Y|X_1, T) \tag{2.22}$$

$$R_1 \leq I(X_1; Y|X_2) \tag{2.23}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\Big\} \tag{2.24}$$

and

$$\mathcal{DB}_{PC}^{(2)} = \Big\{(R_1, R_2) : R_1 \leq I(X_1; Y|X_2, T) \tag{2.25}$$

$$R_2 \leq I(X_2; Y|X_1, T) + H(X_2|Y, X_1, T) \tag{2.26}$$

$$R_2 \leq I(X_2; Y|X_1) \tag{2.27}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\Big\} \tag{2.28}$$

where both $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$ are evaluated over the set of input distributions of the form $p(t, x_1, x_2) = p(t)p(x_1|t)p(x_2|t)$. We should remark here that these two outer bounds can also be obtained by extending the approach of Zhang, Berger and Schalkwijk [71] to the multiple access channel with feedback.

Lemma 2.1 *For the binary additive noisy MAC-FB given in (2.20), the following equalities hold for any distribution of the form* $p(t, x_1, x_2) = p(t)p(x_1|t)p(x_2|t)$,

$$H(X_1|Y, X_2, T) = \frac{1}{2}H(X_1|T) \tag{2.29}$$

$$H(X_2|Y, X_1, T) = \frac{1}{2}H(X_2|T) \tag{2.30}$$

The proof of Lemma 2.1 is given in the Appendix.

Using Lemma 2.1, we can simplify $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$ as,

$$\mathcal{DB}_{PC}^{(1)} = \Big\{(R_1, R_2) : R_1 \leq \min\left(I(X_1; Y|X_2), H(X_1|T)\right) \tag{2.31}$$

$$R_2 \leq \frac{1}{2}H(X_2|T) \tag{2.32}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\Big\} \tag{2.33}$$

and

$$\mathcal{DB}_{PC}^{(2)} = \Big\{(R_1, R_2) : R_1 \leq \frac{1}{2}H(X_1|T) \tag{2.34}$$

$$R_2 \leq \min\left(I(X_2; Y|X_1), H(X_2|T)\right) \tag{2.35}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\Big\} \tag{2.36}$$

where both bounds are evaluated over the set of distributions of the form $p(t, x_1, x_2) = p(t)p(x_1|t)p(x_2|t)$ and the auxiliary random variable T is subject to a cardinality constraint of $|\mathcal{T}| \leq |\mathcal{X}_1||\mathcal{X}_2| + 3$. The evaluation of the above outer bounds is rather cumbersome because for binary inputs, the bound on $|\mathcal{T}|$ is $|\mathcal{T}| \leq 7$. To the best of our

knowledge, no one has been able to conduct an exhaustive search over an auxiliary random variable whose cardinality is larger than 4. In Section 2.8, we will obtain an alternate characterization for our outer bounds using composite functions and their properties. For that, we will first develop some useful properties of composite functions in the next section.

A valid outer bound is given by the intersection of $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$,

$$\mathcal{DB}_{PC} = \mathcal{DB}_{PC}^{(1)} \bigcap \mathcal{DB}_{PC}^{(2)} \tag{2.37}$$

We will show that this outer bound is strictly smaller than the cut-set bound at all points on the capacity region where feedback increases capacity.

2.7 Composite Functions and Their Properties

Before obtaining a characterization of our outer bounds, we will define a composite function and prove two lemmas regarding its properties. These lemmas will be essential in obtaining simple characterizations for our outer bounds and the Cover-Leung achievable rate region. Throughout the dissertation, we will refer to the entropy function as $h^{(k)}(s_1, \ldots s_k)$ which is defined as,

$$h^{(k)}(s_1, \ldots, s_k) = -\sum_{i=1}^{k} s_i \log(s_i) \tag{2.38}$$

for $s_i \geq 0$, $i = 1 \ldots, k$, and $\sum_{i=1}^{k} s_i = 1$, where all logarithms are to the base 2. We will denote $h^{(2)}(s, 1-s)$ simply as $h(s)$. To characterize our bounds, we will make

use of the following function

$$\phi(s) = \begin{cases} \frac{1-\sqrt{1-2s}}{2}, & \text{for } 0 \leq s \leq 1/2 \\ \frac{1-\sqrt{2s-1}}{2}, & \text{for } 1/2 < s \leq 1 \end{cases} \tag{2.39}$$

It was shown in [63] that the composite function $h(\phi(s))$ is symmetric around $s = 1/2$ and concave in s for $0 \leq s \leq 1$. The functions $\phi(s)$ and $h(\phi(s))$ are illustrated in Figure 2.2. From the definition of $\phi(s)$ in (2.39) it is clear that for any $s \in [0, 1]$, the function $\phi(s)$ satisfies the following property

$$\phi(2s(1-s)) = \min(s, 1-s) \tag{2.40}$$

As a consequence, the following holds as well

$$h(\phi(2s(1-s))) = h(s) \tag{2.41}$$

For any $s \in [0, 1]$, the following holds from the definition of $\phi(s)$,

$$s = \begin{cases} \phi(2s(1-s)), & 0 \leq s \leq \frac{1}{2} \\ 1 - \phi(2s(1-s)), & \frac{1}{2} < s \leq 1 \end{cases} \tag{2.42}$$

For any $x \in [0, \frac{1}{2}]$ and $y \in [0, \frac{1}{2}]$, let us define a function

$$f(x, y) = \phi(x) + \phi(y) - 2\phi(x)\phi(y) \tag{2.43}$$

$$= \frac{1 - \sqrt{(1-2x)(1-2y)}}{2} \tag{2.44}$$

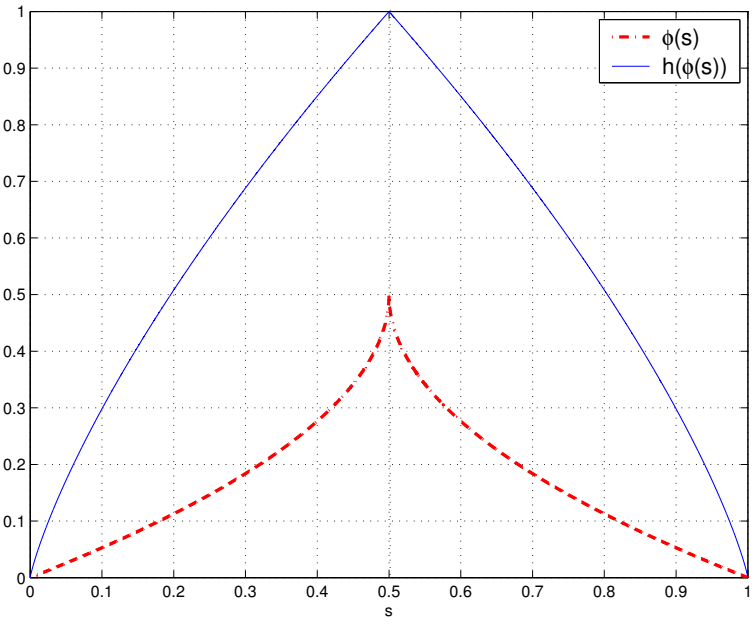

Figure 2.2: Functions $\phi(s)$ and $h(\phi(s))$.

From the above definition, it is clear that the function $f(x, y)$ lies in the range $[0, \frac{1}{2}]$.

We now state two lemmas regarding the function $f(x, y)$.

Lemma 2.2 *The variable*

$$v = s_1 + s_2 - 2s_1s_2 \tag{2.45}$$

is always lower bounded by $f(2s_1(1 - s_1), 2s_2(1 - s_2))$ *for any* $s_1 \in [0, 1], s_2 \in [0, 1]$.

Lemma 2.3 *The function* $f(x, y)$ *is jointly convex in* (x, y) *for* $0 \leq x \leq \frac{1}{2}, 0 \leq y \leq \frac{1}{2}$.

The proofs of Lemmas 2.2 and 2.3 are given in the Appendix.

2.8 Evaluation of the Dependence Balance Outer Bound

We now present the main result of this section.

Theorem 2.1 *The feedback capacity region of the binary additive noisy MAC given by (2.20) is contained in the region*

$$\mathcal{DB}_{PC} = \mathcal{DB}_{PC}^{(1)} \bigcap \mathcal{DB}_{PC}^{(2)} \tag{2.46}$$

where

$$\begin{aligned} \mathcal{DB}_{PC}^{(1)} = \bigcup_{(u_1,u_2,u)\in\mathcal{P}} \Bigg\{ (R_1,R_2) : R_1 &\leq \min\left(\frac{1}{2}h(u), h(\phi(2u_1))\right) \\ R_2 &\leq \frac{1}{2}h(\phi(2u_2)) \\ R_1+R_2 &\leq h\left(\frac{1-u}{2}\right) \Bigg\} \end{aligned} \tag{2.47}$$

and

$$\begin{aligned} \mathcal{DB}_{PC}^{(2)} = \bigcup_{(u_1,u_2,u)\in\mathcal{P}} \Bigg\{ (R_1,R_2) : R_1 &\leq \frac{1}{2}h(\phi(2u_1)) \\ R_2 &\leq \min\left(\frac{1}{2}h(u), h(\phi(2u_2))\right) \\ R_1+R_2 &\leq h\left(\frac{1-u}{2}\right) \Bigg\} \end{aligned} \tag{2.48}$$

and the set $\mathcal{P}$ is defined as

$$\mathcal{P} = \left\{(u_1,u_2,u) : 0 \leq u_1 \leq \frac{1}{4}; 0 \leq u_2 \leq \frac{1}{4}; f(2u_1,2u_2) \leq u \leq 1-(u_1+u_2)\right\} \tag{2.49}$$

Proof: We will explicitly characterize our outer bounds $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$. Let the cardinality of the auxiliary random variable T be fixed and arbitrary, say $|\mathcal{T}|$. Then, the joint distribution $p(t)p(x_1|t)p(x_2|t)$ can be described by the following variables:

$$\begin{aligned} q_{1t} &= \Pr(X_1 = 0|T = t), \quad t = 1, \ldots, |\mathcal{T}| \\ q_{2t} &= \Pr(X_2 = 0|T = t), \quad t = 1, \ldots, |\mathcal{T}| \\ p_t &= \Pr(T = t), \qquad\quad t = 1, \ldots, |\mathcal{T}| \end{aligned} \tag{2.50}$$

We will characterize our outer bounds in terms of three variables u_1, u_2 and u which are functions of $p(t, x_1, x_2)$, and are defined as,

$$u_1 = \sum_t p_t q_{1t}(1 - q_{1t}) = \sum_t p_t u_{1t} \tag{2.51}$$

$$u_2 = \sum_t p_t q_{2t}(1 - q_{2t}) = \sum_t p_t u_{2t} \tag{2.52}$$

$$u = \sum_t p_t(q_{1t} + q_{2t} - 2q_{1t}q_{2t}) = \sum_t p_t u_t \tag{2.53}$$

where we have defined

$$u_{1t} = q_{1t}(1 - q_{1t}) \tag{2.54}$$

$$u_{2t} = q_{2t}(1 - q_{2t}) \tag{2.55}$$

$$u_t = q_{1t} + q_{2t} - 2q_{1t}q_{2t} \tag{2.56}$$

It should be noted that since $0 \leq q_{jt} \leq 1$, for $j = 1, 2$, $t = 1, \ldots, |\mathcal{T}|$, the variables u_1, u_2, u_{1t} and u_{2t} all lie in the range $[0, \frac{1}{4}]$. Our outer bounds $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$ are comprised of the following information theoretic entities:

1. $H(X_1|T)$, $H(X_2|T)$
2. $I(X_1; Y|X_2)$, $I(X_2; Y|X_1)$
3. $I(X_1, X_2; Y)$.

We will first obtain upper bounds for each one of these entities individually in terms of (u_1, u_2, u).

We upper bound $H(X_1|T)$ as follows,

$$H(X_1|T) = \sum_t p_t h(q_{1t}) \tag{2.57}$$

$$= \sum_t p_t h(\phi(2q_{1t}(1 - q_{1t}))) \tag{2.58}$$

$$= \sum_t p_t h(\phi(2u_{1t})) \tag{2.59}$$

$$\leq h(\phi(2u_1)) \tag{2.60}$$

where (2.58) follows due to (2.41), (2.59) follows from (2.54), and (2.60) follows from the fact that $h(\phi(s))$ is concave in s and the application of Jensen's inequality [14]. Using a similar set of inequalities for $H(X_2|T)$, we obtain

$$H(X_2|T) \leq h(\phi(2u_2)) \tag{2.61}$$

We will now upper bound $I(X_1;Y|X_2)$ in terms of the variable u. For this purpose, let us first define

$$a = P_{X_1X_2}(0,0) = \sum_t p_t q_{1t} q_{2t} \tag{2.62}$$

$$b = P_{X_1X_2}(0,1) = \sum_t p_t q_{1t} (1 - q_{2t}) \tag{2.63}$$

$$c = P_{X_1X_2}(1,0) = \sum_t p_t (1 - q_{1t}) q_{2t} \tag{2.64}$$

$$d = P_{X_1X_2}(1,1) = 1 - a - b - c. \tag{2.65}$$

We now proceed as,

$$I(X_1;Y|X_2) = H(Y|X_2) - H(Y|X_1,X_2) \tag{2.66}$$

$$= H(Y|X_2) - 1 \tag{2.67}$$

$$= (a+c) h^{(3)}\left(\frac{a}{2(a+c)}, \frac{1}{2}, \frac{c}{2(a+c)}\right) + (b+d) h^{(3)}\left(\frac{b}{2(b+d)}, \frac{1}{2}, \frac{d}{2(b+d)}\right) - 1 \tag{2.68}$$

$$\leq h^{(3)}\left(\frac{a+d}{2}, \frac{1}{2}, \frac{b+c}{2}\right) - 1 \tag{2.69}$$

$$= \frac{1}{2} h(b+c) \tag{2.70}$$

$$= \frac{1}{2} h(u) \tag{2.71}$$

where (2.69) follows by the concavity of the entropy function and the application of Jensen's inequality [14]. Using a similar set of inequalities, we also have

$$I(X_2; Y|X_1) \leq \frac{1}{2} h(u) \tag{2.72}$$

We will now obtain an upper bound on $I(X_1, X_2; Y)$. First note that

$$I(X_1, X_2; Y) = H(Y) - H(Y|X_1, X_2) \tag{2.73}$$

$$= h^{(4)}(P_Y(0), P_Y(1), P_Y(2), P_Y(3)) - 1 \tag{2.74}$$

where

$$P_Y(0) = \sum_t p_t q_{1t} q_{2t}/2 \tag{2.75}$$

$$P_Y(1) = \sum_t p_t \big(q_{1t} + q_{2t} - q_{1t} q_{2t}\big)/2 \tag{2.76}$$

$$P_Y(2) = \sum_t p_t \big(1 - q_{1t} q_{2t}\big)/2 \tag{2.77}$$

$$P_Y(3) = \sum_t p_t (1 - q_{1t})(1 - q_{2t})/2 \tag{2.78}$$

Using the following fact,

$$h^{(4)}(\alpha,\beta,\gamma,\theta) = \frac{1}{2}h^{(4)}(\alpha,\beta,\gamma,\theta) + \frac{1}{2}h^{(4)}(\theta,\gamma,\beta,\alpha) \tag{2.79}$$

$$\leq h^{(4)}\left(\frac{\alpha+\theta}{2}, \frac{\beta+\gamma}{2}, \frac{\beta+\gamma}{2}, \frac{\alpha+\theta}{2}\right) \tag{2.80}$$

$$= h\left(\alpha+\theta\right) + h\left(\frac{1}{2}\right) \tag{2.81}$$

$$= h\left(1-(\beta+\gamma)\right) + 1 \tag{2.82}$$

where (2.80) follows by the concavity of the entropy function and the application of Jensen's inequality [14], we now obtain an upper bound on $I(X_1, X_2; Y)$ by continuing from (2.74),

$$I(X_1, X_2; Y) = h^{(4)}(P_Y(0), P_Y(1), P_Y(2), P_Y(3)) - 1 \tag{2.83}$$

$$\leq h\left(1-(P_Y(1)+P_Y(2))\right) + h\left(\frac{1}{2}\right) - 1 \tag{2.84}$$

$$= h\left(\frac{1-u}{2}\right) \tag{2.85}$$

where (2.84) follows by (2.82) and (2.85) follows from the fact that $P_Y(1) + P_Y(2) = (1+u)/2$ using (2.76) and (2.77), where u is as defined in (2.53).

We have obtained upper bounds on the information theoretic entities which comprise our outer bounds in terms of three variables u_1, u_2 and u. We will now give a feasible region for these triples based on the structures of these variables. We claim that the following set is feasible:

$$\mathcal{P} = \left\{(u_1, u_2, u) : 0 \leq u_1 \leq \frac{1}{4}; 0 \leq u_2 \leq \frac{1}{4}; f(2u_1, 2u_2) \leq u \leq 1 - (u_1 + u_2)\right\} \quad (2.86)$$

First, note that for any $q_{1t} \in [0, 1]$, the following holds: $u_{1t} = q_{1t}(1 - q_{1t}) \leq \frac{1}{4}$. Similarly, $u_{2t} = q_{2t}(1 - q_{2t}) \leq \frac{1}{4}$. Hence, we have

$$0 \leq u_1 \leq \frac{1}{4} \quad (2.87)$$

$$0 \leq u_2 \leq \frac{1}{4} \quad (2.88)$$

We now obtain a lower bound on u as

$$u = \sum_t p_t u_t \quad (2.89)$$

$$\geq \sum_t p_t f(2u_{1t}, 2u_{2t}) \quad (2.90)$$

$$\geq f\left(2\sum_t p_t u_{1t}, 2\sum_t p_t u_{2t}\right) \quad (2.91)$$

$$= f(2u_1, 2u_2) \quad (2.92)$$

where (2.90) follows by Lemma 2.2 and (2.91) follows by Lemma 2.3 and the application of Jensen's inequality [14]. We now obtain another lower bound on u,

$$u = \sum_t p_t u_t \tag{2.93}$$

$$= \sum_t p_t(q_{1t} + q_{2t} - 2q_{1t}q_{2t}) \tag{2.94}$$

$$= \sum_t p_t(q_{1t} - q_{1t}^2 + q_{2t} - q_{2t}^2 + (q_{1t} - q_{2t})^2) \tag{2.95}$$

$$\geq \sum_t p_t(q_{1t} - q_{1t}^2 + q_{2t} - q_{2t}^2) \tag{2.96}$$

$$= \sum_t p_t q_{1t}(1 - q_{1t}) + \sum_t p_t q_{2t}(1 - q_{2t}) \tag{2.97}$$

$$= u_1 + u_2 \tag{2.98}$$

Finally, we obtain an upper bound on u in terms of u_1 and u_2,

$$u = \sum_t p_t u_t \tag{2.99}$$

$$= \sum_t p_t(q_{1t} + q_{2t} - 2q_{1t}q_{2t}) \tag{2.100}$$

$$= \sum_t p_t(q_{1t} + q_{2t} - 2q_{1t}q_{2t} + q_{1t}^2 + (1 - q_{2t})^2 - q_{1t}^2 - (1 - q_{2t})^2) \tag{2.101}$$

$$\leq \sum_t p_t(q_{1t} + q_{2t} - 2q_{1t}q_{2t} + q_{1t}^2 + (1 - q_{2t})^2 - 2q_{1t}(1 - q_{2t})) \tag{2.102}$$

$$= 1 - (u_1 + u_2) \tag{2.103}$$

where (2.102) follows by the inequality $q_{1t}^2 + (1 - q_{2t})^2 \geq 2q_{1t}(1 - q_{2t})$.

By noting

$$f(2u_1, 2u_2) - (u_1 + u_2) = \frac{1 - \sqrt{(1-4u_1)(1-4u_2)}}{2} - (u_1 + u_2) \tag{2.104}$$

$$= \frac{(1-4u_1) + (1-4u_2) - 2\sqrt{(1-4u_1)(1-4u_2)}}{4} \tag{2.105}$$

$$= \frac{(\sqrt{1-4u_1} - \sqrt{1-4u_2})^2}{4} \tag{2.106}$$

$$\geq 0 \tag{2.107}$$

and using (2.92), we note that the lower bound in (2.98) is redundant.

Therefore, from (2.92) and (2.103), we have the following feasible range for the variable u in terms of u_1 and u_2,

$$f(2u_1, 2u_2) \leq u \leq 1 - (u_1 + u_2) \tag{2.108}$$

Combining (2.87), (2.88) and (2.108), we obtain the set of feasible (u_1, u_2, u) given in (2.86).

From (2.107), observe that $f(2u_1, 2u_2) = u_1 + u_2$ only if $u_1 = u_2$. The lower bound $u_1 + u_2 \leq u$ was sufficient for characterizing the symmetric feedback capacity of the binary erasure MAC [63]. Moreover, this characterization was possible by using only one variable u. On the other hand, our outer bounds are asymmetric in terms of the expressions appearing in the individual upper bounds for R_1 and R_2. Therefore, the bifurcation of information contained in any input distribution $p(t)p(x_1|t)p(x_2|t)$ in terms of three variables (u_1, u_2, u) and an improved lower bound on the variable u using the non-linear bivariate function $f(2u_1, 2u_2)$ turn out to be crucial in capturing

this asymmetry[2]. This can be considered as a heuristic explanation as to why we are able to obtain explicit characterizations of our outer bounds and the Cover-Leung achievable rate region for both channel models considered in this section.

It should be noted that the set of triples $\mathcal{P}$ obtained in (2.86) may not necessarily be the smallest feasible set of all triples (u_1, u_2, u). Since we are interested in a maximization over these set of triples, a possibly larger set $\mathcal{P}$ suffices.

Using the upper bounds on $H(X_1|T)$, $H(X_2|T)$, $I(X_1;Y|X_2)$, $I(X_2;Y|X_1)$ and $I(X_1,X_2;Y)$ in (2.60), (2.61), (2.71), (2.72) and (2.85) in terms of (u_1, u_2, u) along with a feasible set of triples $\mathcal{P}$ in (2.86), we arrive at the desired characterizations for $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$ given in (2.47) and (2.48), respectively. Finally, the intersection of two outer bounds is also a valid outer bound. Therefore, the outer bound $\mathcal{DB}_{PC}$ given in (2.46) contains the feedback capacity region of the binary additive noisy MAC. □

We will plot these outer bounds and their intersection in Figure 2.4. In the next section, we will explicitly characterize our upper bounds for the symmetric-rate point on the feedback capacity region of the binary additive noisy MAC.

2.9 Explicit Characterization of the Symmetric-Rate Upper Bound

For the binary additive noisy MAC-FB in consideration, it was shown by Kramer [37] that the symmetric-rate cut-set bound is 0.45915 bits/transmission. It was also shown in [37] that the Cover-Leung achievable symmetric-rate is 0.43621 bits/transmission

[2]Note that from the definition of u in (2.53), we also have $u = \Pr(X_1 \neq X_2)$. Therefore, roughly speaking, $1-u$ reflects the correlation between X_1 and X_2. Hence, obtaining a good lower bound on u is equivalent to limiting the correlation between X_1 and X_2. This interpretation is in accordance with the basic idea of dependence balance.

and it was improved to 0.43879 bits/transmission by using superposition coding and binning with code trees. For completeness and comparison with existing bounds, we will first completely characterize our outer bound for the symmetric-rate by providing the input distribution $p(t)p(x_1|t)p(x_2|t)$ which achieves it. By symmetric-rate we mean a rate R such that the rate pair (R, R) lies in the capacity region of MAC-FB. For the symmetric-rate, both $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$ will yield the same upper bound. Hence, we will focus on $\mathcal{DB}_{PC}^{(1)}$. Using (2.47), we are interested in obtaining the largest R over all $(u_1, u_2, u) \in \mathcal{P}$ such that

$$R \leq \min\left(\frac{1}{2}h(u), h(\phi(2u_1))\right) \tag{2.109}$$

$$R \leq \frac{1}{2}h(\phi(2u_2)) \tag{2.110}$$

$$2R \leq h\left(\frac{1-u}{2}\right) \tag{2.111}$$

We will show that a seemingly weaker version of the above bound will improve upon the symmetric-rate cut-set bound. We will also show that the weaker bound is in fact the same as the above bound, and its sole purpose is the simplicity of evaluation and insight into the input distribution that attains it. We first obtain a weakened version of (2.109) as

$$R \leq \min\left(\frac{1}{2}h(u), h(\phi(2u_1))\right) \leq h(\phi(2u_1)) \tag{2.112}$$

Next, consider (2.111)

$$2R \leq h\left(\frac{1-u}{2}\right) \tag{2.113}$$

$$= h\left(\frac{1}{2} - \frac{u}{2}\right) \tag{2.114}$$

$$\leq h\left(\frac{1}{2} - \frac{f(2u_1, 2u_2)}{2}\right) \tag{2.115}$$

where (2.115) follows from (2.92) and the fact that the binary entropy function $h(s)$ is monotonically increasing in s for $s \in [0, \frac{1}{2}]$. Combining (2.110), (2.112) and (2.115), we are interested in the largest R such that

$$R \leq \max_{u_1, u_2 \in [0, \frac{1}{4}]} \min\left(h(\phi(2u_1)), \frac{1}{2}h(\phi(2u_2)), \frac{1}{2}h\left(\frac{1}{2} - \frac{f(2u_1, 2u_2)}{2}\right)\right) \tag{2.116}$$

We note that this upper bound on the symmetric-rate depends only on u_1 and u_2, and therefore, we replace the feasible set $\mathcal{P}$ with $u_1, u_2 \in [0, \frac{1}{4}]$.

We know that $h(\phi(s))$ is concave in s for $s \in [0, 1]$. Hence, it follows that both $h(\phi(2u_1))$ and $\frac{1}{2}h(\phi(2u_2))$ are concave in u_1 and u_2, respectively, and hence concave in the pair (u_1, u_2). We also have the following lemma.

Lemma 2.4 *The function*

$$g(u_1, u_2) = \frac{1}{2}h\left(\frac{1 - f(2u_1, 2u_2)}{2}\right) \tag{2.117}$$

is monotonically decreasing and jointly concave in the pair (u_1, u_2) *for* $u_1, u_2 \in [0, \frac{1}{4}]$.

The proof of Lemma 2.4 is given in the Appendix.

Using Lemma 2.4, we conclude that all three functions in the min(.) in (2.116) are concave in (u_1, u_2). Invoking the fact that the minimum of concave functions is concave, we conclude that the maximum in (2.116) is unique. We will now show that the unique pair (u_1^*, u_2^*) that attains this maximum satisfies the property that $h(\phi(2u_1^*)) = \frac{1}{2}h(\phi(2u_2^*)) = g(u_1^*, u_2^*)$.

For this purpose, we first characterize those pairs $(\tilde{u}_1, \tilde{u}_2)$ such that the following holds,

$$h(\phi(2\tilde{u}_1)) = \frac{1}{2}h(\phi(2\tilde{u}_2)) = g(\tilde{u}_1, \tilde{u}_2) \tag{2.118}$$

By using (2.118), we obtain two equations for $\tilde{u}_1$ and $\tilde{u}_2$, as

$$h(\phi(2\tilde{u}_1)) = \frac{1}{2}h\left(\frac{1-\phi(2\tilde{u}_1)}{3-2\phi(2\tilde{u}_1)}\right) \tag{2.119}$$

$$\phi(2\tilde{u}_2) = \frac{1-\phi(2\tilde{u}_1)}{3-2\phi(2\tilde{u}_1)} \tag{2.120}$$

From (2.119), one can see that $2\tilde{u}_1$ is the unique solution $s \in [0, \frac{1}{2}]$ of the equation

$$h(\phi(s)) = \frac{1}{2}h\left(\frac{1-\phi(s)}{3-2\phi(s)}\right) \tag{2.121}$$

Obtaining the optimal $\tilde{u}_1$ from the above equation is illustrated in Figure 2.3. The unique solutions $(\tilde{u}_1, \tilde{u}_2)$ of (2.119) and (2.120) are

$$\tilde{u}_1 = 0.086063, \qquad \tilde{u}_2 = 0.218333 \tag{2.122}$$

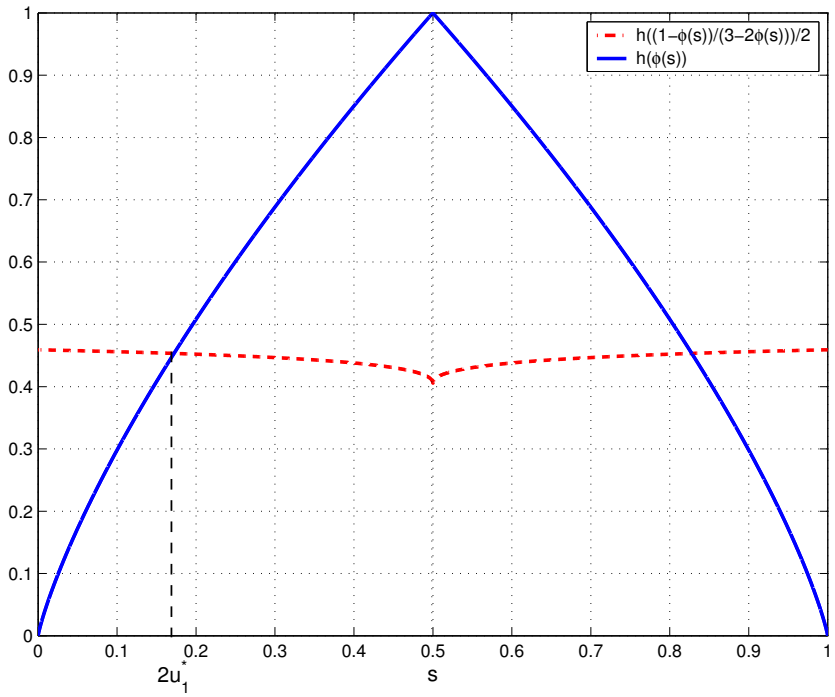

Figure 2.3: Characterization of the optimal u_1^*.

We will now show that this pair $(\tilde{u}_1, \tilde{u}_2)$ yields the maximum in (2.116).

Returning to the maximization problem (2.116), first denote $\mathcal{S}$ as the region of allowable (u_1, u_2),

$$\mathcal{S} = \left\{(u_1, u_2) : 0 \leq u_1 \leq \frac{1}{4}; 0 \leq u_2 \leq \frac{1}{4}\right\} \tag{2.123}$$

Also define a subset of this region

$$\tilde{\mathcal{S}} = \left\{(u_1, u_2) : u_1 \in (\tilde{u}_1, \frac{1}{4}]; u_2 \in (\tilde{u}_2, \frac{1}{4}]\right\} \tag{2.124}$$

where $(\tilde{u}_1, \tilde{u}_2)$ is given by (2.122). We will now show that the pair $(\tilde{u}_1, \tilde{u}_2)$ yields the solution of the maximization problem in (2.116). Consider the following two cases,

1. If $(u_1, u_2) \in \tilde{\mathcal{S}}$, then by Lemma 4, we have that $g(u_1, u_2) \leq g(\tilde{u}_1, \tilde{u}_2)$, using which we obtain,

$$\min\left(h(\phi(2u_1)), \frac{1}{2}h(\phi(2u_2)), g(u_1, u_2)\right) \leq g(u_1, u_2) \leq g(\tilde{u}_1, \tilde{u}_2) \tag{2.125}$$

2. If $(u_1, u_2) \in \mathcal{S} \setminus \tilde{\mathcal{S}}$, we either have $u_1 \leq \tilde{u}_1$ or $u_2 \leq \tilde{u}_2$ or both. Using this along with the fact that $h(\phi(2s))$ is monotonically increasing in s for $s \in [0, \frac{1}{4}]$, we obtain

$$\min\left(h(\phi(2u_1)), \frac{1}{2}h(\phi(2u_2)), g(u_1, u_2)\right) \leq h(\phi(2\tilde{u}_1)) \tag{2.126}$$

The above two cases show the following,

$$\max_{u_1 \in [0, \frac{1}{4}], u_2 \in [0, \frac{1}{4}]} \min\left(h(\phi(2u_1)), \frac{1}{2}h(\phi(2u_2)), g(u_1, u_2)\right) = h(\phi(2\tilde{u}_1)) \tag{2.127}$$

$$= \frac{1}{2}h(\phi(2\tilde{u}_2)) \tag{2.128}$$

$$= g(\tilde{u}_1, \tilde{u}_2) \tag{2.129}$$

Thus, the maximum in (2.116) is obtained at $(u_1^*, u_2^*) = (\tilde{u}_1, \tilde{u}_2)$. We now obtain a distribution $p(t)p(x_1|t)p(x_2|t)$ which attains this symmetric-rate upper bound. Fix T

to be binary, and select the involved probabilities as

$$p_0 = p_1 = \frac{1}{2} \tag{2.130}$$

$$q_{10} = 1 - q_{11} = \phi(2u_1^*) \tag{2.131}$$

$$q_{20} = 1 - q_{21} = \phi(2u_2^*) \tag{2.132}$$

The reason for constructing such an input distribution is that, at this specific distribution, we have the following exact equalities,

$$H(X_1|T) = h(\phi(2u_1^*)) \tag{2.133}$$

$$\frac{1}{2}H(X_2|T) = \frac{1}{2}h(\phi(2u_2^*)) \tag{2.134}$$

$$\frac{1}{2}I(X_1, X_2; Y) = g(u_1^*, u_2^*) \tag{2.135}$$

and we achieve the outer bound we developed with equality. Substituting the values of (u_1^*, u_2^*), we obtain a distribution given by,

$$p_0 = p_1 = \frac{1}{2} \tag{2.136}$$

$$q_{10} = 1 - q_{11} = 0.095109 \tag{2.137}$$

$$q_{20} = 1 - q_{21} = 0.322050 \tag{2.138}$$

The above input distribution yields a symmetric-rate of 0.45330 bits/transmission.

Moreover, the u^* corresponding to this distribution is given by

$$u^* = \sum_t p_t(q_{1t} + q_{2t} - 2q_{1t}q_{2t}) \tag{2.139}$$

$$= f(2u_1^*, 2u_2^*) \tag{2.140}$$

$$= 0.355899 \tag{2.141}$$

where (2.140) is by construction of the input distribution $p(t, x_1, x_2)$ and (2.141) is obtained by substituting the distribution specified in (2.136)-(2.138). Moreover, $\phi(2u_2^*) < u^* < \frac{1}{2}$, hence we also have that

$$\frac{1}{2}h(u^*) \geq \frac{1}{2}h(\phi(2u_2^*)) = h(\phi(2u_1^*)) \tag{2.142}$$

This shows that the weakened version of the upper bound obtained in (2.116) is indeed tight and a binary auxiliary random variable T with uniform distribution over $\{0, 1\}$ is sufficient to attain this symmetric-rate upper bound.

2.10 Evaluation of the Cover-Leung Achievable Rate Region

For completeness we will also obtain a simple characterization of the Cover-Leung inner bound for our binary additive noisy MAC-FB. For this purpose, we follow a two-step approach. In the first step, we first obtain an outer bound on the achievable rate region in terms of two variables (u_1, u_2). In the second step, we specify an input distribution, as a function of (u_1, u_2), which achieves the outer bound. We therefore arrive at an alternate characterization of the Cover-Leung achievable rate region in

terms of the variables (u_1, u_2).

The Cover-Leung achievable rate region [13] is given as,

$$\mathcal{CL} = \Big\{(R_1, R_2) : R_1 \leq I(X_1; Y|X_2, T) \tag{2.143}$$

$$R_2 \leq I(X_2; Y|X_1, T) \tag{2.144}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\Big\} \tag{2.145}$$

where the random variables (T, X_1, X_2, Y) have the joint distribution,

$$p(t, x_1, x_2, y) = p(t)p(x_1|t)p(x_2|t)p(y|x_1, x_2) \tag{2.146}$$

and the random variable T is subject to a cardinality constraint of $|\mathcal{T}| \leq \min(|\mathcal{X}_1||\mathcal{X}_2|+1, |\mathcal{Y}| + 2)$.

We now state the main result of this section.

Theorem 2.2 *The Cover-Leung achievable rate region for the binary additive noisy MAC given by (2.20) is given as*

$$\mathcal{CL} = \bigcup_{(u_1,u_2)\in\mathcal{S}} \Bigg\{(R_1, R_2) : R_1 \leq \frac{1}{2}h(\phi(2u_1))$$

$$R_2 \leq \frac{1}{2}h(\phi(2u_2))$$

$$R_1 + R_2 \leq h\left(\frac{1 - f(2u_1, u_2)}{2}\right)\Bigg\} \tag{2.147}$$

where the set $\mathcal{S}$ is defined as

$$\mathcal{S} = \left\{(u_1, u_2) : 0 \leq u_1 \leq \frac{1}{4}; 0 \leq u_2 \leq \frac{1}{4}\right\} \tag{2.148}$$

Proof: For the binary additive noisy MAC in consideration, the constraints in (2.143)-(2.145) simplify as

$$R_1 \leq \frac{1}{2}H(X_1|T) \tag{2.149}$$

$$R_2 \leq \frac{1}{2}H(X_2|T) \tag{2.150}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y) \tag{2.151}$$

We will first obtain an outer bound on the region specified by (2.149)-(2.151) in terms of two variables (u_1, u_2). For every pair (u_1, u_2), we will then specify an input distribution which will attain this outer bound. Note that the three constraints (2.149)-(2.151) are of similar form as in the case of $\mathcal{DB}_{PC}^{(1)}$ and $\mathcal{DB}_{PC}^{(2)}$, and we proceed in a similar manner to obtain upper bounds on the three terms above in terms of u_1 and u_2 as,

$$R_1 \leq \frac{1}{2}h(\phi(2u_1)) \tag{2.152}$$

$$R_2 \leq \frac{1}{2}h(\phi(2u_2)) \tag{2.153}$$

$$R_1 + R_2 \leq h\left(\frac{1 - f(2u_1, u_2)}{2}\right) \tag{2.154}$$

where the variables (u_1, u_2) belong to the set $\mathcal{S}$ defined in (2.123). Hence, an outer

bound on the rate region specified by (2.149)-(2.151) is given as $\mathcal{O}$, where

$$\mathcal{O} = \bigcup_{(u_1,u_2)\in\mathcal{S}} \Bigg\{ (R_1, R_2) : R_1 \leq \frac{1}{2} h(\phi(2u_1)) \\ R_2 \leq \frac{1}{2} h(\phi(2u_2)) \\ R_1 + R_2 \leq h\left(\frac{1 - f(2u_1, u_2)}{2}\right) \Bigg\} \tag{2.155}$$

Let (u_1, u_2) be any arbitrary pair which belongs to $\mathcal{S}$. Consider an input distribution for which $|\mathcal{T}| = 2$, and T is uniform over $\{0, 1\}$ and,

$$p_0 = p_1 = \frac{1}{2} \tag{2.156}$$

$$q_{10} = 1 - q_{11} = \phi(2u_1) \tag{2.157}$$

$$q_{20} = 1 - q_{21} = \phi(2u_2) \tag{2.158}$$

For this input distribution, we obtain the following exact equalities

$$H(X_1|T) = h(\phi(2u_1)) \tag{2.159}$$

$$H(X_2|T) = h(\phi(2u_2)) \tag{2.160}$$

$$I(X_1, X_2; Y) = h\left(\frac{1 - f(2u_1, 2u_2)}{2}\right) \tag{2.161}$$

We have thus shown that the outer bound we obtained on the achievable rate region in terms of (u_1, u_2) can be attained by a set of input distributions for which the involved auxiliary random variable T is binary and uniform. This in turn implies that a binary and uniform random variable T is sufficient to characterize the entire Cover-Leung

achievable rate region for the binary additive noisy MAC-FB. By varying over all such input distributions, or equivalently, by varying (u_1, u_2) in the set $\mathcal{S}$, we obtain the entire Cover-Leung achievable rate region given in (2.147). $\square$

We should remark here that when evaluating the $\mathcal{DB}_{PC}$ bound in the previous section for $Z = X_1$ and $Z = X_2$, it was not necessary to specify the distribution which achieves the bound, since it was an outer bound. On the other hand, when evaluating the Cover-Leung bound, since it is an achievability, it is necessary to give a distribution which achieves the bound.

The dependence balance bounds corresponding to the parallel channel choices $Z = X_1$ and $Z = X_2$, along with the cut-set upper bound and the Cover-Leung achievable rate region are shown in Figures 2.4 and 2.5. It is interesting to note that our bound improves upon the cut-set bound at all points where the Cover-Leung achievable rate region is strictly larger than the capacity region without feedback. In other words, our bound improves upon the cut-set bound at all points where feedback increases capacity.

We should remark that our choices of parallel channels; namely, $Z = X_1$ and $Z = X_2$ are the simplest ones which ensure that $I(X_1; X_2|Y, Z, T) = 0$ but they yield fixed information leaks. We believe that by a more elaborate choice of a parallel channel, i.e., by carefully selecting a parameterized parallel channel $p^+(z|x_1, x_2, y, t)$ such that $I(X_1; X_2|Y, Z, T) = 0$, one would still be able to restrict the input distributions to a conditionally independent form and then optimize the parameters of the parallel channel to minimize the information leak terms. This approach can potentially improve upon our outer bound. However, for explicitly characterizing such

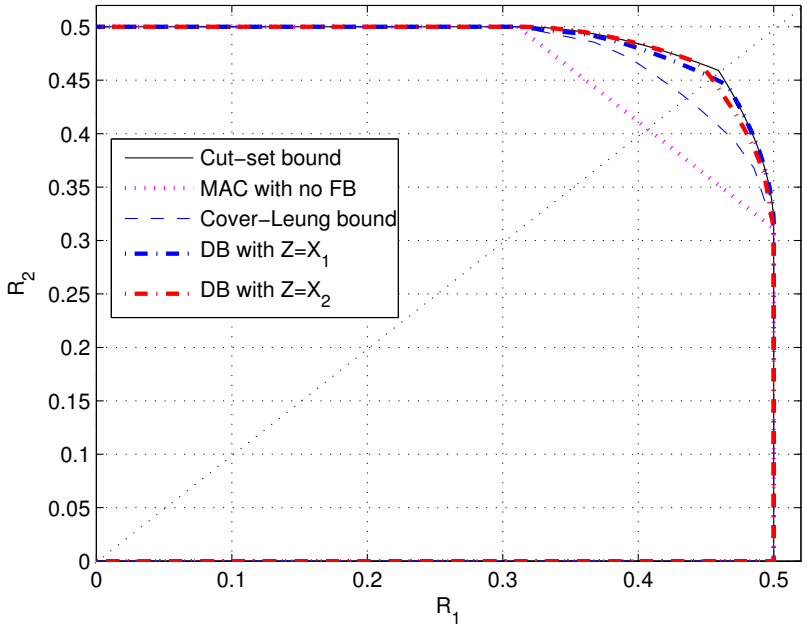

Figure 2.4: Illustration of our bounds for the capacity of binary additive noisy MAC-FB.

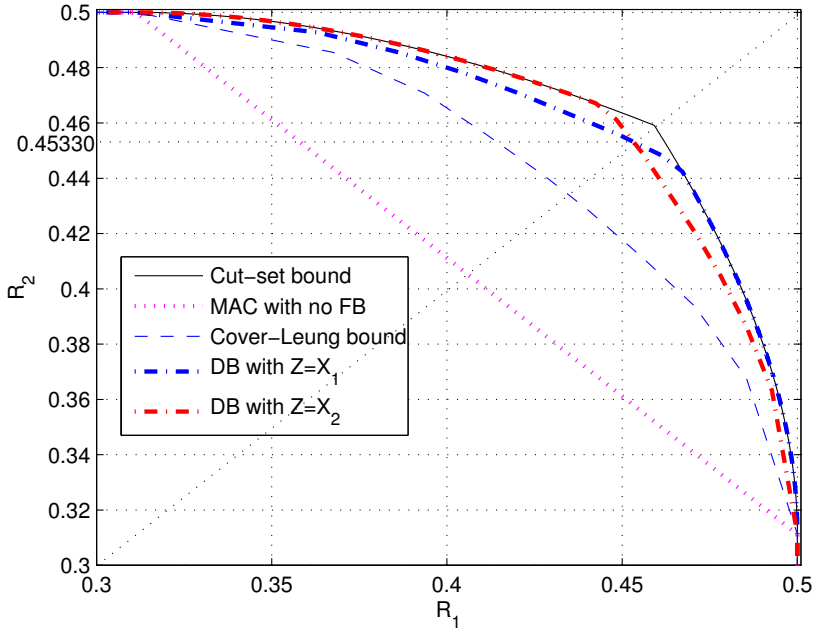

Figure 2.5: An enlarged illustration of the portion of Figure 2.4 where feedback increases capacity.

outer bounds, one might require a new approach and possibly a different composite function than the one used in this chapter.

2.11 The Capacity Region of the Binary Erasure MAC-FB

The capacity region of a class of discrete memoryless MAC-FB was characterized in [62] by establishing a converse and it was shown to be equal to the Cover-Leung achievable rate region. This class of channels satisfy the property that at least one of the channel inputs say X_1, can be written as a deterministic function of the other channel input X_2 and the channel output Y. The binary erasure MAC, where $Y = X_1 + X_2$, falls into this class of channels. In addition, the binary erasure MAC-FB is the noiseless version of the binary additive noisy MAC-FB studied in this chapter.

Willems showed in [63] that a binary selection of auxiliary random variable is sufficient to obtain the sum-rate point of the capacity region of the binary erasure MAC-FB. In this section, we will show that by using our results for composite functions which were presented in previous sections, it is possible to obtain all points on the boundary of this capacity region using a binary auxiliary random variable. The feedback capacity region of this channel is given by the Cover-Leung achievable rate region given in (2.143)-(2.145) which can be simplified for the binary erasure

MAC-FB as,

$$R_1 \leq H(X_1|T) \tag{2.162}$$

$$R_2 \leq H(X_2|T) \tag{2.163}$$

$$R_1 + R_2 \leq H(Y) \tag{2.164}$$

We now state the main result of this section.

Theorem 2.3 *The feedback capacity region of the binary erasure MAC is given as,*

$$\begin{aligned} \mathcal{C} = \bigcup_{(u_1,u_2)\in\mathcal{S}} \Big\{ & (R_1, R_2) : R_1 \leq h(\phi(2u_1)) \\ & R_2 \leq h(\phi(2u_2)) \\ & R_1 + R_2 \leq h(f(2u_1, 2u_2)) + 1 - f(2u_1, 2u_2) \Big\} \end{aligned} \tag{2.165}$$

where the set $\mathcal{S}$ is defined as

$$\mathcal{S} = \left\{ (u_1, u_2) : 0 \leq u_1 \leq \frac{1}{4}; 0 \leq u_2 \leq \frac{1}{4} \right\} \tag{2.166}$$

Proof: We start by obtaining three upper bounds on the expressions appearing in the bounds (2.162)-(2.164). We first have,

$$H(X_1|T) \leq h(\phi(2u_1)) \tag{2.167}$$

Similarly, we also have

$$H(X_2|T) \leq h(\phi(2u_2)) \tag{2.168}$$

We now obtain an upper bound on $H(Y)$, by first noting that,

$$H(Y) = h^{(3)}(P_Y(0), P_Y(1), P_Y(2)) \tag{2.169}$$

where

$$P_Y(0) = \sum_t p_t q_{1t} q_{2t} \tag{2.170}$$

$$P_Y(1) = \sum_t p_t (q_{1t} + q_{2t} - 2q_{1t}q_{2t}) \tag{2.171}$$

$$P_Y(2) = \sum_t p_t (1 - q_{1t})(1 - q_{2t}) \tag{2.172}$$

Now, we use the following inequality established in [63],

$$h^{(3)}(a, b, c) = \frac{1}{2} h^{(3)}(a, b, c) + \frac{1}{2} h^{(3)}(c, b, a) \tag{2.173}$$

$$\leq h^{(3)}\left(\frac{a+c}{2}, b, \frac{a+c}{2}\right) \tag{2.174}$$

$$= h(b) + 1 - b \tag{2.175}$$

where (2.174) follows by the concavity of the entropy function and by the application

of Jensen's inequality [14]. Using (2.175) and continuing from (2.169), we obtain

$$H(Y) = h^{(3)}(P_Y(0), P_Y(1), P_Y(2)) \tag{2.176}$$

$$\leq h(P_Y(1)) + 1 - P_Y(1) \tag{2.177}$$

$$= h(u) + 1 - u \tag{2.178}$$

where u is defined in (2.53). Using (2.167), (2.168) and (2.178), we can write an outer bound $\mathcal{O}_1$ on the capacity region as follows,

$$\mathcal{O}_1 = \bigcup_{(u_1,u_2,u)\in\mathcal{P}} \mathcal{O}_1(u_1, u_2, u) \tag{2.179}$$

where

$$\begin{aligned}\mathcal{O}_1(u_1, u_2, u) = \Big\{(R_1, R_2) : R_1 &\leq h(\phi(2u_1)) \\ R_2 &\leq h(\phi(2u_2)) \\ R_1 + R_2 &\leq h(u) + 1 - u\Big\}\end{aligned} \tag{2.180}$$

and the set $\mathcal{P}$ is defined in (2.86). We will now obtain a simpler characterization of $\mathcal{O}_1$ in terms of two variables (u_1, u_2) by showing that $\mathcal{O}_1 \equiv \mathcal{O}_2$, where,

$$\mathcal{O}_2 = \bigcup_{(u_1,u_2)\in\mathcal{S}} \mathcal{O}_2(u_1, u_2) \tag{2.181}$$

where

$$\mathcal{O}_2(u_1,u_2) = \Big\{(R_1,R_2) : R_1 \le h(\phi(2u_1)) \\ R_2 \le h(\phi(2u_2)) \\ R_1+R_2 \le h(f(2u_1,2u_2)) + 1 - f(2u_1,2u_2)\Big\} \tag{2.182}$$

The proof of the claim $\mathcal{O}_1 \equiv \mathcal{O}_2$ is given in the Appendix. Hence, we have an outer bound on the capacity region as given by $\mathcal{O}_2$.

The outer bound $\mathcal{O}_2$ is evaluated over the set of pairs (u_1, u_2) such that $u_1, u_2 \in [0, \frac{1}{4}]$. For any such arbitrary pair (u_1, u_2), an input distribution which achieves the set of rate pairs specified by $\mathcal{O}_2(u_1, u_2)$ is obtained by selecting $|\mathcal{T}| = 2$, and

$$p_0 = p_1 = \frac{1}{2} \tag{2.183}$$

$$q_{10} = 1 - q_{11} = \phi(2u_1) \tag{2.184}$$

$$q_{20} = 1 - q_{21} = \phi(2u_2) \tag{2.185}$$

The set of rates achievable by the distribution specified in (2.183)-(2.185) are obtained as,

$$R_1 \le H(X_1|T) = h(\phi(2u_1)) \tag{2.186}$$

$$R_2 \le H(X_2|T) = h(\phi(2u_2)) \tag{2.187}$$

$$R_1 + R_2 \le H(Y) = h(f(2u_1,2u_2)) + 1 - f(2u_1,2u_2) \tag{2.188}$$

This shows that the capacity region of binary erasure MAC-FB can be obtained by a binary and uniform selection of the auxiliary random variable T. $\square$

The capacity region of the binary erasure MAC with and without feedback and the cut-set bound are illustrated in Figures 2.6 and 2.7. It was shown in [63] that the sum-rate point on the boundary of the capacity region lies strictly below the "total cooperation" line. This is equivalent to saying that the cut-set bound is not tight for the sum-rate point. From our result, it is now clear that the cut-set bound is not tight for asymmetric rate pairs either. In fact, it is not tight at all boundary points where feedback increases capacity.

Moreover, our result also shows that a simple selection of binary and uniform T is sufficient to evaluate the boundary of the capacity region of binary erasure MAC-FB. Simple feedback strategies for a class of two user MAC-FB were developed in [38]. It was shown that for the binary erasure MAC, these feedback strategies yield all rate points for a binary selection of the auxiliary random variable T. Thus, our result shows that these feedback strategies are indeed optimal for the binary erasure MAC-FB and yield all rates on the boundary of its feedback capacity region.

2.12 Conclusions

In this chapter, we obtained a new outer bound on the capacity region of a MAC-FB by using the idea of dependence balance. We considered a binary additive noisy MAC-FB for which it is known that feedback increases capacity but the feedback capacity region is not known. The best known outer bound on the feedback capacity

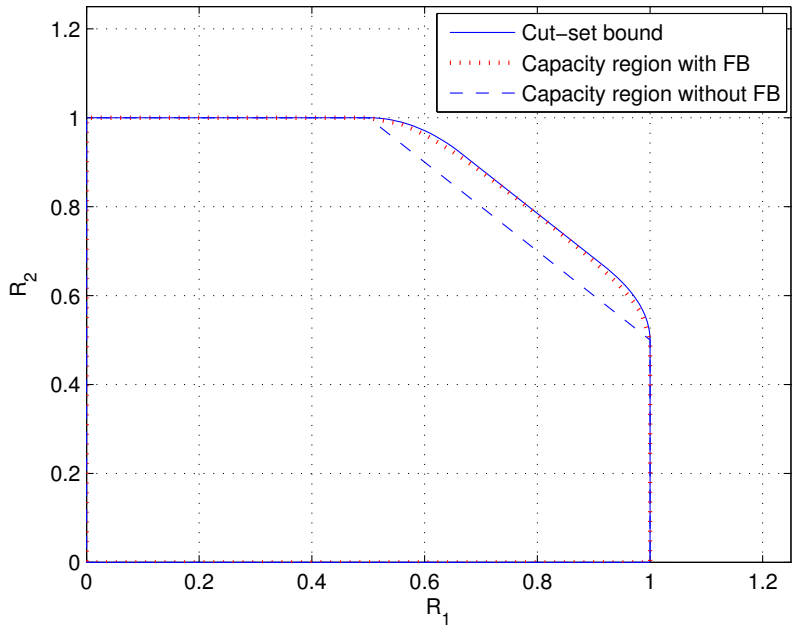

Figure 2.6: Illustration of the capacity region of binary erasure MAC-FB.

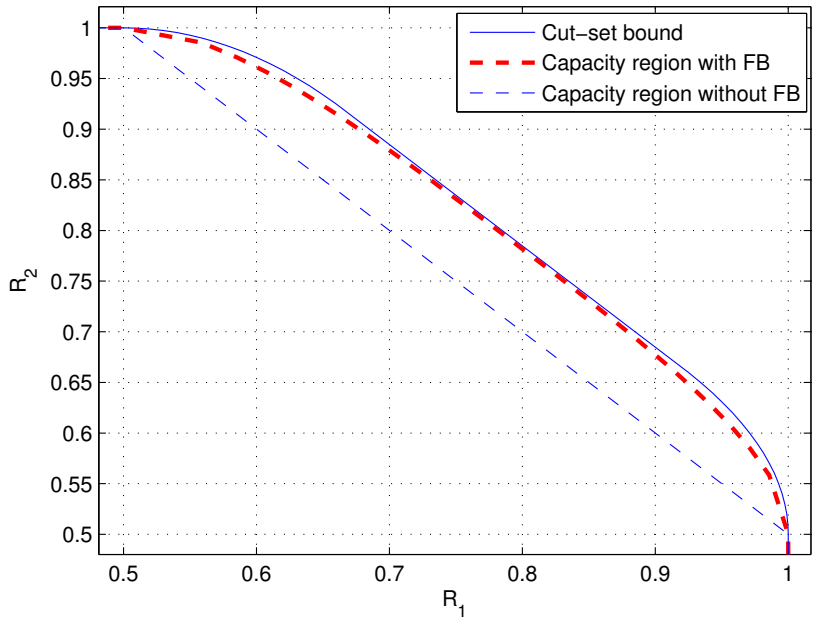

Figure 2.7: An enlarged illustration of the portion of Figure 2.6 where feedback increases capacity.

region of this channel was the cut-set bound. We used the dependence balance bound to improve upon the cut-set bound at all points in the capacity region of this channel where feedback increases capacity. Our result is somewhat surprising once it is realized that the channel we considered in this chapter is the discrete version of the two-user Gaussian MAC-FB considered by Ozarow in [45] where the cut-set bound was shown to be tight.

Our outer bound is difficult to evaluate due to an involved auxiliary random variable T. For binary inputs, the cardinality bound on T is $|\mathcal{T}| \leq 7$ which makes it intractable to evaluate the outer bound. We overcome this difficulty by making use of composite functions and their properties to obtain a simple characterization of our bound. As an application of the properties of the composite functions developed in this chapter, we are also able to completely characterize the Cover-Leung achievable rate region for this channel.

The capacity region of the binary erasure MAC-FB is known and it coincides with the Cover-Leung achievable rate region. Although the capacity region is known in principle, it is not known how to compute the entire region, the difficulty arising again due to the involved auxiliary random variable. We again make use of the composite functions to give an alternate characterization of the capacity region of the binary erasure MAC-FB. In addition, we go on to show that a binary and uniform auxiliary random variable selection is sufficient to evaluate its feedback capacity region.

2.13 Appendix

2.13.1 Proof of Lemma 2.1

For a given distribution $p(t)p(x_1|t)p(x_2|t)$, we have

$$H(X_1|Y,X_2,T) = \sum_{(y,x_2,t)} \Pr(Y=y,X_2=x_2,T=t).H(X_1|Y=y,X_2=x_2,T=t) \tag{2.189}$$

$$= \sum_t \big[\Pr(Y=1,X_2=0,T=t).H(X_1|Y=1,X_2=0,T=t) + \Pr(Y=2,X_2=1,T=t).H(X_1|Y=2,X_2=1,T=t)\big] \tag{2.190}$$

$$= \sum_t \frac{1}{2}\big[\Pr(X_2=0,T=t)H(X_1|T=t) + \Pr(X_2=1,T=t)H(X_1|T=t)\big] \tag{2.191}$$

$$= \frac{1}{2}H(X_1|T) \tag{2.192}$$

where (2.190) follows from the fact that X_1 is uniquely determined when we have $Y=0$ or $Y=3$, or we have $(Y,X_2)=(1,1)$ or $(Y,X_2)=(2,0)$ and (2.191) follows by noting that,

$$\Pr(Y=1,X_2=0,T=t) = \frac{1}{2}\Pr(X_2=0,T=t) \tag{2.193}$$

$$\Pr(Y=2,X_2=1,T=t) = \frac{1}{2}\Pr(X_2=1,T=t) \tag{2.194}$$

and

$$\Pr(X_1 = 0|Y = 1, X_2 = 0, T = t) = \Pr(X_1 = 0|T = t) \tag{2.195}$$

$$\Pr(X_1 = 0|Y = 2, X_2 = 1, T = t) = \Pr(X_1 = 0|T = t) \tag{2.196}$$

We have therefore proved (2.29) and the proof of (2.30) follows similarily. This completes the proof of Lemma 2.1.

2.13.2 Proof of Lemma 2.2

We prove Lemma 2.2 by considering all four possible cases.

1. If $s_1 \in [0, \frac{1}{2}], s_2 \in [0, \frac{1}{2}]$, then from (2.42), $s_1 = \phi(2s_1(1-s_1))$, $s_2 = \phi(2s_2(1-s_2))$ and hence

$$v = f(2s_1(1 - s_1), 2s_2(1 - s_2)) \tag{2.197}$$

2. If $s_1 \in [\frac{1}{2}, 1], s_2 \in [\frac{1}{2}, 1]$, then from (2.42), $s_1 = 1 - \phi(2s_1(1 - s_1))$, $s_2 = 1 - \phi(2s_2(1 - s_2))$ and hence

$$v = f(2s_1(1 - s_1), 2s_2(1 - s_2)) \tag{2.198}$$

3. If $s_1 \in [0, \frac{1}{2}], s_2 \in [\frac{1}{2}, 1]$, then from (2.42), $s_1 = \phi(2s_1(1-s_1))$, $s_2 = 1-\phi(2s_2(1-$

$s_2))$ and hence

$$\begin{aligned} v &= 1 - f(2s_1(1-s_1), 2s_2(1-s_2)) \\ &\overset{(a)}{\geq} f(2s_1(1-s_1), 2s_2(1-s_2)) \end{aligned} \tag{2.199}$$

where (a) follows by the fact that $f(2s_1(1-s_1), 2s_2(1-s_2)) \leq \frac{1}{2}$.

4. If $s_1 \in [\frac{1}{2}, 1], s_2 \in [0, \frac{1}{2}]$, then from (2.42), $s_1 = 1 - \phi(2s_1(1-s_1))$, $s_2 = \phi(2s_2(1-s_2))$ and hence

$$\begin{aligned} v &= 1 - f(2s_1(1-s_1), 2s_2(1-s_2)) \\ &\overset{(b)}{\geq} f(2s_1(1-s_1), 2s_2(1-s_2)) \end{aligned} \tag{2.200}$$

where (b) follows by the fact that $f(2s_1(1-s_1), 2s_2(1-s_2)) \leq \frac{1}{2}$.

Thus, for any pair (s_1, s_2), where $s_1 \in [0,1]$, $s_2 \in [0,1]$, we have shown that $v \geq f(2s_1(1-s_1), 2s_2(1-s_2))$.

2.13.3 Proof of Lemma 2.3

A function $f(x,y)$ is jointly convex [5] in (x,y) if for any two pairs, (x,y) and $(x^{'}, y^{'})$, we have $f(\alpha x + (1-\alpha)x^{'}, \alpha y + (1-\alpha)y^{'}) \leq \alpha f(x,y) + (1-\alpha) f(x^{'}, y^{'})$, for all $\alpha \in [0,1]$.

Showing that the function $f(x,y)$ is jointly convex in (x,y) is equivalent to showing that the Hessian matrix, H of $f(x,y)$ is positive semi-definite, which is equivalent to showing that the eigenvalues of H are non-negative. The Hessian matrix, H, of $f(x,y)$

is

$$H = \begin{pmatrix} \frac{\sqrt{1-2y}}{2(1-2x)^{3/2}} & \frac{-1}{2\sqrt{(1-2x)(1-2y)}} \\ \frac{-1}{2\sqrt{(1-2x)(1-2y)}} & \frac{\sqrt{1-2x}}{2(1-2y)^{3/2}} \end{pmatrix} \tag{2.201}$$

The two eigenvalues of H are

$$\begin{aligned} \lambda_1 &= 0 \\ \lambda_2 &= \frac{1}{2}\left(\frac{\sqrt{1-2y}}{(1-2x)^{3/2}} + \frac{\sqrt{1-2x}}{(1-2y)^{3/2}}\right) \end{aligned} \tag{2.202}$$

which are non-negative for all $0 \leq x \leq \frac{1}{2}$ and $0 \leq y \leq \frac{1}{2}$, thus completing the proof.

2.13.4 Proof of Lemma 2.4

It suffices to show that for a fixed u_2, the function $g(u_1, u_2)$ is monotonically decreasing in u_1. Substituting the value of $f(2u_1, 2u_2)$, we have

$$g(u_1, u_2) = \frac{1}{2}h\left(\frac{1 - (\phi(2u_1) + \phi(2u_2) - 2\phi(2u_1)\phi(2u_2))}{2}\right) \tag{2.203}$$

$$= \frac{1}{2}h\left(\frac{1}{2} - \frac{\phi(2u_2)}{2} - \frac{\phi(2u_1)(1 - 2\phi(2u_2))}{2}\right) \tag{2.204}$$

Now using the fact that $\phi(2s)$ is increasing in s for $s \in [0, \frac{1}{4}]$, we have that for $u_1^{'} \geq u_1$, $\phi(2u_1^{'}) \geq \phi(2u_1)$. Moreover, the following holds

$$\frac{\phi(2u_1^{'})(1 - 2\phi(2u_2))}{2} \geq \frac{\phi(2u_1)(1 - 2\phi(2u_2))}{2} \tag{2.205}$$

since $\phi(2u_2) \leq \frac{1}{2}$. Now using the above inequality along with the fact that the binary entropy function $h(s)$ is increasing for $0 \leq s \leq \frac{1}{2}$, we have that for $u_1^{'} \geq u_1$,

$$\begin{aligned} &\frac{1}{2}h\left(\frac{1}{2} - \frac{\phi(2u_2)}{2} - \frac{\phi(2u_1)(1-2\phi(2u_2))}{2}\right) \\ &\quad \geq \frac{1}{2}h\left(\frac{1}{2} - \frac{\phi(2u_2)}{2} - \frac{\phi(2u_1^{'})(1-2\phi(2u_2))}{2}\right) \end{aligned} \tag{2.206}$$

This shows that for a fixed u_2, the function $g(u_1, u_2)$ is monotonically decreasing in u_1. As the function is symmetric in u_1 and u_2, the monotonicity of $g(u_1, u_2)$ in (u_1, u_2) follows.

To show the concavity of $g(u_1, u_2)$ in the pair (u_1, u_2), we first note from Lemma 2.3 that $f(2u_1, 2u_2)$ is jointly convex in the pair (u_1, u_2). We define another function

$$\xi(u_1, u_2) = \frac{1 - f(2u_1, 2u_2)}{2} \tag{2.207}$$

Note that $\xi(u_1, u_2)$ is jointly concave in the pair (u_1, u_2). Furthermore, the binary entropy function $h(s)$ is concave and nondecreasing for $s \in [0, \frac{1}{2}]$. Hence, rewriting the function $g(u_1, u_2)$ as a composition of two functions, we obtain

$$g(u_1, u_2) = \frac{1}{2}h(\xi(u_1, u_2)) \tag{2.208}$$

From the theory of composite functions [5], we know that a composite function $f_1(f_2(s))$ is concave in s if $f_1(.)$ is concave and nondecreasing and $f_2(s)$ is concave in s. Identifying $f_1(.)$ with $h(.)$ and $f_2(u_1, u_2)$ with $\xi(u_1, u_2)$, the concavity of $g(u_1, u_2)$

in the pair (u_1, u_2) is established.

2.13.5 Proof of the Claim $\mathcal{O}_1 \equiv \mathcal{O}_2$

The inclusion $\mathcal{O}_2 \subseteq \mathcal{O}_1$ is straightforward by forcing $u = f(2u_1, 2u_2)$ in $\mathcal{O}_1$. We will now show that $\mathcal{O}_1 \subseteq \mathcal{O}_2$. For this purpose, we will need the following lemma.

Lemma 2.5 *The function*

$$\mu(s) = h(s) + 1 - s \tag{2.209}$$

is concave in s for $s \in [0, 1]$ and takes its maximum value at $s = \frac{1}{3}$. Moreover, the function $\mu(s)$ is increasing in s for $s \in [0, \frac{1}{3}]$ and decreasing in s for $s \in [\frac{1}{3}, 1]$.

The proof of this lemma follows from the fact that both $h(s)$ and $-s$ are concave in s.

Now consider any arbitrary triple $(u_1, u_2, u) \in \mathcal{P}$. We can classify any such triple into one of the following cases:

1. If $f(2u_1, 2u_2) \leq u \leq \frac{1}{2}$: for any such (u_1, u_2, u), there exists a pair $(\bar{u}_1, \bar{u}_2)$, such that

$$u_1 \leq \bar{u}_1 \leq \frac{1}{4} \tag{2.210}$$

$$u_2 \leq \bar{u}_2 \leq \frac{1}{4} \tag{2.211}$$

$$u = f(2\bar{u}_1, 2\bar{u}_2) \tag{2.212}$$

One such pair $(\bar{u}_1, \bar{u}_2)$ can be obtained as follows. Using the fact that for a fixed u_1, $f(2u_1, 2u_2)$ is increasing in u_2, we select $\bar{u}_1 = u_1$ and solve for $u_2 \leq \bar{u}_2 \leq \frac{1}{4}$ for which $f(2\bar{u}_1, 2\bar{u}_2) = u$. The required $\bar{u}_2$ is obtained as,

$$\bar{u}_2 = \frac{1}{4}\left(1 - \frac{(1-2u)^2}{(1-4u_1)}\right) \tag{2.213}$$

For such a pair $(\bar{u}_1, \bar{u}_2)$, the following inequalities hold,

$$h(\phi(2u_1)) = h(\phi(2\bar{u}_1)) \tag{2.214}$$

$$h(\phi(2u_2)) \leq h(\phi(2\bar{u}_2)) \tag{2.215}$$

$$h(u) + 1 - u = h(f(2\bar{u}_1, 2\bar{u}_2)) + 1 - f(2\bar{u}_1, 2\bar{u}_2) \tag{2.216}$$

2. If $f(2u_1, 2u_2) \leq \frac{1}{2} \leq u \leq 1 - (u_1 + u_2)$, then we have by Lemma 2.5,

$$h(u) + 1 - u \leq h\left(\frac{1}{2}\right) + 1 - \frac{1}{2} \tag{2.217}$$

$$= \frac{3}{2} \tag{2.218}$$

Now consider the pair $(\bar{u}_1, \bar{u}_2) = (\frac{1}{4}, \frac{1}{4})$, for which we have $f(2\bar{u}_1, 2\bar{u}_2) = \frac{1}{2}$. Hence we have that,

$$h(\phi(2u_1)) \leq h(\phi(2\bar{u}_1)) = 1 \tag{2.219}$$

$$h(\phi(2u_2)) \leq h(\phi(2\bar{u}_2)) = 1 \tag{2.220}$$

$$h(u) + 1 - u \leq h(f(2\bar{u}_1, 2\bar{u}_2)) + 1 - f(2\bar{u}_1, 2\bar{u}_2) = \frac{3}{2} \tag{2.221}$$

We have thus shown that for any triple (u_1, u_2, u), there exists a pair $(\bar{u}_1, \bar{u}_2)$, such that $\mathcal{O}_1(u_1, u_2, u) \subseteq \mathcal{O}_2(\bar{u}_1, \bar{u}_2)$, which in turn implies that $\mathcal{O}_1 \subseteq \mathcal{O}_2$, and consequently $\mathcal{O}_1 \equiv \mathcal{O}_2$.

Chapter 3

Dependence Balance Based Outer Bounds for Gaussian Networks with Cooperation and Feedback

3.1 Introduction

The multiple access channel with generalized feedback (MAC-GF) was first introduced by Carleial [8]. The model therein allows for different feedback signals at the two transmitters. For this channel model, Carleial [8] obtained an achievable rate region using block Markov superposition encoding and windowed decoding. An improvement over this achievable rate region was obtained by Willems et. al. in [65] by using block Markov superposition encoding combined with backwards decoding.

Inspired from the uplink MAC-GF channel model, the interference channel with generalized feedback (IC-GF) was studied in [57], [31], (also see the references therein) where achievable rate regions were obtained. It was shown in [57] and [31] that for the Gaussian interference channel with user cooperation (IC-UC), the overheard information at the transmitters has a dual effect of enabling cooperation and mitigating interference, thereby providing improved achievable rates compared to the best known evaluation of the Han-Kobayashi achievable rate region [28], [49].

In this chapter, we use the idea of dependence balance to obtain new outer bounds on the capacity regions of the MAC-GF and the IC-GF. To show the usefulness of our outer bounds, we will consider three different channel models.

We first consider the Gaussian MAC with different noisy feedback signals at the two transmitters. Specifically, transmitter k, $k = 1, 2$, receives a feedback $Y_{F_k} = Y + Z_k$, where Y is the received signal and Z_k is zero-mean, Gaussian random variable with variance $\sigma^2_{Z_k}$. The capacity region is only known when feedback is noiseless, i.e., $Y_{F_1} = Y_{F_2} = Y$, in which case the feedback capacity region equals the cut-set outer bound, as was shown by Ozarow [45]. For the case of noisy feedback in consideration, the cut-set outer bound is insensitive to the noise in feedback links, i.e., it is not sensitive to the variances of Z_1 and Z_2. As the feedback becomes more corrupted, or in other words, as $\sigma^2_{Z_1}, \sigma^2_{Z_2}$ become large, one would expect the feedback to become useless. This fact is not accounted for by the cut-set bound. We show that our outer bound strictly improves upon the cut-set bound for all non-zero values of $(\sigma^2_{Z_1}, \sigma^2_{Z_2})$. Furthermore, as $(\sigma^2_{Z_1}, \sigma^2_{Z_2})$ become large, our outer bound collapses to the capacity region of Gaussian MAC without feedback, thereby establishing the feedback capacity region. We should mention here that applying the idea of dependence balance to obtain improved outer bounds for Gaussian MAC with noisy feedback was proposed by Gastpar and Kramer in [20].

Secondly, we investigate the Gaussian MAC with transmitter cooperation. Sendonaris, Erkip and Aazhang [53] studied a model where each transmitter receives a version of the other transmitter's current channel input corrupted with additive white Gaussian noise. They named this model as *user cooperation* model. This model is particularly

suitable for a wireless setting since the transmitters can potentially overhear each other. An achievable rate region for the user cooperation model was given in [53] using the result of [65] and was shown to strictly exceed the rate region if the transmitters ignore the overheard signals.

We evaluate our outer bound for the user cooperation setting described above. In contrast to the case of noisy feedback, the cut-set bound for the user cooperation model is sensitive to cooperation noise variances, but not too sensitive. Intuitively speaking, as the backward noise variances become large, one would expect the cut-set bound to collapse to the capacity region of the MAC without feedback. Instead, the cut-set bound converges to the capacity region of the Gaussian MAC with noiseless output feedback [45]. On the other hand, in the limit when cooperation noise variances become too large, our bound converges to the capacity region of the Gaussian MAC with no cooperation, thereby yielding a capacity result. For all non-zero and finite values of cooperation noise variances, our outer bound strictly improves upon the cut-set outer bound. Our dependence balance based outer bound coincides with the cut-set bound only when the backward noise variance is identically zero and both outer bounds collapse to the total cooperation line.

Thirdly, we evaluate our outer bound for the Gaussian IC with user cooperation (IC-UC). For all non-zero and finite values of cooperation noise variances, our outer bound strictly improves upon the cut-set outer bound. We should remark here that the approach of dependence balance was also used in [21] to obtain an improved sum-rate upper bound for the Gaussian IC with common, noisy feedback from the receivers.

Evaluation of our outer bounds for MAC-NF, MAC-UC and IC-UC is not straightforward since our outer bounds are expressed in terms of a union of probability densities of three random variables, one of which is an auxiliary random variable. Moreover, these unions are over all such densities which satisfy a non-trivial dependence balance constraint. We overcome this difficulty by proving separately for all three models in consideration, that it is sufficient to consider jointly Gaussian input distributions, satisfying the dependence balance constraint, when evaluating our outer bounds. The proof methodology for showing this claim is entirely different for each of the cases of noisy feedback and user cooperation models. In particular, for the case of MAC-NF, we make use of a recently discovered multivariate generalization [46] of Costa's entropy power inequality (EPI) [10] along with some properties of 3×3 covariance matrices to obtain this result. On the other hand, for the case of MAC-UC and IC-UC, we do not need EPI to show this result and our proof closely follows the proof of a recent result by Bross, Lapidoth and Wigger [7], [60] for the Gaussian MAC with conferencing encoders. The structure of dependence balance constraints for the channel models in consideration are of different form, which explains the different methodology of proofs.

For the most general setting of MAC-GF and IC-GF, our outer bounds are expressed in terms of two auxiliary random variables. For the three channel models in consideration, i.e., MAC-NF, MAC-UC and IC-UC, we suitably modify our outer bounds to express them in terms of only one auxiliary random variable. These modifications are particularly helpful in their explicit evaluation. We also believe that the proof methodology developed for evaluating our outer bounds could be helpful for

other multi-user information theoretic problems.

3.2 System Model

3.2.1 MAC with Generalized Feedback

A discrete memoryless two-user multiple access channel with generalized feedback (MAC-GF) (see Figure 3.1) is defined by: two input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, an output alphabet for the receiver $\mathcal{Y}$, feedback output alphabets $\mathcal{Y}_{F_1}$ and $\mathcal{Y}_{F_2}$ at transmitters 1 and 2, respectively, and a probability transition function $p(y, y_{F_1}, y_{F_2}|x_1, x_2)$, defined for all triples $(y, y_{F_1}, y_{F_2}) \in \mathcal{Y} \times \mathcal{Y}_{F_1} \times \mathcal{Y}_{F_2}$, for every pair $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$.

A (n, M_1, M_2, P_e) code for the MAC-GF consists of two sets of encoding functions $f_{1i} : \mathcal{M}_1 \times \mathcal{Y}_{F_1}^{i-1} \to \mathcal{X}_1$, $f_{2i} : \mathcal{M}_2 \times \mathcal{Y}_{F_2}^{i-1} \to \mathcal{X}_2$ for $i = 1, \ldots, n$ and a decoding function $g : \mathcal{Y}^n \to \mathcal{M}_1 \times \mathcal{M}_2$. The two transmitters produce independent and uniformly distributed messages $W_1 \in \{1, \ldots, M_1\}$ and $W_2 \in \{1, \ldots, M_2\}$, respectively, and transmit them through n channel uses. The average error probability is defined as, $P_e = \Pr[(\hat{W}_1, \hat{W}_2) \neq (W_1, W_2)]$. A rate pair (R_1, R_2) is said to be achievable for MAC-GF if for any $\epsilon \geq 0$, there exists a pair of n encoding functions $\{f_{1i}\}_{i=1}^n$, $\{f_{2i}\}_{i=1}^n$, and a decoding function $g : \mathcal{Y}^n \to \mathcal{M}_1 \times \mathcal{M}_2$ such that $R_1 \leq \log(M_1)/n$, $R_2 \leq \log(M_2)/n$ and $P_e \leq \epsilon$ for sufficiently large n. The capacity region of MAC-GF is the closure of the set of all achievable rate pairs (R_1, R_2).

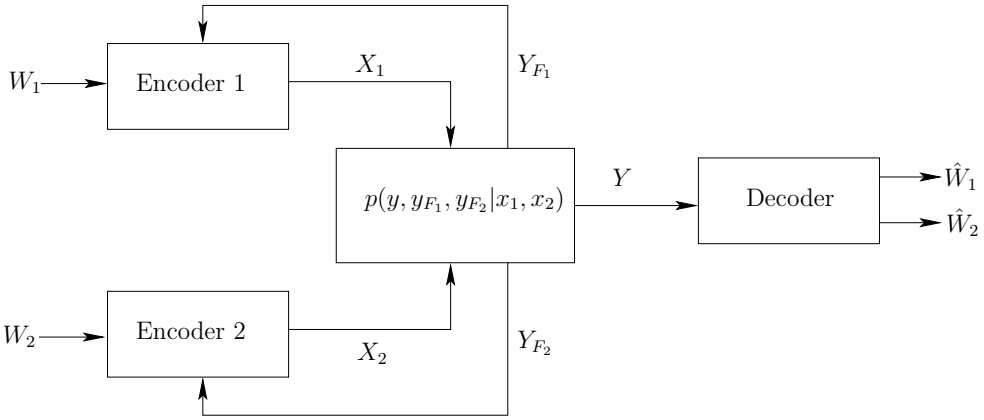

Figure 3.1: The multiple access channel with generalized feedback (MAC-GF).

3.2.2 IC with Generalized Feedback

A discrete memoryless two-user interference channel with generalized feedback (IC-GF) (see Figure 3.2) is defined by: two input alphabets $\mathcal{X}_1$ and $\mathcal{X}_2$, two output alphabets $\mathcal{Y}_1$ and $\mathcal{Y}_2$ at receivers 1 and 2, respectively, two feedback output alphabets $\mathcal{Y}_{F_1}$ and $\mathcal{Y}_{F_2}$ at transmitters 1 and 2, respectively, and a probability transition function $p(y_1, y_2, y_{F_1}, y_{F_2}|x_1, x_2)$, defined for all quadruples $(y_1, y_2, y_{F_1}, y_{F_2}) \in \mathcal{Y}_1 \times \mathcal{Y}_2 \times \mathcal{Y}_{F_1} \times \mathcal{Y}_{F_2}$, for every pair $(x_1, x_2) \in \mathcal{X}_1 \times \mathcal{X}_2$.

A $(n, M_1, M_2, P_e^{(1)}, P_e^{(2)})$ code for IC-GF consists of two sets of encoding functions $f_{1i} : \mathcal{M}_1 \times \mathcal{Y}_{F_1}^{i-1} \to \mathcal{X}_1$, $f_{2i} : \mathcal{M}_2 \times \mathcal{Y}_{F_2}^{i-1} \to \mathcal{X}_2$ for $i = 1, \ldots, n$ and two decoding functions $g_1 : \mathcal{Y}_1^n \to \mathcal{M}_1$ and $g_2 : \mathcal{Y}_2^n \to \mathcal{M}_2$. The two transmitters produce independent and uniformly distributed messages $W_1 \in \{1, \ldots, M_1\}$ and $W_2 \in \{1, \ldots, M_2\}$, respectively, and transmit them through n channel uses. The average error probability at receivers 1 and 2 are defined as, $P_e^{(k)} = \Pr[\hat{W}_k \neq W_k]$ for $k = 1, 2$. A rate pair (R_1, R_2) is said to be achievable for IC-GF if for any pair $\epsilon_1 \geq 0, \epsilon_2 \geq 0$, there exists a pair of n encoding functions $\{f_{1i}\}_{i=1}^n$, $\{f_{2i}\}_{i=1}^n$, and a pair of decoding functions

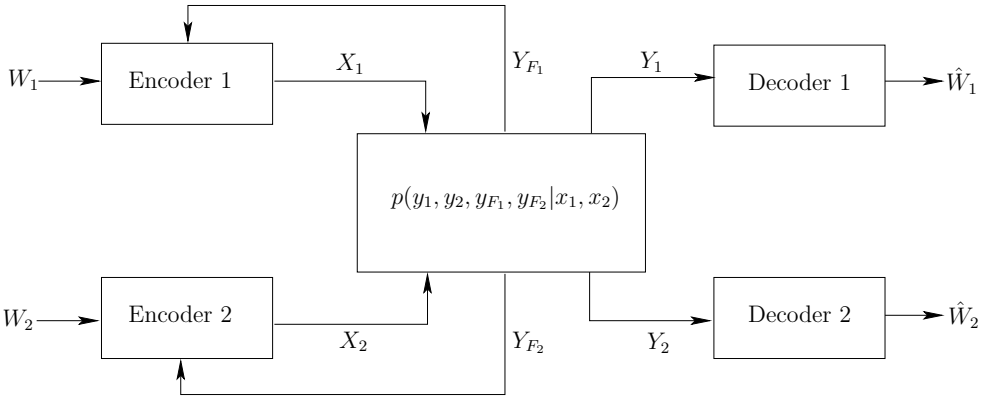

Figure 3.2: The interference channel with generalized feedback (IC-GF).

(g_1, g_2) such that $R_1 \leq \log(M_1)/n$, $R_2 \leq \log(M_2)/n$ and $P_e^{(k)} \leq \epsilon_k$ for sufficiently large n, for $k = 1, 2$. The capacity region of IC-GF is the closure of the set of all achievable rate pairs (R_1, R_2).

3.3 Cut-set Outer Bounds

A general outer bound on the capacity region of a multi-terminal network is the cut-set outer bound [14]. The cut-set outer bound for MAC-GF is given by

$$\mathcal{CS}^{MAC} = \big\{(R_1, R_2) : R_1 \leq I(X_1; Y, Y_{F_2}|X_2) \tag{3.1}$$

$$R_2 \leq I(X_2; Y, Y_{F_1}|X_1) \tag{3.2}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\big\} \tag{3.3}$$

where the random variables X_1, X_2 and (Y, Y_{F_1}, Y_{F_2}) have the joint distribution

$$p(x_1, x_2, y, y_{F_1}, y_{F_2}) = p(x_1, x_2)p(y, y_{F_1}, y_{F_2}|x_1, x_2). \tag{3.4}$$

The cut-set outer bound for IC-GF is given by

$$\mathcal{CS}^{IC} = \big\{(R_1, R_2) : R_1 \leq I(X_1, X_2; Y_1) \tag{3.5}$$

$$R_2 \leq I(X_1, X_2; Y_2) \tag{3.6}$$

$$R_1 \leq I(X_1; Y_1, Y_2, Y_{F_2}|X_2) \tag{3.7}$$

$$R_2 \leq I(X_2; Y_1, Y_2, Y_{F_1}|X_1) \tag{3.8}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y_1, Y_2)\big\} \tag{3.9}$$

where the random variables X_1, X_2 and $(Y_1, Y_2, Y_{F_1}, Y_{F_2})$ have the joint distribution

$$p(x_1, x_2, y_1, y_2, y_{F_1}, y_{F_2}) = p(x_1, x_2)p(y_1, y_2, y_{F_1}, y_{F_2}|x_1, x_2). \tag{3.10}$$

The cut-set bound is seemingly loose since it allows arbitrary correlation among channel inputs by permitting arbitrary input distributions $p(x_1, x_2)$. Using the approach of dependence balance, we will obtain outer bounds for MAC-GF and IC-GF which restrict the corresponding set of input distributions for both channel models. In particular, our outer bounds only permit those input distributions which satisfy the respective non-trivial dependence balance constraints.

3.4 A New Outer Bound for MAC-GF

Theorem 3.1 *The capacity region of MAC-GF is contained in the region*

$$\mathcal{DB}^{MAC} = \big\{(R_1, R_2) : R_1 \leq I(X_1; Y, Y_{F_2}|X_2, T_2) \tag{3.11}$$

$$R_2 \leq I(X_2; Y, Y_{F_1}|X_1, T_1) \tag{3.12}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, Y_{F_1}, Y_{F_2}|T_1, T_2) \tag{3.13}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\big\} \tag{3.14}$$

where the random variables $(T_1, T_2, X_1, X_2, Y, Y_{F_1}, Y_{F_2})$ *have the joint distribution*

$$p(t_1, t_2, x_1, x_2, y, y_{F_1}, y_{F_2}) = p(t_1, t_2, x_1, x_2)p(y, y_{F_1}, y_{F_2}|x_1, x_2) \tag{3.15}$$

and also satisfy the following dependence balance bound

$$I(X_1; X_2|T_1, T_2) \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T_1, T_2) \tag{3.16}$$

The proof of Theorem 3.1 is given in the Appendix.

3.5 A New Outer Bound for IC-GF

Theorem 3.2 *The capacity region of IC-GF is contained in the region*

$$\mathcal{DB}^{IC} = \big\{(R_1, R_2) : R_1 \leq I(X_1, X_2; Y_1) \tag{3.17}$$

$$R_2 \leq I(X_1, X_2; Y_2) \tag{3.18}$$

$$R_1 \leq I(X_1; Y_1, Y_2, Y_{F_2} | X_2, T_2) \tag{3.19}$$

$$R_2 \leq I(X_2; Y_1, Y_2, Y_{F_1} | X_1, T_1) \tag{3.20}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y_1, Y_2, Y_{F_1}, Y_{F_2} | T_1, T_2) \tag{3.21}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y_1, Y_2)\big\} \tag{3.22}$$

where the random variables $(T_1, T_2, X_1, X_2, Y_1, Y_2, Y_{F_1}, Y_{F_2})$ *have the joint distribution*

$$p(t_1, t_2, x_1, x_2, y_1, y_2, y_{F_1}, y_{F_2}) = p(t_1, t_2, x_1, x_2) p(y_1, y_2, y_{F_1}, y_{F_2} | x_1, x_2) \tag{3.23}$$

and also satisfy the following dependence balance bound

$$I(X_1; X_2 | T_1, T_2) \leq I(X_1; X_2 | Y_{F_1}, Y_{F_2}, T_1, T_2) \tag{3.24}$$

The proof of Theorem 3.2 is given in the Appendix.

We note here that one can obtain fixed and adaptive parallel channel extensions of the dependence balance based bounds in a similar fashion as in [30]. The parallel channel extensions could potentially improve upon the outer bounds derived in this chapter. For the scope of this chapter, we will only use Theorems 3.1 and 3.2. In

the next three sections, we will consider specific channel models of MAC with noisy feedback, MAC with user cooperation, and IC with user cooperation and specialize Theorems 3.1 and 3.2 for these channel models. In particular, we will show that for these three channel models, it is sufficient to employ a single auxiliary random variable T, as opposed to two auxiliary random variables T_1 and T_2 appearing in Theorems 3.1 and 3.2.

We should also remark here that dependence balance approach was first applied by Gastpar and Kramer for the Gaussian MAC with noisy feedback in [20] and for the Gaussian IC with noisy feedback (IC-NF) in [21]. An interesting Lagrangian based approach was proposed in [21] to partially evaluate the dependence balance based outer bound for the Gaussian IC-NF and it was shown that dependence balance based bounds strictly improve upon the cut-set outer bound. For this reason, we do not consider the Gaussian IC-NF in this chapter.

3.6 Gaussian MAC with Noisy Feedback

We first consider the Gaussian MAC with noisy feedback (see Figure 3.3). The channel model is given as,

$$Y = X_1 + X_2 + Z \tag{3.25}$$

$$Y_{F_1} = Y + Z_1 \tag{3.26}$$

$$Y_{F_2} = Y + Z_2 \tag{3.27}$$

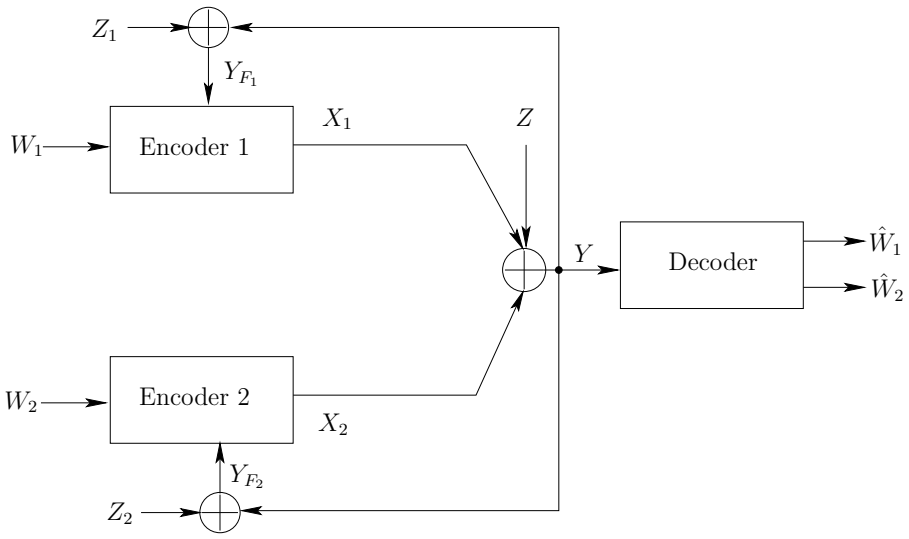

Figure 3.3: The Gaussian MAC with noisy feedback.

where Z,Z_1 and Z_2 are independent, zero-mean, Gaussian random variables with variances σ_Z^2, $\sigma_{Z_1}^2$ and $\sigma_{Z_2}^2$, respectively. Moreover, the channel inputs are subject to average power constraints, $E[X_1^2] \leq P_1$ and $E[X_2^2] \leq P_2$. Note that the channel model described above has a special probability structure, namely,

$$p(y, y_{F_1}, y_{F_2}|x_1, x_2) = p(y|x_1, x_2)p(y_{F_1}|y)p(y_{F_2}|y) \tag{3.28}$$

For any MAC-GF with a transition probability in the form of (3.28), we have the following strengthened version of Theorem 3.1.

Theorem 3.3 *The capacity region of any MAC-GF, with a transition probability in*

the form of (3.28), is contained in the region

$$\mathcal{DB}_{NF}^{MAC} = \big\{(R_1, R_2) : R_1 \leq I(X_1; Y|X_2, T) \tag{3.29}$$

$$R_2 \leq I(X_2; Y|X_1, T) \tag{3.30}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y|T)\big\} \tag{3.31}$$

where the random variables $(T, X_1, X_2, Y, Y_{F_1}, Y_{F_2})$ *have the joint distribution*

$$p(t, x_1, x_2, y, y_{F_1}, y_{F_2}) = p(t, x_1, x_2)p(y|x_1, x_2)p(y_{F_1}|y)p(y_{F_2}|y) \tag{3.32}$$

and also satisfy the following dependence balance bound

$$I(X_1; X_2|T) \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T) \tag{3.33}$$

where the random variable T *is subject to a cardinality constraint* $|\mathcal{T}| \leq |\mathcal{X}_1||\mathcal{X}_2| + 3$.

The proof of Theorem 3.3 is given in the Appendix.

In Section 3.10, we will show that it suffices to consider jointly Gaussian (T, X_1, X_2) satisfying (3.33) when evaluating Theorem 3.3 for the Gaussian MAC with noisy feedback described in (3.25)-(3.27).

3.7 Gaussian MAC with User Cooperation

In this section, we consider the Gaussian MAC with user cooperation [53], where each transmitter receives a noisy version of the other transmitter's channel input.

The user cooperation model (see Figure 3.4) is a special instance of a MAC-GF, where the channel outputs are described as,

$$Y = \sqrt{h_{10}}X_1 + \sqrt{h_{20}}X_2 + Z \tag{3.34}$$

$$Y_{F_1} = \sqrt{h_{21}}X_2 + Z_1 \tag{3.35}$$

$$Y_{F_2} = \sqrt{h_{12}}X_1 + Z_2 \tag{3.36}$$

where Z,Z_1 and Z_2 are independent, zero-mean, Gaussian random variables with variances σ_Z^2, $\sigma_{Z_1}^2$ and $\sigma_{Z_2}^2$, respectively. The channel gains h_{10}, h_{20}, h_{12} and h_{21} are assumed to be fixed and known at all terminals. Moreover, the channel inputs are subject to average power constraints, $E[X_1^2] \leq P_1$ and $E[X_2^2] \leq P_2$. Note that the channel model described above has a special probability structure, namely,

$$p(y, y_{F_1}, y_{F_2}|x_1, x_2) = p(y|x_1, x_2)p(y_{F_1}|x_2)p(y_{F_2}|x_1) \tag{3.37}$$

For any MAC-GF with a transition probability in the form of (3.37), we have the following strengthened version of Theorem 3.1.

Theorem 3.4 *The capacity region of any MAC-GF with a transition probability in*

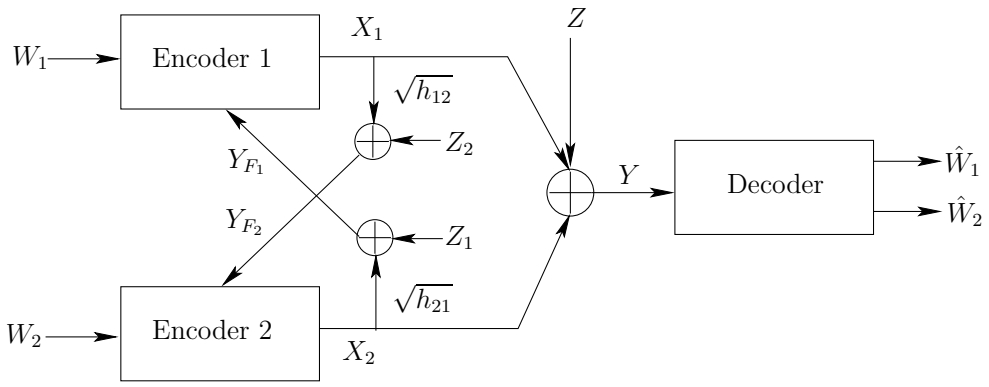

Figure 3.4: The Gaussian MAC with user cooperation.

the form of (3.37), is contained in the region

$$\mathcal{DB}_{UC}^{MAC} = \big\{(R_1, R_2) : R_1 \leq I(X_1; Y, Y_{F_2}|X_2, T) \tag{3.38}$$

$$R_2 \leq I(X_2; Y, Y_{F_1}|X_1, T) \tag{3.39}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, Y_{F_1}, Y_{F_2}|T) \tag{3.40}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y)\big\} \tag{3.41}$$

where the random variables $(T, X_1, X_2, Y, Y_{F_1}, Y_{F_2})$ *have the joint distribution*

$$p(t, x_1, x_2, y, y_{F_1}, y_{F_2}) = p(t, x_1, x_2)p(y|x_1, x_2)p(y_{F_1}|x_2)p(y_{F_2}|x_1) \tag{3.42}$$

and also satisfy the following dependence balance bound

$$I(X_1; X_2|T) \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T) \tag{3.43}$$

where the random variable T *is subject to a cardinality constraint* $|\mathcal{T}| \leq |\mathcal{X}_1||\mathcal{X}_2| + 3$.

The proof of Theorem 3.4 is given in the Appendix.

In Section 3.11, we will show that it suffices to consider jointly Gaussian (T, X_1, X_2) satisfying (3.43) when evaluating Theorem 3.4 for the Gaussian MAC with user cooperation described in (3.34)-(3.36).

3.8 Gaussian IC with User Cooperation

In this section, we will evaluate our outer bound for a user cooperation setting [57], [31], where the transmitters receive noisy versions of the other transmitter's channel input. The user cooperation model (see Figure 3.5) is a special instance of an IC-GF, where the channel outputs are described as,

$$Y_1 = X_1 + \sqrt{b}X_2 + N_1 \tag{3.44}$$

$$Y_2 = \sqrt{a}X_1 + X_2 + N_2 \tag{3.45}$$

$$Y_{F_1} = \sqrt{h_{21}}X_2 + Z_1 \tag{3.46}$$

$$Y_{F_2} = \sqrt{h_{12}}X_1 + Z_2 \tag{3.47}$$

where $N_1, N_2,\ Z_1$ and Z_2 are independent, zero-mean, Gaussian random variables with variances $\sigma^2_{N_1}, \sigma^2_{N_2}, \sigma^2_{Z_1}$ and $\sigma^2_{Z_2}$, respectively. The channel gains a, b, h_{12} and h_{21} are assumed to be fixed and known at all terminals. Moreover, the channel inputs are subject to average power constraints, $E[X_1^2] \leq P_1$ and $E[X_2^2] \leq P_2$. Note that the channel model described above has a special probability structure, namely,

$$p(y_1, y_2, y_{F_1}, y_{F_2}|x_1, x_2) = p(y_1, y_2|x_1, x_2)p(y_{F_1}|x_2)p(y_{F_2}|x_1) \tag{3.48}$$

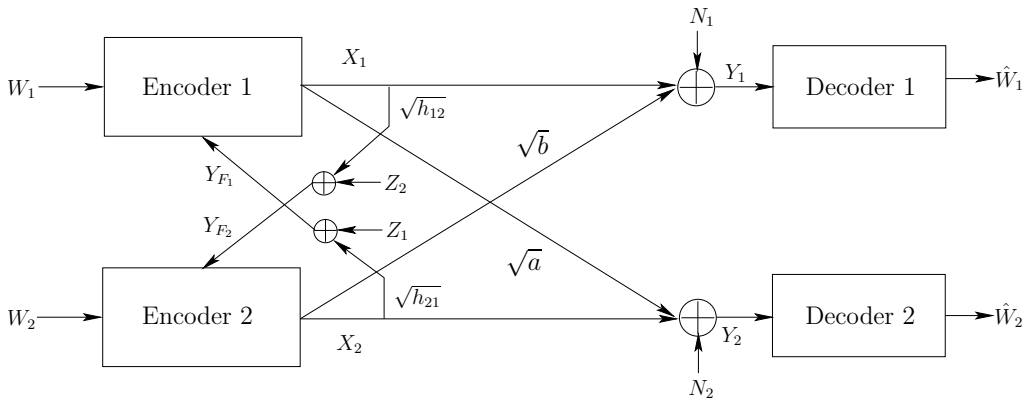

Figure 3.5: The Gaussian IC with user cooperation.

For any IC-GF with a transition probability in the form of (3.48), we have the following strengthened version of Theorem 3.2.

Theorem 3.5 *The capacity region of any IC-GF with a transition probability in the form of (3.48), is contained in the region*

$$\mathcal{DB}_{UC}^{IC} = \big\{(R_1, R_2) : R_1 \le I(X_1, X_2; Y_1) \tag{3.49}$$

$$R_2 \le I(X_1, X_2; Y_2) \tag{3.50}$$

$$R_1 \le I(X_1; Y_1, Y_2, Y_{F_2} | X_2, T) \tag{3.51}$$

$$R_2 \le I(X_2; Y_1, Y_2, Y_{F_1} | X_1, T) \tag{3.52}$$

$$R_1 + R_2 \le I(X_1, X_2; Y_1, Y_2, Y_{F_1}, Y_{F_2} | T) \tag{3.53}$$

$$R_1 + R_2 \le I(X_1, X_2; Y_1, Y_2)\big\} \tag{3.54}$$

where the random variables $(T, X_1, X_2, Y_1, Y_2, Y_{F_1}, Y_{F_2})$ *have the joint distribution*

$$p(t, x_1, x_2, y_1, y_2, y_{F_1}, y_{F_2}) = p(t, x_1, x_2) p(y_1, y_2 | x_1, x_2) p(y_{F_1} | x_2) p(y_{F_2} | x_1) \tag{3.55}$$

and also satisfy the following dependence balance bound

$$I(X_1; X_2|T) \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T) \tag{3.56}$$

where the random variable T is subject to a cardinality constraint $|\mathcal{T}| \leq |\mathcal{X}_1||\mathcal{X}_2| + 3$.

The proof of Theorem 3.5 is given in the Appendix.

In Section 3.12, we will show that it suffices to consider jointly Gaussian (T, X_1, X_2) satisfying (3.56) when evaluating Theorem 3.5 for the Gaussian IC with user cooperation described in (3.44)-(3.47).

3.9 Outline for Evaluating $\mathcal{DB}_{NF}^{MAC}$, $\mathcal{DB}_{UC}^{MAC}$ and $\mathcal{DB}_{UC}^{IC}$

In this section, we outline the common approach for evaluation of our outer bounds, $\mathcal{DB}_{NF}^{MAC}$ for the Gaussian MAC with noisy feedback, $\mathcal{DB}_{UC}^{MAC}$ for the Gaussian MAC with user-cooperation and $\mathcal{DB}_{UC}^{IC}$ for the Gaussian IC with user-cooperation. The main difficulty in evaluating these bounds is to identify the optimal selection of joint densities of (T, X_1, X_2). Our aim will be to prove that it is sufficient to consider jointly Gaussian (T, X_1, X_2) satisfying (3.33) for MAC with noisy feedback, (3.43) for MAC with user cooperation, and (3.56) for IC with user cooperation, respectively, when evaluating the corresponding outer bounds.

First note that the three outer bounds, namely $\mathcal{DB}_{NF}^{MAC}$, $\mathcal{DB}_{UC}^{MAC}$ and $\mathcal{DB}_{UC}^{IC}$ have a similar structure, i.e., all outer bounds involve taking a union over joint densities of (T, X_1, X_2) satisfying the constraints (3.33), (3.43) and (3.56), respectively. Let

us symbolically denote these constraints as a variable (DB), where $(DB) = (3.33)$ for MAC with noisy feedback, $(DB) = (3.43)$ for MAC with user cooperation, and $(DB) = (3.56)$ for IC with user cooperation.

We begin by considering the set of all distributions of three random variables (T, X_1, X_2) which satisfy the power constraints, $E\big[X_1^2\big] \leq P_1$ and $E\big[X_2^2\big] \leq P_2$. Let us formally define this set of input distributions as

$$\mathcal{P} = \{p(t, x_1, x_2) : E\big[X_1^2\big] \leq P_1, E\big[X_2^2\big] \leq P_2\}$$

For simplicity, we abbreviate jointly Gaussian distributions as $\mathcal{JG}$ and distributions which are not jointly Gaussian as $\mathcal{NG}$. We first partition $\mathcal{P}$ into two disjoint subsets,

$$\mathcal{P}_G = \{p(t, x_1, x_2) \in \mathcal{P} : (T, X_1, X_2) \text{ are } \mathcal{JG}\}$$

$$\mathcal{P}_{NG} = \{p(t, x_1, x_2) \in \mathcal{P} : (T, X_1, X_2) \text{ are } \mathcal{NG}\}$$

We further individually partition the sets $\mathcal{P}_G$ and $\mathcal{P}_{NG}$, respectively, as

$$\mathcal{P}_G^{DB} = \{p(t, x_1, x_2) \in \mathcal{P}_G : (T, X_1, X_2) \text{ satisfy } (DB)\}$$

$$\mathcal{P}_G^{\overline{DB}} = \{p(t, x_1, x_2) \in \mathcal{P}_G : (T, X_1, X_2) \text{ do not satisfy } (DB)\}$$

and

$$\mathcal{P}_{NG}^{DB} = \{p(t, x_1, x_2) \in \mathcal{P}_{NG} : (T, X_1, X_2) \text{ satisfy } (DB)\}$$

$$\mathcal{P}_{NG}^{\overline{DB}} = \{p(t, x_1, x_2) \in \mathcal{P}_{NG} : (T, X_1, X_2) \text{ do not satisfy } (DB)\}$$

Finally, we partition the set $\mathcal{P}_{NG}^{DB}$ into two disjoint sets $\mathcal{P}_{NG}^{DB(a)}$ and $\mathcal{P}_{NG}^{DB(b)}$ with $\mathcal{P}_{NG}^{DB} = \mathcal{P}_{NG}^{DB(a)} \bigcup \mathcal{P}_{NG}^{DB(b)}$, as

$$\mathcal{P}_{NG}^{DB(a)} = \big\{p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB} : \text{ covariance matrix of } p(t, x_1, x_2) \text{ is } Q \text{ and there exists a } \mathcal{JG} \ (T_G, X_{1G}, X_{2G}) \text{ with covariance matrix } Q \text{ satisfying } (DB)\big\}$$

$$\mathcal{P}_{NG}^{DB(b)} = \big\{p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB} : \text{ covariance matrix of } p(t, x_1, x_2) \text{ is } Q \text{ and there does not exist a } \mathcal{JG} \ (T_G, X_{1G}, X_{2G}) \text{ with covariance matrix } Q \text{ satisfying } (DB)\big\}$$

So far, we have partitioned the set of input distributions into five disjoint sets: $\mathcal{P}_G^{DB}$, $\mathcal{P}_G^{\overline{DB}}$, $\mathcal{P}_{NG}^{DB(a)}$, $\mathcal{P}_{NG}^{DB(b)}$ and $\mathcal{P}_{NG}^{\overline{DB}}$. To visualize this partition of the set of input distributions, see Figure 3.6. It is clear that the input distributions which fall into the sets $\mathcal{P}_G^{\overline{DB}}$ and $\mathcal{P}_{NG}^{\overline{DB}}$ need not be considered since they do not satisfy the constraint (DB) and do not have any consequence when evaluating our outer bounds. Therefore, we only need to restrict our attention on the three remaining sets $\mathcal{P}_G^{DB}$, $\mathcal{P}_{NG}^{DB(a)}$, and $\mathcal{P}_{NG}^{DB(b)}$ i.e., those input distributions which satisfy the dependence balance bound.

We explicitly evaluate our outer bound in the following three steps:

1. We first explicitly characterize the region of rate pairs provided by our outer bound for the probability distributions in the set $\mathcal{P}_G^{DB}$.

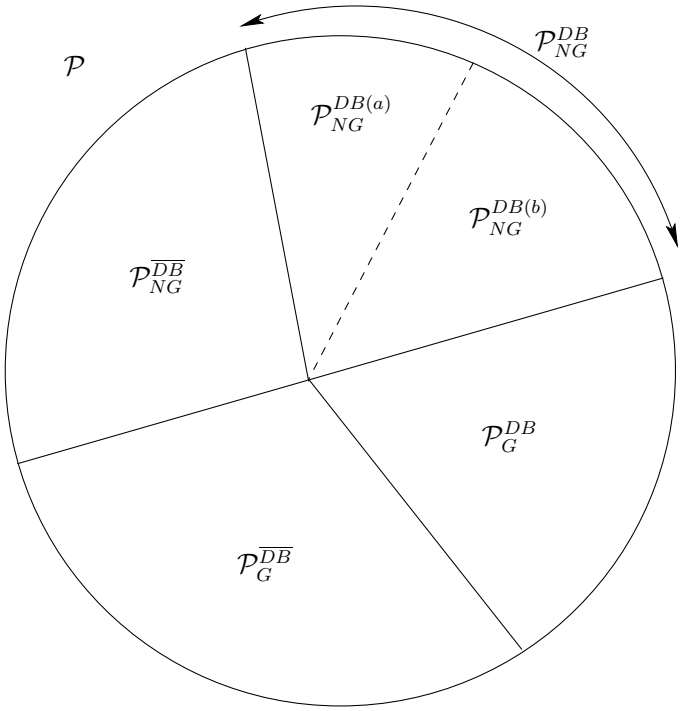

Figure 3.6: A partition of the set of input distributions $\mathcal{P}$.

2. In the second step, we will show that for any input distribution belonging to the set $\mathcal{P}_{NG}^{DB(a)}$, there exists an input distribution in the set $\mathcal{P}_{G}^{DB}$ which yields a set of larger rate pairs. This leads to the conclusion that we do not need to consider the input distributions in the set $\mathcal{P}_{NG}^{DB(a)}$ in evaluating our outer bound.

3. We next focus on the set $\mathcal{P}_{NG}^{DB(b)}$ and show that for any non-Gaussian input distribution $p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB(b)}$, we can construct a jointly Gaussian input distribution satisfying (DB), i.e., we can find a corresponding input distribution in $\mathcal{P}_{G}^{DB}$, which yields a set of rates which includes the set of rates of the fixed non-Gaussian input distribution $p(t, x_1, x_2)$.

The main step in evaluating our outer bounds is step 3 described above. The proofs of step 3 for noisy feedback and user cooperation models are entirely different

and do not follow from each other. The evaluation in step 1 is slightly different for all three settings, also owing to the channel models. Hence, we will separately focus on these models in the following three sections. Contrary to steps 1 and 3, step 2 is common for all channel models. Therefore, we first present the common result for all channel models here. In step 2, we consider any non-Gaussian input distribution $p(t, x_1, x_2)$ in $\mathcal{P}_{NG}^{DB(a)}$ with a covariance matrix Q. For such an input distribution, we know by the maximum entropy theorem [14], that the rates provided by a jointly Gaussian triple with the same covariance matrix Q are always at least as large as the rates provided by the chosen non-Gaussian distribution. Therefore, for any input distribution in $\mathcal{P}_{NG}^{DB(a)}$, there always exists an input distribution in $\mathcal{P}_{G}^{DB}$, satisfying (DB), which yields larger rates. This means that we can ignore the set $\mathcal{P}_{NG}^{DB(a)}$ altogether while evaluating our outer bounds.

To set the stage for our evaluations in steps 1 and 3 for the three channel models, let us define $\mathcal{Q}$ as the set of all valid 3×3 covariance matrices of three random variables (T, X_1, X_2). A typical element Q in the set $\mathcal{Q}$ takes the following form,

$$\begin{aligned} Q &= E\big[(X_1\, X_2\, T)(X_1\, X_2\, T)^T\big] \\ &= \begin{pmatrix} P_1 & \rho_{12}\sqrt{P_1 P_2} & \rho_{1T}\sqrt{P_1 P_T} \\ \rho_{12}\sqrt{P_1 P_2} & P_2 & \rho_{2T}\sqrt{P_2 P_T} \\ \rho_{1T}\sqrt{P_1 P_T} & \rho_{2T}\sqrt{P_2 P_T} & P_T \end{pmatrix} \end{aligned} \tag{3.57}$$

A necessary condition for Q to be a valid covariance matrix is that it is positive

semi-definite, i.e., $\det(Q) \geq 0$. This is equivalent to saying that,

$$\det(Q) = P_1 P_2 P_T \Delta \geq 0 \tag{3.58}$$

where we have defined for simplicity,

$$\Delta = 1 - \rho_{12}^2 - \rho_{1T}^2 - \rho_{2T}^2 + 2\rho_{1T}\rho_{2T}\rho_{12} \tag{3.59}$$

3.10 Evaluation of $\mathcal{DB}_{NF}^{MAC}$

In this section we explicitly evaluate Theorem 3.3 for the Gaussian MAC with noisy feedback described by (3.25)-(3.27) in Section 3.6. We start with step 1. We consider an input distribution in $\mathcal{P}_G^{DB}$, i.e., a jointly Gaussian triple (T_G, X_{1G}, X_{2G}) with a covariance matrix Q. Let us first characterize the set of rate constraints for this triple. It is straightforward to evaluate the three rate constraints appearing in (3.29)-(3.31) for this input distribution

$$R_1 \leq I(X_{1G}; Y|X_{2G}, T_G) = \frac{1}{2}\log\left(1 + \frac{f_1(Q)}{\sigma_Z^2}\right) \tag{3.60}$$

$$R_2 \leq I(X_{2G}; Y|X_{1G}, T_G) = \frac{1}{2}\log\left(1 + \frac{f_2(Q)}{\sigma_Z^2}\right) \tag{3.61}$$

$$R_1 + R_2 \leq I(X_{1G}, X_{2G}; Y|T_G) = \frac{1}{2}\log\left(1 + \frac{f_3(Q)}{\sigma_Z^2}\right) \tag{3.62}$$

where we have defined

$$f_1(Q) = \mathrm{Var}(X_{1G}|X_{2G}, T_G) = \frac{\Delta P_1}{(1-\rho_{2T}^2)} \tag{3.63}$$

$$f_2(Q) = \mathrm{Var}(X_{2G}|X_{1G}, T_G) = \frac{\Delta P_2}{(1-\rho_{1T}^2)} \tag{3.64}$$

$$\begin{aligned} f_3(Q) &= \mathrm{Var}(X_{1G}|T_G) + \mathrm{Var}(X_{2G}|T_G) + 2\mathrm{Cov}(X_{1G}, X_{2G}|T_G) \\ &= (1-\rho_{1T}^2)P_1 + (1-\rho_{2T}^2)P_2 + 2(\rho_{12} - \rho_{1T}\rho_{2T})\sqrt{P_1 P_2} \end{aligned} \tag{3.65}$$

Finally, evaluating the constraint in (3.33), we conclude that this input distribution satisfies the constraint in (3.33) iff,

$$f_3(Q) \leq f_1(Q) + f_2(Q) + \frac{f_1(Q) f_2(Q)}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2 \sigma_{Z_2}^2}{(\sigma_{Z_1}^2 + \sigma_{Z_2}^2)}\right)} \tag{3.66}$$

To summarize, the set of rate pairs provided by an input distribution in $\mathcal{P}_G^{DB}$, with a covariance matrix Q, are given by those in (3.60)-(3.62), where $f_i(Q)$, $i = 1, 2, 3$, in those inequalities are subject to the constraint in (3.66). As we have discussed earlier, from evaluation of step 2 in Section 3.9, we know that all rate pairs contributed by input distributions in $\mathcal{P}_{NG}^{DB(a)}$ are covered by those given in $\mathcal{P}_G^{DB}$.

We now arrive at step 3 of our evaluation. Consider any input distribution $p(t, x_1, x_2)$ in $\mathcal{P}_{NG}^{DB(b)}$ with a covariance matrix Q. By the definition of the set $\mathcal{P}_{NG}^{DB(b)}$, we know that Q does not satisfy (3.33), which implies

$$f_3(Q) > f_1(Q) + f_2(Q) + \frac{f_1(Q) f_2(Q)}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2 \sigma_{Z_2}^2}{(\sigma_{Z_1}^2 + \sigma_{Z_2}^2)}\right)} \tag{3.67}$$

We also note that for any (T, X_1, X_2) with a covariance matrix Q,

$$R_1 \leq I(X_1; Y|X_2, T) \leq \frac{1}{2}\log\left(1 + \frac{f_1(Q)}{\sigma_Z^2}\right) \tag{3.68}$$

$$R_2 \leq I(X_2; Y|X_1, T) \leq \frac{1}{2}\log\left(1 + \frac{f_2(Q)}{\sigma_Z^2}\right) \tag{3.69}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y|T) \leq \frac{1}{2}\log\left(1 + \frac{f_3(Q)}{\sigma_Z^2}\right) \tag{3.70}$$

which is a simple consequence of the maximum entropy theorem [14]. Note that so far, we have not used the fact that the given non-Gaussian input distribution satisfies the dependence balance constraint in (3.33). We will now make use of this fact by rewriting (3.33) as follows,

$$0 \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T) - I(X_1; X_2|T) \tag{3.71}$$

$$= I(X_1; Y_{F_1}, Y_{F_2}|X_2, T) - I(X_1; Y_{F_1}, Y_{F_2}|T) \tag{3.72}$$

$$= h(Y_{F_1}, Y_{F_2}|X_1, T) + h(Y_{F_1}, Y_{F_2}|X_2, T) - h(Y_{F_1}, Y_{F_2}|T) - h(Y_{F_1}, Y_{F_2}|X_1, X_2, T) \tag{3.73}$$

We express the above constraint as,

$$h(Y_{F_1}, Y_{F_2}|T) + h(Y_{F_1}, Y_{F_2}|X_1, X_2, T) \leq h(Y_{F_1}, Y_{F_2}|X_1, T) + h(Y_{F_1}, Y_{F_2}|X_2, T) \tag{3.74}$$

Before proceeding, we state a recently discovered multivariate generalization [46] of Costa's EPI [10].

Lemma 3.1 *For any arbitrary random vector* $\mathbf{Y} \in \mathbb{R}^2$*, independent of* $\mathbf{V} \in \mathbb{R}^2$*,*

where $\mathbf{V}$ *is a zero-mean, Gaussian random vector with each component having unit variance, the entropy power* $N(\Lambda^{1/2}\mathbf{Y}+\mathbf{V})$ *is concave in* Λ*, where the entropy power is defined as*

$$N(\mathbf{Y}) = \frac{1}{(2\pi e)} e^{h(\mathbf{Y})} \tag{3.75}$$

and Λ *is a diagonal matrix with components* (λ_1, λ_2)*.*

We can therefore write for any pair of diagonal matrices Λ_1, Λ_2 and for any $\mu \in [0,1]$,

$$\mu N(\Lambda_1^{1/2}\mathbf{Y}+\mathbf{V}) + (1-\mu)N(\Lambda_2^{1/2}\mathbf{Y}+\mathbf{V}) \leq N((\mu\Lambda_1 + (1-\mu)\Lambda_2)^{1/2}\mathbf{Y}+\mathbf{V}) \tag{3.76}$$

We start by obtaining a lower bound for the first term $h(Y_{F_1}, Y_{F_2}|T)$ in (3.74),

$$\begin{aligned} h(Y_{F_1}, Y_{F_2}|T) &= \int f_T(t) h(Y+Z_1, Y+Z_2|T=t)dt & (3.77)\\ &\geq \int f_T(t) \frac{1}{2}\log\left((2\pi\mathrm{e})^2\sigma_{Z_1}^2\sigma_{Z_2}^2 + 2\pi\mathrm{e}(\sigma_{Z_1}^2+\sigma_{Z_2}^2)\mathrm{e}^{h(Y|T=t)}\right)dt & (3.78)\\ &\geq \frac{1}{2}\log\left((2\pi\mathrm{e})^2\sigma_{Z_1}^2\sigma_{Z_2}^2 + 2\pi\mathrm{e}(\sigma_{Z_1}^2+\sigma_{Z_2}^2)\mathrm{e}^{h(Y|T)}\right) & (3.79)\end{aligned}$$

where (3.78) follows from the conditional version of Lemma 3.1, by selecting the following Λ_1, Λ_2 and μ

$$\Lambda_1 = \begin{pmatrix} \kappa & 0 \\ 0 & 0 \end{pmatrix}, \quad \Lambda_2 = \begin{pmatrix} 0 & 0 \\ 0 & \kappa \end{pmatrix} \tag{3.80}$$

where

$$\kappa = \frac{(\sigma_{Z_1}^2 + \sigma_{Z_2}^2)}{\sigma_{Z_1}^2 \sigma_{Z_2}^2} \tag{3.81}$$

and

$$\mu = \frac{\sigma_{Z_2}^2}{(\sigma_{Z_1}^2 + \sigma_{Z_2}^2)} \tag{3.82}$$

and by making the following substitutions,

$$V_1 = \frac{Z_1}{\sigma_{Z_1}}, \quad V_2 = \frac{Z_2}{\sigma_{Z_2}} \tag{3.83}$$

where $\mathbf{V} = [V_1 \quad V_2]^T$ and $\mathbf{Y} = [Y \quad Y]^T$. A derivation of (3.78) is given in the Appendix. Next, (3.79) follows from the fact that $\log(\mathrm{e}^x c_1 + c_2)$ is convex in x for $c_1, c_2 \geq 0$ and a subsequent application of Jensen's inequality [14][1].

We next obtain an upper bound for the right hand side of (3.74) by using the maximum entropy theorem as,

$$\begin{aligned} &h(Y_{F_1}, Y_{F_2}|X_1, T) + h(Y_{F_1}, Y_{F_2}|X_2, T) \\ &\qquad \leq \frac{1}{2}\log\left((2\pi\mathrm{e})^4 (f_1(Q)(\sigma_{Z_1}^2 + \sigma_{Z_2}^2) + \eta)(f_2(Q)(\sigma_{Z_1}^2 + \sigma_{Z_2}^2) + \eta)\right) \end{aligned} \tag{3.84}$$

[1] We should remark here, that an application of the regular form of vector EPI yields the following trivial lower bound on $h(Y_{F_1}, Y_{F_2}|T)$ and therefore, the new EPI is crucial for this step.

$$h(Y_{F_1}, Y_{F_2}|T) \geq \frac{1}{2}\log\left((2\pi\mathrm{e})^2 \sigma_{Z_1}^2 \sigma_{Z_2}^2\right)$$

where we have defined

$$\eta = \sigma_{Z_1}^2 \sigma_{Z_2}^2 + \sigma_Z^2(\sigma_{Z_1}^2 + \sigma_{Z_2}^2) \tag{3.85}$$

Now, using (3.74), (3.79) and (3.84), we obtain an upper bound on $h(Y|T)$ as follows,

$$h(Y|T) \leq \frac{1}{2}\log\left((2\pi \mathrm{e})(\sigma_Z^2 + f(Q))\right) \tag{3.86}$$

where we have defined for simplicity,

$$f(Q) = f_1(Q) + f_2(Q) + \frac{f_1(Q) f_2(Q)}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2 \sigma_{Z_2}^2}{(\sigma_{Z_1}^2 + \sigma_{Z_2}^2)}\right)} \tag{3.87}$$

Using (3.86), we obtain an upper bound on the sum-rate $I(X_1, X_2; Y|T)$ for any non-Gaussian distribution in $\mathcal{P}_{NG}^{DB(b)}$ as,

$$R_1 + R_2 \leq I(X_1, X_2; Y|T) \leq \frac{1}{2}\log\left(1 + \frac{f(Q)}{\sigma_Z^2}\right) \tag{3.88}$$

Comparing with (3.70) and using the fact that Q satisfies (3.67), i.e., $f(Q) < f_3(Q)$, we have the following set of inequalities,

$$R_1 + R_2 \leq I(X_1, X_2; Y|T) \leq \frac{1}{2}\log\left(1 + \frac{f(Q)}{\sigma_Z^2}\right) < \frac{1}{2}\log\left(1 + \frac{f_3(Q)}{\sigma_Z^2}\right) \tag{3.89}$$

This leads to the observation that a combined application of the EPI and the dependence balance bound yields a strictly smaller upper bound for $I(X_1, X_2; Y|T)$ for

any distribution in $\mathcal{P}_{NG}^{DB(b)}$ than the one provided by the maximum entropy theorem. Therefore, the rate pairs contributed by an input distribution in $\mathcal{P}_{NG}^{DB(b)}$ with a covariance matrix Q are always included in the set of rate pairs expressed by (3.68), (3.69) and (3.88), where $f(Q)$ is defined in (3.87).

We now arrive at the final step of our evaluation where we will show that for this input distribution in $\mathcal{P}_{NG}^{DB(b)}$, we can always find an input distribution in $\mathcal{P}_{G}^{DB}$, with a set of rate pairs which include the set of rate pairs expressed by (3.68), (3.69) and (3.88). In particular, we will show the existence of a valid covariance matrix S for which the following inequalities hold true,

$$f_1(Q) \leq f_1(S) \tag{3.90}$$

$$f_2(Q) \leq f_2(S) \tag{3.91}$$

$$f(Q) \leq f_3(S) \tag{3.92}$$

and

$$f_3(S) = f_1(S) + f_2(S) + \frac{f_1(S) f_2(S)}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2 \sigma_{Z_2}^2}{(\sigma_{Z_1}^2 + \sigma_{Z_2}^2)}\right)} \tag{3.93}$$

Inequalities in (3.90)-(3.92) will guarantee that a Gaussian input distribution with covariance matrix S yields a larger set of rate pairs than the set of rate pairs expressed by (3.68), (3.69) and (3.88) and the equality in (3.93) guarantees that this input distribution satisfies the dependence balance constraint with equality, hence it is a member of the set $\mathcal{P}_{G}^{DB}$.

Before showing the existence of such an S, we first characterize the set of covariance matrices Q which satisfy (3.67). First recall that for any Q to be a valid covariance matrix, we had the condition $\det(Q) \geq 0$ which is equivalent to $\Delta \geq 0$, which amounts to

$$1 - \rho_{12}^2 - \rho_{1T}^2 - \rho_{2T}^2 + 2\rho_{1T}\rho_{2T}\rho_{12} \geq 0 \tag{3.94}$$

In particular, it is easy to verify that for any given fixed pair $(\rho_{1T}, \rho_{2T}) \in [-1, 1] \times [-1, 1]$, the set of ρ_{12} which yield a valid Q are such that,

$$\rho_{1T}\rho_{2T} - \lambda \leq \rho_{12} \leq \rho_{1T}\rho_{2T} + \lambda \tag{3.95}$$

where we have defined

$$\lambda = \sqrt{(1 - \rho_{1T}^2)(1 - \rho_{2T}^2)} \tag{3.96}$$

We now consider two cases which can arise for a given covariance matrix Q.

Case 1. Q is such that $\rho_{12} = \rho_{1T}\rho_{2T} - \alpha$, for some $\alpha \in [0, \lambda]$: This case is rather trivial and the following simple choice of S works,

$$\rho_{1T}^{(S)} = \rho_{1T}, \quad \rho_{2T}^{(S)} = \rho_{2T} \tag{3.97}$$

$$\rho_{12}^{(S)} = \rho_{1T}\rho_{2T} \tag{3.98}$$

Clearly, this S satisfies the dependence balance bound. Moreover, the following in-

equalities hold as well,

$$f_1(Q) \leq f_1(S) = (1 - \rho_{1T}^2)P_1 \tag{3.99}$$

$$f_2(Q) \leq f_2(S) = (1 - \rho_{2T}^2)P_2 \tag{3.100}$$

$$f(Q) < f_3(Q) \tag{3.101}$$

$$= (1 - \rho_{1T}^2)P_1 + (1 - \rho_{2T}^2)P_2 - 2\alpha\sqrt{P_1 P_2} \tag{3.102}$$

$$\leq (1 - \rho_{1T}^2)P_1 + (1 - \rho_{2T}^2)P_2 \tag{3.103}$$

$$= f_3(S) \tag{3.104}$$

Case 2. Q is such that $\rho_{12} = \rho_{1T}\rho_{2T} + \alpha_0$, for some $\alpha_0 \in (0, \lambda]$ and Q satisfies (3.67): For this case, we will construct a valid covariance matrix S as follows,

$$\rho_{1T}^{(S)} = \rho_{1T}, \quad \rho_{2T}^{(S)} = \rho_{2T} \tag{3.105}$$

$$\rho_{12}^{(S)} = \rho_{1T}\rho_{2T} + \alpha^*, \qquad \text{for some } 0 < \alpha^* < \alpha_0 \tag{3.106}$$

We define a parameterized covariance matrix $Q(\alpha)$ with entries,

$$\rho_{1T}(\alpha) = \rho_{1T}, \quad \rho_{2T}(\alpha) = \rho_{2T} \tag{3.107}$$

$$\rho_{12}(\alpha) = \rho_{1T}\rho_{2T} + \alpha \tag{3.108}$$

where $0 \leq \alpha \leq \alpha_0$. We now define a function of the parameter α of a valid covariance

matrix $Q(\alpha)$ as,

$$g(\alpha) = f_1(Q(\alpha)) + f_2(Q(\alpha)) + \frac{f_1(Q(\alpha))f_2(Q(\alpha))}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2\sigma_{Z_2}^2}{(\sigma_{Z_1}^2+\sigma_{Z_2}^2)}\right)} - f_3(Q(\alpha)) \tag{3.109}$$

Now note the fact that

$$g(0) = \frac{(1-\rho_{1T}^2)(1-\rho_{2T}^2)P_1P_2}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2\sigma_{Z_2}^2}{(\sigma_{Z_1}^2+\sigma_{Z_2}^2)}\right)} > 0 \tag{3.110}$$

We are also given that Q satisfies (3.67) for some α_0, which implies that,

$$g(\alpha_0) < 0 \tag{3.111}$$

Now, we take the first derivative of the function $g(\alpha)$, to obtain,

$$\frac{dg(\alpha)}{d\alpha} = -2\alpha\left(\frac{P_1}{(1-\rho_{2T}^2)} + \frac{P_2}{(1-\rho_{1T}^2)}\right) - \frac{4\alpha P_1P_2}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2\sigma_{Z_2}^2}{(\sigma_{Z_1}^2+\sigma_{Z_2}^2)}\right)}\left(1 - \left(\frac{\alpha}{\lambda}\right)^2\right) - 2\sqrt{P_1P_2}$$

$$\leq 0$$

which implies that $g(\alpha)$ is monotonically decreasing in α. This implies that there exists an $\alpha^* \in (0, \alpha_0)$ such that $g(\alpha^*) = 0$[2]. We use this α^* to construct our new

[2]We should remark here that the existence of an $\alpha^* \in (0, \alpha_0)$, with $g(\alpha^*) = 0$ can also be proved alternatively by invoking the mean value theorem, since we have $g(0) > 0$, $g(\alpha_0) < 0$ and $g(\alpha)$ is a continuous function of α. Monotonicity of $g(\alpha)$ in fact proves a stronger statement that such an α^* exists and is also unique.

covariance matrix S as follows,

$$\rho_{1T}^{(S)} = \rho_{1T}, \quad \rho_{2T}^{(S)} = \rho_{2T} \tag{3.112}$$

$$\rho_{12}^{(S)} = \rho_{1T}\rho_{2T} + \alpha^* \tag{3.113}$$

It now remains to check wether S satisfies the four conditions in (3.90)-(3.93). The condition (3.93) is met with equality, since we have $g(\alpha^*) = 0$. Moreover, $f_1(Q) = f_1(Q(\alpha_0)) \leq f_1(Q(\alpha^*)) = f_1(S)$ since $f_1(Q(\alpha))$ is monotonically decreasing in α for $\alpha \in [0, \lambda]$. Similarly, we also have $f_2(Q) \leq f_2(S)$. Finally,

$$f(Q) = f_1(Q) + f_2(Q) + \frac{f_1(Q)f_2(Q)}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2\sigma_{Z_2}^2}{(\sigma_{Z_1}^2+\sigma_{Z_2}^2)}\right)} \tag{3.114}$$

$$\leq f_1(S) + f_2(S) + \frac{f_1(S)f_2(S)}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2\sigma_{Z_2}^2}{(\sigma_{Z_1}^2+\sigma_{Z_2}^2)}\right)} \tag{3.115}$$

$$= f_3(S) \tag{3.116}$$

This shows the existence of a valid covariance matrix S which satisfies (3.33) and yields a set of rates which includes the set of rates of the given non-Gaussian distribution with the covariance matrix Q.

Above two cases show that for any non-Gaussian distribution $p(t, x_1, x_2)$ in the set $\mathcal{P}_{NG}^{DB(b)}$, we can always find a jointly Gaussian triple (T_G, X_{1G}, X_{2G}) in $\mathcal{P}_G^{DB}$ that yields a set of rates subsuming the set of rates of the given non-Gaussian distribution. This consequently completes the proof of the statement that it is sufficient to consider jointly Gaussian (T, X_1, X_2) in $\mathcal{P}_G^{DB}$ when evaluating our outer bound.

The dependence balance based outer bound can now be written in an explicit form as follows,

$$\mathcal{DB}_{NF}^{MAC} = \bigcup_{Q \in \mathcal{Q}^{DB}} \Bigg\{ (R_1, R_2) : R_1 \leq \frac{1}{2}\log\left(1 + \frac{f_1(Q)}{\sigma_Z^2}\right) \\ R_2 \leq \frac{1}{2}\log\left(1 + \frac{f_2(Q)}{\sigma_Z^2}\right) \\ R_1 + R_2 \leq \frac{1}{2}\log\left(1 + \frac{f_3(Q)}{\sigma_Z^2}\right) \Bigg\} \tag{3.117}$$

where $\mathcal{Q}^{DB}$ is the set of 3×3 covariance matrices of the form (3.57) satisfying,

$$f_3(Q) \leq f_1(Q) + f_2(Q) + \frac{f_1(Q) f_2(Q)}{\left(\sigma_Z^2 + \frac{\sigma_{Z_1}^2 \sigma_{Z_2}^2}{(\sigma_{Z_1}^2 + \sigma_{Z_2}^2)}\right)} \tag{3.118}$$

where

$$f_1(Q) = \frac{\Delta P_1}{(1 - \rho_{2T}^2)} \tag{3.119}$$

$$f_2(Q) = \frac{\Delta P_2}{(1 - \rho_{1T}^2)} \tag{3.120}$$

$$f_3(Q) = (1 - \rho_{1T}^2)P_1 + (1 - \rho_{2T}^2)P_2 + 2(\rho_{12} - \rho_{1T}\rho_{2T})\sqrt{P_1 P_2} \tag{3.121}$$

and

$$\Delta = 1 - \rho_{1T}^2 - \rho_{2T}^2 - \rho_{12}^2 + 2\rho_{1T}\rho_{2T}\rho_{12} \tag{3.122}$$

where ρ_{12}, ρ_{1T} and ρ_{2T} are all in $[-1, 1]$.

The cut-set outer bound given in (3.1)-(3.4) is evaluated for the Gaussian MAC with noisy feedback described in (3.25)-(3.27) as

$$\mathcal{CS}_{NF}^{MAC} = \bigcup_{\rho \in [0,1]} \Bigg\{ (R_1, R_2) : R_1 \leq \frac{1}{2}\log\left(1 + \frac{(1-\rho^2)P_1}{\sigma_Z^2}\right) \\ R_2 \leq \frac{1}{2}\log\left(1 + \frac{(1-\rho^2)P_2}{\sigma_Z^2}\right) \\ R_1 + R_2 \leq \frac{1}{2}\log\left(1 + \frac{P_1 + P_2 + 2\rho\sqrt{P_1 P_2}}{\sigma_Z^2}\right) \Bigg\} \quad (3.123)$$

We briefly mention what our outer bound gives for the the two limiting values of the backward noise variances $\sigma_{Z_1}^2$ and $\sigma_{Z_2}^2$.

1. $\sigma_{Z_1}^2, \sigma_{Z_2}^2 \to 0$: this case corresponds to the Gaussian MAC with noiseless feedback and the constraint (3.118) simplifies to

$$f_3(Q) \leq f_1(Q) + f_2(Q) + \frac{f_1(Q) f_2(Q)}{\sigma_Z^2} \quad (3.124)$$

which is simply stating that the sum-rate constraint should be at most as large as the sum of the individual rate constraints, i.e., another equivalent way of writing is

$$\frac{1}{2}\log\left(1 + \frac{f_3(Q)}{\sigma_Z^2}\right) \leq \frac{1}{2}\log\left(1 + \frac{f_1(Q)}{\sigma_Z^2}\right) + \frac{1}{2}\log\left(1 + \frac{f_2(Q)}{\sigma_Z^2}\right) \quad (3.125)$$

This is the same constraint as obtained by Ozarow in [45], and our outer bound coincides with the cut-set bound and yields the capacity region of the Gaussian

MAC with noiseless feedback.

2. $\sigma_{Z_1}^2, \sigma_{Z_2}^2 \to \infty$: this case corresponds to very noisy feedback and our outer bound should collapse to the no-feedback capacity region of the Gaussian MAC. For this case, the constraint (3.118) simplifies to,

$$f_3(Q) \leq f_1(Q) + f_2(Q) \tag{3.126}$$

On substituting the values of $f_1(Q), f_2(Q)$ and $f_3(Q)$ in the above inequality, we obtain

$$(\rho_{12} - \rho_{1T}\rho_{2T}) \leq \frac{((1-\rho_{1T}^2)P_1 + (1-\rho_{2T}^2)P_2)}{2\sqrt{P_1 P_2}} \left(\frac{\Delta}{\lambda^2} - 1\right) \tag{3.127}$$

$$\leq 0 \tag{3.128}$$

where the last inequality comes from the fact that for any valid covariance matrix, $\Delta \leq \lambda^2$. This implies that the dependence balance bound only allows such covariance matrices Q for which $\rho_{12} \leq \rho_{1T}\rho_{2T}$. But we know already from (3.97)-(3.98) that we can always find an S for which we can select $\rho_{12}^{(S)} = \rho_{1T}\rho_{2T}$, which satisfies the dependence balance bound and yields larger rates than any Q with $\rho_{12} < \rho_{1T}\rho_{2T}$. Thus, we only need to restrict our attention to those matrices Q for which $\rho_{12} = \rho_{1T}\rho_{2T}$. Such covariance matrices Q correspond to those jointly Gaussian triples which satisfy the Markov chain $X_1 \to T \to X_2$. This can be observed by noting that for any jointly Gaussian (T, X_1, X_2), with a covariance matrix Q, the condition $I(X_1; X_2|T) = 0$ holds iff $\mathrm{Var}(X_1|T) =$

$\mathrm{Var}(X_1|X_2,T)$, which is equivalent to $\rho_{12} = \rho_{1T}\rho_{2T}$. Proof of this statement is immediate by noting that for a jointly Gaussian triple, we have

$$I(X_1;X_2|T) = \frac{1}{2}\log\left(\frac{\mathrm{Var}(X_1|T)}{\mathrm{Var}(X_1|X_2,T)}\right) \tag{3.129}$$

Therefore, T can be interpreted simply as a timesharing random variable and our outer bound yields the capacity region of the Gaussian MAC without feedback.

Figure 3.7 illustrates $\mathcal{DB}_{NF}^{MAC}$, the cut-set bound and the capacity region without feedback for the cases when $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 2$, 5 and 10, where $P_1 = P_2 = \sigma_Z^2 = 1$. Figure 3.8 illustrates $\mathcal{DB}_{NF}^{MAC}$, the cut-set bound, the capacity region without feedback and an achievable rate region based on superposition coding [65] for the case when $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 0.3$ and $P_1 = P_2 = \sigma_Z^2 = 1$.

3.10.1 Remark

For the special case of Gaussian MAC with common, noisy feedback, where

$$Y_{F_1} = Y_{F_2} = Y + V \tag{3.130}$$

the evaluation of $\mathcal{DB}_{NF}^{MAC}$ follows in a similar manner as in the case of different noisy feedback signals. The only difference arises in the application of the EPI. In particular, the regular EPI [14] suffices to provide a non-trivial upper bound on $I(X_1,X_2;Y|T)$ than the one provided by the maximum entropy theorem [14]. The remainder of the proof of evaluation of our outer bound for this channel model follows along the same

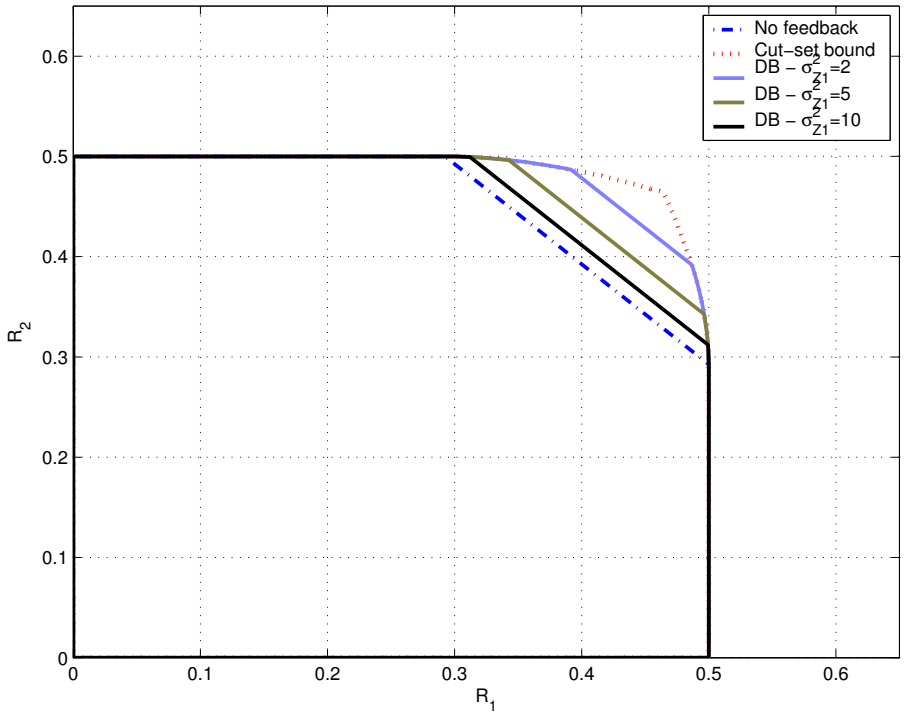

Figure 3.7: Illustration of outer bounds for $P_1 = P_2 = \sigma_Z^2 = 1$ and $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 2, 5, 10$.

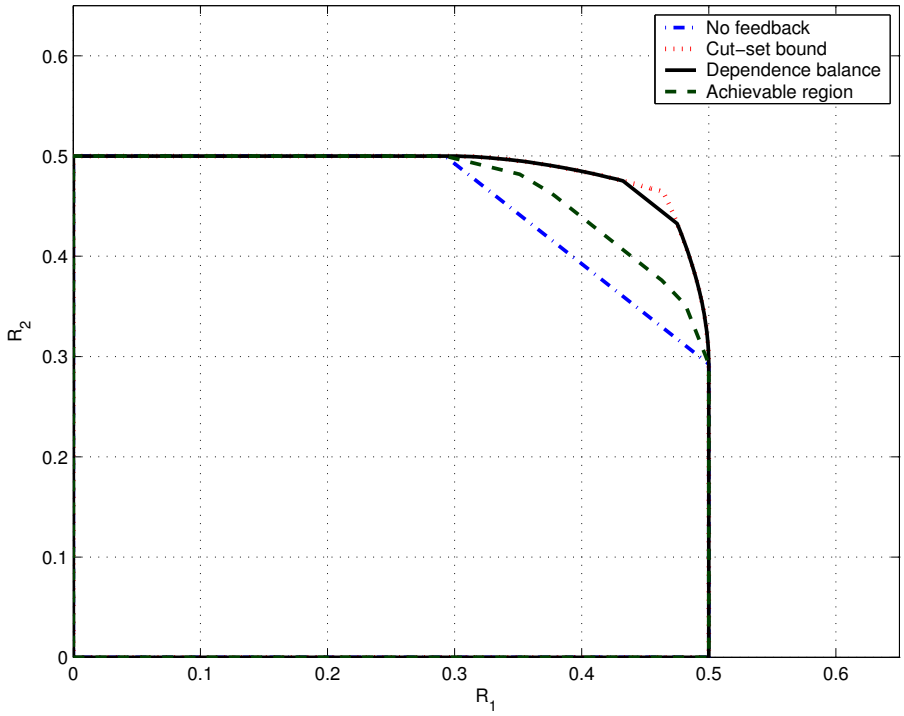

Figure 3.8: Illustration of outer bound and an achievable region based on superposition coding for $P_1 = P_2 = \sigma_Z^2 = 1$ and $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 0.3$.

lines as the proof for different noisy feedback signals. The final expressions of outer bounds for these two channel models only differ over the constraint (3.118). For the case of common, noisy feedback, the set $\mathcal{Q}^{DB}$ comprises of 3×3 covariance matrices of the form (3.57) satisfying,

$$f_3(Q) \leq f_1(Q) + f_2(Q) + \frac{f_1(Q)f_2(Q)}{(\sigma_Z^2 + \sigma_V^2)} \tag{3.131}$$

Now consider the Gaussian MAC with different noisy feedback signals Y_{F_1} and Y_{F_2} at the transmitters 1 and 2, respectively. If the variances of feedback noises Z_1 and Z_2 are such that, $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = \sigma_V^2$, then the dependence balance constraint (3.118) simplifies as

$$f_3(Q) \leq f_1(Q) + f_2(Q) + \frac{f_1(Q)f_2(Q)}{\left(\sigma_Z^2 + \frac{\sigma_V^2}{2}\right)} \tag{3.132}$$

This implies that if a covariance matrix Q satisfies the constraint (3.131), then it also satisfies (3.132) but the converse statement may not always be true. This means that the resulting outer bound for the Gaussian MAC with common noisy feedback, with feedback noise variance σ_V^2 can be strictly smaller than the resulting outer bound for Gaussian MAC with different noisy feedback signals, when the feedback noise variances are $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = \sigma_V^2$.

3.11 Evaluation of $\mathcal{DB}_{UC}^{MAC}$

In this section we will explicitly evaluate Theorem 3.4 for the Gaussian MAC with user cooperation described by (3.34)-(3.36) in Section 3.7. We start with step 1 and characterize the set of jointly Gaussian triples (T_G, X_{1G}, X_{2G}) in $\mathcal{P}_G^{DB}$. For this purpose, we rewrite (3.43) as follows,

$$0 \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T) - I(X_1; X_2|T) \tag{3.133}$$

$$= I(X_1; Y_{F_1}, Y_{F_2}|X_2, T) - I(X_1; Y_{F_1}, Y_{F_2}|T) \tag{3.134}$$

$$= h(Y_{F_1}, Y_{F_2}|X_1, T) + h(Y_{F_1}, Y_{F_2}|X_2, T) - h(Y_{F_1}, Y_{F_2}|T) - h(Y_{F_1}, Y_{F_2}|X_1, X_2, T) \tag{3.135}$$

and express the above constraint as follows,

$$h(Y_{F_1}, Y_{F_2}|T) + h(Y_{F_1}, Y_{F_2}|X_1, X_2, T) \leq h(Y_{F_1}, Y_{F_2}|X_1, T) + h(Y_{F_1}, Y_{F_2}|X_2, T) \tag{3.136}$$

Making use of the following equalities,

$$h(Y_{F_1}, Y_{F_2}|X_1, X_2, T) = \frac{1}{2}\log\left((2\pi\mathrm{e})^2\sigma_{Z_1}^2\sigma_{Z_2}^2\right) \tag{3.137}$$

$$h(Y_{F_1}, Y_{F_2}|X_1, T) = \frac{1}{2}\log\left((2\pi\mathrm{e})\sigma_{Z_2}^2\right) + h(Y_{F_1}|X_1, T) \tag{3.138}$$

$$h(Y_{F_1}, Y_{F_2}|X_2, T) = \frac{1}{2}\log\left((2\pi\mathrm{e})\sigma_{Z_1}^2\right) + h(Y_{F_2}|X_2, T) \tag{3.139}$$

we obtain a simplified expression for (3.136) as,

$$h(Y_{F_1}, Y_{F_2}|T) \leq h(Y_{F_1}|X_1, T) + h(Y_{F_2}|X_2, T) \tag{3.140}$$

We further simplify (3.140) as follows,

$$\begin{aligned}
0 &\leq h(Y_{F_1}|X_1, T) + h(Y_{F_2}|X_2, T) - h(Y_{F_1}, Y_{F_2}|T) && (3.141)\\
&= h(Y_{F_1}|X_1, T) + h(Y_{F_2}|X_2, T) - h(Y_{F_1}|T) - h(Y_{F_2}|Y_{F_1}, T) && (3.142)\\
&= -I(Y_{F_1}; X_1|T) + h(Y_{F_2}|X_2, T) - h(Y_{F_2}|Y_{F_1}, T) && (3.143)\\
&= -I(Y_{F_1}; X_1|T) + h(Y_{F_2}|X_2, Y_{F_1}, T) - h(Y_{F_2}|Y_{F_1}, T) && (3.144)\\
&= -I(Y_{F_1}; X_1|T) - I(Y_{F_2}; X_2|Y_{F_1}, T) && (3.145)
\end{aligned}$$

where (3.144) follows from the Markov chain $Y_{F_1} \to X_2 \to (T, Y_{F_2})$. Therefore, the dependence balance constraint in (3.43) is equivalent to following two equalities,

$$I(Y_{F_1}; X_1|T) = 0 \tag{3.146}$$

$$I(Y_{F_2}; X_2|Y_{F_1}, T) = 0 \tag{3.147}$$

Next, we show that if any jointly Gaussian triple (T, X_1, X_2) satisfies the constraints (3.146)-(3.147) then it satisfies the Markov chain $X_1 \to T \to X_2$. Conversely, we will show that if any jointly Gaussian triple (T, X_1, X_2) satisfies $X_1 \to T \to X_2$, then it satisfies (3.146)-(3.147).

We start by evaluating (3.146) and (3.147) for a jointly Gaussian (T_G, X_{1G}, X_{2G})

which is equivalent to,

$$0 = I(\sqrt{h_{21}}X_{2G} + Z_1; X_{1G}|T_G) \tag{3.148}$$

$$0 = I(\sqrt{h_{12}}X_{1G} + Z_2; X_{2G}|\sqrt{h_{21}}X_{2G} + Z_1, T_G) \tag{3.149}$$

These equalities are equivalent to

$$\mathrm{Cov}(X_{1G}, X_{2G}|T_G) = 0 \tag{3.150}$$

Using the same argument as in (3.129), we obtain the following condition

$$\rho_{12} = \rho_{1T}\rho_{2T} \tag{3.151}$$

This implies that a jointly Gaussian triple satisfies (3.146)-(3.147) iff $\rho_{12} = \rho_{1T}\rho_{2T}$.

On the other hand, consider any jointly Gaussian triple (T_G, X_{1G}, X_{2G}), with a covariance matrix Q which satisfies the Markov chain $X_{1G} \to T_G \to X_{2G}$. This is equivalent to $I(X_{1G}; X_{2G}|T_G) = 0$, which is equivalent to

$$\rho_{12} = \rho_{1T}\rho_{2T} \tag{3.152}$$

This implies that if a jointly Gaussian triple (T, X_1, X_2) satisfies the Markov chain $X_1 \to T \to X_2$, then it satisfies (3.152) and therefore it also satisfies (3.146)-(3.147) and vice versa. As a consequence, we have explicitly characterized the set $\mathcal{P}_G^{DB}$, i.e., it comprises of only such jointly Gaussian distributions, (T_G, X_{1G}, X_{2G}), for which

$X_{1G} \rightarrow T_G \rightarrow X_{2G}$.

We can now write the set of rate pairs provided by our outer bound for a jointly Gaussian triple (T_G, X_{1G}, X_{2G}) in the set $\mathcal{P}_G^{DB}$ as

$$R_1 \leq I(X_{1G}; Y, Y_{F_2}|X_{2G}, T_G) \tag{3.153}$$

$$R_2 \leq I(X_{2G}; Y, Y_{F_1}|X_{1G}, T_G) \tag{3.154}$$

$$R_1 + R_2 \leq I(X_{1G}, X_{2G}; Y, Y_{F_1}, Y_{F_2}|T_G) \tag{3.155}$$

$$R_1 + R_2 \leq I(X_{1G}, X_{2G}; Y) \tag{3.156}$$

where (T_G, X_{1G}, X_{2G}) satisfies the Markov chain $X_{1G} \rightarrow T_G \rightarrow X_{2G}$. Moreover, from the evaluation of step 2 in Section 3.9, we know that all rate pairs contributed by input distributions in $\mathcal{P}_{NG}^{DB(a)}$ are covered by those given in $\mathcal{P}_G^{DB}$. Therefore, we do not need to consider the set $\mathcal{P}_{NG}^{DB(a)}$ in evaluating our outer bound.

We now arrive at step 3 of the evaluation of our outer bound where we will show that for any non-Gaussian input distribution $p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB(b)}$, we can always find an input distribution in $\mathcal{P}_G^{DB}$, with a set of rate pairs which include the set of rate pairs of the fixed non-Gaussian input distribution $p(t, x_1, x_2)$. Consider any triple (T, X_1, X_2) with a non-Gaussian input distribution $p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB(b)}$, with a valid covariance matrix Q. By the definition of the set $\mathcal{P}_{NG}^{DB(b)}$, and as a consequence of (3.151), this covariance matrix has the property that $\rho_{12} \neq \rho_{1T}\rho_{2T}$. Moreover, this non-Gaussian distribution satisfies the dependence balance bound, i.e., it satisfies (3.146) and (3.147). For our purpose, we only need (3.146). Since $I(Y_{F_1}; X_1|T) = 0$,

this implies

$$E[(\sqrt{h_{21}}X_2 + Z_1)X_1|T] = E[\sqrt{h_{21}}X_2 + Z_1|T]E[X_1|T] \tag{3.157}$$

$$= \sqrt{h_{21}}E[X_2|T]E[X_1|T] \tag{3.158}$$

on the other hand, we also have $E[(\sqrt{h_{21}}X_2 + Z_1)X_1|T] = \sqrt{h_{21}}E[X_1X_2|T]$, which implies

$$E[X_1X_2|T] = E[X_2|T]E[X_1|T] \tag{3.159}$$

We will now construct another triple $(T^{'}, X_1, X_2)$ with a covariance matrix S by selecting

$$T^{'} = E[X_1|T] \tag{3.160}$$

This particular selection is closely related to the recent work of Bross, Lapidoth and Wigger [7] where it was shown that jointly Gaussian distributions are sufficient to characterize the capacity region of Gaussian MAC with conferencing encoders. Although, we should also remark that when evaluating our outer bound for user cooperation, we do not have a conditionally independent structure among (T, X_1, X_2) to start with. This structure arises from the dependence balance constraint (3.43), permiting us to use this approach.

Returning to (3.160), we note that $T^{'}$ is a deterministic function of T and therefore,

following is a valid Markov chain.

$$T^{'} \rightarrow T \rightarrow (X_1, X_2) \rightarrow (Y, Y_{F_1}, Y_{F_2}) \tag{3.161}$$

We will now obtain the off diagonal elements of the covariance matrix S of the triple $(T^{'}, X_1, X_2)$ as follows,

$$E[X_1 T^{'}] = E_T[E[X_1 T^{'}|T]] \tag{3.162}$$

$$= E_T[E[X_1|T]E[X_1|T]] \tag{3.163}$$

$$= \mathrm{Var}(T^{'}) \tag{3.164}$$

and

$$E[X_2 T^{'}] = E_T[E[X_2 T^{'}|T]] \tag{3.165}$$

$$= E_T[E[X_2|T]E[X_1|T]] \tag{3.166}$$

and finally,

$$E[X_1 X_2] = E_T[E[X_1 X_2|T]] \tag{3.167}$$

$$= E_T[E[X_1|T]E[X_2|T]] \tag{3.168}$$

where (3.168) follows from (3.159). Therefore, the triple $(T^{'}, X_1, X_2)$ satisfies

$$E[X_1 X_2] = \frac{E[X_1 T^{'}] E[X_2 T^{'}]}{\mathrm{Var}(T^{'})} \tag{3.169}$$

Now using the fact that

$$E[X_1 X_2] = \rho_{12} \sqrt{P_1 P_2} \tag{3.170}$$

$$E[X_1 T^{'}] = \rho_{1T^{'}} \sqrt{P_1 P_{T^{'}}} \tag{3.171}$$

$$E[X_2 T^{'}] = \rho_{2T^{'}} \sqrt{P_2 P_{T^{'}}} \tag{3.172}$$

and substituting in (3.169) we obtain that the covariance matrix S satisfies

$$\rho_{12} = \rho_{1T^{'}} \rho_{2T^{'}} \tag{3.173}$$

Therefore, from (3.151) any jointly Gaussian $(T_G^{'}, X_{1G}, X_{2G})$ triple with a covariance matrix S, with entries $(\rho_{12}, \rho_{1T^{'}}, \rho_{2T^{'}})$ satisfies (3.43).

We now arrive at the final step of the evaluation. In particular, we will show that the rates of this jointly Gaussian triple $(T_G^{'}, X_{1G}, X_{2G})$ will include the rates of the given non-Gaussian triple (T, X_1, X_2). For the triple $(T_G^{'}, X_{1G}, X_{2G})$, we have the following set of inequalities,

$$I(X_{1G}; Y, Y_{F_2} | X_{2G}, T_G^{'}) = h(Y, Y_{F_2} | X_{2G}, T_G^{'}) - h(Y, Y_{F_2} | X_{1G}, X_{2G}, T_G^{'}) \tag{3.174}$$

$$= h(\sqrt{h_{10}}X_{1G} + Z, \sqrt{h_{12}}X_{1G} + Z_2|X_{2G}, T_G^{'}) - h(Y, Y_{F_2}|X_{1G}, X_{2G}, T_G^{'}) \quad (3.175)$$

$$\geq h(\sqrt{h_{10}}X_1 + Z, \sqrt{h_{12}}X_1 + Z_2|X_2, T^{'}) - h(Y, Y_{F_2}|X_{1G}, X_{2G}, T_G^{'}) \quad (3.176)$$

$$\geq h(\sqrt{h_{10}}X_1 + Z, \sqrt{h_{12}}X_1 + Z_2|X_2, T^{'}, T) - h(Y, Y_{F_2}|X_1, X_2, T) \quad (3.177)$$

$$= h(\sqrt{h_{10}}X_1 + Z, \sqrt{h_{12}}X_1 + Z_2|X_2, T) - h(Y, Y_{F_2}|X_1, X_2, T) \quad (3.178)$$

$$= I(X_1; Y, Y_{F_2}|X_2, T) \quad (3.179)$$

where (3.176) follows from the fact that $(T^{'}, X_1, X_2)$ and $(T_G^{'}, X_{1G}, X_{2G})$ have the same covariance matrix S and by using the maximum entropy theorem. Next, (3.177) follows from the fact that conditioning reduces differential entropy and finally (3.178) follows from the fact that $T^{'}$ is a deterministic function of T and by invoking the Markov chain in (3.161). Similarly, we also have

$$I(X_{2G}; Y, Y_{F_1}|X_{1G}, T_G^{'}) \geq I(X_2; Y, Y_{F_1}|X_1, T) \quad (3.180)$$

$$I(X_{1G}, X_{2G}; Y, Y_{F_1}, Y_{F_2}|T_G^{'}) \geq I(X_1, X_2; Y, Y_{F_1}, Y_{F_2}|T) \quad (3.181)$$

Finally, we have

$$I(X_{1G}, X_{2G}; Y) = h(Y) - h(Y|X_{1G}, X_{2G}) \quad (3.182)$$

$$= h(\sqrt{h_{10}}X_{1G} + \sqrt{h_{20}}X_{2G} + Z) - h(Z) \quad (3.183)$$

$$\geq h(\sqrt{h_{10}}X_1 + \sqrt{h_{20}}X_2 + Z) - h(Z) \quad (3.184)$$

$$= I(X_1, X_2; Y) \quad (3.185)$$

Therefore, we conclude that for any non-Gaussian distribution $p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB(b)}$, there exists a jointly Gaussian distribution $p(t, x_1, x_2) \in \mathcal{P}_G^{DB}$ which satisfies the dependence balance bound (3.43) and yields a set of rates which include the set of rates given by the fixed non-Gaussian distribution. Hence, it suffices to consider jointly Gaussian distributions in $\mathcal{P}_G^{DB}$ to evaluate our outer bound.

The dependence balance based outer bound can now be written in an explicit form as follows,

$$\mathcal{DB}_{UC}^{MAC} = \bigcup_{(\rho_{1T},\rho_{2T})\in[0,1]\times[0,1]} \Bigg\{ (R_1, R_2) : R_1 \leq \frac{1}{2}\log\left(1 + f_1(\rho_{1T})\right) \\ R_2 \leq \frac{1}{2}\log\left(1 + f_2(\rho_{2T})\right) \\ R_1 + R_2 \leq \frac{1}{2}\log\left(1 + f_3(\rho_{1T}, \rho_{2T})\right) \\ R_1 + R_2 \leq \frac{1}{2}\log\left(1 + f_4(\rho_{1T}, \rho_{2T})\right) \Bigg\} \quad (3.186)$$

where

$$f_1(\rho_{1T}) = (1 - \rho_{1T}^2)P_1\left(\frac{h_{10}}{\sigma_Z^2} + \frac{h_{12}}{\sigma_{Z_2}^2}\right) \quad (3.187)$$

$$f_2(\rho_{2T}) = (1 - \rho_{2T}^2)P_2\left(\frac{h_{20}}{\sigma_Z^2} + \frac{h_{21}}{\sigma_{Z_1}^2}\right) \quad (3.188)$$

$$f_3(\rho_{1T}, \rho_{2T}) = f_1(\rho_{1T}) + f_2(\rho_{2T}) + (1 - \rho_{1T}^2)(1 - \rho_{2T}^2)P_1P_2\beta \quad (3.189)$$

$$f_4(\rho_{1T}, \rho_{2T}) = \frac{(h_{10}P_1 + h_{20}P_2 + 2\rho_{1T}\rho_{2T}\sqrt{h_{10}h_{20}P_1P_2})}{\sigma_Z^2} \quad (3.190)$$

and

$$\beta = \frac{(h_{12}h_{21}\sigma_Z^2 + h_{20}h_{12}\sigma_{Z_1}^2 + h_{10}h_{21}\sigma_{Z_2}^2)}{\sigma_Z^2\sigma_{Z_1}^2\sigma_{Z_2}^2} \tag{3.191}$$

The cut-set outer bound given in (3.1)-(3.4) is evaluated for the Gaussian MAC with user cooperation described in (3.34)-(3.36) as

$$\begin{aligned}\mathcal{CS}_{UC}^{MAC} = \bigcup_{\rho\in[0,1]} \Bigg\{ (R_1, R_2) : R_1 &\leq \frac{1}{2}\log\left(1 + (1-\rho^2)P_1\left(\frac{h_{10}}{\sigma_Z^2} + \frac{h_{12}}{\sigma_{Z_2}^2}\right)\right) \\ R_2 &\leq \frac{1}{2}\log\left(1 + (1-\rho^2)P_2\left(\frac{h_{20}}{\sigma_Z^2} + \frac{h_{21}}{\sigma_{Z_1}^2}\right)\right) \\ R_1 + R_2 &\leq \frac{1}{2}\log\left(1 + \frac{h_{10}P_1 + h_{20}P_2 + 2\rho\sqrt{h_{10}h_{20}P_1P_2}}{\sigma_Z^2}\right)\Bigg\}\end{aligned} \tag{3.192}$$

We now mention how our outer bound compares with the cut-set bound for the limiting cases of cooperation noise variances.

1. $\sigma_{Z_1}^2, \sigma_{Z_2}^2 \to 0$: this case corresponds to total cooperation between transmitters. In this case, both dependence balance bound and the cut-set bound degenerate to the total cooperation line,

$$R_1 + R_2 \leq \frac{1}{2}\log\left(1 + \frac{h_{10}P_1 + h_{20}P_2 + 2\sqrt{h_{10}h_{20}P_1P_2}}{\sigma_Z^2}\right) \tag{3.193}$$

2. $\sigma_{Z_1}^2, \sigma_{Z_2}^2 \to \infty$: this case corresponds to very noisy cooperation links. In this

case, we have

$$f_1(\rho_{1T}) = \frac{(1-\rho_{1T}^2)h_{10}P_1}{\sigma_Z^2} \tag{3.194}$$

$$f_2(\rho_{2T}) = \frac{(1-\rho_{2T}^2)h_{20}P_2}{\sigma_Z^2} \tag{3.195}$$

$$f_3(\rho_{1T}, \rho_{2T}) = f_1(\rho_{1T}) + f_2(\rho_{2T}) \tag{3.196}$$

$$< \frac{(h_{10}P_1 + h_{20}P_2 + 2\rho_{1T}\rho_{2T}\sqrt{h_{10}h_{20}P_1P_2})}{\sigma_Z^2} \tag{3.197}$$

and the dependence balance bound collapses to the capacity region of the Gaussian MAC with no cooperation. On the other hand, the cut-set bound collapses to the capacity region of the Gaussian MAC with noiseless feedback [45].

Figure 3.9 illustrates the outer bounds and achievable rate region [53] for the case when $P_1 = P_2 = 5, \sigma_Z^2 = 2$ and $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 1$ and $h_{10} = h_{20} = h_{12} = h_{21} = 1$. Figure 3.10 illustrates the outer bounds for the case when $P_1 = P_2 = \sigma_Z^2 = 1$ and $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 20$ and $h_{10} = h_{20} = h_{12} = h_{21} = 1$. For this case, the achievable rate region does not provide any visual improvement over no-cooperation. Figure 3.11 illustrates these bounds and the achievable rate region for the asymmetric setting where $P_1 = P_2 = \sigma_Z^2 = 1$ and $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 1$ and $h_{10} = h_{20} = 1$, $h_{12} = 3, h_{21} = 2$. Figure 3.12 illustrates these bounds and the achievable rate region for the one sided cooperation where $P_1 = P_2 = \sigma_Z^2 = 1$ and $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 1$ and $h_{10} = h_{20} = 1$, $h_{12} = 2, h_{21} = 0$.

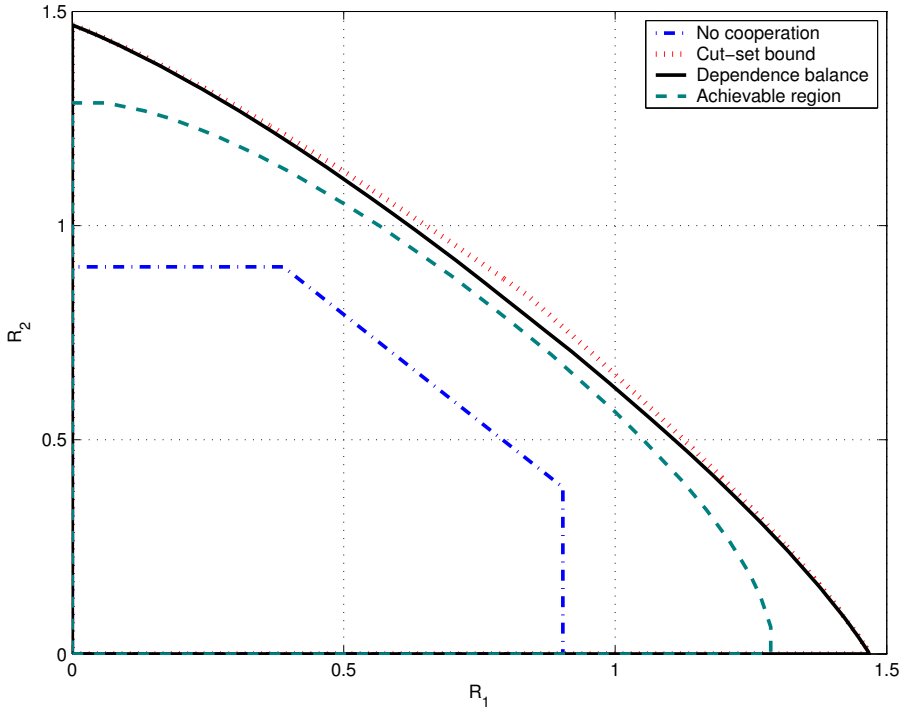

Figure 3.9: Illustration of bounds for $P_1 = P_2 = 5, \sigma_Z^2 = 2$, $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 1$ and $h_{10} = h_{20} = h_{12} = h_{21} = 1$.

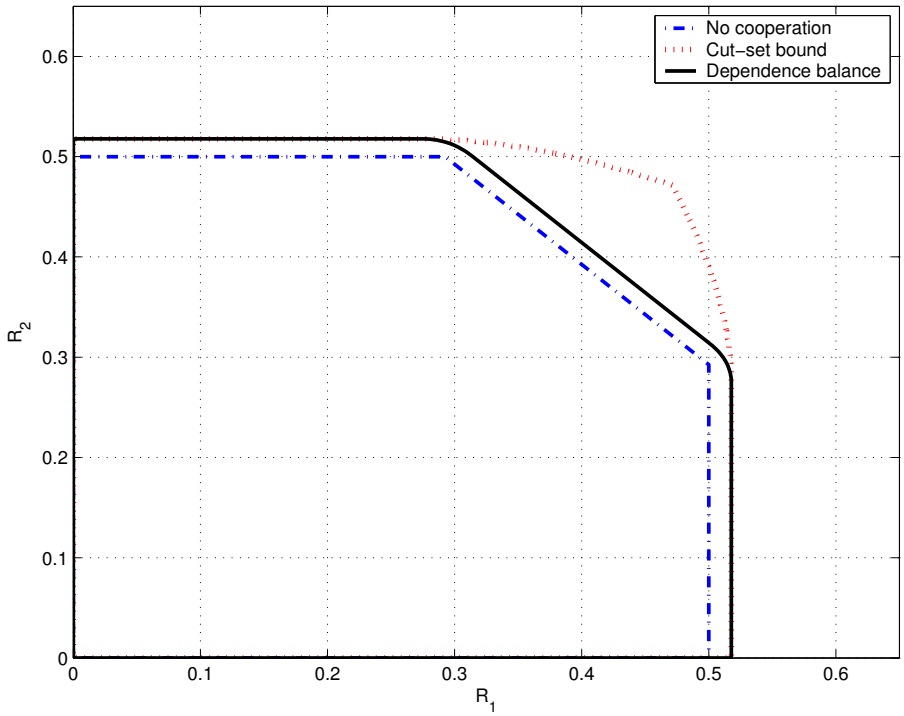

Figure 3.10: Illustration of outer bounds for $P_1 = P_2 = \sigma_Z^2 = 1$, $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 20$ and $h_{10} = h_{20} = h_{12} = h_{21} = 1$.

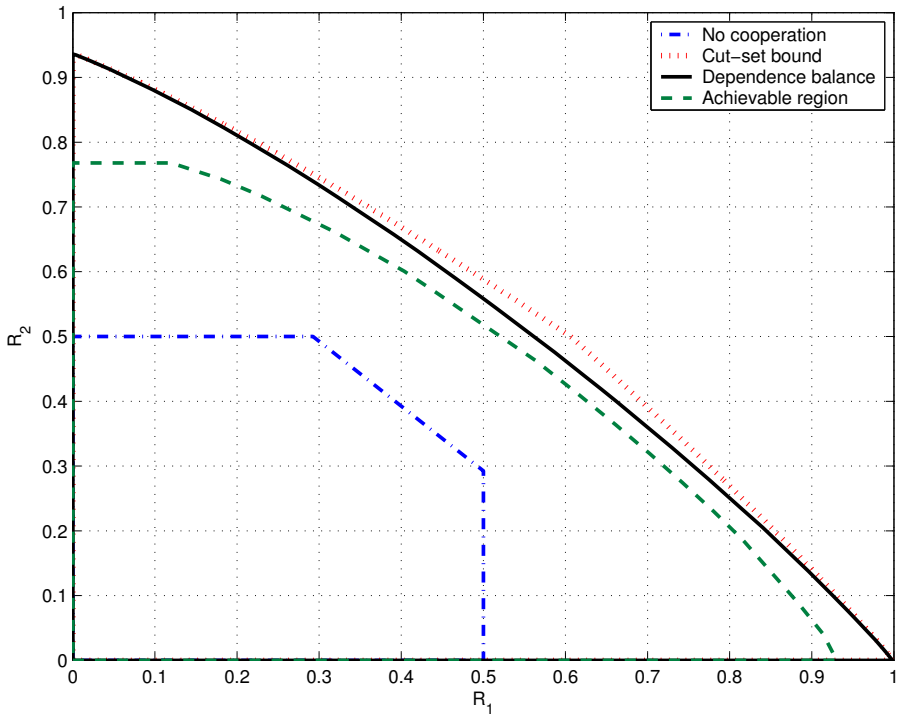

Figure 3.11: Illustration of outer bounds for $P_1 = P_2 = \sigma_Z^2 = 1$, $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 1$ and $h_{10} = h_{20} = 1$, $h_{12} = 3, h_{21} = 2$.

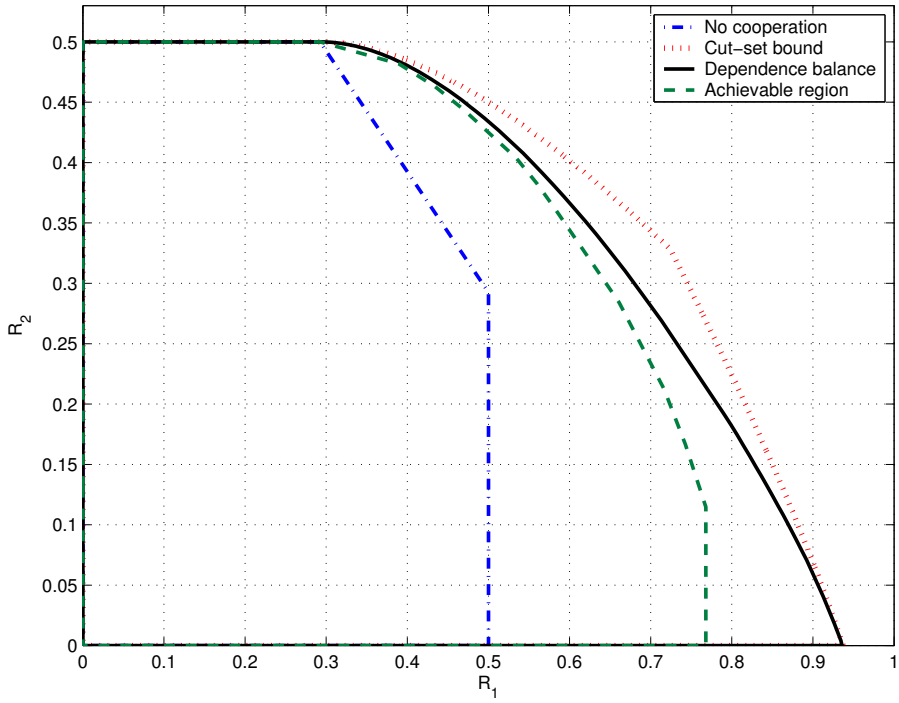

Figure 3.12: Illustration of outer bounds for $P_1 = P_2 = \sigma_Z^2 = 1$, $\sigma_{Z_1}^2 = \sigma_{Z_2}^2 = 1$ and $h_{10} = h_{20} = 1$, $h_{12} = 2, h_{21} = 0$.

3.12 Evaluation of $\mathcal{DB}_{UC}^{IC}$

In this section we will explicitly evaluate Theorem 3.5 for the Gaussian IC with user cooperation described by (3.44)-(3.47) in Section 3.8. We start with step 1 and first characterize the set of jointly Gaussian triples (T_G, X_{1G}, X_{2G}) in $\mathcal{P}_G^{DB}$. For this purpose, we rewrite (3.56) as follows,

$$h(Y_{F_1}, Y_{F_2}|T) + h(Y_{F_1}, Y_{F_2}|X_1, X_2, T) \leq h(Y_{F_1}, Y_{F_2}|X_1, T) + h(Y_{F_1}, Y_{F_2}|X_2, T) \tag{3.198}$$

Making use of the following equalities,

$$h(Y_{F_1}, Y_{F_2}|X_1, X_2, T) = \frac{1}{2}\log\left((2\pi\mathrm{e})^2\sigma_{Z_1}^2\sigma_{Z_2}^2\right) \tag{3.199}$$

$$h(Y_{F_1}, Y_{F_2}|X_1, T) = \frac{1}{2}\log\left((2\pi\mathrm{e})\sigma_{Z_2}^2\right) + h(Y_{F_1}|X_1, T) \tag{3.200}$$

$$h(Y_{F_1}, Y_{F_2}|X_2, T) = \frac{1}{2}\log\left((2\pi\mathrm{e})\sigma_{Z_1}^2\right) + h(Y_{F_2}|X_2, T) \tag{3.201}$$

we obtain a simplified expression for (3.198) as,

$$h(Y_{F_1}, Y_{F_2}|T) \leq h(Y_{F_1}|X_1, T) + h(Y_{F_2}|X_2, T) \tag{3.202}$$

which can be further simplified as in the derivation of $\mathcal{DB}_{UC}^{MAC}$ to the following two equalities,

$$I(Y_{F_1}; X_1|T) = 0 \tag{3.203}$$

$$I(Y_{F_2}; X_2|Y_{F_1}, T) = 0 \tag{3.204}$$

We next follow the same set of arguments used in Section 3.11 to arrive at the fact that a jointly Gaussian triple (T, X_1, X_2) satisfies (3.203)-(3.204) iff $X_1 \rightarrow T \rightarrow X_2$.

We can now write the set of rate pairs provided by our outer bound for a jointly Gaussian triple (T_G, X_{1G}, X_{2G}) in the set $\mathcal{P}_G^{DB}$ as

$$R_1 \leq I(X_{1G}, X_{2G}; Y_1) \tag{3.205}$$

$$R_2 \leq I(X_{1G}, X_{2G}; Y_2) \tag{3.206}$$

$$R_1 \leq I(X_{1G}; Y_1, Y_2, Y_{F_2}|X_{2G}, T) \tag{3.207}$$

$$R_2 \leq I(X_{2G}; Y_1, Y_2, Y_{F_1}|X_{1G}, T) \tag{3.208}$$

$$R_1 + R_2 \leq I(X_{1G}, X_{2G}; Y_1, Y_2, Y_{F_1}, Y_{F_2}|T) \tag{3.209}$$

$$R_1 + R_2 \leq I(X_{1G}, X_{2G}; Y_1, Y_2)\big\} \tag{3.210}$$

where the triple (T_G, X_{1G}, X_{2G}) satisfies the Markov chain $X_{1G} \rightarrow T_G \rightarrow X_{2G}$. Moreover, from the evaluation of step 2 in Section 3.9, we know that all rate pairs contributed by input distributions in $\mathcal{P}_{NG}^{DB(a)}$ are covered by those given in $\mathcal{P}_G^{DB}$. Therefore, we do not need to consider the set $\mathcal{P}_{NG}^{DB(a)}$ in evaluating our outer bound.

We now arrive at step 3 of the evaluation of our outer bound for the Gaussian IC

with user cooperation. Consider any triple (T, X_1, X_2) with a non-Gaussian distribution $p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB(b)}$, with a valid covariance matrix Q. As in the derivation of $\mathcal{DB}_{UC}^{MAC}$, we first construct another triple $(T^{'}, X_1, X_2)$ with a covariance matrix S by selecting

$$T^{'} = E[X_1|T] \tag{3.211}$$

Following this step, we next make use of the Markov chain

$$T^{'} \rightarrow T \rightarrow (X_1, X_2) \rightarrow (Y_1, Y_2, Y_{F_1}, Y_{F_2}) \tag{3.212}$$

to show the existence of a jointly Gaussian $(T_G^{'}, X_{1G}, X_{2G})$ with a covariance matrix S and which satisfies (3.56).

We now arrive at the final step of the evaluation. In particular, we will show that the rates of this jointly Gaussian triple $(T_G^{'}, X_{1G}, X_{2G})$ will include the rates of the given non-Gaussian triple (T, X_1, X_2). For the triple $(T_G^{'}, X_{1G}, X_{2G})$, we have the following set of inequalities,

$$I(X_{1G}; Y_1, Y_2, Y_{F_2}|X_{2G}, T_G^{'}) = h(Y_1, Y_2, Y_{F_2}|X_{2G}, T_G^{'}) - h(Y_1, Y_2, Y_{F_2}|X_{1G}, X_{2G}, T_G^{'}) \tag{3.213}$$

$$= h(X_{1G} + N_1, \sqrt{a}X_{1G} + N_2, \sqrt{h_{12}}X_{1G} + Z_2|X_{2G}, T_G^{'}) - h(Y_1, Y_2, Y_{F_2}|X_{1G}, X_{2G}, T_G^{'}) \tag{3.214}$$

$$\geq h((X_1 + N_1, \sqrt{a}X_1 + N_2, \sqrt{h_{12}}X_1 + Z_2|X_2, T^{'}) - h(Y_1, Y_2, Y_{F_2}|X_{1G}, X_{2G}, T_G^{'}) \tag{3.215}$$

$$\geq h((X_1 + N_1, \sqrt{a}X_1 + N_2, \sqrt{h_{12}}X_1 + Z_2|X_2, T^{'}, T) - h(Y_1, Y_2, Y_{F_2}|X_{1G}, X_{2G}, T_G^{'}) \tag{3.216}$$

$$= h((X_1 + N_1, \sqrt{a}X_1 + N_2, \sqrt{h_{12}}X_1 + Z_2|X_2, T) - h(Y_1, Y_2, Y_{F_2}|X_1, X_2, T) \tag{3.217}$$

$$= I(X_1; Y_1, Y_2, Y_{F_2}|X_2, T) \tag{3.218}$$

where (3.215) follows from the fact that $(T^{'}, X_1, X_2)$ and $(T_G^{'}, X_{1G}, X_{2G})$ have the same covariance matrix S and using the maximum entropy theorem. Next, (3.216) follows from the fact that conditioning reduces differential entropy and finally (3.217) follows from the fact that $T^{'}$ is a deterministic function of T and invoking the Markov chain in (3.212). Similarly, we also have

$$I(X_{2G}; Y_1, Y_2, Y_{F_1}|X_{1G}, T_G^{'}) \geq I(X_2; Y_1, Y_2, Y_{F_1}|X_1, T) \tag{3.219}$$

$$I(X_{1G}, X_{2G}; Y_1, Y_2, Y_{F_1}, Y_{F_2}|T_G^{'}) \geq I(X_1, X_2; Y_1, Y_2, Y_{F_1}, Y_{F_2}|T) \tag{3.220}$$

Finally, we have

$$I(X_{1G}, X_{2G}; Y_1) = h(Y_1) - h(Y_1|X_{1G}, X_{2G}) \tag{3.221}$$

$$= h(X_{1G} + \sqrt{b}X_{2G} + N_1) - h(N_1) \tag{3.222}$$

$$\geq h(X_1 + \sqrt{b}X_2 + N_1) - h(N_1) \tag{3.223}$$

$$= I(X_1, X_2; Y_1) \tag{3.224}$$

and similarly, we also have,

$$I(X_{1G}, X_{2G}; Y_2) \geq I(X_1, X_2; Y_2) \tag{3.225}$$

$$I(X_{1G}, X_{2G}; Y_1, Y_2) \geq I(X_1, X_2; Y_1, Y_2) \tag{3.226}$$

Therefore, we conclude that for any non-Gaussian distribution $p(t, x_1, x_2) \in \mathcal{P}_{NG}^{DB(b)}$, there exists a jointly Gaussian distribution $p(t, x_1, x_2) \in \mathcal{P}_G^{DB}$ which satisfies the dependence balance bound (3.56) and yields a set of rates which includes the set of rates given by the fixed non-Gaussian distribution. Hence, it suffices to consider jointly Gaussian distributions in $\mathcal{P}_G^{DB}$ to evaluate our outer bound.

The dependence balance based outer bound can now be written in an explicit form as,

$$\begin{aligned}\mathcal{DB}_{UC}^{IC} = \bigcup_{(\rho_{1T},\rho_{2T})\in[0,1]\times[0,1]} \Bigg\{ (R_1, R_2) : R_1 &\leq \frac{1}{2}\log\left(1 + f_1(\rho_{1T}, \rho_{2T})\right) \\ R_2 &\leq \frac{1}{2}\log\left(1 + f_2(\rho_{1T}, \rho_{2T})\right) \\ R_1 &\leq \frac{1}{2}\log\left(1 + f_3(\rho_{1T})\right) \\ R_2 &\leq \frac{1}{2}\log\left(1 + f_4(\rho_{2T})\right) \\ R_1 + R_2 &\leq \frac{1}{2}\log\left(1 + f_5(\rho_{1T}, \rho_{2T})\right) \\ R_1 + R_2 &\leq \frac{1}{2}\log\left(1 + f_6(\rho_{1T}, \rho_{2T})\right) \Bigg\}\end{aligned} \tag{3.227}$$

where

$$f_1(\rho_{1T},\rho_{2T}) = \frac{(P_1 + bP_2 + 2\rho_{1T}\rho_{2T}\sqrt{bP_1P_2})}{\sigma^2_{N_1}} \tag{3.228}$$

$$f_2(\rho_{1T},\rho_{2T}) = \frac{(aP_1 + P_2 + 2\rho_{1T}\rho_{2T}\sqrt{aP_1P_2})}{\sigma^2_{N_2}} \tag{3.229}$$

$$f_3(\rho_{1T}) = (1-\rho^2_{1T})P_1\left(\frac{1}{\sigma^2_{N_1}} + \frac{a}{\sigma^2_{N_2}} + \frac{h_{12}}{\sigma^2_{Z_2}}\right) \tag{3.230}$$

$$f_4(\rho_{2T}) = (1-\rho^2_{2T})P_2\left(\frac{b}{\sigma^2_{N_1}} + \frac{1}{\sigma^2_{N_2}} + \frac{h_{21}}{\sigma^2_{Z_1}}\right) \tag{3.231}$$

$$f_5(\rho_{1T},\rho_{2T}) = f_1(\rho_{1T},\rho_{2T}) + f_2(\rho_{1T},\rho_{2T}) + \frac{(1-\rho^2_{1T}\rho^2_{2T})P_1P_2(1-\sqrt{ab})^2}{\sigma^2_{N_1}\sigma^2_{N_2}} \tag{3.232}$$

$$f_6(\rho_{1T},\rho_{2T}) = f_3(\rho_{1T}) + f_4(\rho_{2T}) + (1-\rho^2_{1T})(1-\rho^2_{2T})P_1P_2\beta \tag{3.233}$$

where

$$\beta = \frac{h_{12}h_{21}}{\sigma^2_{Z_1}\sigma^2_{Z_2}} + \frac{(1-\sqrt{ab})^2}{\sigma^2_{N_1}\sigma^2_{N_2}} + \frac{h_{12}}{\sigma^2_{Z_2}}\left(\frac{1}{\sigma^2_{N_2}} + \frac{b}{\sigma^2_{N_1}}\right) + \frac{h_{21}}{\sigma^2_{Z_1}}\left(\frac{1}{\sigma^2_{N_1}} + \frac{a}{\sigma^2_{N_2}}\right) \tag{3.234}$$

The cut-set outer bound given in (3.5)-(3.10) is evaluated for the Gaussian IC with user cooperation described in (3.44)-(3.47) as

$$\mathcal{CS}^{IC}_{UC} = \bigcup_{\rho\in[0,1]}\left\{(R_1,R_2): R_1 \le \frac{1}{2}\log\left(1+\frac{P_1+bP_2+2\rho\sqrt{bP_1P_2}}{\sigma^2_{N_1}}\right)\right.$$
$$\left. R_2 \le \frac{1}{2}\log\left(1+\frac{aP_1+P_2+2\rho\sqrt{aP_1P_2}}{\sigma^2_{N_2}}\right)\right.$$

$$R_1 \leq \frac{1}{2}\log\left(1+(1-\rho^2)P_1\left(\frac{1}{\sigma^2_{N_1}}+\frac{a}{\sigma^2_{N_2}}+\frac{h_{12}}{\sigma^2_{Z_2}}\right)\right)$$
$$R_2 \leq \frac{1}{2}\log\left(1+(1-\rho^2)P_2\left(\frac{b}{\sigma^2_{N_1}}+\frac{1}{\sigma^2_{N_2}}+\frac{h_{21}}{\sigma^2_{Z_1}}\right)\right)$$
$$R_1+R_2 \leq \frac{1}{2}\log\left(1+k_1(\rho)+k_2(\rho)+\frac{(1-\rho^2)P_1P_2(1-\sqrt{ab})^2}{\sigma^2_{N_1}\sigma^2_{N_2}}\right)\Bigg\} \tag{3.235}$$

where

$$k_1(\rho) = \frac{P_1+bP_2+2\rho\sqrt{bP_1P_2}}{\sigma^2_{N_1}} \tag{3.236}$$

$$k_1(\rho) = \frac{aP_1+P_2+2\rho\sqrt{aP_1P_2}}{\sigma^2_{N_2}} \tag{3.237}$$

Figure 3.13 illustrates our outer bound, cut-set bound, an achievable rate region with cooperation [31], capacity region without cooperation [50] for the case when $P_1 = P_2 = \sigma^2_{N_1} = \sigma^2_{N_1} = 1$ and $\sigma^2_{Z_1} = \sigma^2_{Z_2} = 1$ and $a = b = 1$ and $h_{12} = h_{21} = 2$. Figure 3.14 illustrates the outer bound, cut-set bound and achievable region without cooperation [49] when $P_1 = P_2 = \sigma^2_{N_1} = \sigma^2_{N_1} = 1$ and $\sigma^2_{Z_1} = \sigma^2_{Z_2} = 1$ and $a = b = 0.5$ and $h_{12} = h_{21} = 0.1$. Figure 3.15 illustrates our sum rate upper bound and the cut-set bound as function of h, where $h = h_{12} = h_{21}$ and $P_1 = P_2 = \sigma^2_{N_1} = \sigma^2_{N_1} = 1$ and $\sigma^2_{Z_1} = \sigma^2_{Z_2} = 1$, $a = b = 0.5$.

3.13 Conclusions

We obtained new outer bounds for the capacity regions of the two-user MAC with generalized feedback and the two-user IC with generalized feedback. We explicitly evaluated these outer bounds for three channel models. In particular, we evaluated

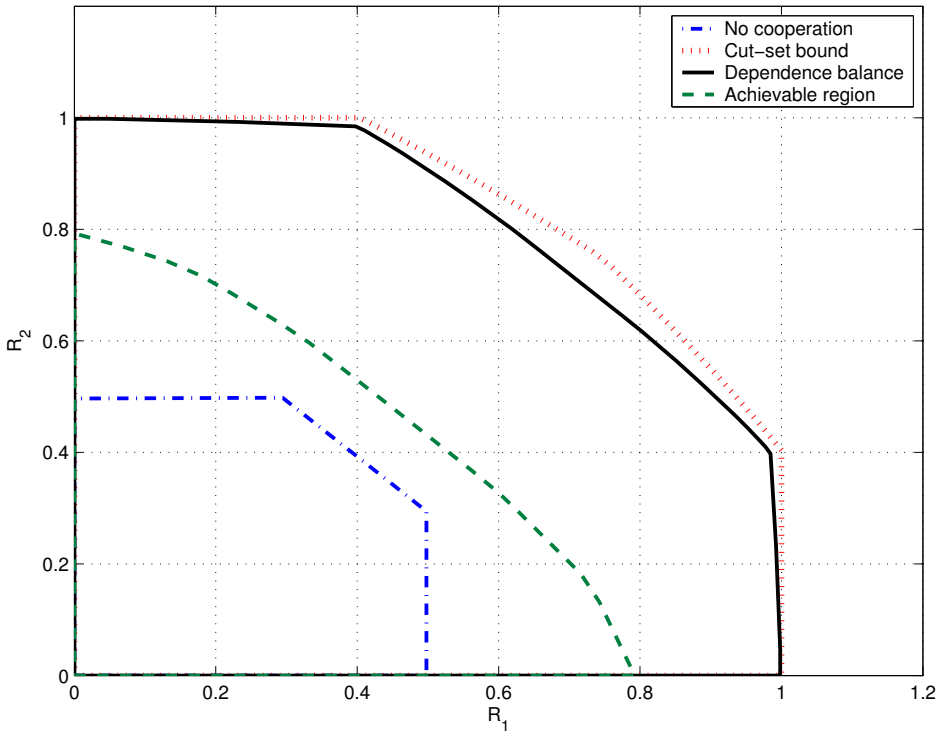

Figure 3.13: Illustration of bounds for $P_1 = P_2 = \sigma^2_{N_1} = \sigma^2_{N_2} = 1$, $\sigma^2_{Z_1} = \sigma^2_{Z_2} = 1$ and $a = b = 1$ and $h_{12} = h_{21} = 2$.

our outer bounds for the Gaussian MAC with different noisy feedback signals at the transmitters, the Gaussian MAC with user cooperation and the Gaussian IC with user cooperation. Our outer bounds strictly improve upon the cut-set bound for all three channel models.

For the evaluation of our outer bounds for the Gaussian scenarios of interest, we proposed a systematic approach to deal with capacity bounds involving auxiliary random variables. This approach was appropriately tailored according to the channel model in consideration which permitted us to obtain explicit expressions for our outer bounds. To evaluate our outer bounds, we have to consider all input distributions satisfying the dependence balance constraint. The main difficulty in evaluating our outer bounds arises from the fact that there might exist some non-Gaussian input

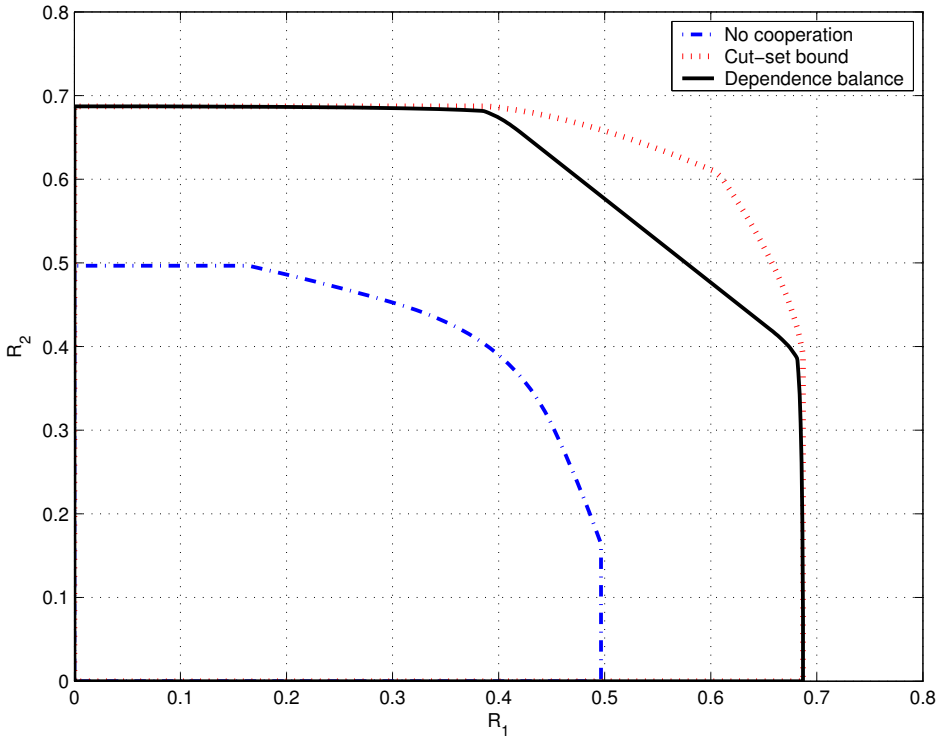

Figure 3.14: Illustration of bounds for for $P_1 = P_2 = \sigma^2_{N_1} = \sigma^2_{N_2} = 1$, $\sigma^2_{Z_1} = \sigma^2_{Z_2} = 1$ and $a = b = 0.5$ and $h_{12} = h_{21} = 0.1$.

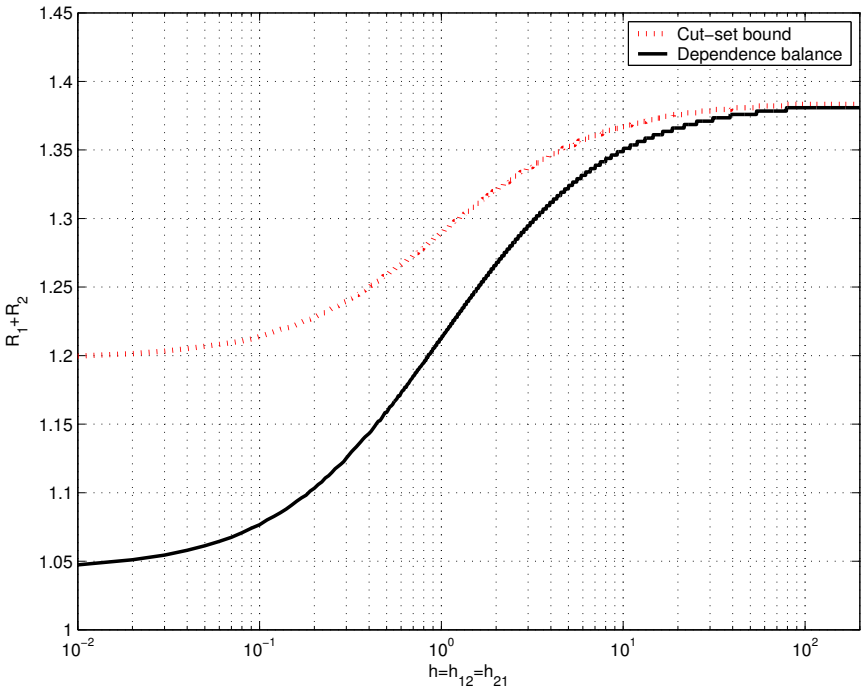

Figure 3.15: Illustration of sum-rate upper bound and the cut-set bound as a function of h, where $h = h_{12} = h_{21}$.

distribution $p(t, x_1, x_2)$ with a covariance matrix Q, such that $p(t, x_1, x_2)$ satisfies the dependence balance constraint but there does not exist a jointly Gaussian triple with the covariance matrix Q satisfying the dependence balance constraint. Therefore, the regular methodology of evaluating outer bounds, i.e., the approach of applying maximum entropy theorem [14] fails beyond this particular point. Through our explicit evaluation for all three channel models, we were able to show the existence of a jointly Gaussian triple with a covariance matrix S which satisfies the dependence balance constraint and yields larger rates than the fixed non-Gaussian distribution.

In particular, for the case of Gaussian MAC with noisy feedback, we made use of a recently discovered multivariate EPI [46], which is a generalization of Costa's EPI [10]. It is worth nothing that this result could not be obtained from the classical vector EPI. For the case of Gaussian MAC with user cooperation and the Gaussian IC with user cooperation, our proof closely follows a recent result of Bross, Wigger and Lapidoth [7] and [60] for the Gaussian MAC with conferencing encoders.

3.14 Appendix

3.14.1 Proof of Theorem 3.1

We will prove Theorem 3.1 by first deriving an upper bound for R_1 as

$$nR_1 = H(W_1) = H(W_1|W_2) \tag{3.238}$$

$$= I(W_1; Y^n, Y_{F_2}^n|W_2) + H(W_1|W_2, Y^n, Y_{F_2}^n) \tag{3.239}$$

$$\leq I(W_1; Y^n, Y_{F_2}^n | W_2) + n\epsilon_1^{(n)} \tag{3.240}$$

$$= \sum_{i=1}^{n} I(W_1; Y_i, Y_{F_2 i} | W_2, Y^{i-1}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.241}$$

$$= \sum_{i=1}^{n} (H(Y_i, Y_{F_2 i} | W_2, Y^{i-1}, Y_{F_2}^{i-1}) - H(Y_i, Y_{F_2 i} | W_1, W_2, Y^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.242}$$

$$= \sum_{i=1}^{n} (H(Y_i, Y_{F_2 i} | W_2, X_{2i}, Y^{i-1}, Y_{F_2}^{i-1}) - H(Y_i, Y_{F_2 i} | X_{2i}, W_1, W_2, Y^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.243}$$

$$\leq \sum_{i=1}^{n} (H(Y_i, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1}) - H(Y_i, Y_{F_2 i} | X_{2i}, W_1, W_2, Y^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.244}$$

$$\leq \sum_{i=1}^{n} (H(Y_i, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1}) - H(Y_i, Y_{F_2 i} | X_{1i}, X_{2i}, W_1, W_2, Y^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.245}$$

$$= \sum_{i=1}^{n} (H(Y_i, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1}) - H(Y_i, Y_{F_2 i} | X_{1i}, X_{2i}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.246}$$

$$= \sum_{i=1}^{n} I(X_{1i}; Y_i, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.247}$$

$$= nI(X_{1Q}; Y_Q, Y_{F_2 Q} | X_{2Q}, Q, Y_{F_2}^{Q-1}) + n\epsilon_1^{(n)} \tag{3.248}$$

$$= nI(X_1; Y, Y_{F_2} | X_2, T_2) + n\epsilon_1^{(n)} \tag{3.249}$$

where (3.240) follows from Fano's inequality [14], (3.243) follows from the fact that X_{2i} is a function of $(W_2, Y_{F_2}^{i-1})$ and by introducing X_{2i} in both terms, (3.244) follows from the fact that conditioning reduces entropy and we drop (W_2, Y^{i-1}) from the conditioning in the first term, (3.245) follows from the fact that conditioning reduces entropy and by introducing X_{1i} in the second term and (3.246) follows from the memoryless property of the channel. Finally, we define $X_1 = X_{1Q}$, $X_2 = X_{2Q}$, $T_1 = (Q, Y_{F_1}^{Q-1})$, $T_2 = (Q, Y_{F_2}^{Q-1})$, $Y = Y_Q$, $Y_{F_1} = Y_{F_1 Q}$ and $Y_{F_2} = Y_{F_2 Q}$, where Q is a

random variable which is uniformly distributed over $\{1, \ldots, n\}$ and is independent of all other random variables. Similarly, we have

$$R_2 \leq I(X_2; Y, Y_{F_1} | X_1, T_1) \tag{3.250}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, Y_{F_1}, Y_{F_2} | T_1, T_2) \tag{3.251}$$

In addition to (3.251), we also have the following sum-rate constraint which also appears in the cut-set outer bound,

$$\begin{aligned}
n(R_1 + R_2) &= H(W_1, W_2) && (3.252)\\
&= I(W_1, W_2; Y^n) + H(W_1, W_2 | Y^n) && (3.253)\\
&\leq I(W_1, W_2; Y^n) + n\epsilon^{(n)} && (3.254)\\
&= \sum_{i=1}^{n} (H(Y_i | Y^{i-1}) - H(Y_i | W_1, W_2, Y^{i-1})) + n\epsilon^{(n)} && (3.255)\\
&\leq \sum_{i=1}^{n} (H(Y_i | Y^{i-1}) - H(Y_i | X_{1i}, X_{2i}, W_1, W_2, Y^{i-1})) + n\epsilon^{(n)} && (3.256)\\
&= \sum_{i=1}^{n} (H(Y_i | Y^{i-1}) - H(Y_i | X_{1i}, X_{2i})) + n\epsilon^{(n)} && (3.257)\\
&\leq \sum_{i=1}^{n} (H(Y_i) - H(Y_i | X_{1i}, X_{2i})) + n\epsilon^{(n)} && (3.258)\\
&= \sum_{i=1}^{n} I(X_{1i}, X_{2i}; Y_i) + n\epsilon^{(n)} && (3.259)\\
&= nI(X_{1Q}, X_{2Q}; Y_Q | Q) + n\epsilon^{(n)} && (3.260)\\
&\leq nI(X_{1Q}, X_{2Q}; Y_Q) + n\epsilon^{(n)} && (3.261)\\
&= nI(X_1, X_2; Y) + n\epsilon^{(n)} && (3.262)
\end{aligned}$$

It is necessary to include this seemingly trivial upper bound on the sum-rate. The reason for including this sum-rate upper bound is that one cannot claim that for any input distribution $p(t_1, t_2, x_1, x_2)$, we have $I(X_1, X_2; Y, Y_{F_1}, Y_{F_2}|T_1, T_2) \leq I(X_1, X_2; Y)$. In other words, we cannot claim that the sum-rate bound in (3.262) will always be redundant. Therefore, by including it, we can make sure that our outer bound is at most equal to the cut-set outer bound but never larger than it. Although, as we will see in the proof of Theorem 3.3 for the case of noisy feedback, the sum-rate upper bound in (3.262) will turn out to be redundant.

The proof of the dependence balance constraint in (3.16) is along the same lines as in [30] by starting from the inequality

$$0 \leq I(W_1; W_2|Y_{F_1}^n, Y_{F_2}^n) - I(W_1; W_2) \tag{3.263}$$

to arrive at

$$I(X_1; X_2|T_1, T_2) \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T_1, T_2) \tag{3.264}$$

This completes the proof of Theorem 3.1.

3.14.2 Proof of Theorem 3.2

We will prove Theorem 3.2 by first deriving an upper bound for R_1 as

$$nR_1 = H(W_1) = H(W_1|W_2) \tag{3.265}$$

$$= I(W_1; Y_1^n, Y_2^n, Y_{F_2}^n | W_2) + H(W_1 | W_2, Y_1^n, Y_2^n, Y_{F_2}^n) \tag{3.266}$$

$$\leq I(W_1; Y_1^n, Y_2^n, Y_{F_2}^n | W_2) + n\epsilon_1^{(n)} \tag{3.267}$$

$$= \sum_{i=1}^{n} I(W_1; Y_{1i}, Y_{2i}, Y_{F_2 i} | W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.268}$$

$$= \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i} | W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i} | W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.269}$$

$$= \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i} | W_2, X_{2i}, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{2i}, W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.270}$$

$$\leq \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1})$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{2i}, W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.271}$$

$$\leq \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1})$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{1i}, X_{2i}, W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.272}$$

$$= \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1}) - H(Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{1i}, X_{2i}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.273}$$

$$= \sum_{i=1}^{n} I(X_{1i}; Y_{1i}, Y_{2i}, Y_{F_2 i} | X_{2i}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.274}$$

$$= nI(X_1; Y_1, Y_2, Y_{F_2} | X_2, T_2) + n\epsilon_1^{(n)} \tag{3.275}$$

where (3.267) follows from Fano's inequality [14], (3.270) follows from the fact that X_{2i} is a function of $(W_2, Y_{F_2}^{i-1})$ and by introducing X_{2i} in both terms, (3.271) follows from the fact that conditioning reduces entropy and we drop $(W_2, Y_1^{i-1}, Y_2^{i-1})$ from the conditioning in the first term, (3.272) follows from the fact that conditioning reduces

entropy and by introducing X_{1i} in the conditioning in the second term and (3.273) follows from the memoryless property of the channel. Finally, we define $X_1 = X_{1Q}$, $X_2 = X_{2Q}$, $T_1 = (Q, Y_{F_1}^{Q-1})$, $T_2 = (Q, Y_{F_2}^{Q-1})$, $Y_1 = Y_{1Q}$, $Y_2 = Y_{2Q}$, $Y_{F_1} = Y_{F_1Q}$ and $Y_{F_2} = Y_{F_2Q}$, where Q is a random variable which is uniformly distributed over $\{1, \ldots, n\}$ and is independent of all other random variables.

Similarly, we have

$$R_2 \leq I(X_2; Y_1, Y_2, Y_{F_1} | X_1, T_1) \tag{3.276}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y_1, Y_2, Y_{F_1}, Y_{F_2} | T_1, T_2) \tag{3.277}$$

and we also have from the cut-set bound

$$R_1 \leq I(X_1, X_2; Y_1) \tag{3.278}$$

$$R_2 \leq I(X_2, X_2; Y_2) \tag{3.279}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y_1, Y_2) \tag{3.280}$$

The proof of the dependence balance constraint is along the same lines as in [30] by starting from the inequality

$$0 \leq I(W_1; W_2 | Y_{F_1}^n, Y_{F_2}^n) - I(W_1; W_2) \tag{3.281}$$

to arrive at

$$I(X_1; X_2|T_1, T_2) \leq I(X_1; X_2|Y_{F_1}, Y_{F_2}, T_1, T_2) \tag{3.282}$$

This completes the proof of Theorem 3.2.

3.14.3 Proof of Theorem 3.3

For any MAC-GF, with transition probabilities in the form of (3.28), we will obtain a strengthened version of Theorem 3.1. We start by obtaining an upper bound on R_1 as

$$nR_1 = H(W_1) = H(W_1|W_2) \tag{3.283}$$

$$= I(W_1; Y^n, Y_{F_1}^n, Y_{F_2}^n|W_2) + H(W_1|W_2, Y^n, Y_{F_1}^n, Y_{F_2}^n) \tag{3.284}$$

$$\leq I(W_1; Y^n, Y_{F_1}^n, Y_{F_2}^n|W_2) + n\epsilon_1^{(n)} \tag{3.285}$$

$$= \sum_{i=1}^{n} I(W_1; Y_i, Y_{F_1 i}, Y_{F_2 i}|W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.286}$$

$$= \sum_{i=1}^{n} I(W_1; Y_i|W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.287}$$

$$= \sum_{i=1}^{n} (H(Y_i|W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) - H(Y_i|W_1, W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.288}$$

$$= \sum_{i=1}^{n} (H(Y_i|X_{2i}, W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) - H(Y_i|X_{2i}, W_1, W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.289}$$

$$\leq \sum_{i=1}^{n}(H(Y_i|X_{2i}, W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) - H(Y_i|X_{1i}, X_{2i}, W_1, W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}))$$

$$+ n\epsilon_1^{(n)} \tag{3.290}$$

$$= \sum_{i=1}^{n}(H(Y_i|X_{2i}, W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) - H(Y_i|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.291}$$

$$\leq \sum_{i=1}^{n}(H(Y_i|X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) - H(Y_i|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.292}$$

$$= \sum_{i=1}^{n} I(X_{1i}; Y_i|X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.293}$$

$$= nI(X_{1Q}; Y_Q|X_{2Q}, Q, Y_{F_1}^{Q-1}, Y_{F_2}^{Q-1}) + n\epsilon_1^{(n)} \tag{3.294}$$

$$= nI(X_1; Y|X_2, T) + n\epsilon_1^{(n)} \tag{3.295}$$

where (3.285) follows from Fano's inequality [14], and (3.287) follows from the following Markov chain,

$$(Y_{F_1 i}, Y_{F_2 i}) \rightarrow Y_i \rightarrow (W_1, W_2, Y^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) \tag{3.296}$$

and (3.289) follows from the fact that X_{2i} is a function of $(W_2, Y_{F_2}^{i-1})$, (3.290) follows from the fact that conditioning reduces entropy, (3.291) from the memoryless property of the channel and (3.292) follows by dropping (W_2, Y^{i-1}) from the first term and obtaining an upper bound. We finally arrive at (3.295) by defining the auxiliary random variable $T = (Q, Y_{F_1}^{Q-1}, Y_{F_2}^{Q-1})$, where Q is a random variable which is uniformly distributed over $\{1, \ldots, n\}$ and is independent of all other random variables.

Similarly, we also have

$$R_2 \leq I(X_2; Y|X_1, T) \tag{3.297}$$

and

$$R_1 + R_2 \leq I(X_1, X_2; Y, Y_{F_1}, Y_{F_2}|T) \tag{3.298}$$

$$= I(X_1, X_2; Y|T) \tag{3.299}$$

where (3.299) follows from the Markov chain $(Y_{F_1}, Y_{F_2}) \rightarrow Y \rightarrow (X_1, X_2, T)$. Moreover, as a consequence of (3.299), the sum-rate bound

$$R_1 + R_2 \leq I(X_1, X_2; Y) \tag{3.300}$$

obtained in (3.262) is redundant for any MAC-GF with transition probabilities in the form of (3.28). The proof of the dependence balance constraint is the same as in Theorem 3.1. This completes the proof of Theorem 3.3.

3.14.4 Proof of Theorem 3.4

The main idea behind the strengthening of Theorem 3.1 for user cooperation is to use the special conditional probability structure of (3.37). Using this conditional structure, we will obtain an outer bound involving only one auxiliary random variable. We first note that without any loss of generality, the conditional distributions $p(y_{F_1 i}|x_{2i})$

and $p(y_{F_2 i}|x_{1i})$ can be alternatively expressed as two deterministic functions [39], [64], i.e.,

$$Y_{F_1 i} = g_1(X_{2i}, Z_{1i}) \tag{3.301}$$

$$Y_{F_2 i} = g_2(X_{1i}, Z_{2i}) \tag{3.302}$$

where the random variables Z_{1i} and Z_{2i} are independent and identically distributed for all $i \in \{1, \ldots, n\}$ and are also independent of the messages (W_1, W_2). We now prove Theorem 3.4 by first obtaining an upper bound on R_1 as follows,

$$\begin{aligned}
nR_1 &= H(W_1) = H(W_1|W_2) && (3.303)\\
&= I(W_1; Y^n, Y_{F_2}^n, Z_1^n|W_2) + H(W_1|W_2, Y^n, Y_{F_2}^n, Z_1^n) && (3.304)\\
&\leq I(W_1; Y^n, Y_{F_2}^n, Z_1^n|W_2) + n\epsilon_1^{(n)} && (3.305)\\
&= I(W_1; Z_1^n|W_2) + I(W_1; Y^n, Y_{F_2}^n|W_2, Z_1^n) + n\epsilon_1^{(n)} && (3.306)\\
&= I(W_1; Y^n, Y_{F_2}^n|W_2, Z_1^n) + n\epsilon_1^{(n)} && (3.307)\\
&= \sum_{i=1}^{n} I(W_1; Y_i, Y_{F_2 i}|W_2, Y^{i-1}, Y_{F_2}^{i-1}, Z_1^n) + n\epsilon_1^{(n)} && (3.308)\\
&= \sum_{i=1}^{n} (H(Y_i, Y_{F_2 i}|W_2, Y^{i-1}, Y_{F_2}^{i-1}, Z_1^n) - H(Y_i, Y_{F_2 i}|W_1, W_2, Y^{i-1}, Y_{F_2}^{i-1}, Z_1^n)) \\
&\qquad + n\epsilon_1^{(n)} && (3.309)\\
&= \sum_{i=1}^{n} (H(Y_i, Y_{F_2 i}|W_2, X_{2i}, X_2^{i-1}, Z_1^n, Y^{i-1}, Y_{F_2}^{i-1}) \\
&\qquad - H(Y_i, Y_{F_2 i}|W_1, W_2, Y^{i-1}, Y_{F_2}^{i-1}, Z_1^n)) + n\epsilon_1^{(n)} && (3.310)
\end{aligned}$$

$$\leq \sum_{i=1}^{n}(H(Y_i, Y_{F_2 i}|W_2, X_{2i}, X_2^{i-1}, Z_1^n, Y^{i-1}, Y_{F_2}^{i-1})$$

$$- H(Y_i, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}, W_1, W_2, Y^{i-1}, Z_1^n)) + n\epsilon_1^{(n)} \tag{3.311}$$

$$= \sum_{i=1}^{n}(H(Y_i, Y_{F_2 i}|W_2, X_{2i}, X_2^{i-1}, Z_1^n, Y^{i-1}, Y_{F_2}^{i-1})$$

$$- H(Y_i, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.312}$$

$$= \sum_{i=1}^{n}(H(Y_i, Y_{F_2 i}|X_{2i}, X_2^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}, Y^{i-1}, W_2, Z_1^n)$$

$$- H(Y_i, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.313}$$

$$\leq \sum_{i=1}^{n}(H(Y_i, Y_{F_2 i}|X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) - H(Y_i, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.314}$$

$$= \sum_{i=1}^{n} I(X_{1i}; Y_i, Y_{F_2 i}|X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.315}$$

$$= nI(X_{1Q}; Y_Q, Y_{F_2 Q}|X_{2Q}, Q, Y_{F_1}^{Q-1}, Y_{F_2}^{Q-1}) + n\epsilon_1^{(n)} \tag{3.316}$$

$$= nI(X_1; Y, Y_{F_2}|X_2, T) + n\epsilon_1^{(n)} \tag{3.317}$$

where (3.305) follows from Fano's inequality [14], (3.307) follows from the independence of (W_1, W_2) and Z_1^n, (3.310) follows by adding (X_{2i}, X_2^{i-1}) in the conditioning of the first term. This is possible since (X_{2i}, X_2^{i-1}) is a function of $(W_2, Y_{F_2}^{i-1})$. We further upper bound by introducing $(X_{1i}, X_{2i}, Y_{F_1}^{i-1})$ in the conditioning in the second term to arrive at (3.311). In (3.312), we use the memoryless property of the channel to drop $(W_1, W_2, Y^{i-1}, Z_1^n)$ from the conditioning in the second term while retaining $(Y_{F_1}^{i-1}, Y_{F_2}^{i-1})$.

Next, we make use of the special channel structure of (3.37). More specifically, using (3.301), we observe that $Y_{F_1}^{i-1}$ is a deterministic function of X_2^{i-1} and Z_1^{i-1} and

therefore, it is introduced in the conditioning in the first term in (3.313). This is the crucial part of the proof which enables us to obtain an outer bound involving only one auxiliary random variable as opposed to two auxiliary random variables. Next, we upper bound (3.313) by dropping $(W_2, Y^{i-1}, X_2^{i-1}, Z_1^n)$ from the first term to arrive at (3.314). Finally, we define $T = (Q, Y_{F_1}^{Q-1}, Y_{F_2}^{Q-1})$, $X_1 = X_{1Q}$, $X_2 = X_{2Q}$, $Y = Y_Q$, $Y_{F_1} = Y_{F_1Q}$ and $Y_{F_2} = Y_{F_2Q}$, where Q is a random variable which is uniformly distributed over $\{1, \ldots, n\}$ and is independent of all other random variables. Similarly, we have

$$R_2 \leq I(X_2; Y, Y_{F_1} | X_1, T) \tag{3.318}$$

$$R_1 + R_2 \leq I(X_1, X_2; Y, Y_{F_1}, Y_{F_2} | T) \tag{3.319}$$

The derivation of the constraint (3.41) is the same as in Theorem 3.1 and is omitted. Moreover, from the proof of the dependence balance constraint in (3.16), we observe that $Y_{F_1}^{i-1}$ and $Y_{F_2}^{i-1}$ appear together in the conditioning. Therefore, from our earlier definition of $T = (Q, Y_{F_1}^{Q-1}, Y_{F_2}^{Q-1})$, we directly have from the proof of (3.16)

$$I(X_1; X_2 | T) \leq I(X_1; X_2 | Y_{F_1}, Y_{F_2}, T) \tag{3.320}$$

This completes the proof of Theorem 3.4.

3.14.5 Proof of Theorem 3.5

The idea behind obtaining a strengthened version of Theorem 3.2 for IC with user cooperation is to use the special transition probability structure of (3.48). Using the same argument as in the proof of Theorem 3.4, we can express $Y_{F_1 i}$ and $Y_{F_2 i}$ as,

$$Y_{F_1 i} = g_1(X_{2i}, Z_{1i}) \tag{3.321}$$

$$Y_{F_2 i} = g_2(X_{1i}, Z_{2i}) \tag{3.322}$$

where the random variables Z_{1i} and Z_{2i} are independent and identically distributed for all $i \in \{1, \ldots, n\}$ and are also independent of the messages (W_1, W_2). We now prove Theorem 3.5 by first obtaining an upper bound on R_1 as follows,

$$nR_1 = H(W_1) = H(W_1|W_2) \tag{3.323}$$

$$= I(W_1; Y_1^n, Y_2^n, Y_{F_2}^n, Z_1^n|W_2) + H(W_1|W_2, Y_1^n, Y_2^n, Y_{F_2}^n, Z_1^n) \tag{3.324}$$

$$\leq I(W_1; Y_1^n, Y_2^n, Y_{F_2}^n, Z_1^n|W_2) + n\epsilon_1^{(n)} \tag{3.325}$$

$$= I(W_1; Z_1^n|W_2) + I(W_1; Y_1^n, Y_2^n, Y_{F_2}^n|W_2, Z_1^n) + n\epsilon_1^{(n)} \tag{3.326}$$

$$= I(W_1; Y_1^n, Y_2^n, Y_{F_2}^n|W_2, Z_1^n) + n\epsilon_1^{(n)} \tag{3.327}$$

$$= \sum_{i=1}^{n} I(W_1; Y_{1i}, Y_{2i}, Y_{F_2 i}|W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1}, Z_1^n) + n\epsilon_1^{(n)} \tag{3.328}$$

$$= \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i}|W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1}, Z_1^n)$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i}|W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1}, Z_1^n)) + n\epsilon_1^{(n)} \tag{3.329}$$

$$= \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i}|W_2, X_{2i}, X_2^{i-1}, Z_1^n, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i}|W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1}, Z_1^n)) + n\epsilon_1^{(n)} \tag{3.330}$$

$$\leq \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i}|W_2, X_{2i}, X_2^{i-1}, Z_1^n, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}, W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Z_1^n)) + n\epsilon_1^{(n)} \tag{3.331}$$

$$= \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i}|W_2, X_{2i}, X_2^{i-1}, Z_1^n, Y_1^{i-1}, Y_2^{i-1}, Y_{F_2}^{i-1})$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.332}$$

$$= \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i}|X_{2i}, X_2^{i-1}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}, Y_1^{i-1}, Y_2^{i-1}, W_2, Z_1^n)$$

$$- H(Y_{1i}, Y_{2i}, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)} \tag{3.333}$$

$$\leq \sum_{i=1}^{n} (H(Y_{1i}, Y_{2i}, Y_{F_2 i}|X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) - H(Y_{1i}, Y_{2i}, Y_{F_2 i}|X_{1i}, X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1})) + n\epsilon_1^{(n)}$$

$$\tag{3.334}$$

$$= \sum_{i=1}^{n} I(X_{1i}; Y_{1i}, Y_{2i}, Y_{F_2 i}|X_{2i}, Y_{F_1}^{i-1}, Y_{F_2}^{i-1}) + n\epsilon_1^{(n)} \tag{3.335}$$

$$= nI(X_{1Q}; Y_{1Q}, Y_{2Q}, Y_{F_2 Q}|X_{2Q}, Q, Y_{F_1}^{Q-1}, Y_{F_2}^{Q-1}) + n\epsilon_1^{(n)} \tag{3.336}$$

$$= nI(X_1; Y_1, Y_2, Y_{F_2}|X_2, T) + n\epsilon_1^{(n)} \tag{3.337}$$

where (3.325) follows from Fano's inequality [14], (3.327) follows from the independence of (W_1, W_2) and Z_1^n, (3.330) follows by adding (X_{2i}, X_2^{i-1}) in the conditioning of the first term. This is possible since (X_{2i}, X_2^{i-1}) is a function of $(W_2, Y_{F_2}^{i-1})$. We further upper bound by introducing $(X_{1i}, X_{2i}, Y_{F_1}^{i-1})$ in the conditioning in the second term to arrive at (3.331). In (3.332), we use the memoryless property of the chan-

nel to drop $(W_1, W_2, Y_1^{i-1}, Y_2^{i-1}, Z_1^n)$ from the conditioning in the second term while retaining $(Y_{F_1}^{i-1}, Y_{F_2}^{i-1})$.

Next, we make use of the special channel structure of (3.48). More specifically, using (3.321), we observe that $Y_{F_1}^{i-1}$ is a deterministic function of X_2^{i-1} and Z_1^{i-1} and therefore, it is introduced in the conditioning in the first term in (3.333). Next, we upper bound (3.333) by dropping $(W_2, X_2^{i-1}, Y_1^{i-1}, Y_2^{i-1}, Z_1^n)$ from the first term to arrive at (3.334). Finally, we define $T = (Q, Y_{F_1}^{Q-1}, Y_{F_2}^{Q-1})$, $X_1 = X_{1Q}$, $X_2 = X_{2Q}$, $Y_1 = Y_{1Q}$, $Y_2 = Y_{2Q}$, $Y_{F_1} = Y_{F_1Q}$ and $Y_{F_2} = Y_{F_2Q}$, where Q is a random variable which is uniformly distributed over $\{1, \ldots, n\}$ and is independent of all other random variables. Similarly, we have

$$R_2 \leq I(X_2; Y_1, Y_2, Y_{F_1} | X_1, T) \tag{3.338}$$

The derivations of the remaining constraints are similar to the proof of Theorem 2 since both $Y_{F_1}^{i-1}$ and $Y_{F_2}^{i-1}$ appear together in the conditioning and T can be defined appropriately without any difficulty. The proof of dependence balance constraint in (3.56) is the same as in Theorem 3.2. This completes the proof of Theorem 3.5.

3.14.6 Proof of (3.78)

In the following derivation of (3.78), we have dropped conditioning on $T = t$, for the purpose of simplicity. Substituting (3.80), (3.81), (3.82) and (3.83) in (3.76), we have

$$N(\Lambda_1^{1/2}\mathbf{Y} + \mathbf{V}) = N(\sqrt{\kappa}Y + V_1, V_2) \tag{3.339}$$

$$= \frac{1}{(2\pi\mathrm{e})}\mathrm{e}^{h(\sqrt{\kappa}Y+V_1,V_2)} \tag{3.340}$$

$$= \frac{1}{\sqrt{(2\pi\mathrm{e})}}\mathrm{e}^{h(\sqrt{\kappa}Y+V_1)} \tag{3.341}$$

We also note the following inequality,

$$h(\sqrt{\kappa}Y + V_1) \geq \frac{1}{2}\log(\mathrm{e}^{2h(\sqrt{\kappa}Y)} + 2\pi\mathrm{e}) \tag{3.342}$$

$$= \frac{1}{2}\log(\kappa\mathrm{e}^{2h(Y)} + 2\pi\mathrm{e}) \tag{3.343}$$

where (3.342) follows from the scalar EPI [14] and (3.343) follows from the fact that for any scalar c, $h(cY) = h(Y) + \log(|c|)$ [14]. Substituting (3.343) in (3.341), we obtain

$$N(\Lambda_1^{1/2}\mathbf{Y} + \mathbf{V}) \geq \left(\frac{\kappa\mathrm{e}^{2h(Y)} + 2\pi\mathrm{e}}{(2\pi\mathrm{e})}\right)^{1/2} \tag{3.344}$$

Similarly, we also have

$$N(\Lambda_2^{1/2}\mathbf{Y} + \mathbf{V}) \geq \left(\frac{\kappa\mathrm{e}^{2h(Y)} + 2\pi\mathrm{e}}{(2\pi\mathrm{e})}\right)^{1/2} \tag{3.345}$$

Therefore, we have

$$\mu N(\Lambda_1^{1/2}\mathbf{Y}+\mathbf{V})+(1-\mu)N(\Lambda_2^{1/2}\mathbf{Y}+\mathbf{V}) \geq \left(\frac{\kappa \mathrm{e}^{2h(Y)}+2\pi\mathrm{e}}{(2\pi\mathrm{e})}\right)^{1/2} \tag{3.346}$$

Moreover, the right hand side of (3.76) simplifies to,

$$N((\mu\Lambda_1+(1-\mu)\Lambda_2)^{1/2}\mathbf{Y}+\mathbf{V}) = \frac{1}{(2\pi\mathrm{e})}\mathrm{e}^{h(\sqrt{\mu\kappa}Y+V_1,\sqrt{(1-\mu)\kappa}Y+V_2)} \tag{3.347}$$

$$= \frac{1}{(2\pi\mathrm{e})}\mathrm{e}^{h((\mu\Lambda_1+(1-\mu)\Lambda_2)^{1/2}[Y_{F_1} \quad Y_{F_2}]^T)} \tag{3.348}$$

$$= \frac{1}{(2\pi\mathrm{e})\sqrt{\sigma_{Z_1}^2\sigma_{Z_2}^2}}\mathrm{e}^{h(Y_{F_1},Y_{F_2})} \tag{3.349}$$

Using (3.345)-(3.349) and substituting in (3.76), we obtain

$$\left(\frac{\kappa \mathrm{e}^{2h(Y)}+2\pi\mathrm{e}}{(2\pi\mathrm{e})}\right)^{1/2} \leq \frac{1}{(2\pi\mathrm{e})\sqrt{\sigma_{Z_1}^2\sigma_{Z_2}^2}}\mathrm{e}^{h(Y_{F_1},Y_{F_2})} \tag{3.350}$$

Simplifying (3.350) by substituting the value of κ and reintroducing the conditioning on $T=t$, we have the proof of (3.78),

$$h(Y_{F_1},Y_{F_2}|T=t) \geq \frac{1}{2}\log\left((2\pi\mathrm{e})^2\sigma_{Z_1}^2\sigma_{Z_2}^2+2\pi\mathrm{e}(\sigma_{Z_1}^2+\sigma_{Z_2}^2)\mathrm{e}^{h(Y|T=t)}\right) \tag{3.351}$$

Chapter 4

On the Capacity of State-Dependent Channels with Rate-Limited State Information at Receiver and Transmitter

4.1 Introduction

The study of state-dependent channels was initiated by Shannon in [55] where the channel state information (CSI) is assumed to be available at the transmitter in a causal fashion. Shannon derived the capacity of this channel by showing that it is equal to the capacity of another discrete memoryless channel with the same output alphabet and an enlarged input alphabet of size $|\mathcal{X}|^{|\mathcal{T}|}$, where $|\mathcal{T}|$ is the size of the state alphabet.

The case of non-causal CSI at the transmitter was first considered by Kuznetsov and Tsybakov [40] where achievable rates were provided, although capacity was not found. Gelfand and Pinsker derived the capacity of the state-dependent channel with non-causal CSI at the transmitter in their landmark paper [23]. The result of [23] was used by Costa [9] to evaluate the capacity of a channel with input power constraint and when the channel is an additive Gaussian state channel corrupted with independent additive Gaussian noise. This problem is commonly referred to as the dirty paper

coding (DPC) problem and has received much attention recently.

Heegard and El Gamal [29] studied state-dependent channels with various modifications regarding the rate-limited knowledge of the state at the transmitter and the receiver. For the general case when the transmitter is supplied the state information at a rate R_e and the receiver is supplied the state information at a rate R_d, an achievable rate was obtained in [29] as a function of (R_e, R_d). So far, for all the cases where the capacity has been established, the achievable rate proposed by Heegard and El Gamal has turned out to be optimal [34]. The two seemingly simple cases are still open:

1) When $R_e = 0$ and we wish to determine the capacity as a function of R_d. This situation corresponds to rate-limited CSI at the receiver (CSIR) and no CSI at the transmitter (CSIT). Such channels can also be interpreted as a special type of *primitive* relay channel [36]. A primitive relay channel is defined by a channel input X, a channel output Y and a relay output T, and a set of probability functions $p(y, t|x)$ for all $x \in \mathcal{X}$. In this setting, the relay does not have an explicit coded input to the channel. Moreover, it is also assumed that there is an orthogonal link of finite capacity R_d, from the relay to the receiver. Zhang [70] considered this relay channel and obtained a partial converse for a degraded case. For a comprehensive survey on related work on primitive relay channels, see [35]. Recently, Kim [36] established the capacity of a class of semi-deterministic primitive relay channels, for which the relay output T can be expressed as a deterministic function of the channel input X and the channel output Y, i.e., if $T = g(Y, X)$. The cut-set upper bound [14] was shown to be the capacity through an algebraic reduction of the compress-and-forward (CAF)

achievable rate [12] to the cut-set upper bound. This was the first instance where the CAF achievability scheme was shown to be capacity achieving for any relay channel.

Ahlswede and Han [2] obtained an achievable rate for the state-dependent channel with rate-limited CSIR and conjectured it to be the capacity. It follows from the result of [36] that this conjecture is true for a sub-class of such channels where the state T can be expressed as a deterministic function of X and Y, i.e., $T = g(X, Y)$. An example of this class is a case when X, T and Y are all binary, $T \sim \text{Ber}(\delta)$ and independent of X, and the channel is given by $Y = X \oplus T$, where $\oplus$ denotes modulo-2 addition. Note that, in this case, T is a deterministic function of X and Y, since $T = X \oplus Y$. A capacity result following up on the aforementioned modulo additive noise channel was obtained in [4], where it was assumed that the receiver observes $Y = X \oplus Z$ and the relay observes a noisy version of the forward noise, i.e., $T = Z \oplus \tilde{Z}$. Clearly, if $\tilde{Z} = 0$, then this channel reduces to the class studied in [36]. However, when $\tilde{Z} \neq 0$, T cannot be written as a deterministic function of X and Y, and this modulo additive class lies outside of the class of channels considered in [36]. By proving a converse, it was shown in [4] that CAF scheme is capacity achieving for this modulo additive case. The remarkable fact was that the capacity was shown to be strictly less than the cut-set upper bound for certain values of R_d. However, it is worth noting that the converse proved in [4] relied on the modulo additive nature of the forward channel. We obtain a new upper bound on the capacity of state-dependent channels with rate-limited CSIR. Our upper bound serves a dual purpose. Firstly, using our upper bound, we recover the capacity results obtained in [36] for the case where $T = g(X, Y)$ and the capacity result obtained in [4] for the modulo additive noise

case. Secondly, we confirm the validity of the conjecture due to Ahlswede-Han [2] for another class of channels which does not fall into any of the classes considered in [36] and [4].

2) Secondly, we investigate the case when $R_d = 0$ and we wish to characterize the capacity as a function of R_e. This situation corresponds to rate-limited CSI at the transmitter and no CSIR. This problem can be interpreted as the rate-limited version of the Gelfand-Pinsker problem [23]. An achievable rate for this channel model can be obtained via [29]. We provide a new upper bound on the capacity of state-dependent channels with rate-limited CSIT and no CSIR.

Using our upper bound, we explicitly characterize the rate-limited CSIT capacity of a sub-class of the state-dependent channels for which we prove the validity of Ahlswede-Han conjecture mentioned in case 1). We show that for this sub-class of state-dependent channels, capacity expressions for both rate-limited CSIT and rate-limited CSIR channel models are the same. In other words, as far as the rate-limited CSIT and rate-limited CSIR capacities are concerned, it does not matter whether the transmitter or the receiver has access to rate-limited knowledge about the channel state T. Secondly, we obtain a new upper bound for the capacity of the rate-limited DPC channel model. We show that for a certain range of values of R_e, our upper bound strictly improves upon the upper bound of DPC capacity obtained by Costa [9]. We also provide an evaluation of the achievable rates for this channel model using the result of [29]. We show that this achievable rate is optimal for limiting values of R_e, i.e., it matches our upper bound as $R_e \to 0$ and as $R_e \to \infty$.

4.2 State-Dependent Channel Model

A discrete memoryless state-dependent channel is defined by a channel input alphabet $\mathcal{X}$, a state alphabet $\mathcal{T}$, a channel output alphabet $\mathcal{Y}$ and a transition probability function $p(y|x,t)$ defined for every pair $(x,t) \in \mathcal{X} \times \mathcal{T}$. The state sequence T^n is assumed to be i.i.d. and is generated according to a fixed distribution $p(t)$.

4.2.1 Rate-Limited CSI at the Receiver

We first consider a state-dependent channel where the receiver is supplied with the state information at a rate R_d. An (n, M, R_d, P_e) code for this channel is defined by a state encoding function, $f_s : \mathcal{T}^n \to \{1, 2, \ldots, K\}$, where $K \leq 2^{nR_d}$, a channel encoding function, $f_e : \{1, 2, \ldots, M\} \to \mathcal{X}^n$ and a decoding function, $g : \mathcal{Y}^n \times \{1, 2, \ldots, K\} \to \{1, 2, \ldots, M\}$. The transmitter produces a message W which is uniformly distributed on the set $\{1, \ldots, M\}$ and transmits it in n channel uses. The average probability of error is defined as $P_e = \Pr[\hat{W} \neq W]$. A rate R is said to be achievable for this channel if for any $\epsilon > 0$, there exists an (n, M, R_d, P_e) code such that $R \leq \log(M)/n$, $K \leq 2^{nR_d}$ and $P_e < \epsilon$ for sufficiently large n. The capacity of this channel, $C(R_d)$, is the supremum of all achievable rates R. This channel can also be interpreted as a special type of relay channel, with the state-encoder acting as a relay and supplying state information to the decoder via an orthogonal link of capacity R_d.

4.2.2 Rate-Limited CSI at the Transmitter

We will next consider a state-dependent channel where the transmitter is supplied with the state information at a rate R_e. An (n, M, R_e, P_e) code for this channel is defined by a state encoding function, $f_s : \mathcal{T}^n \to \{1, 2, \ldots, K\}$, where $K \leq 2^{nR_e}$, a channel encoding function, $f_e : \{1, 2, \ldots, M\} \times \{1, 2, \ldots, K\} \to \mathcal{X}^n$ and a decoding function, $g : \mathcal{Y}^n \to \{1, 2, \ldots, M\}$. The transmitter produces a message W which is uniformly distributed on the set $\{1, \ldots, M\}$ and transmits it in n channel uses. The average probability of error is defined as $P_e = \Pr[\hat{W} \neq W]$. A rate R is said to be achievable for this channel if for any $\epsilon > 0$, there exists an (n, M, R_e, P_e) code such that $R \leq \log(M)/n$, $K \leq 2^{nR_e}$ and $P_e < \epsilon$ for sufficiently large n. The capacity of this channel, $C(R_e)$, is the supremum of all achievable rates R.

4.3 The State-Dependent Channel with Rate-Limited CSIR

We will provide a new upper bound on the capacity of state-dependent channels with rate-limited CSIR and no CSIT (see Figure 4.1).

Theorem 4.1 *The capacity of state-dependent channel with rate-limited CSIR, $\mathcal{C}(R_d)$, is upper bounded by $\mathcal{UB}(R_d)$, where*

$$\begin{aligned} \mathcal{UB}(R_d) = \sup \min\{&I(X, V; Y), I(X; Y|T)\} \\ \text{s.t. } &I(T; V) \leq R_d \\ \text{over } &p(x)p(t)p(v|t) \end{aligned} \tag{4.1}$$

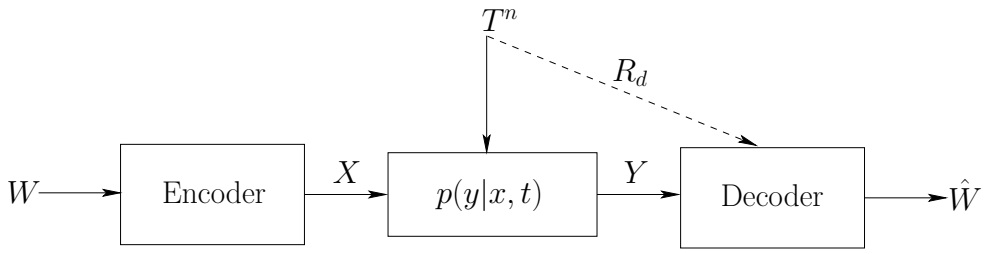

Figure 4.1: The state-dependent channel with rate-limited state information at the receiver.

where the supremum can be restricted over those joint distributions for which $|\mathcal{V}| \leq |\mathcal{T}| + 2$.

The proof of Theorem 4.1 is given in the Appendix.

Achievable rates for this channel model were obtained by Ahlswede and Han [2] and can also be obtained via the results of [12, 29]. These achievable rates can be expressed as,

$$\begin{aligned} \mathcal{LB}(R_d) = \sup\, & I(X;Y|V) \\ & \text{s.t. } I(T;V|Y) \leq R_d \\ & \text{over } p(x)p(t)p(v|t) \end{aligned} \tag{4.2}$$

4.3.1 Comparison with the Cut-Set Upper Bound

Note that the state-dependent channel with rate-limited CSIR and no CSIT can also be interpreted as a relay channel [12]. The best known upper bound for the relay channel is the cut-set bound [14], which reduces for the relay channel in consideration

to [35, 36]

$$\mathcal{CS}(R_d) = \max_{p(x)} \min\{I(X;Y) + R_d, I(X;Y|T)\} \tag{4.3}$$

On comparing (4.1) with the cut-set bound in (4.3), it can be observed that our bound differs from the cut-set bound in the multiple access cut. We will now show that our upper bound is in general smaller than the cut-set bound. We start by upper bounding the expression $I(X, V; Y)$ as follows,

$$\begin{aligned}
I(X, V; Y) &= I(X;Y) + I(V;Y|X) && (4.4)\\
&= I(X;Y) + H(V|X) - H(V|Y, X) && (4.5)\\
&= I(X;Y) + H(V) - H(V|Y, X) && (4.6)\\
&\leq I(X;Y) + H(V) - H(V|T, Y, X) && (4.7)\\
&= I(X;Y) + H(V) - H(V|T) && (4.8)\\
&= I(X;Y) + I(T;V) && (4.9)\\
&\leq I(X;Y) + R_d && (4.10)
\end{aligned}$$

where (4.6) follows from the fact that V is independent of X, (4.7) follows from the fact that conditioning reduces entropy, (4.8) follows from the Markov chain $(X, Y) \rightarrow T \rightarrow V$ and (4.10) follows by using the fact that $I(T;V) \leq R_d$. Using (4.1) and

(4.10), we have the following

$$\mathcal{UB}(R_d) \leq \max_{p(x)} \min\{I(X;Y) + R_d, I(X;Y|T)\} \tag{4.11}$$

Thus, our upper bound obtained in (4.1) is in general smaller than the cut-set bound given in (4.3). It was shown in [36] that the cut-set bound is tight for the case when $T = g(X, Y)$ and is achieved by the CAF achievability scheme. Note the fact that for this special class of channels, the inequality in (4.7) is in fact an equality and our upper bound equals the cut-set bound.

4.3.2 The Modulo Additive State-Dependent Channel

A specific modulo additive state-dependent channel with rate-limited CSIR and no CSIT was considered in [4] for which the channel is given as,

$$Y = X \oplus Z \tag{4.12}$$

$$T = Z \oplus \tilde{Z} \tag{4.13}$$

where X, Y, T, Z and $\tilde{Z}$ are all binary and $Z \sim \text{Ber}(\delta)$, $\tilde{Z} \sim \text{Ber}(\tilde{\delta})$. Clearly this channel does not fall into the class of channels studied in [36], where T can be written as a deterministic function of X and Y. It was shown that the capacity of this channel is given by [4, Theorem 1]

$$\mathcal{C}(R_d) = \max_{p(v|t):I(T;V)\leq R_d} 1 - H(Z|V) \tag{4.14}$$

We will show that our bound is equal to the capacity for this class of channels. First, note that

$$I(X,V;Y) = H(Y) - H(Y|X,V) \tag{4.15}$$

$$= H(Y) - H(Z|V) \tag{4.16}$$

$$\leq 1 - H(Z|V) \tag{4.17}$$

where (4.17) follows by the fact that the entropy of a binary random variable is upper bounded by 1. Next, consider the other cut,

$$I(X;Y|T) = H(Y|T) - H(Y|X,T) \tag{4.18}$$

$$= H(Y|T) - H(Z|T) \tag{4.19}$$

$$\leq 1 - H(Z|T) \tag{4.20}$$

Moreover, from (4.17) and (4.20), it can be observed that the bound $I(X;Y|T)$ is redundant since $V \to T \to Z$ implies $H(Z|T) \leq H(Z|V)$. Hence, our upper bound reduces to

$$\mathcal{UB}(R_d) = \max_{p(v|t):I(T;V)\leq R_d} 1 - H(Z|V) \tag{4.21}$$

We should remark that the converse obtained in [4] for this channel utilized the modulo additive nature of the channel. For such a channel, a uniform distribution on X makes the channel output Y independent of noise Z, thereby making the proceedings

in the converse easier. Our upper bound does not rely on the specific nature of the channel and holds for all state-dependent channels.

We have shown that for all the classes for which the capacity, $\mathcal{C}(R_d)$, is known, our upper bound is tight. To illustrate the usefulness of our bound, we will consider a state-dependent channel which does not fall into any of these classes and establish its capacity.

4.3.3 Capacity Result for a Symmetric Binary Erasure Channel with Two States

We will show that for a particular binary input state-dependent channel with two states, our upper bound yields the capacity which turns out to be strictly less than the cut-set bound. The state T is binary with $\Pr(T = 0) = \alpha$. The channel input X is binary and channel output Y is ternary. For channel states $T = 0, 1$, the transition probabilities, $p(y|x, t)$, are given as follows (see Figure 4.2),

$$B_0 = \begin{bmatrix} 0 & 1-\epsilon & \epsilon \\ \epsilon & 1-\epsilon & 0 \end{bmatrix} \qquad B_1 = \begin{bmatrix} \epsilon & 1-\epsilon & 0 \\ 0 & 1-\epsilon & \epsilon \end{bmatrix}$$

It should be noted that this class of channels does not fall into the class of channels considered in [36] since T cannot be obtained as a deterministic function of X and Y. Moreover, the channel output Y cannot be expressed in the form as $Y = X \oplus Z$, for some $p(t|z)$, where $\oplus$ is modulo-2 addition, since the cardinality of Y is different

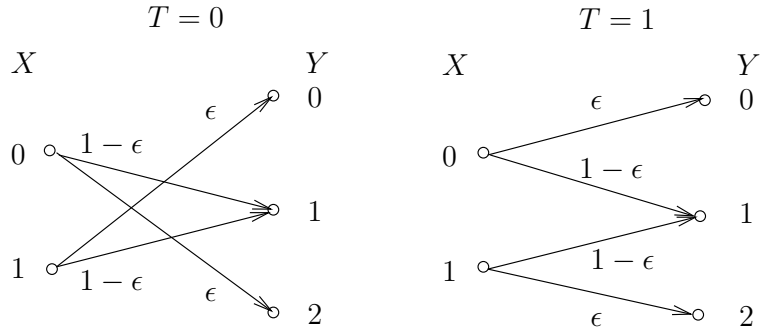

Figure 4.2: A symmetric binary erasure channel with two states.

from the cardinality of X. Hence, the converse technique developed in [4] for modulo additive relay channels does not apply to this channel. However, our upper bound holds for any $p(y|x,t)$. We begin by evaluating the achievable rates given by the CAF scheme in (4.2),

$$\begin{aligned} \mathcal{C}(R_d) \geq & \sup I(X;Y|V) \\ & \text{s.t. } I(T;V|Y) \leq R_d \\ & \text{for some } p(x,t,v) = p(x)p(t)p(v|t) \end{aligned} \tag{4.22}$$

We first define $\Pr(X=0) = p$ and obtain the involved probabilities,

$$\Pr(Y=0) = \epsilon(\alpha * p) \tag{4.23}$$

$$\Pr(Y=1) = 1-\epsilon \tag{4.24}$$

$$\Pr(Y=2) = \epsilon(1-\alpha * p) \tag{4.25}$$

and

$$\Pr(Y = 0|T = 0) = \epsilon(1 - p) \tag{4.26}$$

$$\Pr(Y = 1|T = 0) = 1 - \epsilon \tag{4.27}$$

$$\Pr(Y = 2|T = 0) = \epsilon p \tag{4.28}$$

and

$$\Pr(Y = 0|T = 1) = \epsilon p \tag{4.29}$$

$$\Pr(Y = 1|T = 1) = 1 - \epsilon \tag{4.30}$$

$$\Pr(Y = 2|T = 1) = \epsilon(1 - p) \tag{4.31}$$

where we have defined $a * b = a(1 - b) + b(1 - a)$. Furthermore, we also note the following inequality,

$$h^{(3)}(a, b, c) = \frac{1}{2}h^{(3)}(a, b, c) + \frac{1}{2}h^{(3)}(c, b, a) \tag{4.32}$$

$$\leq h^{(3)}\left(\frac{a + c}{2}, b, \frac{a + c}{2}\right) \tag{4.33}$$

$$= h(b) + 1 - b \tag{4.34}$$

Using this fact, we have

$$H(Y) = h^{(3)}\left(\epsilon(\alpha * p), 1 - \epsilon, \epsilon(1 - \alpha * p)\right) \tag{4.35}$$

$$\leq h(\epsilon) + \epsilon \tag{4.36}$$

Also, a uniform distribution on X, yields the maximum entropy for Y, and makes Y and T independent. Note that the maximum entropy of Y in this case is $h(\epsilon) + \epsilon$ which is strictly less than $\log(3)$ for all $\epsilon \in [0, 1]$. Hence, for a uniform X, we have

$$H(Y|V) = H(Y) \tag{4.37}$$

$$= h(\epsilon) + \epsilon \tag{4.38}$$

We also define,

$$\eta_v = \Pr(T = 1|V = v), \qquad v = 1, \ldots, |\mathcal{V}| \tag{4.39}$$

Using this definition, we can write $H(Y|X, V)$ for any distribution $p(x)$ on X as follows,

$$H(Y|X, V) = \sum_v p(v) \sum_x p(x) H(Y|X = x, V = v) \tag{4.40}$$

$$= \sum_v p(v) h^{(3)} \left(\eta_v \epsilon, 1 - \epsilon, (1 - \eta_v)\epsilon\right) \tag{4.41}$$

$$= H(U|V) \tag{4.42}$$

where we have defined a random variable U with $|\mathcal{U}| = 3$ and $p(u|t)$, expressed as a stochastic matrix B which is given as

$$B = \begin{pmatrix} \epsilon & 1 - \epsilon & 0 \\ 0 & 1 - \epsilon & \epsilon \end{pmatrix} \tag{4.43}$$

Thus, $H(Y|X,V)$ is invariant to the distribution of X. Moreover, by construction, the random variables (T,U,V) satisfy the Markov chain $V \to T \to U$.

We now return to the evaluation of the rates given by the CAF scheme given in (4.22). Using (4.38) and (4.42), we have for a uniform distribution on X,

$$I(X;Y|V) = H(Y|V) - H(Y|X,V) \tag{4.44}$$

$$= h(\epsilon) + \epsilon - H(U|V) \tag{4.45}$$

Furthermore, for uniform X, we have $I(T;V|Y) = I(T;V)$, thus the constraint in (4.22) simplifies to $I(T;V) \leq R_d$. For simplicity, define the set

$$\mathcal{L}(\gamma) = \{p(v|t) : H(T|V) \geq \gamma;\ V \to T \to U\} \tag{4.46}$$

Using (4.45) and (4.46), we obtain a lower bound on the capacity as

$$\mathcal{C}(R_d) \geq h(\epsilon) + \epsilon - \inf_{p(v|t) \in \mathcal{L}(h(\alpha) - R_d)} H(U|V) \tag{4.47}$$

We now evaluate our upper bound. Using the fact that $\min(I(X,V;Y), I(X;Y|T)) \leq$

$I(X, V; Y)$, we obtain a weaker version of our upper bound in (4.1) as

$$\mathcal{C}(R_d) \leq \sup I(X, V; Y) \tag{4.48}$$

$$= \sup(H(Y) - H(Y|X, V)) \tag{4.49}$$

$$\leq \sup(h(\epsilon) + \epsilon - H(Y|X, V)) \tag{4.50}$$

$$= h(\epsilon) + \epsilon - \inf H(Y|X, V) \tag{4.51}$$

$$= h(\epsilon) + \epsilon - \inf_{p(v|t) \in \mathcal{L}(h(\alpha) - R_d)} H(U|V) \tag{4.52}$$

where (4.50) follows from (4.36), and the sup in (4.48)-(4.50) is taken over all $p(x)$ and those $p(v|t)$ which satisfy $I(T; V) \leq R_d$.

Hence, from (4.47) and (4.52), the capacity is given by

$$\mathcal{C}(R_d) = h(\epsilon) + \epsilon - \inf_{p(v|t) \in \mathcal{L}(h(\alpha) - R_d)} H(U|V) \tag{4.53}$$

We will now explicitly evaluate the capacity expression obtained in (4.53) and compare it with the cut-set bound. For this purpose, we need a result on the conditional entropy of dependent random variables [66]. Let T, U be a pair of dependent random variables with a joint distribution $p(t, u)$. For $0 \leq \gamma \leq H(T)$, define the function $G(\gamma)$ as the infimum of $H(U|V)$, with respect to all discrete random variables V such that $H(T|V) = \gamma$ and the random variables V and U are conditionally independent given T. For the case when T is binary and $p(u|t)$, expressed as a stochastic matrix

B, takes the form in (4.43), we have from [66],

$$G(\gamma) = \inf_{p(v|t)\in\mathcal{L}(\gamma)} H(U|V) \tag{4.54}$$

$$= h(\epsilon) + \epsilon\gamma \tag{4.55}$$

We will use this result from [66] in explicitly evaluating the capacity in (4.53). First note that, if $R_d \geq h(\alpha)$, then

$$G(h(\alpha) - R_d) = G(0) = h(\epsilon) \tag{4.56}$$

whereas, if $R_d < h(\alpha)$, then

$$G(h(\alpha) - R_d) = h(\epsilon) + \epsilon(h(\alpha) - R_d) \tag{4.57}$$

Using (4.56) and (4.57), the capacity expression in (4.53) evaluates to,

$$\mathcal{C}(R_d) = \begin{cases} \epsilon, & R_d \geq h(\alpha) \\ \epsilon(1 - h(\alpha)) + \epsilon R_d, & R_d < h(\alpha) \end{cases} \tag{4.58}$$

which can be written in a compact form as,

$$\mathcal{C}(R_d) = \min(\epsilon(1 - h(\alpha)) + \epsilon R_d, \epsilon) \tag{4.59}$$

The cut-set bound is obtained by evaluating (4.3) for the channel in consideration. Evaluation of the cut-set bound is straightforward by noting that $I(X;Y)$ and

$I(X;Y|T)$ are both maximized by a uniform $p(x)$. For a uniform distribution on X, we have $I(X;Y) = \epsilon(1-h(\alpha))$ and $I(X;Y|T) = \epsilon$. Hence, the cut-set bound is given as,

$$\mathcal{CS}(R_d) = \min(\epsilon(1-h(\alpha)) + R_d, \epsilon) \tag{4.60}$$

The difference between the capacity and the cut-set bound is evident from the first term in the min operation, i.e., the capacity expression in (4.59) has an ϵR_d appearing in the minimum, as opposed to R_d appearing in the cut-set bound at the corresponding place in (4.60). The cut-set bound and the capacity are shown in Figure 4.3 as functions of R_d for $\alpha = 0.3$ and $\epsilon = 0.4$.

In conclusion, for this channel which does not fall into the classes of channels studied in [36] and [4], our upper bound equals the CAF achievable rate, thus yielding the capacity, which is strictly less than the cut-set bound for $R_d < h(\alpha)$.

4.3.4 A Channel with Binary Multiplicative State and Binary Additive Noise

We will evaluate our upper bound and compare it with the cut-set bound for the case when X, T and N are binary and the channel is given as,

$$Y = TX + N \tag{4.61}$$

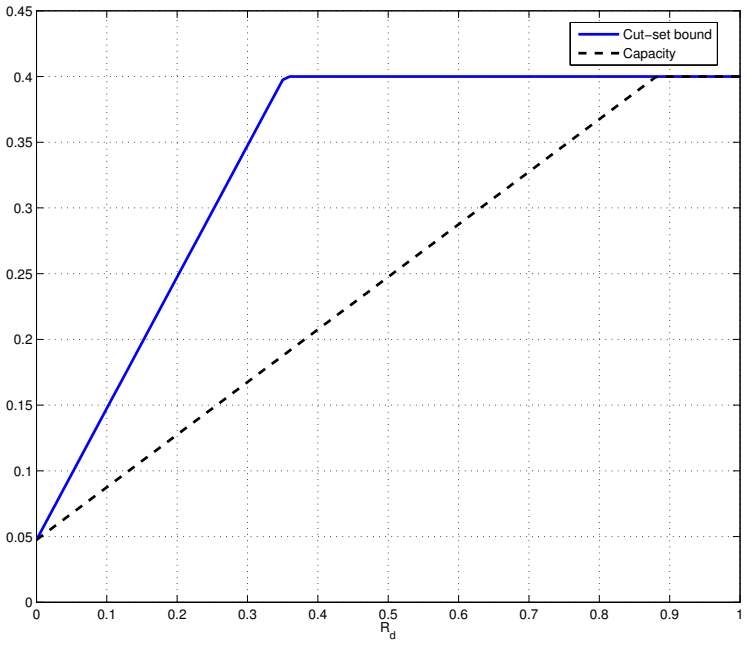

Figure 4.3: Capacity of the binary symmetric erasure channel for $\alpha = 0.3$ and $\epsilon = 0.4$.

The channel output Y takes values in the set $\{0, 1, 2\}$. The random variables T and N are distributed as $T \sim \text{Ber}(\alpha)$ and $N \sim \text{Ber}(\delta)$. This state-dependent channel does not fall into the sub-class of channels considered in [36]. Moreover, the converse obtained in [4] does not apply for this channel since the output cannot be written as a modulo addition.

To evaluate our upper bound, let us define

$$\Pr(X = 1) = p, \qquad \Pr(T = 1) = \alpha, \qquad \Pr(N = 1) = \delta \tag{4.62}$$

We then obtain $H(Y)$ as follows

$$H(Y) = h^{(3)}(P_Y(0), P_Y(1), P_Y(2)) \tag{4.63}$$

where

$$P_Y(0) = p(1-\alpha)(1-\delta) + (1-p)(1-\delta) \tag{4.64}$$

$$P_Y(1) = (1-p)\delta + p[(1-\alpha)\delta + \alpha(1-\delta)] \tag{4.65}$$

$$P_Y(2) = p\alpha\delta \tag{4.66}$$

and $H(Y|X)$ is obtained as,

$$H(Y|X) = (1-p)H(N) + pH(T+N) \tag{4.67}$$

$$= (1-p)h(\delta) + ph^{(3)}((1-\alpha)(1-\delta), \alpha * \delta, \alpha\delta) \tag{4.68}$$

The broadcast cut is obtained as,

$$I(X;Y|T) = H(Y|T) - H(Y|X,T) \tag{4.69}$$

$$= (1-\alpha)h(\delta) + \alpha h^{(3)}((1-p)(1-\delta), p * \delta, p\delta) - h(\delta) \tag{4.70}$$

The cut-set bound is given by,

$$\mathcal{CS}(R_d) = \max_p \min\{I(X;Y) + R_d, I(X;Y|T)\} \tag{4.71}$$

We now evaluate our bound by first considering,

$$I(X,V;Y) = H(Y) - H(Y|X,V) \tag{4.72}$$

We have already evaluated $H(Y)$ in (4.63). Consider $H(Y|X,V)$:

$$H(Y|X,V) = \sum_{(x,v)} P_X(x)P_V(v)H(Y|X=x,V=v) \tag{4.73}$$

$$= \sum_{v} P_V(v)\big[(1-p)H(Y|X=0,V=v) + pH(Y|X=1,V=v)\big] \tag{4.74}$$

$$= \sum_{v} P_V(v)\big[(1-p)H(N) + pH(T+N|V=v)\big] \tag{4.75}$$

$$= \sum_{v} P_V(v)\big[(1-p)h(\delta) + pH(T+N|V=v)\big] \tag{4.76}$$

$$= \sum_{v} P_V(v)\big[(1-p)h(\delta) + pH(B|V=v)\big] \tag{4.77}$$

$$= (1-p)h(\delta) + pH(B|V) \tag{4.78}$$

where we have defined another random variable $B = T + N$. We are interested in lower bounding $H(B|V)$. We also know that any permissible conditional distribution $p(v|t)$ satisfies the constraint $I(T;V) \leq R_d$. Using this, we also have the following,

$$H(T|V) \geq h(\alpha) - R_d \tag{4.79}$$

Let us also define,

$$P_{T|V}(T=1|V=v) = \eta_v, \qquad v \in 1,\ldots,|\mathcal{V}| \tag{4.80}$$

We now return to calculating $H(B|V)$

$$\Pr(B = b|V = v) = \sum_t P_{T|V}(t|v) P_{B|T,V}(b|t, v) \tag{4.81}$$

$$= (1 - \eta_v)\Pr(b|T = 0, V = v) + \eta_v \Pr(b|T = 1, V = v) \tag{4.82}$$

Since the random variable B takes values in the set $\{0, 1, 2\}$, we obtain,

$$\Pr(B = 0|V = v) = (1 - \eta_v)(1 - \delta) \tag{4.83}$$

$$\Pr(B = 1|V = v) = \eta_v * \delta \tag{4.84}$$

$$\Pr(B = 2|V = v) = \eta_v \delta \tag{4.85}$$

We finally obtain,

$$H(B|V) = \sum_v P_V(v) h^{(3)}((1 - \eta_v)(1 - \delta), \eta_v * \delta, \eta_v \delta) \tag{4.86}$$

For the special case when the additive noise is $N \sim \text{Ber}(1/2)$, the above expression simplifies to

$$H(B|V) = \sum_v P_V(v) h^{(3)} \left(\frac{(1 - \eta_v)}{2}, \frac{1}{2}, \frac{\eta_v}{2} \right) \tag{4.87}$$

$$= \sum_v P_V(v) \left(\frac{1}{2} h(\eta_v) + 1 \right) \tag{4.88}$$

$$= \frac{1}{2} H(T|V) + 1 \tag{4.89}$$

$$\geq \frac{1}{2} \left(h(\alpha) - R_d \right) + 1 \tag{4.90}$$

where (4.90) follows from (4.79). Substituting (4.90) in (4.78) we obtain

$$H(Y|X,V) = (1-p)h(\delta) + pH(B|V) \tag{4.91}$$

$$\geq (1-p)h(\delta) + p\left(\frac{1}{2}\left(h(\alpha) - R_d\right) + 1\right) \tag{4.92}$$

Continuing from (4.72), we obtain an upper bound on $I(X,V;Y)$ as follows,

$$I(X,V;Y) = H(Y) - H(Y|X,V) \tag{4.93}$$

$$\leq H(Y) - 1 - \frac{p}{2}(h(\alpha) - R_d) \tag{4.94}$$

Moreover, the first term appearing in the cut-set bound simplifies to

$$I(X;Y) + R_d = H(Y) - H(Y|X) + R_d \tag{4.95}$$

$$= H(Y) - 1 - \frac{p}{2}h(\alpha) + R_d \tag{4.96}$$

We thus obtain our upper bound as,

$$\mathcal{UB}(R_d) = \max_{p\in[0,1]} \min\left[H(Y) - 1 - \frac{p}{2}h(\alpha) + \frac{p}{2}R_d, I(X;Y|T)\right] \tag{4.97}$$

whereas the cut-set bound is,

$$\mathcal{CS}(R_d) = \max_{p\in[0,1]} \min\left[H(Y) - 1 - \frac{p}{2}h(\alpha) + R_d, I(X;Y|T)\right] \tag{4.98}$$

The difference between the cut-set bound and our upper bound is evident from the

first term in the min operation, i.e., our upper bound has a $pR_d/2$ term in (4.97), as opposed to R_d at the corresponding place in (4.98).

Both these bounds along with the CAF rate are illustrated in Figure 4.4 as a function of R_d for the case when $\alpha = 1/2$ and $\delta = 1/2$. We should remark here that although our bound is strictly smaller than the cut-set bound for certain values of R_d, it is strictly larger than the rates given by the CAF scheme.

4.3.5 Discussion

Using the fact that $\min(I(X,V;Y), I(X;Y|T)) \leq I(X,V;Y)$, and observing that $I(X,V;Y) = I(V;Y) + I(X;Y|V)$, it can be noted that our upper bound in (4.1) can be further upper bounded as

$$\mathcal{C}(R_d) \leq \sup I(V;Y) + I(X;Y|V) \tag{4.99}$$

$$\text{s.t. } I(T;V) \leq R_d \tag{4.100}$$

$$\text{for some } p(x)p(v|t) \tag{4.101}$$

On the other hand, the capacity is always lower bounded by the CAF rate,

$$\mathcal{C}(R_d) \geq \sup I(X;Y|V) \tag{4.102}$$

$$\text{s.t. } I(T;V|Y) \leq R_d \tag{4.103}$$

$$\text{for some } p(x)p(v|t) \tag{4.104}$$

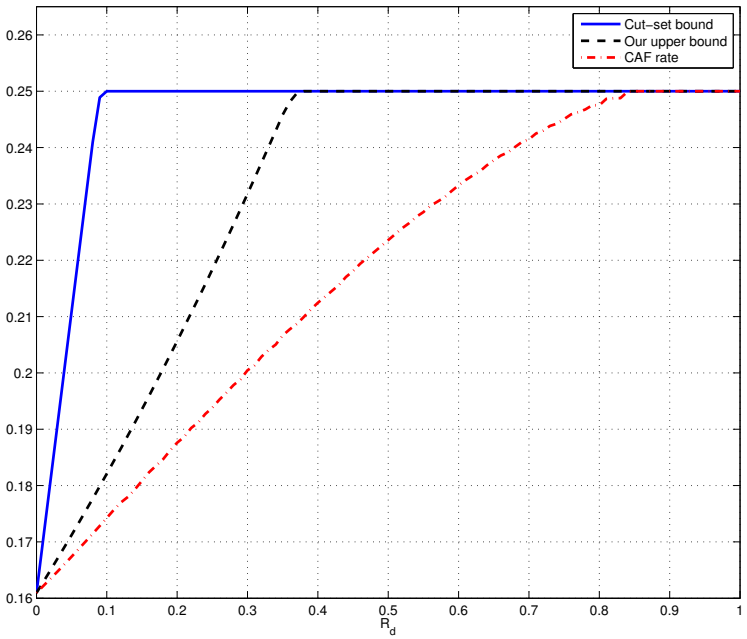

Figure 4.4: Comparison of upper bound with cut-set bound when $T, N \sim \text{Ber}(1/2)$.

Now using the following fact,

$$I(T;V|Y) = H(V|Y) - H(V|T) \tag{4.105}$$

$$= I(T;V) - I(V;Y) \tag{4.106}$$

we can rewrite the CAF lower bound on the capacity as

$$\mathcal{C}(R_d) \geq \sup I(X;Y|V) \tag{4.107}$$

$$\text{s.t. } I(T;V) - I(V;Y) \leq R_d \tag{4.108}$$

$$\text{for some } p(x)p(v|t) \tag{4.109}$$

We can see that the CAF lower bound on the capacity involves taking a supremum of $I(X;Y|V)$ subject to the constraint $I(T;V) - I(V;Y) \leq R_d$ whereas our upper bound involves taking a supremum of a larger quantity $I(V;Y) + I(X;Y|V)$ subject to a stricter constraint $I(T;V) \leq R_d$.

Although these two maximization problems are different, for the class of channels for which capacity was obtained, at the capacity achieving distribution $p(x)$, we had $I(V;Y) = 0$. Thus, for the class of channels considered in Sections 4.3.2 and 4.3.3, these two maximization problems are equivalent. This observation yields a heuristic explanation as to why we were able to obtain the capacity for this class of state-dependent channels.

4.3.6 A New Lower Bound on Critical R_d

In [11], Cover posed a slightly different problem regarding the primitive relay channel. Considering the capacity as a function of R_d, i.e., $\mathcal{C}(R_d)$, first observe the following facts,

$$\mathcal{C}(0) = \sup_{p(x)} I(X;Y) \tag{4.110}$$

$$\mathcal{C}(\infty) = \sup_{p(x)} I(X;Y|T) \tag{4.111}$$

Moreover, $\mathcal{C}(R_d)$ is a nondecreasing function of R_d. Cover posed the following question in [11]: What is the smallest value of R_d, say R_d^*, for which $\mathcal{C}(R_d^*) = \mathcal{C}(\infty)$? As an application of our upper bound, we implicitly provide a new lower bound on R_d^*.

For the class of channels considered in Section 4.3.3, we obtained the capacity. As

a consequence, we can explicitly characterize R_d^* for this class of channels as $h(\alpha)$. Furthermore, for the class of channels considered in Section 4.3.4, our upper bound on the capacity yields an improved lower bound on R_d^* than the one provided by the cut-set bound, which is clearly evident in Figure 4.4.

4.4 The State-Dependent Channel with Rate-Limited CSIT

We will provide a new upper bound on the capacity of state-dependent channels with rate-limited CSIT and no CSIR (see Figure 4.5).

Theorem 4.2 *The capacity of state-dependent channel with rate-limited CSIT, $\mathcal{C}(R_e)$, is upper bounded by $\mathcal{UB}(R_e)$, where*

$$\mathcal{UB}(R_e) = \sup_{T \to V \to (U,X): I(T;V) \leq R_e} I(U;Y) \tag{4.112}$$

The proof of Theorem 4.2 is given in the Appendix.

Heegard and El Gamal proposed the following achievable rates for this channel, which can be obtained from [29] by substituting $S_0 = c$, $S_d = c$ and $S_e = V$, where c is a constant,

$$\mathcal{LB}(R_e) = \max_{p(v|t), p(u,x|v): I(T;V) \leq R_e} I(U;Y) - I(U;V) \tag{4.113}$$

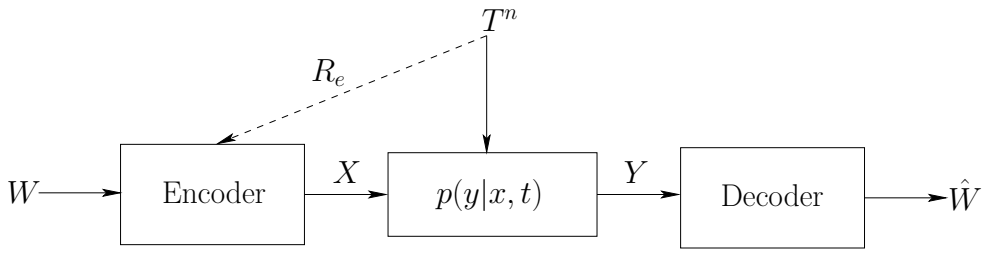

Figure 4.5: The state-dependent channel with rate-limited state information at the transmitter.

4.4.1 No CSI at the Transmitter

We now mention what our upper bound implies for the case when $R_e = 0$, which corresponds to no channel state information at the transmitter. In this case, it is straightforward to check from $\mathcal{LB}(R_e)$, by substituting $V = \phi, U = X$ that the following rates are achievable

$$\mathcal{LB}(0) \geq \max_{p(x)} I(X;Y) \tag{4.114}$$

Whereas, from our outer bound, we note the following identities. Since $R_e = 0$, we have $I(T;V) = 0$. From the Markov chain $T \to V \to (U,X)$, we have $I(T;U,X) \leq I(T;V) = 0$, which implies that T is independent of (U,X). Finally, we also observe

that

$$\mathcal{UB}(0) \leq \max_{p(u,x)} I(U;Y) \tag{4.115}$$

$$\leq \max_{p(u,x)} I(U,X;Y) \tag{4.116}$$

$$= \max_{p(u,x)} I(X;Y) + I(U;Y|X) \tag{4.117}$$

$$= \max_{p(x)} I(X;Y) \tag{4.118}$$

where $I(U;Y|X) = 0$ from the following

$$I(U;Y|X) \leq I(U;Y,T|X) \tag{4.119}$$

$$= I(U;T|X) + I(U;Y|X,T) \tag{4.120}$$

$$= 0 \tag{4.121}$$

Moreover, this upper bound is tight and is obtained by the selection $U = X$. This establishes the capacity when $R_e = 0$.

4.4.2 The Modulo Additive State-Dependent Channel

For the case when $Y = X \oplus Z$, and $T = Z \oplus \tilde{Z}$, and $|\mathcal{X}| = |\mathcal{Y}| = \mathcal{K}$, we can further upper bound our upper bound to obtain an upper bound for this class of channels

which was also obtained in [4], as follows,

$$\mathcal{C}(R_e) \leq \max I(U;Y) \tag{4.122}$$

$$= \max H(Y) - H(Y|U) \tag{4.123}$$

$$\leq \max \log(\mathcal{K}) - H(Y|U) \tag{4.124}$$

$$\leq \max \log(\mathcal{K}) - H(Y|X,U) \tag{4.125}$$

$$= \max \log(\mathcal{K}) - H(Z|X,U) \tag{4.126}$$

$$\leq \max \log(\mathcal{K}) - H(Z|V) \tag{4.127}$$

$$= \log(\mathcal{K}) - \min_{p(v|t):I(T;V)\leq R_e} H(Z|V) \tag{4.128}$$

where (4.127) follows from the Markov chain $Z \rightarrow T \rightarrow V \rightarrow (U,X)$ which implies $I(Z;U,X) \leq I(Z;V)$, which in turn implies $H(Z|X,U) \geq H(Z|V)$.

For the case when X, Y and T are binary, this bound becomes

$$\mathcal{C}(R_e) \leq 1 - \min_{p(v|t):I(T;V)\leq R_e} H(Z|V) \tag{4.129}$$

where $Z \rightarrow T \rightarrow V$ forms a Markov chain. It was shown in [4] that the above upper bound is tight and matches the achievable rate of [29] for the case when $T \sim \text{Ber}(1/2)$.

4.4.3 Capacity Result for a Symmetric Binary Erasure Channel with Two States

We will now consider the class of state-dependent channels considered in Section 4.3.3. For a sub-class of such channels, we will explicitly characterize the capacity with rate-limited CSIT. We start by further upper bounding $\mathcal{UB}(R_e)$ as follows,

$$\begin{aligned}
\mathcal{UB}(R_e) &= \max I(U;Y) && (4.130)\\
&= \max H(Y) - H(Y|U) && (4.131)\\
&\leq \max h(\epsilon) + \epsilon - H(Y|U) && (4.132)\\
&\leq \max h(\epsilon) + \epsilon - H(Y|V,U,X) && (4.133)\\
&= \max h(\epsilon) + \epsilon - H(\tilde{U}|V) && (4.134)\\
&= h(\epsilon) + \epsilon - \inf H(\tilde{U}|V) && (4.135)
\end{aligned}$$

where (4.132) follows from the fact that $H(Y) \leq h(\epsilon) + \epsilon$ which was proved in (4.36), (4.133) follows from the fact that conditioning reduces entropy and (4.134) follows from easily verifying the following,

$$H(Y|X,V,U) = H(\tilde{U}|V) \quad (4.136)$$

where $\tilde{U}$ is a random variable with $|\tilde{\mathcal{U}}| = 3$ and $p(\tilde{u}|t)$, expressed as a stochastic matrix B as,

$$B = \begin{pmatrix} \epsilon & 1-\epsilon & 0 \\ 0 & 1-\epsilon & \epsilon \end{pmatrix} \tag{4.137}$$

and the random variables $(\tilde{U}, T, V)$ satisfy the Markov chain $\tilde{U} \to T \to V$ by construction. Following similar steps as in Section 4.3.3, we continue from (4.135) to arrive at the following upper bound for $\mathcal{C}(R_e)$,

$$\mathcal{C}(R_e) \leq \min(\epsilon(1 - h(\alpha)) + \epsilon R_e, \epsilon) \tag{4.138}$$

We will now show that the upper bound obtained in (4.138) is tight for the case when $\alpha = 1/2$ by providing an explicit evaluation of $\mathcal{LB}(R_e)$ which matches our upper bound. We revisit the achievable rate stated in (4.113)

$$\mathcal{LB}(R_e) = \max_{p(v|t), p(u,x|v): I(T;V) \leq R_e} I(U;Y) - I(U;V) \tag{4.139}$$

Given the triple (ϵ, α, R_e), we will provide a set of random variables (T, V, U, X) satisfying the three conditions,

$$T \to V \to (U, X) \tag{4.140}$$

$$(V, U) \to (X, T) \to Y \tag{4.141}$$

$$I(T;V) \leq R_e \tag{4.142}$$

We first select $|\mathcal{V}| = 2$ and choose the conditional distribution $p(v|t)$ as follows,

$$\Pr(V = 0|T = 1) = \Pr(V = 1|T = 0) = \mu \tag{4.143}$$

In other words, V is connected to the channel state T through a binary symmetric channel with crossover probability μ. For such $p(v|t)$, we have

$$I(T; V) = h(\alpha * \mu) - h(\mu) \tag{4.144}$$

$$= 1 - h(\mu) \tag{4.145}$$

The crossover probability μ is chosen such that

$$1 - h(\mu) = R_e \tag{4.146}$$

so that the condition (4.142) is met with equality. We next select $|\mathcal{U}| = 2$, with U uniformly distributed on $\{0, 1\}$ and independent of V, i.e., $I(U; V) = 0$. We finally select X as a deterministic function of (U, V) as follows,

$$X = U \oplus V \tag{4.147}$$

For this selection of (T, V, U, X), we have

$$I(U;Y) - I(U;V) = I(U;Y) \tag{4.148}$$

$$= H(Y) - H(Y|U) \tag{4.149}$$

$$= h(\epsilon) + \epsilon - H(Y|U) \tag{4.150}$$

$$= h(\epsilon) + \epsilon - h^{(3)}(\mu\epsilon, 1-\epsilon, (1-\mu)\epsilon) \tag{4.151}$$

$$= \epsilon(1 - h(\mu)) \tag{4.152}$$

where (4.148) follows from the fact that V and U are independent. The case when $R_e \geq h(\alpha) = 1$ corresponds to the classical Gelfand-Pinsker setting [23] and we select $\mu = 0$ and the resulting lower bound is

$$\mathcal{LB}(R_e) = \epsilon, \quad \text{for } R_e \geq 1 \tag{4.153}$$

For the case when $R_e < 1$, we choose μ according to (4.146), i.e., $\mu = h^{-1}(1 - R_e)$ and obtain an achievable rate as follows,

$$\mathcal{LB}(R_e) \geq \epsilon(1 - h(\mu)) \tag{4.154}$$

$$= \epsilon R_e \tag{4.155}$$

where (4.155) follows from (4.146). Combining (4.153) and (4.155), we can now write a lower bound on the capacity as,

$$\mathcal{C}(R_e) \geq \min(\epsilon R_e, \epsilon) \tag{4.156}$$

whereas from (4.138), we have for $\alpha = 1/2$,

$$\mathcal{C}(R_e) \leq \min(\epsilon R_e, \epsilon) \tag{4.157}$$

and therefore

$$\mathcal{C}(R_e) = \min(\epsilon R_e, \epsilon) \tag{4.158}$$

We should remark here that the capacity of such state dependent channels with rate-limited CSIR and no CSIT was characterized in Section 4.3.3 as

$$\mathcal{C}(R_d) = \min(\epsilon R_d, \epsilon) \tag{4.159}$$

This implies that if the state information is supplied at a fixed rate, then it does not matter whether this information is available at the transmitter or at the receiver and the capacity is the same for both channel models.

4.4.4 Rate-Limited Dirty Paper Coding

We will now provide an upper bound for the case when the forward channel is an additive Gaussian noise channel and the channel states are also additive and Gaussian (see Figure 4.6). In particular, the channel is described as

$$Y = X + T + Z \tag{4.160}$$

where the channel input X is subject to an average power constraint P, the channel state T and the channel input X are independent of Z, where Z is a zero-mean, Gaussian random variable with variance σ_Z^2. Moreover, the state random variable T is a zero-mean Gaussian random variable with variance σ_T^2. The capacity of this channel is known when the state sequence is non-causally known at the transmitter. This result was obtained by Costa in [9] and the capacity was found to be

$$\mathcal{C}_{DPC} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2}\right) \tag{4.161}$$

We will provide an upper bound for the case when the transmitter is supplied information about the channel state T at a rate of R_e. It is clear that when $R_e \to \infty$, this situation corresponds to the setting of [9] and we have

$$\mathcal{C}(\infty) = \mathcal{C}_{DPC} = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2}\right) \tag{4.162}$$

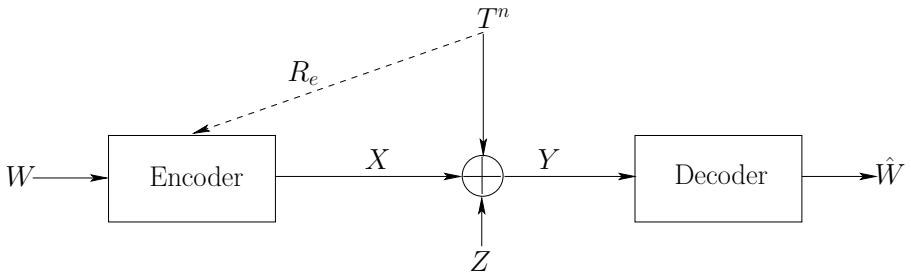

Figure 4.6: The rate-limited DPC channel model.

On the other hand, when $R_e = 0$, we know that

$$\mathcal{C}(0) = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2 + \sigma_T^2}\right) \tag{4.163}$$

which is the capacity of a channel with total Gaussian noise $T + Z$, i.e., when there is no state information at the transmitter and the state random variable T acts as additional additive Gaussian noise besides Z.

Capacity of the rate-limited dirty paper channel, i.e., $\mathcal{C}(R_e)$ is not known for $0 < R_e < \infty$. Trivial lower/upper bounds for any $0 < R_e < \infty$ are

$$\frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2 + \sigma_T^2}\right) \leq \mathcal{C}(R_e) \leq \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2}\right) \tag{4.164}$$

We will show that a strengthened version of our upper bound is strictly less than $\mathcal{C}_{DPC}$ for certain values of R_e. The main result of this section is stated in the following theorem,

Theorem 4.3 *The capacity of rate-limited DPC channel model, $\mathcal{C}(R_e)$, is upper*

bounded by $\mathcal{UB}(R_e)$*, where,*

$$\mathcal{UB}(R_e) = \begin{cases} \frac{1}{2}\log\left(\frac{P+\sigma_T^2+\sigma_Z^2}{\sigma_Z^2+\sigma_T^2 e^{-2R_e}}\right), & 0 \leq R_e < R_e^c \\ \frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right), & R_e^c \leq R_e < \infty \end{cases} \tag{4.165}$$

The proof of Theorem 4.3 is given in the Appendix.

We now obtain achievable rates for rate-limited DPC. In particular, we will obtain a potentially sub-optimal evaluation of the following achievable rate given in [29]

$$\mathcal{LB}(R_e) = \max_{p(v|t),p(u,x|v):I(T;V)\leq R_e} I(U;Y) - I(U;V) \tag{4.166}$$

The main idea behind this achievable scheme is a combination of rate-distortion type coding [14] along with Gelfand-Pinsker type binning [23]. We select the following auxiliary random variable,

$$V = T + \tilde{N} \tag{4.167}$$

where $\tilde{N}$ is a zero-mean Gaussian random variable with variance $\sigma_{\tilde{N}}^2$ and is independent of T. Here, $\tilde{N}$ can be interpreted as the compression noise. From the constraint $I(T;V) \leq R_e$, we have

$$I(T;V) = I(T;T+\tilde{N}) \tag{4.168}$$

$$= \frac{1}{2}\log\left(1+\frac{\sigma_T^2}{\sigma_{\tilde{N}}^2}\right) \leq R_e \tag{4.169}$$

From (4.169), we obtain a constraint on the permissible variance $\sigma^2_{\tilde{N}}$ of the compression noise $\tilde{N}$ as,

$$\sigma^2_{\tilde{N}} \geq \frac{\sigma^2_T}{e^{2R_e} - 1} \tag{4.170}$$

Next, we select X as a zero-mean Gaussian random variable with variance P, which is independent of V. We select the random variable U as

$$U = X + \alpha V \tag{4.171}$$

We are now ready to evaluate the achievable rates for this selection of random variables (V, X, U). So far, we have not specified α. We will later optimize α, as a function of R_e, to obtain the best possible achievable rate for this selection of auxiliary random variables.

We start by simplifying the expression in (4.166),

$$I(U;Y) - I(U;V) = h(U|V) - h(U|Y) \tag{4.172}$$

We first consider

$$h(U|V) = h(X + \alpha V|V) \tag{4.173}$$

$$= h(X|V) \tag{4.174}$$

$$= h(X) \tag{4.175}$$

$$= \frac{1}{2}\log(2\pi e P) \tag{4.176}$$

where (4.175) follows since X and V are selected to be independent. Now consider

$$h(U|Y) = h(X + \alpha V|X + T + Z) \tag{4.177}$$

$$= h(X + \alpha(T + \tilde{N})|X + T + Z) \tag{4.178}$$

$$= \frac{1}{2}\log\left((2\pi e)\frac{P\sigma_Z^2 + \mu(\alpha, R_e)}{P + \sigma_T^2 + \sigma_Z^2}\right) \tag{4.179}$$

where

$$\mu(\alpha, R_e) = \alpha^2\sigma_Z^2\sigma_T^2 + (1-\alpha)^2 P\sigma_T^2 + \frac{\alpha^2\sigma_T^2(P + \sigma_T^2 + \sigma_Z^2)}{e^{2R_e} - 1} \tag{4.180}$$

Combining (4.176) and (4.179) and substituting in (4.172) we obtain an achievable rate as a function of α, for any R_e as,

$$\mathcal{LB}(R_e, \alpha) = \frac{1}{2}\log\left(\frac{P(P + \sigma_T^2 + \sigma_Z^2)}{P\sigma_Z^2 + \mu(\alpha, R_e)}\right) \tag{4.181}$$

Next, we optimize the above achievable rate with respect to α. This is equivalent

to minimizing $\mu(\alpha, R_e)$. We first note that $\mu(\alpha, R_e)$ is convex in α and therefore, the minimum of $\mu(\alpha, R_e)$ is obtainded at $\alpha^*(R_e)$ where $d\mu(\alpha^*, R_e)/d\alpha = 0$. We therefore have the following

$$\alpha^*(R_e) = \frac{P}{P + \sigma_Z^2 + \frac{P+\sigma_T^2+\sigma_Z^2}{e^{2R_e}-1}} \tag{4.182}$$

We substitute (4.182) in (4.181) to obtain a closed form expression for the achievable rate as follows

$$\mathcal{LB}(R_e) = \frac{1}{2}\log\left(\frac{P + \sigma_T^2 e^{-2R_e} + \sigma_Z^2}{\sigma_Z^2 + \sigma_T^2 e^{-2R_e}}\right) \tag{4.183}$$

We now consider the two extreme cases for the values of R_e. If $R_e = 0$, then from (4.182), the optimal selection of α is

$$\alpha^*(0) = 0 \tag{4.184}$$

and the achievable rate is

$$\mathcal{LB}(0) = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_T^2 + \sigma_Z^2}\right) \tag{4.185}$$

which yields the capacity $\mathcal{C}(0)$. If $R_e = \infty$, then the optimal selection of α is

$$\alpha^*(\infty) = \frac{P}{P + \sigma_Z^2} \tag{4.186}$$

and the achievable rate is

$$\mathcal{LB}(\infty) = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2}\right) \tag{4.187}$$

which yields the DPC capacity $\mathcal{C}_{DPC}$. We should remark here that this $\alpha^*(\infty)$ is the same selection used by Costa in [9] to obtain the DPC capacity.

Figure 4.7 shows our upper bound in (4.165), the achievable rate in (4.183), the DPC upper bound (4.161) and the capacity when $R_e = 0$ in (4.163) for the case when $P = 10$, $\sigma_Z^2 = \sigma_T^2 = 1$.

4.5 Conclusions

We obtained a new upper bound on the capacity of state-dependent channels with rate-limited CSI at the transmitter and rate-limited CSI at the receiver. For the case of rate-limited CSIR and no CSIT, our upper bound recovers all previous known capacity results. Using our upper bound, we obtained the capacity of a new sub-class of such channels and we also showed that it is strictly smaller than the cut-set upper bound. This result validates a conjecture by Ahlswede and Han [2] for these channels. For the case of rate-limited CSIT and no CSIR, we showed that our upper bound matches the upper bound obtained in [4] for modulo additive state channels. For a particular class of state-dependent channels, we explicitly characterized both rate-limited CSIR and rate-limited CSIT capacities, $\mathcal{C}(R_d)$ and $\mathcal{C}(R_e)$, in Sections 4.3.3 and 4.4.4, respectively. We showed that for this class of state-dependent channels, it does not matter whether the rate-limited CSI is supplied at the transmitter or the

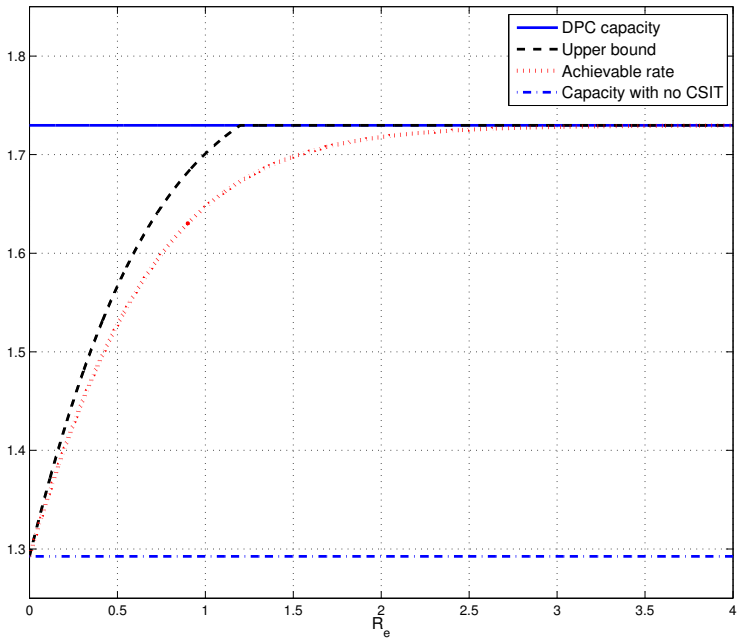

Figure 4.7: Illustration of bounds when $P = 10$, $\sigma_T^2 = \sigma_Z^2 = 1$.

receiver and the respective capacity expressions are the same.

Furthermore, we evaluated our upper bound for the rate-limited DPC problem. We showed that for all finite values of $(P, \sigma_Z^2, \sigma_T^2)$, our upper bound is strictly smaller than the DPC upper bound for a certain range of R_e. We also provided a potentially sub-optimal evaluation of the achievable rates [29] for the rate-limited DPC problem.

4.6 Appendix

4.6.1 Proof of Theorem 4.1

Let us denote the random variable J as the output of the finite capacity link with capacity R_d, i.e., $J = f_s(T^n)$. We will now obtain an upper bound on the rate as

follows,

$$
\begin{aligned}
nR &= H(W) && (4.188)\\
&= I(W; Y^n, J) + H(W|Y^n, J) && (4.189)\\
&\leq I(W; Y^n, J) + n\epsilon_n && (4.190)\\
&\leq I(X^n; Y^n, J) + n\epsilon_n && (4.191)\\
&= I(X^n; Y^n|J) + n\epsilon_n && (4.192)\\
&= \sum_{i=1}^{n} I(X^n; Y_i|J, Y^{i-1}) + n\epsilon_n && (4.193)\\
&= \sum_{i=1}^{n} \Big[H(Y_i|J, Y^{i-1}) - H(Y_i|J, Y^{i-1}, X^n)\Big] + n\epsilon_n && (4.194)\\
&\leq \sum_{i=1}^{n} \Big[H(Y_i) - H(Y_i|J, Y^{i-1}, X^n)\Big] + n\epsilon_n && (4.195)\\
&\leq \sum_{i=1}^{n} \Big[H(Y_i) - H(Y_i|J, T^{i-1}, Y^{i-1}, X^n)\Big] + n\epsilon_n && (4.196)\\
&= \sum_{i=1}^{n} \Big[H(Y_i) - H(Y_i|J, T^{i-1}, X^n)\Big] + n\epsilon_n && (4.197)\\
&= \sum_{i=1}^{n} \Big[H(Y_i) - H(Y_i|J, T^{i-1}, X_i)\Big] + n\epsilon_n && (4.198)\\
&= \sum_{i=1}^{n} I(X_i, J, T^{i-1}; Y_i) + n\epsilon_n && (4.199)\\
&= \sum_{i=1}^{n} I(X_i, V_i; Y_i) + n\epsilon_n && (4.200)\\
&= nI(X, V; Y) + n\epsilon_n && (4.201)
\end{aligned}
$$

where (4.190) follows by Fano's inequality [14], (4.191) follows from the data processing inequality, (4.192) follows from the fact that X^n is independent of T^n and

is hence independent of J, (4.195) follows from the fact that conditioning reduces entropy and hence we upper bound by dropping (J, Y^{i-1}) from the first term. Next, (4.196) follows by adding T^{i-1} in the conditional entropy in the second term and obtaining an upper bound, (4.197) follows from the memoryless property of the channel, i.e., given (X^{i-1}, T^{i-1}), the channel output Y^{i-1} is independent of everything else and (4.198) follows from the following Markov chain, $X^{-i} \rightarrow (X_i, J, T^{i-1}) \rightarrow Y_i$, where $X^{-i} = (X^{i-1}, X_{i+1}^n)$. Finally, (4.200) follows by defining $V_i = (J, T^{i-1})$, and we introduce a random variable Q, uniform on $\{1, 2, \ldots, n\}$ to define $X = (X_i, Q)$, $Y = (Y_i, Q)$ and $V = (V_i, Q)$ to arrive at (4.201). The proof of the Markov chain used to arrive at (4.198) is given as follows.

$$\Pr(Y_i, X^{-i} | X_i, J, T^{i-1}) = \frac{\Pr(Y_i, X^{-i}, X_i, J, T^{i-1})}{\Pr(X_i, J, T^{i-1})} \tag{4.202}$$

$$= \frac{\sum_{t_i} \mathrm{P}(t_i) \Pr(Y_i, X^{-i}, X_i, J, T^{i-1} | t_i)}{\Pr(X_i, J, T^{i-1})} \tag{4.203}$$

$$= \frac{\sum_{t_i} \mathrm{P}(t_i) \Pr(X_i, J, T^{i-1} | t_i) \Pr(Y_i, X^{-i} | X_i, t_i, J, T^{i-1})}{\Pr(X_i, J, T^{i-1})} \tag{4.204}$$

$$= \frac{\sum_{t_i} \mathrm{P}(t_i)\mathrm{Pr}(X_i, J, T^{i-1}|t_i)\mathrm{Pr}(X^{-i}|X_i, t_i, J, T^{i-1})\mathrm{Pr}(Y_i|X_i, t_i, J, T^{i-1}, X^{-i})}{\mathrm{Pr}(X_i, J, T^{i-1})} \tag{4.205}$$

$$= \frac{\sum_{t_i} \mathrm{P}(t_i)\mathrm{Pr}(X_i, J, T^{i-1}|t_i)\mathrm{Pr}(X^{-i}|X_i)\mathrm{Pr}(Y_i|X_i, t_i, J, T^{i-1})}{\mathrm{Pr}(X_i, J, T^{i-1})} \tag{4.206}$$

$$= \mathrm{Pr}(X^{-i}|X_i)\frac{\sum_{t_i} \mathrm{P}(t_i)\mathrm{Pr}(X_i, J, T^{i-1}|t_i)\mathrm{Pr}(Y_i|X_i, t_i, J, T^{i-1})}{\mathrm{Pr}(X_i, J, T^{i-1})} \tag{4.207}$$

$$= \mathrm{Pr}(X^{-i}|X_i)\sum_{t_i} \mathrm{P}(t_i|X_i, J, T^{i-1})\mathrm{Pr}(Y_i|X_i, J, T^{i-1}, t_i) \tag{4.208}$$

$$= \mathrm{Pr}(X^{-i}|X_i)\mathrm{Pr}(Y_i|X_i, J, T^{i-1}) \tag{4.209}$$

In addition to (4.201), we also need the following trivial upper bound on the rate,

$$nR \leq I(X^n; Y^n, T^n) + n\epsilon_n \tag{4.210}$$

$$= I(X^n; Y^n|T^n) + n\epsilon_n \tag{4.211}$$

$$= \sum_{i=1}^{n} I(X^n; Y_i|T^n, Y^{i-1}) + n\epsilon_n \tag{4.212}$$

$$= \sum_{i=1}^{n} \Big[H(Y_i|T^n, Y^{i-1}) - H(Y_i|T^n, Y^{i-1}, X^n)\Big] + n\epsilon_n \tag{4.213}$$

$$= \sum_{i=1}^{n} \Big[H(Y_i|T_i) - H(Y_i|T^n, Y^{i-1}, X^n)\Big] + n\epsilon_n \tag{4.214}$$

$$= \sum_{i=1}^{n} \Big[H(Y_i|T_i) - H(Y_i|T_i, X_i)\Big] + n\epsilon_n \tag{4.215}$$

$$= \sum_{i=1}^{n} I(X_i; Y_i|T_i) + n\epsilon_n \tag{4.216}$$

$$= nI(X; Y|T) + n\epsilon_n \tag{4.217}$$

where (4.210) follows by Fano's inequality, (4.211) follows because X^n is independent

of T^n, (4.214) follows by dropping (Y^{i-1}, T^{-i}) from the conditioning in the first term, (4.215) follows from the memoryless property of the channel, i.e., given (X_i, T_i), the channel output Y_i is independent of everything else.

We now obtain a bound on the allowable distributions of the involved random variables. Using the fact that the CSIR is available at a rate not exceeding R_d, we have that

$$nR_d \geq I(T^n; J) \tag{4.218}$$

$$= \sum_{i=1}^{n} I(T_i; J|T^{i-1}) \tag{4.219}$$

$$= \sum_{i=1}^{n} I(T_i; J, T^{i-1}) \tag{4.220}$$

$$= nI(T; V) \tag{4.221}$$

where (4.220) follows from the fact that T_i are i.i.d.

Combining (4.201), (4.217) and (4.221), we have an upper bound on the capacity, $\mathcal{C}(R_d)$, as

$$\begin{aligned} \mathcal{UB}(R_d) = \sup \min\{&I(X, V; Y), I(X; Y|T)\} \\ \text{s.t. } &I(T; V) \leq R_d \\ \text{over } &p(x)p(t)p(v|t) \end{aligned} \tag{4.222}$$

where it follows from support lemma [16] that the supremum can be restricted over those joint distributions for which $|\mathcal{V}| \leq |\mathcal{T}| + 2$.

4.6.2 Proof of Theorem 4.2

We denote J as the output of the state encoder, i.e., $J = f_s(T^n)$. We start by obtaining an upper bound on R as,

$$\begin{aligned} nR &= H(W) && (4.223)\\ &= I(W;Y^n) + H(W|Y^n) && (4.224)\\ &\leq I(W;Y^n) + n\epsilon_n && (4.225)\\ &= \sum_{i=1}^{n} I(W;Y_i|Y^{i-1}) + n\epsilon_n && (4.226)\\ &= \sum_{i=1}^{n} I(W,Y^{i-1};Y_i) - \sum_{i=1}^{n} I(Y_i;Y^{i-1}) + n\epsilon_n && (4.227) \end{aligned}$$

where (4.225) follows from Fano's inequality [14]. Moreover, we also have the following condition from the fact that the state information is available to the encoder at a rate R_e,

$$\begin{aligned} nR_e &\geq H(J) && (4.228)\\ &\geq I(J;T^n) && (4.229)\\ &= \sum_{i=1}^{n} I(J;T_i|T^{i-1}) && (4.230)\\ &= \sum_{i=1}^{n} I(J,T^{i-1};T_i) && (4.231) \end{aligned}$$

where (4.231) follows from the fact that T_is are i.i.d. Finally, we note the following Markov chain,

$$T_i \rightarrow (J, T^{i-1}) \rightarrow (W, Y^{i-1}, X_i) \tag{4.232}$$

This Markov chain is proved as follows,

$$I(T_i; W, Y^{i-1}, X_i | J, T^{i-1}) = I(T_i; W | J, T^{i-1}) + I(T_i; Y^{i-1}, X_i | W, J, T^{i-1}) \tag{4.233}$$

$$= I(T_i; Y^{i-1}, X_i | W, J, T^{i-1}) \tag{4.234}$$

$$= I(T_i; Y^{i-1} | W, J, T^{i-1}) \tag{4.235}$$

$$= I(T_i; Y^{i-1} | W, J, X^{i-1}, T^{i-1}) \tag{4.236}$$

$$= 0 \tag{4.237}$$

where (4.234) follows from the fact that the message W is independent of (J, T^n), (4.235) and (4.236) follow since X^n is a function of (W, J), and (4.237) follows from the memoryless property of the channel, i.e., the following is a Markov chain $Y^{i-1} \rightarrow (X^{i-1}, T^{i-1}) \rightarrow (T_i, W, J)$.

We now define

$$U_i = (W, Y^{i-1}) \tag{4.238}$$

$$V_i = (J, T^{i-1}) \tag{4.239}$$

Returning to (4.227), we have

$$nR \leq \sum_{i=1}^{n} I(W, Y^{i-1}; Y_i) - \sum_{i=1}^{n} I(Y_i; Y^{i-1}) + n\epsilon_n \tag{4.240}$$

$$\leq \sum_{i=1}^{n} I(W, Y^{i-1}; Y_i) + n\epsilon_n \tag{4.241}$$

$$= nI(U_Q; Y_Q|Q) + n\epsilon_n \tag{4.242}$$

$$\leq nI(U_Q, Q; Y_Q) + n\epsilon_n \tag{4.243}$$

$$= nI(U; Y) + n\epsilon_n \tag{4.244}$$

and returning to (4.231), we have

$$nR_e \geq \sum_{i=1}^{n} I(J, T^{i-1}; T_i) \tag{4.245}$$

$$= nI(V_Q; T_Q|Q) \tag{4.246}$$

$$= nI(V_Q, Q; T_Q) \tag{4.247}$$

$$= nI(V; T) \tag{4.248}$$

where (4.248) follows from the fact that T_is are i.i.d. and therefore T_Q is independent of Q, where Q is uniformly distributed over $\{1, \ldots, n\}$ and is independent of all other random variables, and we have defined $U = (Q, U_Q)$, $V = (Q, V_Q)$, $Y = Y_Q$, $X = X_Q$ and $T = T_Q$. Finally, we prove the following Markov chain

$$T \to V \to (U, X) \tag{4.249}$$

We prove this Markov chain as follows,

$$I(T;U,X|V) = I(T_Q;U_Q,Q,X_Q|V_Q,Q) \tag{4.250}$$

$$= I(T_Q;U_Q,X_Q|V_Q,Q) \tag{4.251}$$

$$= \sum_{q=1}^{n} \Pr(Q=q) I(T_q;U_q,X_q|V_q,Q=q) \tag{4.252}$$

$$= 0 \tag{4.253}$$

where (4.253) follows by using the Markov chain in (4.232) for every $q = 1, \ldots, n$.

We now combine (4.244), (4.248) and (4.249) to express our upper bound on the capacity of the state-dependent channel with rate-limited state information at the transmitter as,

$$\mathcal{UB}(R_e) = \max_{p(v|t),p(u,x|v):I(T;V)\leq R_e} I(U;Y) \tag{4.254}$$

4.6.3 Proof of Theorem 4.3

We start by obtaining an upper bound on R as,

$$nR = H(W) \tag{4.255}$$

$$= I(W;Y^n,J) + H(W|Y^n,J) \tag{4.256}$$

$$\leq I(W;Y^n,J) + n\epsilon_n \tag{4.257}$$

$$= I(W;Y^n|J) + n\epsilon_n \tag{4.258}$$

$$= h(Y^n|J) - h(Y^n|W,J) + n\epsilon_n \tag{4.259}$$

where (4.257) follows from Fano's inequality [14] and (4.258) follows from the fact that the message W and the random variable J are independent. The main idea behind this strengthened upper bound is to consider a larger quantity $I(W;Y^n,J)$ in (4.257) as opposed to $I(W;Y^n)$ in (4.225). This approach will permit us to invoke the Markov chain $X^n \rightarrow J \rightarrow T^n$ which will subsequently yield an improved upper bound.

Returning to (4.259), we will separately obtain an upper bound on $h(Y^n|J)$ and a lower bound on $h(Y^n|W,J)$. We start by considering the first term in (4.259),

$$h(Y^n|J) = \sum_{i=1}^{n} h(Y_i|J,Y^{i-1}) \tag{4.260}$$

$$\leq \sum_{i=1}^{n} h(Y_i|J) \tag{4.261}$$

$$\leq \frac{n}{2}\log\left((2\pi e)(P+\sigma_T^2+\sigma_Z^2)\right) \tag{4.262}$$

where (4.261) follows from the fact that conditioning reduces entropy and by dropping Y^{i-1} from the conditioning, and (4.262) follows from the following sequence of inequalities,

$$\sum_{i=1}^{n} h(Y_i|J) \leq \sum_{i=1}^{n} \frac{1}{2}\log(2\pi e \mathrm{Var}(Y_i|J)) \tag{4.263}$$

$$= \sum_{i=1}^{n} \frac{1}{2}\log(2\pi e(\mathrm{Var}(X_i|J)+\mathrm{Var}(T_i|J)+\mathrm{Var}(Z_i|J))) \tag{4.264}$$

$$\leq \sum_{i=1}^{n} \frac{1}{2}\log(2\pi e(\mathrm{Var}(X_i)+\mathrm{Var}(T_i)+\mathrm{Var}(Z_i))) \tag{4.265}$$

$$= \sum_{i=1}^{n} \frac{1}{2} \log(2\pi e(\mathrm{Var}(X_i) + \sigma_T^2 + \sigma_Z^2)) \tag{4.266}$$

$$\leq \frac{n}{2} \log\left((2\pi e)(P + \sigma_T^2 + \sigma_Z^2)\right) \tag{4.267}$$

where (4.263) follows from the maximum entropy theorem [14], (4.264) follows from the fact that Z^n is independent of (X^n, T^n, J) and the Markov chain $X_i \to J \to T_i$, which also implies that $\mathrm{Cov}(X_i, T_i|J) = 0$ for all $i = 1, \ldots, n$, (4.265) follows from the fact that expected conditional variance is upper bounded by unconditional variance, (4.266) follows from the fact that $\mathrm{Var}(T_i) = \sigma_T^2$ and $\mathrm{Var}(Z_i) = \sigma_Z^2$ for all $i = 1, \ldots, n$ and (4.267) follows from the concavity of log function and the average input power constraint P.

We now consider the second term in (4.259) and obtain a lower bound as,

$$h(Y^n|W, J) \geq h(Y^n|X^n, W, J) \tag{4.268}$$

$$= h(T^n + Z^n|X^n, W, J) \tag{4.269}$$

$$= h(T^n + Z^n|J) \tag{4.270}$$

$$\geq \frac{n}{2} \log\left(e^{\frac{2}{n}h(T^n|J)} + 2\pi e\sigma_Z^2\right) \tag{4.271}$$

$$\geq \frac{n}{2} \log\left((2\pi e)(\sigma_T^2 e^{-2R_e} + \sigma_Z^2)\right) \tag{4.272}$$

where (4.268) follows from the fact that conditioning reduces entropy, (4.270) follows from the Markov chain $T^n \to J \to (X^n, W)$ and (4.271) follows from the vector

entropy power inequality (EPI) [14]. Finally, (4.272) follows from the following,

$$nR_e \geq H(J) \tag{4.273}$$

$$\geq I(J;T^n) \tag{4.274}$$

$$= h(T^n) - h(T^n|J) \tag{4.275}$$

which yields

$$h(T^n|J) \geq \frac{n}{2}\left(\log(2\pi e\sigma_T^2) - 2R_e\right) \tag{4.276}$$

and we substitute (4.276) in (4.271) to arrive at (4.272).

We now substitute (4.262) and (4.272) in (4.259) to finally arrive at our upper bound,

$$\mathcal{UB}(R_e) = \frac{1}{2}\log\left(\frac{P+\sigma_T^2+\sigma_Z^2}{\sigma_Z^2+\sigma_T^2 e^{-2R_e}}\right) \tag{4.277}$$

When $R_e = 0$, our upper bound is clearly optimal,

$$\mathcal{UB}(0) = \frac{1}{2}\log\left(\frac{P+\sigma_T^2+\sigma_Z^2}{\sigma_Z^2+\sigma_T^2}\right) \tag{4.278}$$

$$= \mathcal{C}(0) \tag{4.279}$$

On the other hand, our upper bound is strictly smaller than the DPC upper bound,

$\mathcal{C}(\infty)$, for $0 < R_e < R_e^c$, where

$$R_e^c = \frac{1}{2}\log\left(1 + \frac{P}{\sigma_Z^2}\right) \tag{4.280}$$

For $R_e \geq R_e^c$, the DPC upper bound is strictly smaller than our upper bound. Therefore, we take the smaller of these two bounds and obtain a compact expression for the upper bound as,

$$\mathcal{UB}(R_e) = \begin{cases} \frac{1}{2}\log\left(\frac{P+\sigma_T^2+\sigma_Z^2}{\sigma_Z^2+\sigma_T^2 e^{-2R_e}}\right), & 0 \leq R_e < R_e^c \\ \frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right), & R_e^c \leq R_e < \infty \end{cases} \tag{4.281}$$

Chapter 5

Diamond Channel with Partially Separated Relays

5.1 Introduction

The parallel relay network or the diamond channel consists of a transmitter connected to two relays through a broadcast channel $p(y, z|x)$, where Z is the output of relay 1 and Y is the output of relay 2. The relays are connected to the receiver through a multiple access channel. The diamond channel differs from the classical relay channel [12] in the sense that there is no direct link between the transmitter and the receiver. The diamond channel was introduced by Schein and Gallager in [52], where several cases of the diamond channel were studied.

In [32], a special class of diamond channel was considered where relay 2 receives the input X and relay 1 receives Z through a noisy channel $p(z|x)$. Moreover, the relays are connected to the receiver through an orthogonal multiple access channel. In other words, relays 1 and 2 have finite capacity, orthogonal links of capacities R_z and R_y, respectively, to the receiver. The capacity of this class of diamond channels was characterized in [32] and was shown to be strictly less than the cut-set upper bound [14].

In this chapter, we consider the diamond channel with a general broadcast channel and an orthogonal multiple access channel as in [32] (see Figure 5.1). For this class of diamond channels, we establish the capacity when the broadcast channel is deterministic, i.e., when Y and Z are deterministic functions of X. We show that the capacity is given by the cut-set bound and is achieved by Gelfand-Pinsker-Marton coding to the relays. We next consider the case when the broadcast channel is physically degraded, i.e., when $X \to Y \to Z$ forms a Markov chain. We provide an upper bound on the capacity of this class of diamond channels and show that this bound yields the capacity when in addition to $X \to Y \to Z$, the channel model is such that, $Y = f(X)$ for any deterministic function f. Note that when $Y = X$, we recover the result obtained in [32].

We finally consider this class of diamond channel with partially separated relays, i.e., when the output of relay 2 is available to relay 1. This channel model is equivalent to the model when there is feedback from the receiver to relay 2. One of the main contributions of this chapter is to establish the capacity of this model, when a) the broadcast channel is physically degraded, i.e, when $X \to Y \to Z$ forms a Markov chain, and b) the broadcast channel is semi deterministic, i.e., when $Y = f(X)$. For both these cases, we show that the capacity is given by the cut-set bound. These two results also show the fact that even feedback to one of the relays strictly increases the capacity of the diamond channel.

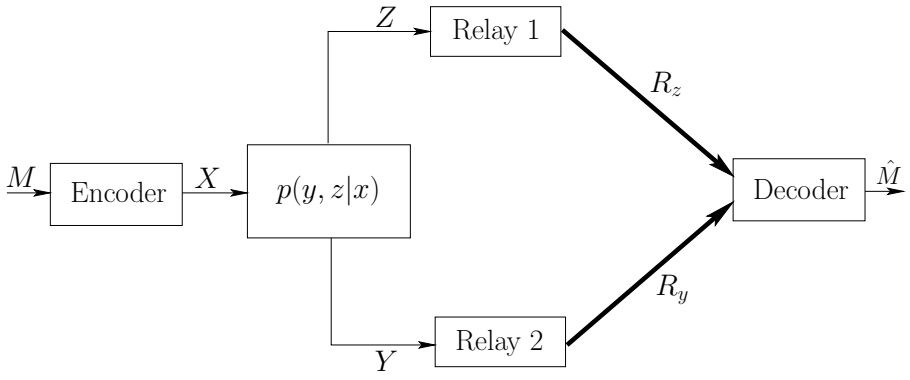

Figure 5.1: The diamond channel.

5.2 Diamond Channel

A diamond channel with a general broadcast channel and an orthogonal multiple access channel is described by an input alphabet $\mathcal{X}$, two output alphabets $\mathcal{Y}, \mathcal{Z}$, and transition probabilities $p(y, z|x)$.

A (n, f, f_1, f_2, g) code for this diamond channel is described by,

$$f : \{1, \ldots, \mathcal{M}\} \to \mathcal{X}^n \tag{5.1}$$

$$f_1 : \mathcal{Z}^n \to \{1, \ldots, |f_1|\} \tag{5.2}$$

$$f_2 : \mathcal{Y}^n \to \{1, \ldots, |f_2|\} \tag{5.3}$$

$$g : \{1, \ldots, |f_1|\} \times \{1, \ldots, |f_2|\} \to \{1, \ldots, \mathcal{M}\} \tag{5.4}$$

where f is the encoding function at the transmitter, f_1 is the encoding function at relay 1, f_2 is the encoding function at relay 2, and g is the decoding function at the receiver.

The transmitter sends $X^n = f(M)$ as the input to the broadcast channel, where $M \in \{1, \ldots, \mathcal{M}\}$ and the message M is decoded as $\hat{M} = g(f_1(Z^n), f_2(Y^n))$. The

probability of error is defined as $P_e = \Pr(M \neq \hat{M})$. A rate triple (R, R_y, R_z) is achievable if for every $0 < \epsilon < 1$, $\eta > 0$, and sufficiently large n, there exists a (n, f, f_1, f_2, g) code such that $P_e \leq \epsilon$, and,

$$\frac{1}{n}\log\mathcal{M} \geq R - \eta \tag{5.5}$$

$$\frac{1}{n}\log|f_1| \leq R_z + \eta \tag{5.6}$$

$$\frac{1}{n}\log|f_2| \leq R_y + \eta \tag{5.7}$$

The capacity $\mathcal{C}(R_y, R_z)$ is defined as the largest R such that (R, R_y, R_z) is achievable.

5.2.1 Deterministic Broadcast

In this section, we consider diamond channels with deterministic broadcast channel, i.e., when the channel outputs Y and Z are deterministic functions of X. We characterize the capacity of this class of diamond channels in the following theorem.

Theorem 5.1 *The capacity of the diamond channel, $\mathcal{C}(R_y, R_z)$, with deterministic broadcast channel is given as,*

$$\mathcal{C}(R_y, R_z) = \max_{p(x)} \min(H(Y,Z), R_y + R_z, R_y + H(Z), R_z + H(Y)) \tag{5.8}$$

The converse follows from the cut-set upper bound [14]. To prove the achievability, we will make use of the capacity region of the deterministic broadcast channel without common messages [22, 44]. The capacity region of a deterministic broadcast channel

without common messages is given as the set of rate pairs (R_1, R_2) satisfying,

$$R_1 \leq H(Z) \tag{5.9}$$

$$R_2 \leq H(Y) \tag{5.10}$$

$$R_1 + R_2 \leq H(Y, Z) \tag{5.11}$$

Now, for any input distribution $p(x)$, consider the expression,

$$G(p(x)) = \min(H(Y, Z), R_y + R_z, R_y + H(Z), R_z + H(Y)) \tag{5.12}$$

Depending on the value of (R_y, R_z), we have four cases (see Figure 5.2):

Case A: If (R_y, R_z) are such that,

$$R_y \leq H(Y) \tag{5.13}$$

$$R_z \leq H(Z) \tag{5.14}$$

$$R_y + R_z \leq H(Y, Z) \tag{5.15}$$

then, we have $G(p(x)) = R_y + R_z$ and we can achieve a rate of $R_y + R_z$ for the diamond channel by using a broadcast channel code with the rates,

$$R_1 = R_z, \quad R_2 = R_y \tag{5.16}$$

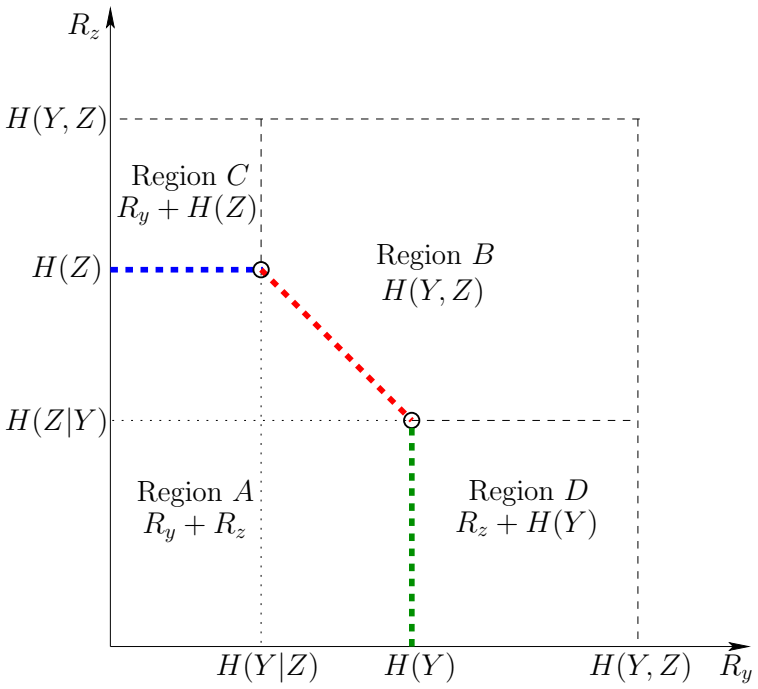

Figure 5.2: Achievability for the diamond channel with deterministic broadcast.

Case B: If (R_y, R_z) are such that,

$$R_y \geq H(Y|Z) \tag{5.17}$$

$$R_z \geq H(Z|Y) \tag{5.18}$$

$$R_y + R_z \geq H(Y,Z) \tag{5.19}$$

then, we have $G(p(x)) = H(Y,Z)$ and we can achieve a rate of $H(Y,Z)$ for the diamond channel by using a broadcast channel code with the rates,

$$R_1 = H(Z), \quad R_2 = H(Y|Z) \tag{5.20}$$

or alternatively,

$$R_1 = H(Z|Y), \quad R_2 = H(Y) \tag{5.21}$$

Case C: If (R_y, R_z) are such that,

$$R_y \leq H(Y|Z) \tag{5.22}$$

$$R_y + R_z \leq H(Y, Z) \tag{5.23}$$

then, we have $G(p(x)) = R_y + H(Z)$ and we can achieve a rate of $R_y + H(Z)$ for the diamond channel by using a broadcast channel code with the rates,

$$R_1 = H(Z), \quad R_2 = R_y \tag{5.24}$$

Case D: If (R_y, R_z) are such that, $G(p(x)) = R_z + H(Y)$, then, similar to Case C, we can achieve a rate of $R_z + H(Y)$ for the diamond channel by using a broadcast channel code with the rates,

$$R_1 = R_z, \quad R_2 = H(Y) \tag{5.25}$$

We remark here that the achievability is counterintuitive since one might have expected to use the general broadcast channel code with common messages [22], [27], but as our result shows this is not necessary. We also note here that the cut-set bound continues to hold when relays are partially separated, i.e., the encoded output

of relay 2 is available to both relay 1 and the decoder. Our result also shows that the capacity of this diamond channel remains the same even if the relays are partially separated.

5.2.2 Physically Degraded Broadcast

In this section, we consider diamond channels with physically degraded broadcast channel, i.e., when the channel $p(y, z|x)$ is such that

$$p(y, z|x) = p(y|x)p(z|y) \tag{5.26}$$

In the following theorem, we provide a new upper bound on the capacity $\mathcal{C}(R_y, R_z)$.

Theorem 5.2 *The capacity of the diamond channel, $\mathcal{C}(R_y, R_z)$, with physically degraded broadcast channel is upper bounded by the maximum R such that,*

$$R \leq I(U; Z) + I(X; Y|U) \tag{5.27}$$

$$R_y \geq H(Y|U, V) - H(Y|X) \tag{5.28}$$

$$R_z \geq I(Z; V|U, Y) \tag{5.29}$$

$$R_y + R_z \geq R + I(Z; V|U, Y) \tag{5.30}$$

for joint distributions of the form,

$$p(x, u, y, z, v) = p(u, x)p(y|x)p(z|y)p(v|z, u) \tag{5.31}$$

where $|\mathcal{U}| \leq |\mathcal{X}| + 4$, $|\mathcal{V}| \leq |\mathcal{X}||\mathcal{Z}| + 4|\mathcal{X}| + 3$.

Alternatively, the capacity of the diamond channel is upper bounded as,

$$\mathcal{C}(R_y, R_z) \leq \max \min(I(U;Z) + I(X;Y|U), R_y + R_z - I(Z;V|U,Y)) \tag{5.32}$$
$$\text{such that } R_y \geq H(Y|U,V) - H(Y|X), R_z \geq I(Z;V|U,Y)$$

The proof of Theorem 5.2 is given in the Appendix. We next have the following theorem.

Theorem 5.3 *The capacity of the diamond channel,* $\mathcal{C}(R_y, R_z)$*, with degraded broadcast channel, when* $Y = f(X)$*, is given by the maximum* R *such that,*

$$R \leq I(U;Z) + I(X;Y|U) \tag{5.33}$$

$$R_y \geq H(Y|U,V) \tag{5.34}$$

$$R_z \geq I(Z;V|U,Y) \tag{5.35}$$

$$R_y + R_z \geq R + I(Z;V|U,Y) \tag{5.36}$$

for joint distributions of the form,

$$p(x,u,y,z,v) = p(u,x)p(y|x)p(z|y)p(v|z,u) \tag{5.37}$$

As a corollary, by setting $Y = X$ in Theorem 5.3, we recover the capacity result obtained in [32].

The converse for Theorem 5.3 follows from Theorem 5.2. We will directly show the achievability of $I(U;Z) + I(X;Y|U)$, when,

$$R_y \geq H(Y|U,V) \tag{5.38}$$

$$R_z \geq I(Z;V|U,Y) \tag{5.39}$$

$$R_y + R_z \geq I(U;Z) + I(X;Y|U) + I(Z;V|U,Y) \tag{5.40}$$

Figure 5.3 shows that this region corresponds to an inverse pentagon, with corner points (a) and (b), given as,

$$R_z^{(a)} = I(Z;V|U,Y) \tag{5.41}$$

$$R_y^{(a)} = I(U;Z) + I(X;Y|U) \tag{5.42}$$

and

$$R_z^{(b)} = I(U;Z) + I(Z;V|U) \tag{5.43}$$

$$R_y^{(b)} = I(X;Y|U) - I(Y;V|U) \tag{5.44}$$

$$= I(X;Y|U) - I(X;V|U) \tag{5.45}$$

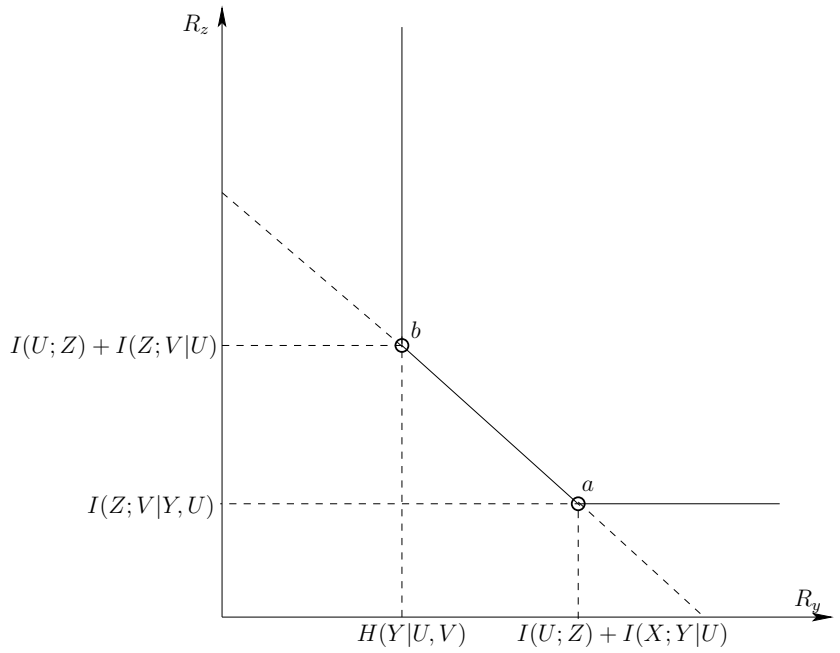

Figure 5.3: Achievability for the diamond channel with degraded broadcast.

where in (5.45), we have used the following,

$$I(X;V|U) = I(X,Y;V|U) - I(Y;V|X,U) \tag{5.46}$$

$$= I(X,Y;V|U) \tag{5.47}$$

$$= I(Y;V|U) + I(X;V|Y,U) \tag{5.48}$$

$$= I(Y;V|U) \tag{5.49}$$

where (5.46) follows from the fact that $Y = f(X)$ and (5.49) follows from the Markov chain, $X \to Y \to (V,U)$.

Reliable transmission is possible at a rate $I(U;Z)+I(X;Y|U)$ at the corner point (a) only by using relay 2 and using a single-user channel code since

$$I(U;Z)+I(X;Y|U) \leq I(U;Y)+I(X;Y|U) \tag{5.50}$$

$$= I(X,U;Y) \tag{5.51}$$

$$= I(X;Y) \tag{5.52}$$

We will now show that reliable transmission is possible at a rate $I(U;Z)+I(X;Y|U)$ at the corner point (a).

Codebook generation: The encoder generates $2^{nI(U;Z)}$ $u(w_1)$ sequences using $p(u)$, where $w_1 = 1,\ldots,2^{nI(U;Z)}$ and for every u sequence, it generates $2^{nI(X;Y|U)}$ $x(w_1,w_2)$ sequences, where $w_2 = 1,\ldots,2^{nI(X;Y|U)}$. The encoder bins the x sequences in $2^{nI(X;Y|U)-I(X;V|U)}$ bins, and the bin index of $x(w_1,w_2)$ is denoted as $b_X(x(w_1,w_2))$. Relay 1 creates $2^{nI(Z;V|U)}$ $v(j)$ sequences using $p(v|z,u)$, where $j = 1,\ldots,2^{nI(Z;V|U)}$.

To transmit the message (w_1,w_2), the encoder puts $x(w_1,w_2)$ as the input to the channel.

Encoding at relay 1: Upon receiving z, relay 1 decodes w_1 by decoding the u sequence. It next searches for a v sequence which is jointly typical with $(z,\hat{u})$. Relay 1 transmits the decoded codeword $\hat{w}_1$ and the v sequence. Total rate needed by relay 1 is $I(U;Z)+I(Z;V|U)$.

Encoding at relay 2: Upon receiving y sequence, relay 2 decodes w_1 by decoding the u sequence and proceeds to decode w_2 by decoding x. Relay 2 transmits the bin-index of the correctly decoded x sequence, $b_X(x(\hat{w}_1,\hat{w}_2))$. Total rate needed by

relay 2 is $I(X;Y|U) - I(X;V|U) = H(Y|U,V)$.

Decoding: Upon receiving $\hat{w}_1$ and v sequence from relay 1 and the bin index $b_X(x(\hat{w}_1, \hat{w}_2))$ from relay 2, decoder tries to find a unique $\hat{w}_2$ in the bin $b_X(x(\hat{w}_1, \hat{w}_2))$ such that $(x(\hat{w}_1, \hat{w}_2), u(\hat{w}_1), v)$ are jointly typical. The decoder can correctly decode w_2 with high probability since the number of x sequences in each bin is approximately $2^{nI(X;V|U)}$.

5.3 Diamond Channel with Partially Separated Relays

We will now consider a variation of the diamond channel, where the relays are partially separated. In other words, the output of relay 2 is available to relay 1 (see Figure 5.4).

A (n, f, f_1, f_2, g) code for the diamond channel with partially separated relays is described by,

$$f : \{1, \ldots, \mathcal{M}\} \to \mathcal{X}^n \tag{5.53}$$

$$f_2 : \mathcal{Y}^n \to \{1, \ldots, |f_2|\} \tag{5.54}$$

$$f_1 : \mathcal{Z}^n \times \{1, \ldots, |f_2|\} \to \{1, \ldots, |f_1|\} \tag{5.55}$$

$$g : \{1, \ldots, |f_1|\} \times \{1, \ldots, |f_2|\} \to \{1, \ldots, \mathcal{M}\} \tag{5.56}$$

where f is the encoding function at the transmitter, f_1 is the encoding function at relay 1, f_2 is the encoding function at relay 2, and g is the decoding function at the receiver.

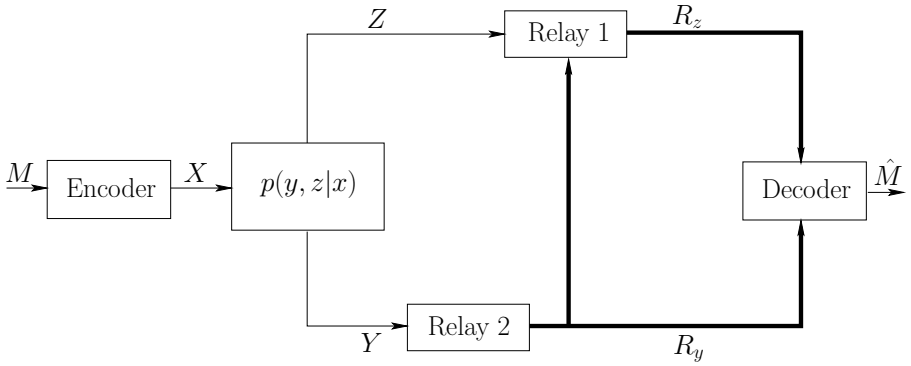

Figure 5.4: The diamond channel with partially separated relays.

The transmitter sends $X^n = f(M)$ as the input to the broadcast channel, where $M \in \{1, \ldots, \mathcal{M}\}$ and the message M is decoded as $\hat{M} = g(f_1(Z^n, f_2(Y^n)), f_2(Y^n))$. The probability of error is defined as $P_e = \Pr(M \neq \hat{M})$. A rate triple (R, R_y, R_z) is achievable if for every $0 < \epsilon < 1$, $\eta > 0$, and sufficiently large n, there exists a (n, f, f_1, f_2, g) code such that $P_e \leq \epsilon$, and,

$$\frac{1}{n}\log\mathcal{M} \geq R - \eta \tag{5.57}$$

$$\frac{1}{n}\log|f_1| \leq R_z + \eta \tag{5.58}$$

$$\frac{1}{n}\log|f_2| \leq R_y + \eta \tag{5.59}$$

The capacity $\mathcal{C}^{PS}(R_y, R_z)$ is defined as the largest R such that (R, R_y, R_z) is achievable.

5.3.1 Physically Degraded Broadcast

In this section, we consider the case when the broadcast channel of the diamond channel is physically degraded, i.e., when, $p(y, z|x) = p(y|x)p(z|y)$. In the following

theorem, we characterize the capacity of this class of channels.

Theorem 5.4 *The capacity of the diamond channel, $\mathcal{C}^{PS}(R_y, R_z)$, with physically degraded broadcast channel and partially separated relays is given as,*

$$\mathcal{C}^{PS}(R_y, R_z) = \max_{p(x)} \min(I(X;Y), R_y + R_z, R_y + I(X;Z)) \tag{5.60}$$

The converse follows from the cut-set upper bound [14]. We will prove the achievability as follows. Fix an input distribution $p(x)$ and consider the function,

$$G(p(x)) = \min(I(X;Y), R_y + R_z, R_y + I(X;Z)) \tag{5.61}$$

Figure 5.5 shows all possible cases for the pair (R_y, R_z). It suffices to show that reliable transmission is possible at the rate $\min(I(X;Y), R_y + R_z, R_y + I(X;Z))$ at the three corner points P_1, P_2 and P_3.

Reliable transmission is possible at a rate $I(X;Y)$ at the corner point P_1, when $R_y = I(X;Y)$ and $R_z = 0$ by using a single-user channel code for relay 2 at a rate $I(X;Y)$. Reliable transmission is possible at a rate $I(X;Z)$ at the corner point P_3, when $R_y = 0$ and $R_z = I(X;Z)$, by using a single-user channel code for relay 1 at a rate $I(X;Z)$.

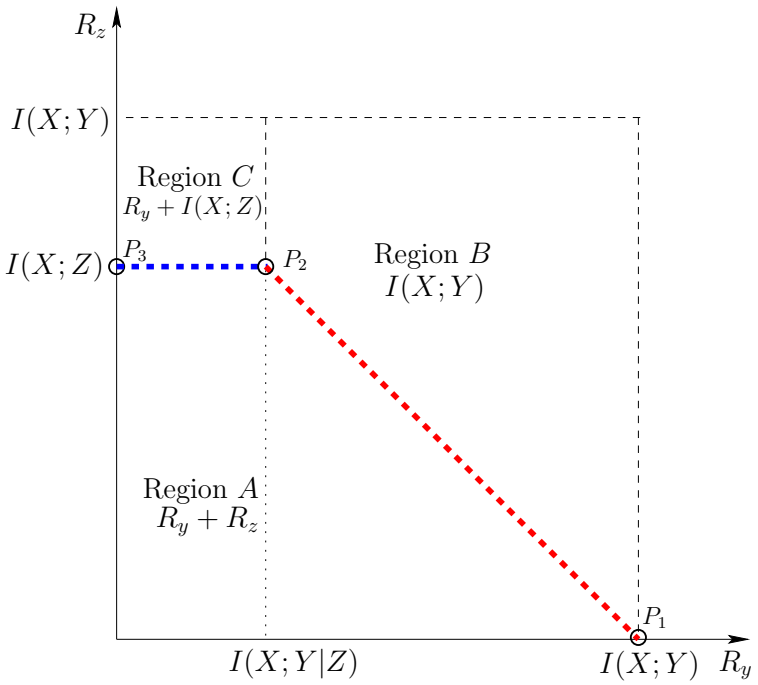

Figure 5.5: Achievability for the diamond channel with degraded broadcast.

Therefore, to complete the achievability, we need to show that reliable transmission is possible at the rate $I(X;Y)$ when,

$$R_y = I(X;Y|Z) \tag{5.62}$$

$$= I(X;Y) - I(X;Z) \tag{5.63}$$

$$R_z = I(X;Z) \tag{5.64}$$

The encoder generates $2^{nI(X;Y)}$ x sequences, $x(w)$, according to $\prod_{i=1}^{n} p(x_i(w))$, where, $w = 1, \ldots, 2^{nI(X;Y)}$ and bins these sequences in $2^{n(I(X;Y)-I(X;Z))}$ bins uniformly and independently. Denote the bin index of $x(w)$ as $b_j(x(w))$, where $j = 1, \ldots, 2^{nI(X;Y|Z)}$ and the sub-index number of $x(w)$ as $l_s(x(w))$, where $s = 1, \ldots, 2^{nI(X;Z)}$. To transmit the message w, the encoder puts $x(w)$ as the input to the channel.

Relay 2 can reliably decode the message w with high probability. Relay 2 transmits the bin index, $b_j(x(\hat{w}))$ of the decoded codeword. Relay 1 uses the channel output sequence z and the bin index $b_j(x(\hat{w}))$ to decode the message w. Relay 1 can decode the correct message w with high probability since the number of x sequences in each bin is at most $2^{nI(X;Z)}$. Relay 1 transmits the sub-index number $l_s(x(\hat{w}))$ of the decoded message.

Decoder receives the bin index $b_j(\hat{w})$ from relay 2 and the sub-index number $l_s(x(\hat{w}))$ from relay 1. The decoder decodes the sub-index $l_s(x(\hat{w}))$ in the received bin $b_j(\hat{w})$ as the correct message.

We remark here that this achievability scheme is closely related to the scheme for successive encoding of correlated sources [18]. It was shown in [18] for the case of lossless source coding with partially connected encoders, that the rate-region can be strictly improved upon the case of separated encoders [3, 67]. It is also evident that due to the fact that relays are partially separated, we can achieve the cut-set upper bound which is not always achievable when the relays are separated.

5.3.2 Semi-Deterministic Broadcast

We will now consider the case when the broadcast channel of the diamond channel is such that $Y = f(X)$ for any deterministic function f. In the following theorem, we characterize the capacity of this class of diamond channels.

Theorem 5.5 *The capacity of the diamond channel, $\mathcal{C}^{PS}(R_y, R_z)$ with semi-deterministic*

broadcast channel and partially separated relays is given as,

$$\mathcal{C}^{PS}(R_y, R_z) = \max_{p(x)} \min(I(X;Z) + H(Y|Z), R_y + R_z, R_y + I(X;Z), R_z + H(Y)) \tag{5.65}$$

The converse follows from the cut-set upper bound [14]. We will prove the achievability as follows.

Figure 5.6 shows all possible cases for the pair (R_y, R_z). It suffices to show that reliable transmission is possible at the rate

$$\min(I(X;Z) + H(Y|Z), R_y + R_z, R_y + I(X;Z), R_z + H(Y)) \tag{5.66}$$

at the four corner points P_1, P_2, P_3 and P_4.

Reliable transmission is possible at a rate $I(X;Z)$ at the corner point P_1, when $R_z = I(X;Z)$ and $R_y = 0$ by using a single-user channel code for relay 1 at a rate $I(X;Z)$. Reliable transmission is possible at a rate $H(Y)$ at the corner point P_2, when $R_z = 0$ and $R_y = I(X;Y) = H(Y)$, by using a single-user channel code for relay 2 at a rate $I(X;Y)$.

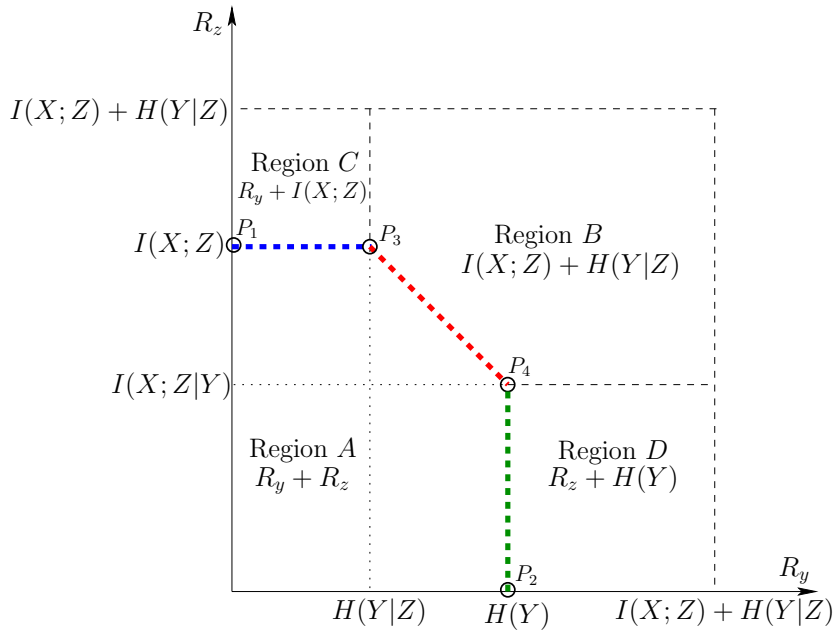

Figure 5.6: Achievability for the diamond channel with semi-deterministic broadcast.

Now, consider the corner point P_3, where we have,

$$R_y = H(Y|Z) \tag{5.67}$$

$$R_z = I(X;Z) \tag{5.68}$$

$$= I(X;Z|Y) + I(Z;Y) \tag{5.69}$$

$$= [I(X;Z,Y) - I(X;Y)] + I(Z;Y) \tag{5.70}$$

where (5.69) follows from the fact that $Y = f(X)$.

The encoder generates $2^{nI(X;Y,Z)}$ $x(w)$ sequences, where $w = 1, \ldots, 2^{nI(X;Y,Z)}$. The encoder also bins the $x(w)$ sequences in $2^{nI(X;Z|Y)}$ bins, where the bin index of the sequence $x(w)$ is denoted as $b_j(x(w))$, where $j = 1, \ldots, 2^{nI(X;Z|Y)}$. To transmit the message w, the encoder puts $x(w)$ as the input to the channel.

Upon observing the channel output y, relay 2 compresses the y sequences at a rate $H(Y|Z)$ with Z as side-information and transmits the compression bin-index, where the bin index of y sequence is denoted as $b_Y(y)$. The rate needed by relay 2 is $H(Y|Z)$.

Upon observing the z sequence from the channel and the bin index $b_Y(y)$ from relay 2, relay 1 first estimates the y sequence. It can estimate the correct y sequence with high probability since the number of y sequences in each bin is at most $2^{nI(Z;Y)}$. Let the sub-index of the estimated sequence y in the bin $b_Y(y)$ be denoted as $l_Y(b_Y(y), z)$. Relay 1 then proceeds to decode the message by decoding x by using z and the estimated y sequence. Relay 1 transmits the bin index of the decoded x sequence, $b_j(x(\hat{w}))$ and the sub-index of the decoded y sequence, $l_Y(b_Y(y), z)$. The total rate needed by relay 1 is $I(X;Z|Y) + I(Z;Y) = I(X;Z)$.

Upon observing $b_Y(y)$ from relay 2 and the pair $(l_Y(b_Y(y), z), b_j(x(\hat{w})))$ from relay 1, the decoder first finds the correct y sequence as the $l_Y(b_Y(y), z)$th sub-index in the bin $b_Y(y)$. It next decodes the message by searching for a unique $x(w)$ in the bin $b_j(x(\hat{w}))$ such that $(x(w), y)$ are jointly typical. This is possible since the number of x sequences in each x-bin is approximately $2^{nI(X;Y,Z)}/2^{nI(X;Z|Y)} = 2^{nI(X;Y)}$. Therefore, the decoder can decode the message and reliable transmission is possible at a rate $I(X;Z) + H(Y|Z)$.

Now, consider the corner point P_4, where we have,

$$R_y = H(Y) \tag{5.71}$$

$$R_z = I(X;Z|Y) = I(X;Z,Y) - I(X;Y) \tag{5.72}$$

For this case, relay 2 can describe the y sequence to both relay 1 and the decoder. Relay 2 uses z and y to correctly decode the message and transmits the bin-index, $b_j(x(\hat{w}))$ of the decoded x sequence. The total rate needed by relay 1 is $I(X;Z|Y)$. Upon receiving y sequence from relay 2 and $b_j(x(\hat{w}))$ from relay 1, the decoder decodes the message by searching for a unique $x(w)$ in the bin $b_j(x(\hat{w}))$ such that $(x(w), y)$ are jointly typical. This is possible since the number of x sequences in each x-bin is approximately $2^{nI(X;Y,Z)}/2^{nI(X;Z|Y)} = 2^{nI(X;Y)}$. Therefore, the decoder can decode the message and reliable transmission is possible at a rate $I(X;Z) + H(Y|Z)$.

We remark here, that the main idea behind achievability of the rate $I(X;Z) + H(Y|Z)$ at the corner point P_3 is to use compress-and-forward at relay 2, where relay 2 compresses its output by using relay 1 output as the side information [36]. This approach of compress-and-forward to achieve the cut-set bound is different than that we have seen for the case of physically degraded relay channel, where both relay 1 and relay 2 are able to decode the message.

The capacity of the diamond channel with separated relays when $Y = X$ and Z is a noisy function of X was obtained in [32]. We note that this channel falls in the class of diamond channels with semi-deterministic broadcast component, since $Y = f(X)$. Moreover, this channel also falls in the class of diamond channels with

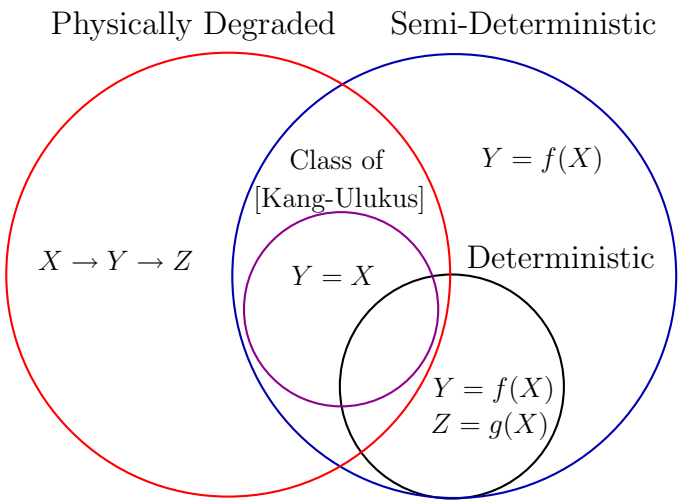

Figure 5.7: Illustration of some classes of diamond channels.

physically degraded broadcast component, since $X \to Y \to Z$ forms a Markov chain. To observe these inclusions, see Figure 5.7. Now, note that for this channel, it was shown in [32] that the cut-set upper bound is strictly sub-optimal when the relays are separated. On the other hand, when the relays are partially separated, we have from Theorems 5.4 and 5.5, that the cut-set upper bound is optimal. Since the case of partially separated relays is equivalent to having feedback from the decoder to relay 2, our results therefore show that feedback to even one of the relays strictly improves the capacity of the diamond channel.

5.4 Conclusions

We considered several variations of the diamond channel with an orthogonal multiple access component. We established the capacity for the case when the broadcast channel is deterministic. We next provided an upper bound on the capacity when the broadcast channel is physically degraded. This upper bound was shown to be

tight for a sub-class of such channels. We next considered the variation of diamond channel where the relays are partially separated and established the capacity when the broadcast channel is a) physically degraded and b) semi-deterministic. For both of these cases, we showed that the cut-set bound is tight.

5.5 Appendix

5.5.1 Proof of Theorem 5.2

We denote the outputs of relay 1 and relay 2 as,

$$J_y = f_y(Y^n), \quad J_z = f_z(Z^n) \tag{5.73}$$

We have by Fano's inequality,

$$H(W|J_y, J_z) \leq n\epsilon_n \tag{5.74}$$

We start by bounding the rates R_y and R_z,

$$\begin{aligned} nR_y &\geq H(J_y) && (5.75)\\ &\geq H(J_y|J_z) && (5.76)\\ &\geq I(J_y; Y^n|J_z) && (5.77)\\ &= H(Y^n|J_z) - H(Y^n|J_y, J_z) && (5.78) \end{aligned}$$

$$= \sum_{i=1}^{n} H(Y_i|J_z, Y^{i-1}) - H(Y^n|J_y, J_z) \tag{5.79}$$

$$\geq \sum_{i=1}^{n} H(Y_i|J_z, Y^{i-1}, Z_{i+1}^n) - H(Y^n|J_y, J_z) \tag{5.80}$$

$$\geq \sum_{i=1}^{n} H(Y_i|J_z, Y^{i-1}, Z_{i+1}^n) - \sum_{i=1}^{n} H(Y_i|X_i) - n\epsilon_n \tag{5.81}$$

where (5.81) follows from,

$$H(Y^n|J_y, J_z) \leq H(Y^n, W|J_y, J_z) \tag{5.82}$$

$$= H(W|J_y, J_z) + H(Y^n|W, J_y, J_z) \tag{5.83}$$

$$= H(W|J_y, J_z) + H(Y^n|X^n, W, J_y, J_z) \tag{5.84}$$

$$\leq n\epsilon_n + H(Y^n|X^n, J_y, J_z) \tag{5.85}$$

$$= n\epsilon_n + \sum_{i=1}^{n} H(Y_i|X^n, J_y, J_z, Y^{i-1}) \tag{5.86}$$

$$\leq n\epsilon_n + \sum_{i=1}^{n} H(Y_i|X_i) \tag{5.87}$$

where (5.84) follows from the fact that X^n is a deterministic function of the message W and (5.85) follows from (5.74) and the memoryless property of the broadcast channel.

The second rate constraint is obtained as,

$$nR_z \geq H(J_z) \tag{5.88}$$

$$\geq H(J_z|Y^n) \tag{5.89}$$

$$\geq I(J_z; Z^n|Y^n) \tag{5.90}$$

$$= H(Z^n|Y^n) - H(Z^n|J_z, Y^n) \tag{5.91}$$

$$= \sum_{i=1}^{n} H(Z_i|Y_i) - H(Z^n|J_z, Y^n) \tag{5.92}$$

$$= \sum_{i=1}^{n} H(Z_i|Y_i, Y^{i-1}, Z_{i+1}^n) - H(Z^n|J_z, Y^n) \tag{5.93}$$

$$= \sum_{i=1}^{n} H(Z_i|Y_i, Y^{i-1}, Z_{i+1}^n) - \sum_{i=1}^{n} H(Z_i|J_z, Y^n, Z_{i+1}^n) \tag{5.94}$$

$$= \sum_{i=1}^{n} H(Z_i|Y_i, Y^{i-1}, Z_{i+1}^n) - \sum_{i=1}^{n} H(Z_i|J_z, Y_i, Y^{i-1}, Z_{i+1}^n, Y_{i+1}^n) \tag{5.95}$$

$$\geq \sum_{i=1}^{n} H(Z_i|Y_i, Y^{i-1}, Z_{i+1}^n) - \sum_{i=1}^{n} H(Z_i|J_z, Y_i, Y^{i-1}, Z_{i+1}^n) \tag{5.96}$$

$$= \sum_{i=1}^{n} I(J_z; Z_i|Y_i, Y^{i-1}, Z_{i+1}^n) \tag{5.97}$$

where (5.93) follows from the memoryless property of the channel and (5.96) follows from the fact that conditioning reduces entropy. We next bound the sum rate $R_y + R_z$ as follows

$$n(R_y + R_z) = H(J_y, J_z) \tag{5.98}$$

$$\geq I(J_y, J_z; Y^n, Z^n) \tag{5.99}$$

$$= I(J_y, J_z; Y^n) + I(Z^n; J_y, J_z|Y^n) \tag{5.100}$$

$$\geq nR - n\epsilon_n + I(Z^n; J_y, J_z|Y^n) \tag{5.101}$$

$$\geq nR - n\epsilon_n + I(Z^n; J_z|Y^n) \tag{5.102}$$

$$\geq nR - n\epsilon_n + \sum_{i=1}^{n} I(Z_i; J_z|Y_i, Y^{i-1}, Z_{i+1}^n) \tag{5.103}$$

where (5.101) follows from the following sequence of inequalities,

$$I(J_y, J_z; Y^n) = I(J_y, J_z; W, Y^n) - I(J_y, J_z; W|Y^n) \tag{5.104}$$

$$= I(J_y, J_z; W, Y^n) \tag{5.105}$$

$$= I(J_y, J_z; W) + I(J_y, J_z; Y^n|W) \tag{5.106}$$

$$\geq I(J_y, J_z; W) \tag{5.107}$$

$$= H(W) - H(W|J_y, J_z) \tag{5.108}$$

$$\geq nR - n\epsilon_n \tag{5.109}$$

where (5.105) follows from the following Markov chain,

$$W \rightarrow Y^n \rightarrow (J_y, J_z) \tag{5.110}$$

We will now bound the rate of the code as follows,

$$nR = H(W) \tag{5.111}$$

$$= I(W; Y^n) + H(W|Y^n) \tag{5.112}$$

$$= I(W; Y^n) + H(W|Y^n, J_y, J_z) \tag{5.113}$$

$$\leq I(W; Y^n) + H(W|J_y, J_z) \tag{5.114}$$

$$\leq H(Y^n) - H(Y^n|W) + n\epsilon_n \tag{5.115}$$

$$\leq H(Y^n) - H(Y^n|X^n, W) + n\epsilon_n \tag{5.116}$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i|X_i) + n\epsilon_n \tag{5.117}$$

$$= H(Y^n) - \sum_{i=1}^{n} H(Y_i|X_i, Y^{i-1}, Z_{i+1}^n) + n\epsilon_n \tag{5.118}$$

$$= \sum_{i=1}^{n} H(Y_i|Y^{i-1}) - \sum_{i=1}^{n} H(Y_i|X_i, Y^{i-1}, Z_{i+1}^n) + n\epsilon_n \tag{5.119}$$

$$\leq \sum_{i=1}^{n} I(Z_{i+1}^n; Z_i) + \sum_{i=1}^{n} H(Y_i|Y^{i-1}) - \sum_{i=1}^{n} H(Y_i|X_i, Y^{i-1}, Z_{i+1}^n) + n\epsilon_n \tag{5.120}$$

$$= \sum_{i=1}^{n} I(Y^{i-1}, Z_{i+1}^n; Z_i) + \sum_{i=1}^{n} H(Y_i|Y^{i-1}, Z_{i+1}^n) - \sum_{i=1}^{n} H(Y_i|X_i, Y^{i-1}, Z_{i+1}^n) + n\epsilon_n \tag{5.121}$$

$$= \sum_{i=1}^{n} I(Y^{i-1}, Z_{i+1}^n; Z_i) + \sum_{i=1}^{n} I(X_i; Y_i|Y^{i-1}, Z_{i+1}^n) + n\epsilon_n \tag{5.122}$$

where (5.113) follows from (5.110) and (5.121) follows from Csiszar's sum lemma [16]. Now defining,

$$U_i = (Y^{i-1}, Z_{i+1}^n) \tag{5.123}$$

$$V_i = J_z \tag{5.124}$$

We therefore have from (5.81), (5.97), (5.103) and (5.122),

$$nR \leq \sum_{i=1}^{n} I(U_i; Z_i) + I(X_i; Y_i|U_i) + n\epsilon_n \tag{5.125}$$

$$nR_y \geq \sum_{i=1}^{n} H(Y_i|U_i, V_i) - \sum_{i=1}^{n} H(Y_i|X_i) - n\epsilon_n \tag{5.126}$$

$$nR_z \geq \sum_{i=1}^{n} I(V_i; Z_i|U_i, Y_i) \tag{5.127}$$

$$n(R_y + R_z) \geq nR + \sum_{i=1}^{n} I(Z_i; V_i|U_i, Y_i) - n\epsilon_n \tag{5.128}$$

and defining

$$X = X_Q, \quad Y = Y_Q, \quad Z = Z_Q \tag{5.129}$$

$$U = (U_Q, Q), \quad V = V_Q \tag{5.130}$$

where Q is uniformly distributed on $\{1, \ldots, n\}$ and independent of all other random variables, we arrive at,

$$R \leq I(U;Z) + I(X;Y|U) \tag{5.131}$$

$$R_y \geq H(Y|U,V) - H(Y|X) \tag{5.132}$$

$$R_z \geq I(Z;V|U,Y) \tag{5.133}$$

$$R_y + R_z \geq R + I(Z;V|U,Y) \tag{5.134}$$

where the joint distribution of the random variables is as follows,

$$p(x,u,y,z,v) = p(x,u)p(y|x)p(z|y)p(v|z,u) \tag{5.135}$$

Chapter 6

Secure Source Coding with a Helper

6.1 Introduction

The study of information theoretic secrecy was initiated by Shannon in [54]. Following Shannon's work, significant contributions were made by Wyner [68] who established the rate-equivocation region of a degraded broadcast channel. Wyner's result was generalized to the case of a general broadcast channel by Csiszar and Korner [15]. Recently, there has been a resurgence of activity in studying multi-terminal and vector extensions of [68], [15].

In this chapter, we investigate a secure transmission problem from a source coding perspective. In particular, we first consider a simple setup consisting of four terminals. Terminal 1 (say Alice) observes an i.i.d. source X^n which it intends to transmit losslessly to terminal 2 (say Bob). A malicious but passive user (say Eve) gets to observe the coded output of Alice. In other words, the communication link between Alice and Bob is public, i.e., insecure. It is clear that since the malicious user gets the same information as the legitimate user, there cannot be any positive secret rate of transmission. On the other hand, if there is a helper, say Helen, who observes an

i.i.d. source Y^n which is correlated with the source X^n and transmits information over a secure rate-limited link to Bob, then one can aim for creating uncertainty at the eavesdropper (see Figure 6.1[1]). For the model shown in Figure 6.1, we completely characterize the rate-equivocation region. From our result, we observe that the classical achievablity scheme of Ahlswede and Korner [3] and Wyner [67] for source coding with rate-limited side information is robust in the presence of a passive eavesdropper.

Secondly, we consider the model where Alice also has access to the coded output of Helen and completely characterize the rate-equivocation region. We will call this model the two-sided helper model (see Figure 6.2). From our result, we observe that the availability of additional coded side information at Alice allows her to increase uncertainty of the source at Eve even though the rate needed by Alice to transmit the source losslessly to Bob remains the same. This observation is in contrast with the case of insecure source coding with side information where providing coded side information to Alice is of no value [3].

We next generalize the setup of Figure 6.2 to the case when there are both secure and insecure rate-limited links from Helen and there is additional side information W^n at Bob and additional side information Z^n at Eve. In particular, there is a secure link of capacity R_{sec}, whose output is available at Alice and Bob and an insecure link, of capacity R_{ins}, whose output is available at all three terminals, i.e., at Alice, Bob and Eve (see Figure 6.3). The presence of both secure and insecure links from Helen can be interpreted as a source-coding analogue of a degraded broadcast channel from Helen where Alice and Bob receive both secure and insecure streams J_{sec} and J_{ins},

[1]In Figures 6.1, 6.2 and 6.3, secure links are shown by **bold** lines.

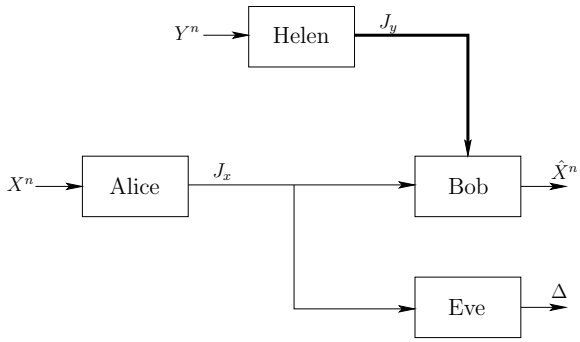

Figure 6.1: One-sided helper.

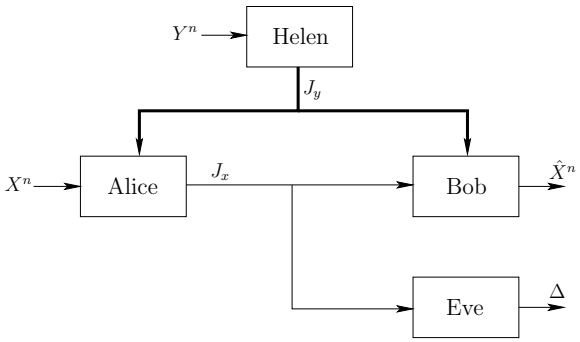

Figure 6.2: Two-sided helper.

whereas, Eve only receives the insecure stream J_{ins}. We completely characterize the rate-equivocation region for this model when $Y^n \to X^n \to (W^n, Z^n)$ forms a Markov chain.

We explicitly compute the rate-equivocation region for the cases of one-sided helper and two-sided helper for a pair of binary symmetric sources. We show that having access to Helen's coded output at Alice yields a strictly larger equivocation than the case of one-sided helper.

6.2 Related Work

The secure source coding setup shown in Figure 6.1 was considered in [26] where it was also assumed that Eve has access to additional correlated side information Z^n. Inner and outer bounds for the rate-equivocation region were provided for this setup, which do not match in general. The rate-equivocation region was completely characterized in [26] for the case when Bob has complete uncoded side information Y^n and Eve has additional side information Z^n. This result also follows from [48] where a similar three terminal setup was studied and the maximum uncertainty at Eve was

characterized under the assumption of no rate constraint in the lossless transmission of the source to Bob. A similar model was also studied in [43] where Bob intends to reconstruct both X^n and Y^n losslessly. It was shown that Slepian-Wolf binning suffices for characterizing the rate-equivocation region when the eavesdropper does not have additional correlated side information. This setup was generalized in [25] to the case when the eavesdropper has additional side information Z^n, and inner and outer bounds were provided, which do not match in general.

In [24], a multi-receiver secure broadcasting problem was studied, where Alice intends to transmit a source X^n to K legitimate users. The kth user has access to a correlated source Y_k^n, where $Y_k^n = X^n \oplus B_k^n$, for $k = 1, \dots K$, and the eavesdropper has access to Z^n, where $Z^n = X^n \oplus E^n$, and the noise sequences $(B_1^n, \dots, B_K^n, E^n)$ are mutually independent and also independent of the source X^n. Furthermore, it was assumed that Alice also has access to $(Y_1^n, \dots Y_K^n)$. For sources with such modulo-additive structure, it was shown that to maximize the uncertainty at the eavesdropper, Alice cannot do any better than describing the error sequences $(B_1^n, \dots, B_K^n)$ to the legitimate users. This model is related to the two-sided helper model shown in Figure 6.2; see Section 6.5 for details.

For the model shown in Figure 6.3, when we set $R_{sec} = R_{ins} = 0$, i.e., in the absence of Helen, we recover the result obtained in [48]. Therefore, our result can also be viewed as a generalization of the result obtained in [48].

By setting $R_{sec} = 0$, i.e., in the absence of the secure rate-limited link, the resulting model is related to the model considered in [17] where the aim is to generate a secret key between two terminals via an insecure rate-limited two-sided helper. In the model

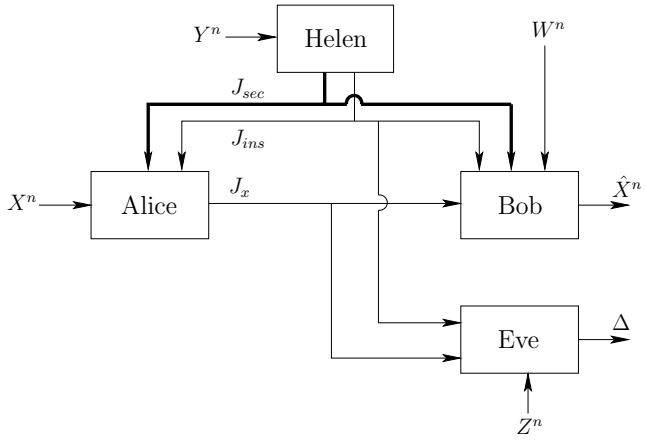

Figure 6.3: Secure and insecure links from two-sided helper.

studied in this work, the aim is to securely transmit the source X^n to Bob. Note that, when $R_{sec} = 0$ and $W = \phi$, both the secret key generation capacity [17] and secure transmission rate are zero since Eve has access to both J_{ins} and J_x along with Z^n. On the other hand, in the presence of a secure link, i.e., when $R_{sec} > 0$, even when $W = \phi$, we can still create uncertainty at the eavesdropper. This is possible since Helen can choose not to transmit any information on the insecure link and transmit only a coded description of Y^n by using the secure link at the rate R_{sec}, which plays the role of a correlated key. Furthermore, being correlated with the source X^n, the coded description of Y^n also permits Alice to lower the rate of transmission when compared to the case of using an uncorrelated secret key, where Alice transmits at a rate $H(X)$.

6.3 Summary of Main Results

In Section 6.4, we present the rate-equivocation region for the case of one-sided helper. We show that Slepian-Wolf binning alone at Alice is optimal for this case. We present

the rate-equivocation region for the case of two-sided helper in Section 6.5. For the case of two-sided helper, Alice uses a conditional rate-distortion code to create an auxiliary U from the source X and the coded output V received from Helen. This code construction is reminiscent of lossy-source coding with two-sided helper [33], [59], [47]. For the case of lossy source coding, a conditional rate-distortion code is used where U is selected to satisfy the distortion criterion. On the other hand, the purpose of U in secure lossless source coding is to confuse the eavesdropper. From this result, we demonstrate the insufficiency of Slepian-Wolf binning at Alice by explicitly utilizing the side information at Alice. This observation is further highlighted in Section 6.6 where we compare the rate-equivocation regions of two-sided helper and one-sided helper cases for a pair of binary symmetric sources. For this example, we show that for all $R_y > 0$, the information leakage to the eavesdropper for the two-sided helper is strictly less than the case of one-sided helper. We finally generalize the result of two-sided helper to the case when there are both secure and insecure rate-limited links from the two-sided helper and additional side informations W and Z, at Bob and Eve, respectively. The presence of secure and insecure rate-limited links from Helen can be viewed as a source-coding analogue of a degraded broadcast channel from Helen to (Alice, Bob) and Eve. We characterize the rate-equivocation region for this model when the sources satisfy the condition $Y \rightarrow X \rightarrow (W, Z)$.

6.4 One-Sided Helper

6.4.1 System model

We consider the following source coding problem. Alice observes an n-length source sequence X^n, which is intended to be transmitted losslessly to Bob. The coded output of Alice can be observed by the malicious user Eve. Moreover, Helen observes a correlated source Y^n and there exists a noiseless rate-limited channel from Helen to Bob. We assume that the link from Helen to Bob is a secure link and the coded output of Helen is not observed by Eve (see Figure 6.1). The sources (X^n, Y^n) are generated i.i.d. according to $p(x, y)$ where $p(x, y)$ is defined over the finite product alphabet $\mathcal{X} \times \mathcal{Y}$. The aim of Alice is to create maximum uncertainty at Eve regarding the source X^n while losslessly transmitting the source to Bob.

An $(n, 2^{nR_x}, 2^{nR_y})$ code for this model consists of an encoding function at Alice, $f_x : X^n \to \{1, \ldots, 2^{nR_x}\}$, an encoding function at Helen, $f_y : Y^n \to \{1, \ldots, 2^{nR_y}\}$, and a decoding function at Bob, $g : \{1, \ldots, 2^{nR_x}\} \times \{1, \ldots, 2^{nR_y}\} \to X^n$. The uncertainty about the source X^n at Eve is measured by $H(X^n|f_x(X^n))/n$. The probability of error in the reconstruction of X^n at Bob is defined as $P_e^n = \Pr(g(f_x(X^n), f_y(Y^n)) \neq X^n)$. A triple (R_x, R_y, Δ) is achievable if for any $\epsilon > 0$, there exists a $(n, 2^{nR_x}, 2^{nR_y})$ code such that $P_e^n \leq \epsilon$ and $H(X^n|f_x(X^n))/n \geq \Delta$. We denote the set of all achievable (R_x, R_y, Δ) rate triples as $\mathcal{R}_{1-sided}$.

6.4.2 Result

The main result is given in the following theorem.

Theorem 6.1 *The set of achievable rate triples $\mathcal{R}_{1-sided}$ for secure source coding with one-sided helper is given as*

$$\mathcal{R}_{1-sided} = \Big\{(R_x, R_y, \Delta) : R_x \geq H(X|V) \tag{6.1}$$

$$R_y \geq I(Y;V) \tag{6.2}$$

$$\Delta \leq I(X;V)\Big\} \tag{6.3}$$

where the joint distribution of the involved random variables is as follows,

$$p(x, y, v) = p(x, y)p(v|y) \tag{6.4}$$

and it suffices to consider such distributions for which $|\mathcal{V}| \leq |\mathcal{Y}| + 2$.

The proof of Theorem 6.1 is given in the Appendix.

We note that the inner and outer bounds for source coding model considered in this section can be obtained from the results presented in [26, Theorem 3.1] although these bounds do not match in general. These bounds match when Bob has complete uncoded side information Y^n, i.e., when $R_y \geq H(Y)$.

The achievability scheme which yields the rate region described in Theorem 6.1 is summarized as follows:

1. Helen describes the source Y to Bob through a coded output V.

2. Alice performs Slepian-Wolf binning of the source X with respect to the coded side information, V, available at Bob.

Therefore, our result shows that the achievable scheme of Ahlswede, Korner [3] and Wyner [67] is optimal in the presence of an eavesdropper. Moreover, on dropping the security constraint, Theorem 1 yields the result of [3], [67].

6.5 Two-Sided Helper

6.5.1 System model

We next consider the following generalization of the model considered in Section 6.4. In this model, Alice also has access to the coded output of Helen besides the source sequence X^n (see Figure 6.2). An $(n, 2^{nR_x}, 2^{nR_y})$ code for this model consists of an encoding function at Alice, $f_x : X^n \times \{1, \ldots, 2^{nR_y}\} \rightarrow \{1, \ldots, 2^{nR_x}\}$, an encoding function at Helen, $f_y : Y^n \rightarrow \{1, \ldots, 2^{nR_y}\}$, and a decoding function at Bob, $g : \{1, \ldots, 2^{nR_x}\} \times \{1, \ldots, 2^{nR_y}\} \rightarrow X^n$. The uncertainty about the source X^n at Eve is measured by $H(X^n|f_x(X^n))/n$. The probability of error in the reconstruction of X^n at Bob is defined as $P_e^n = \Pr(g(f_x(X^n, f_y(Y^n)), f_y(Y^n)) \neq X^n)$. A triple (R_x, R_y, Δ) is achievable if for any $\epsilon > 0$, there exists a $(n, 2^{nR_x}, 2^{nR_y})$ code such that $P_e^n \leq \epsilon$ and $H(X^n|f_x(X^n))/n \geq \Delta$. We denote the set of all achievable (R_x, R_y, Δ) rate triples as $\mathcal{R}_{2-sided}$.

6.5.2 Result

The main result is given in the following theorem.

Theorem 6.2 *The set of achievable rate triples $\mathcal{R}_{2-sided}$ for secure source coding with*

two-sided helper is given as

$$\mathcal{R}_{2-sided} = \Big\{(R_x, R_y, \Delta) : R_x \geq H(X|V) \tag{6.5}$$

$$R_y \geq I(Y;V) \tag{6.6}$$

$$\Delta \leq \min(I(X;V|U), R_y)\Big\} \tag{6.7}$$

where the joint distribution of the involved random variables is as follows,

$$p(x, y, v, u) = p(x, y)p(v|y)p(u|x, v) \tag{6.8}$$

and it suffices to consider distributions such that $|\mathcal{V}| \leq |\mathcal{Y}|+2$ *and* $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}|+2|\mathcal{X}|$.

The proof of Theorem 6.2 is given in the Appendix. We remark here that the proof of converse for Theorem 6.2 is closely related to the proof of the converse of the rate-distortion function with a two-sided helper [33], [59], [47].

The achievability scheme which yields the rate region described in Theorem 6.2 is summarized as follows:

1. Helen describes the source Y to both Bob and Alice through a coded output V.

2. Using the coded output V and the source X, Alice jointly quantizes (X, V) to an auxiliary random variable U. She subsequently bins the U sequences at the rate $I(X;U|V)$ such that Bob can decode U by using the side information V from Helen.

3. Alice also bins the source X at a rate $H(X|U, V)$ so that having access to

(U, V), Bob can correctly decode the source X. The total rate used by Alice is $I(X;U|V) + H(X|U,V) = H(X|V)$.

Therefore, the main difference between the achievability schemes for Theorems 6.1 and 6.2 is at the encoding at Alice and decoding at Bob. Also note that selecting a constant U in Theorem 6.2 corresponds to Slepian-Wolf binning of X at Alice which resulted in an equivocation of $I(X;V)$ in Theorem 6.1. We will show in the next section through an example that the uncertainty about the source at Eve for the case of two-sided helper can be strictly larger than the case of one-sided helper and selecting U as a constant is clearly suboptimal.

Besides reflecting the fact that the uncertainty at Eve can be strictly larger than the case of a one-sided helper, Theorem 6.2 has another interesting interpretation. If Alice and Helen can use sufficiently large rates to securely transmit the source X^n to Bob, then the helper can simply transmit a secret key of entropy $H(X)$ to both Alice and Bob. Alice can then use this secret key to losslessly transmit the source to Bob in perfect secrecy by using a one-time pad [54]. In other words, when R_x and R_y are larger than $H(X)$, one can immediately obtain this result from Theorem 6.2 by selecting V to be independent of (X, Y) and uniformly distributed on $\{1, \ldots, |\mathcal{X}|\}$. Finally, selecting $U = X \oplus V$, we observe that $\min(R_y, I(X;V|U)) = H(X)$, yielding perfect secrecy. We note that, here, V plays the role of a secret key.

Now consider the model where the side information Y^n is of the form $Y^n = X^n \oplus B^n$, where $|\mathcal{B}| = |\mathcal{X}|$, and B^n is independent of X^n. Moreover, assume that the side information Y^n is available to both Alice and Bob in an uncoded manner. For

this model, it follows from [24] that, to maximize the uncertainty at the eavesdropper, Alice cannot do any better than describing the error sequence B^n to Bob. Note that our two-sided helper model differs from this model in two aspects: first, in our case, the common side information available to Alice and Bob is coded and rate-limited, secondly, the sources in our model do not have to be in modulo-additive form.

Our encoding scheme at Alice for the case of two-sided helper comprises of two steps: (a) using the coded side information V and the source X, Alice creates U and transmits the bin index of U at a rate $I(X;U|V)$ so that Bob can estimate U using V, and, (b) Alice bins the source X at a rate $H(X|U,V)$ and transmits the bin index of the source X. Note that if for a pair of sources (X,Y), the optimal V is of the form $V = X \oplus B$, where $|\mathcal{B}| = |\mathcal{X}|$ and B is independent of X, then it suffices to choose $U = B$, so that $I(X;V|U) = H(X)$ and $H(X|U,V) = 0$. In other words, for such sources, step (b) in our achievability scheme is not necessary, which is similar to the achievability for the case of modulo-additive sources in [24]. On the other hand, for a general pair of sources (X,Y), the optimal V may not be of the form $V = X \oplus B$ and the optimal U may not always satisfy $H(X|U,V) = 0$. Therefore, we need the step (b) for our achievability scheme. This differentiates our achievable scheme from that of [24], which holds for modulo-additive sources with uncoded side information.

Also note that if Y^n is not of the form $X^n \oplus B^n$, and if $R_y \geq H(X)$, then Helen can transmit a secret key which will enable perfectly secure transmission of X^n by using a one-time pad [54]. This phenomenon does not always occur when the side information Y^n is available to both Alice and Bob in an uncoded fashion [24].

6.6 An Example: Binary Symmetric Sources

Before proceeding to further generalizations of Theorems 6.1 and 6.2, we explicitly evaluate Theorems 6.1 and 6.2 for a pair of binary sources.

Let X and Y be binary sources with $X \sim \text{Ber}(1/2), Y \sim \text{Ber}(1/2)$ and $X = Y \oplus E$, where $E \sim \text{Ber}(\delta)$. For this pair of sources, the region described in Theorem 6.1 can be completely characterized as,

$$\begin{aligned}\mathcal{R}_{1-sided}(R_y) = \big\{(R_x, \Delta) :\ & R_x \geq h(\delta * h^{-1}(1 - R_y)) \\ & \Delta \leq 1 - h(\delta * h^{-1}(1 - R_y))\big\}\end{aligned} \tag{6.9}$$

and the region in Theorem 6.2 can be completely characterized as,

$$\begin{aligned}\mathcal{R}_{2-sided}(R_y) = \big\{(R_x, \Delta) :\ & R_x \geq h(\delta * h^{-1}(1 - R_y)) \\ & \Delta \leq \min(R_y, 1)\big\}\end{aligned} \tag{6.10}$$

where $h(.)$ is the binary entropy function, and $a * b = a(1 - b) + b(1 - a)$.

We start with the derivation of (6.9). Without loss of generality, we assume that $R_y \leq H(Y)$. Achievability follows by selecting $V = Y \oplus N$, where $N \sim \text{Ber}(\alpha)$, where

$$\alpha = h^{-1}(1 - R_y) \tag{6.11}$$

Substituting, we obtain

$$H(X|V) = h(\delta * h^{-1}(1 - R_y)) \tag{6.12}$$

$$I(X;V) = 1 - h(\delta * h^{-1}(1 - R_y)) \tag{6.13}$$

which completes the achievability. Note that Y is independent of E, and the random variables X, Y, and V form a Markov chain, i.e., $X \to Y \to V$. Using this Markov chain, the converse follows by simple application of Mrs. Gerber's lemma [69] as follows. Let us be given $R_y \in (0, 1)$. We have

$$R_y \geq I(Y;V) \tag{6.14}$$

$$= H(Y) - H(Y|V) \tag{6.15}$$

$$= 1 - H(Y|V) \tag{6.16}$$

which implies $H(Y|V) \geq 1 - R_y$. Mrs. Gerber's lemma states that for $X = Y \oplus E$, with $E \sim \text{Ber}(\delta)$, if $H(Y|V) \geq \beta$, then $H(X|V) \geq h(\delta * h^{-1}(\beta))$. We therefore have,

$$R_x \geq H(X|V) \tag{6.17}$$

$$\geq h(\delta * h^{-1}(1 - R_y)) \tag{6.18}$$

and

$$\Delta \leq I(X;V) \tag{6.19}$$

$$= H(X) - H(X|V) \tag{6.20}$$

$$= 1 - H(X|V) \tag{6.21}$$

$$\leq 1 - h(\delta * h^{-1}(1 - R_y)) \tag{6.22}$$

This completes the converse.

For the case of two-sided helper, we compute the equivocation Δ as follows. We choose V as $V = Y \oplus N$ where $N \sim \text{Ber}(\alpha)$ as in the case of one-sided helper. We choose U as,

$$U = X \oplus V \tag{6.23}$$

$$= Y \oplus E \oplus Y \oplus N \tag{6.24}$$

$$= E \oplus N \tag{6.25}$$

Since $X \sim \text{Ber}(1/2)$, E is independent of X, and therefore $U = E \oplus N$ is also independent of X. We next compute the term $I(X;V|U)$ as follows,

$$I(X;V|U) = H(X|U) \tag{6.26}$$

$$= H(X) \tag{6.27}$$

$$= 1 \tag{6.28}$$

and therefore

$$\min(R_y, I(X;V|U)) = \min(R_y, 1) \tag{6.29}$$

For the converse part, we also have that

$$\Delta \leq \min(R_y, I(X;V|U)) \tag{6.30}$$

$$\leq \min(R_y, H(X)) \tag{6.31}$$

$$= \min(R_y, 1) \tag{6.32}$$

The rate from Alice, R_x and the equivocation Δ for the cases of one-sided and two-sided helper are shown in Figure 6.4 for the case when $\delta = 0.05$. For the one-sided helper, we can observe a trade-off in the amount of information Alice needs to send versus the uncertainty at Eve. For small values of R_y, Alice needs to send more information thereby leaking out more information to Eve. The amount of information leaked is exactly the information sent by Alice. On the other hand, for the case of two-sided helper, the uncertainty at the eavesdropper is always strictly larger than the uncertainty in the one-sided case. Also note that for this pair of sources, perfect secrecy is possible for the case of two-sided helper when $R_y \geq H(Y)$ which is not possible for the case of one-sided helper.

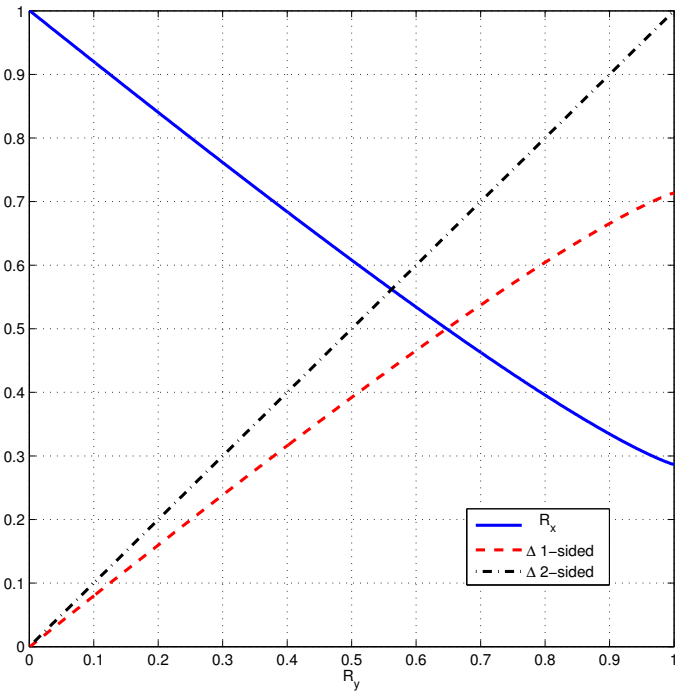

Figure 6.4: The rate-equivocation region for a pair of binary symmetric sources.

6.7 Secure and Insecure Links from Two-Sided Helper

6.7.1 System model

In this section, we consider a generalization of the model considered in Section 6.5. We consider the case when there are two links from Helen (see Figure 6.3). One link of rate R_{sec} is secure, i.e., the output of this link is available to only Alice and Bob. The second link of rate R_{ins} is public and the output of this link is available to Alice, Bob and Eve. The sources (X^n, Y^n, W^n, Z^n) are generated i.i.d. according to $p(x, y, w, z) = p(x, y)p(w, z|x)$ where $p(x, y, w, z)$ is defined over the finite product alphabet $\mathcal{X} \times \mathcal{Y} \times \mathcal{W} \times \mathcal{Z}$.

A $(n, 2^{nR_x}, 2^{nR_{sec}}, 2^{nR_{ins}})$ code for this model consists of an encoding function at

Helen, $f_y : Y^n \to J_{sec} \times J_{ins}$, where $|J_{sec}| \leq 2^{nR_{sec}}$, $|J_{ins}| \leq 2^{nR_{ins}}$, an encoding function at Alice, $f_x : X^n \times J_{sec} \times J_{ins} \to \{1, \ldots, 2^{nR_x}\}$, and a decoding function at Bob, $g : \{1, \ldots, 2^{nR_x}\} \times J_{sec} \times J_{ins} \times W^n \to X^n$. The uncertainty about the source X^n at Eve is measured by $H(X^n|f_x(X^n, J_{sec}, J_{ins}), J_{ins}, Z^n)/n$. The probability of error in the reconstruction of X^n at Bob is defined as $P_e^n = \Pr(g(f_x(X^n, J_{sec}, J_{ins}), J_{sec}, J_{ins}, W^n) \neq X^n)$. A quadruple $(R_x, R_{sec}, R_{ins}, \Delta)$ is achievable if for any $\epsilon > 0$, there exists a $(n, 2^{nR_x}, 2^{nR_{sec}}, 2^{nR_{ins}})$ code such that $P_e^n \leq \epsilon$ and $H(X^n|f_x(X^n, J_{sec}, J_{ins}), J_{ins}, Z^n)/n \geq \Delta$. We denote the set of all achievable $(R_x, R_{sec}, R_{ins}, \Delta)$ rate quadruples as $\mathcal{R}_{sec-ins}^{W,Z}$.

6.7.2 Result

The main result is given in the following theorem.

Theorem 6.3 *The set of achievable rate quadruples $\mathcal{R}_{sec-ins}^{W,Z}$ for secure source coding with secure and insecure links from a two-sided helper, additional side information W at Bob and Z at Eve is given as*

$$\mathcal{R}_{sec-ins}^{W,Z} = \Big\{(R_x, R_{sec}, R_{ins}, \Delta) : R_x \geq H(X|V_1, V_2, W) \tag{6.33}$$

$$R_{sec} \geq I(Y; V_1|W) \tag{6.34}$$

$$R_{ins} \geq I(Y; V_2|W, V_1) \tag{6.35}$$

$$\Delta \leq \min(R_{sec}, I(X; V_1|U, V_2, W)) + I(X; W|U, V_2) - I(X; Z|U, V_2)\Big\} \tag{6.36}$$

where the joint distribution of the involved random variables is as follows,

$$p(x, y, w, z, v_1, v_2, u) = p(x, y)p(w, z|x)p(v_1, v_2|y)p(u|x, v_1, v_2) \tag{6.37}$$

and it suffices to consider such distributions for which $|\mathcal{V}_1| \leq |\mathcal{Y}| + 3$, $|\mathcal{V}_2| \leq |\mathcal{Y}| + 4$ *and* $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{Y}|^2 + 7|\mathcal{X}||\mathcal{Y}| + 12|\mathcal{X}| + 2$.

The proof of Theorem 6.3 is given in the Appendix.

The achievability scheme which yields the rate region described in Theorem 6.3 is summarized as follows:

1. Helen first uses the secure link to describe the source Y to both Alice and Bob at a rate $I(Y; V_1|W)$, where W plays the role of side information. Subsequently, the insecure link is used to provide another description of the correlated source Y at a rate $I(Y; V_2|W, V_1)$, where (W, V_1) plays the role of side information. Therefore, the key idea is to first use the secure link to build common randomness at Alice and Bob and subsequently use this common randomness to send information over the insecure link at a lower rate.

2. Having access to the coded outputs (V_1, V_2) from Helen and the source X, Alice jointly quantizes (X, V_1, V_2) to an auxiliary random variable U. She subsequently bins the U sequences at the rate $I(X; U|V_1, V_2, W)$ such that Bob can decode U by using W and the coded outputs (V_1, V_2) from the helper.

3. She also bins the source X at a rate $H(X|U, V_1, V_2, W)$ so that having access to (U, V_1, V_2, W), Bob can correctly decode the source X. The total rate used by

Alice is $I(X;U|V_1,V_2,W) + H(X|U,V_1,V_2,W) = H(X|V_1,V_2,W)$.

We note here that using Theorem 6.3, we can recover Theorem 6.2 by setting $R_{ins} = 0$, and selecting $W = Z = V_2 = \phi$.

On setting $R_{sec} = 0$, the resulting model is similar to the one considered in [17] although the aim in [17] is to generate a secret key to be shared by Alice and Bob, while we are interested in the secure transmission of the source X.

If $R_{sec} = R_{ins} = 0$, then we recover the result of [48] as a special case by setting $V_1 = V_2 = \phi$. Therefore, Theorem 6.3 can also be viewed as a generalization of the result of [48] where no rate constraint is imposed on the transmission of Alice and the goal is to maximize the uncertainty at Eve while losslessly transmitting the source to Bob.

6.8 Conclusions

In this chapter, we considered several secure source coding problems. We first provided the characterization of the rate-equivocation region for a secure source coding problem with coded side information at the legitimate user. We next generalized this result for two different models with increasing complexity. We characterized the rate-equivocation region for the case of two-sided helper. The value of two-sided coded side information is emphasized by comparing the respective equivocations for a pair of binary sources. It is shown for this example that Slepian-Wolf binning alone is insufficient and using our achievable scheme, one attains strictly larger uncertainty at the eavesdropper than the case of one-sided helper. We next considered the case when

there are both secure and insecure rate-limited links from the helper and characterized the rate-equivocation region.

6.9 Appendix

6.9.1 Proof of Theorem 6.1

Achievability

Fix the distribution $p(x, y, v) = p(x, y)p(v|y)$.

1. Codebook generation at Helen: From the conditional probability distribution $p(v|y)$ compute $p(v) = \sum_y p(y)p(v|y)$. Generate 2^{nR_y} codewords $v(l)$ independently according to $\prod_{i=1}^{n} p(v_i)$, where $l = 1, \ldots, 2^{nR_y}$.

2. Codebook generation at Alice: Randomly bin the x^n sequences into $2^{nH(X|V)}$ bins and index these bins as $m = 1, \ldots, M$, where $M = 2^{nH(X|V)}$.

3. Encoding at Helen: On observing the sequence y^n, Helen tries to find a sequence $v(l)$ such that $(v(l), y^n)$ are jointly typical. From rate-distortion theory, we know that there exists one such sequence as long as $R_y \geq I(V; Y)$. Helen sends the index l of the sequence $v(l)$.

4. Encoding at Alice: On observing the sequence x^n, Alice finds the bin index m_X in which the sequence x^n falls and transmits the bin index m_X.

5. Decoding at Bob: On receiving l and the bin index m_X, Bob tries to find a unique x^n sequence in bin m_X such that $(v(l), x^n)$ are jointly typical. This is

possible since the number of x^n sequences in each bin is roughly $2^{nH(X)}/2^{nH(X|V)}$ which is $2^{nI(X;V)}$. The existence of an x^n such that $(v(l), x^n)$ are jointly typical is guaranteed by the Markov lemma [14] and the uniqueness is guaranteed by the properties of jointly typical sequences [14].

6. Equivocation:

$$\begin{aligned} H(X^n|m_X) &= H(X^n, m_X) - H(m_X) && (6.38)\\ &= H(X^n) + H(m_X|X^n) - H(m_X) && (6.39)\\ &= H(X^n) - H(m_X) && (6.40)\\ &\geq H(X^n) - \log(M) && (6.41)\\ &= H(X^n) - nH(X|V) && (6.42)\\ &= nI(X;V) && (6.43) \end{aligned}$$

Therefore,

$$\Delta \leq I(X;V) \tag{6.44}$$

is achievable. This completes the achievability part.

Converse

Let the output of the helper be J_y, and the output of Alice be J_x, i.e.,

$$J_y = f_y(Y^n) \tag{6.45}$$

$$J_x = f_x(X^n) \tag{6.46}$$

First note that, for noiseless reconstruction of the sequence X^n at the legitimate decoder, we have by Fano's inequality

$$H(X^n|J_x, J_y) \leq n\epsilon_n \tag{6.47}$$

We start by obtaining a lower bound on R_x, the rate of Alice, as follows

$$\begin{aligned}
nR_x &\geq H(J_x) && (6.48)\\
&\geq H(J_x|J_y) && (6.49)\\
&= H(X^n, J_x|J_y) - H(X^n|J_x, J_y) && (6.50)\\
&\geq H(X^n, J_x|J_y) - n\epsilon_n && (6.51)\\
&\geq H(X^n|J_y) - n\epsilon_n && (6.52)\\
&= \sum_{i=1}^{n} H(X_i|X^{i-1}, J_y) - n\epsilon_n && (6.53)\\
&= \sum_{i=1}^{n} H(X_i|V_i) - n\epsilon_n && (6.54)
\end{aligned}$$

$$= nH(X_Q|V_Q, Q) - n\epsilon_n \tag{6.55}$$

$$= nH(X|V) - n\epsilon_n \tag{6.56}$$

where (6.51) follows by (6.47). In (6.54), we have defined

$$V_i = (J_y, X^{i-1}) \tag{6.57}$$

In (6.56), we have defined,

$$X = X_Q, \quad V = (Q, V_Q) \tag{6.58}$$

where Q is uniformly distributed on $\{1, \ldots, n\}$ and is independent of all other random variables.

Next, we obtain a lower bound on R_y, the rate of the helper,

$$nR_y \geq H(J_y) \tag{6.59}$$

$$\geq I(J_y; Y^n) \tag{6.60}$$

$$= \sum_{i=1}^{n} I(J_y, Y^{i-1}; Y_i) \tag{6.61}$$

$$= \sum_{i=1}^{n} I(J_y, Y^{i-1}, X^{i-1}; Y_i) \tag{6.62}$$

$$\geq \sum_{i=1}^{n} I(J_y, X^{i-1}; Y_i) \tag{6.63}$$

$$= \sum_{i=1}^{n} I(V_i; Y_i) \tag{6.64}$$

$$= nI(V_Q; Y_Q|Q) \tag{6.65}$$

$$= nI(V; Y) \tag{6.66}$$

where (6.62) follows from the Markov chain

$$X^{i-1} \to (J_y, Y^{i-1}) \to Y_i \tag{6.67}$$

and in (6.66), we have defined $Y = Y_Q$.

We now have the main step, i.e., an upper bound on the equivocation rate of the eavesdropper,

$$H(X^n|J_x) = H(X^n, J_y|J_x) - H(J_y|X^n, J_x) \tag{6.68}$$

$$= H(J_y|J_x) - H(J_y|X^n, J_x) + H(X^n|J_x, J_y) \tag{6.69}$$

$$= H(J_y|J_x) - H(J_y|X^n) + H(X^n|J_x, J_y) \tag{6.70}$$

$$\leq H(J_y) - H(J_y|X^n) + H(X^n|J_x, J_y) \tag{6.71}$$

$$\leq I(J_y; X^n) + n\epsilon_n \tag{6.72}$$

$$= \sum_{i=1}^{n} I(J_y; X_i|X^{i-1}) + n\epsilon_n \tag{6.73}$$

$$= \sum_{i=1}^{n} I(J_y, X^{i-1}; X_i) + n\epsilon_n \tag{6.74}$$

$$= \sum_{i=1}^{n} I(X_i; V_i) + n\epsilon_n \tag{6.75}$$

$$= nI(X_Q; V_Q|Q) + n\epsilon_n \tag{6.76}$$

$$= nI(X; V) + n\epsilon_n \tag{6.77}$$

where (6.70) follows from the Markov chain

$$J_x \rightarrow X^n \rightarrow J_y \tag{6.78}$$

and (6.72) follows from (6.47). This implies

$$\Delta \leq I(X;V) \tag{6.79}$$

Also note that the following is a Markov chain,

$$V \rightarrow Y \rightarrow X \tag{6.80}$$

Therefore, the joint distribution of the involved random variables is

$$p(x,y,v) = p(x,y)p(v|y) \tag{6.81}$$

From support lemma [16], it can be shown that it suffices to consider such joint distributions for which $|\mathcal{V}| \leq |\mathcal{Y}| + 2$.

In (6.57), we have defined the auxiliary random variable as $V_i = (J_y, X^{i-1})$. We remark here that the converse for Theorem 1 can also be proved by defining, $V_i = (J_y, Y^{i-1})$ as in [14, Section 14.8]. Note that due to the fact that the sources (X^n, Y^n) are generated in an i.i.d. manner, the following is a Markov chain,

$$(J_y, Y^{i-1}, X^{i-1}) \rightarrow Y_i \rightarrow X_i \tag{6.82}$$

This is due to the fact that X_i does not carry any extra information about $(J_y = f_y(Y^n), Y^{i-1}, X^{i-1})$ that is not there in Y_i. Therefore, (6.82) implies that the following are also valid Markov chains,

$$(J_y, X^{i-1}) \to Y_i \to X_i \tag{6.83}$$

$$(J_y, Y^{i-1}) \to Y_i \to X_i \tag{6.84}$$

and the converse for Theorem 6.1 can be proved by defining $V_i = (J_y, X^{i-1})$ or $V_i = (J_y, Y^{i-1})$.

6.9.2 Proof of Theorem 6.2

Achievability

Fix the distribution $p(x, y, v) = p(x, y)p(v|y)p(u|x, v)$.

1. Codebook generation at Helen: From the conditional probability distribution $p(v|y)$ compute $p(v) = \sum_y p(y)p(v|y)$. Generate 2^{nR_y} codewords $v(l)$ independently according to $\prod_{i=1}^{n} p(v_i)$, where $l = 1, \ldots, 2^{nR_y}$.

2. Codebook generation at Alice: From the distribution $p(u|x, v)$, compute $p(u)$. Generate $2^{nI(X,V;U)}$ sequences $u(s)$ independently according to $\prod_{i=1}^{n} p(u_i)$, where $s = 1, \ldots, 2^{nI(X,V;U)}$. Next, bin these sequences uniformly into $2^{nI(X;U|V)}$ bins.

   Also, randomly bin the x^n sequences into $2^{nH(X|U,V)}$ bins and index these bins as $m = 1, \ldots, 2^{nH(X|U,V)}$.

3. Encoding at Helen: On observing the sequence y^n, Helen tries to find a sequence $v(l)$ such that $(v(l), y^n)$ are jointly typical. From rate-distortion theory, we know that there exists one such sequence as long as $R_y \geq I(V;Y)$. Helen sends the index l of the sequence $v(l)$.

4. Encoding at Alice: The key difference from the one-sided helper case is in the encoding at Alice. On observing the sequence x^n, Alice first finds the bin index m_X in which the sequence x^n falls. Alice also has the sequence $v(l)$ received from Helen. Alice next finds a sequence u such that $(u, v(l), x^n)$ are jointly typical. Let the bin index of this resulting u sequence be s_U.

   Alice transmits the pair (s_U, m_X) which is received by Bob and Eve. The total rate used by Alice is $I(X;U|V) + H(X|U,V) = H(X|V)$.

5. Decoding at Bob: On receiving the pair (s_U, m_X) from Alice and the index l from Helen, Bob first searches the bin s_U for a sequence $\hat{u}$ such that $(\hat{u}, v(l))$ are jointly typical. This is possible since the number of u sequences in each auxiliary bin is approximately $2^{nI(X,V;U)}/2^{nI(X;U|V)}$ which is $2^{nI(U;V)}$ and therefore with high probability, Bob will be able to obtain the correct u sequence.

   Using the estimate $\hat{u}$ and $v(l)$, Bob searches for a unique x^n sequence in the bin m_X such that $(\hat{u}, v(l), x^n)$ are jointly typical. This is possible since the number of x^n sequences in each bin is approximately $2^{nH(X)}/2^{nH(X|U,V)}$ which is $2^{nI(U,V;X)}$.

6. Equivocation:

$$H(X^n|s_U, m_X) = H(X^n, m_X, s_U) - H(m_X, s_U) \tag{6.85}$$

$$= H(X^n) + H(m_X, s_U|X^n) - H(m_X, s_U) \tag{6.86}$$

$$= H(X^n) + H(s_U|X^n) - H(m_X, s_U) \tag{6.87}$$

$$\geq H(X^n) + H(s_U|X^n) - H(s_U) - H(m_X) \tag{6.88}$$

$$= H(X^n) - H(m_X) - I(X^n; s_U) \tag{6.89}$$

$$\geq H(X^n) - nH(X|U, V) - I(X^n; s_U) \tag{6.90}$$

$$= nI(X; U, V) - I(X^n; s_U) \tag{6.91}$$

$$\geq nI(X; U, V) - I(X^n; U^n) \tag{6.92}$$

$$\geq nI(X; U, V) - nI(X; U) - n\epsilon_n^{'} \tag{6.93}$$

$$= n(I(X; V|U) - \epsilon_n^{'}) \tag{6.94}$$

where (6.87) follows from the fact that m_X is the bin index of the sequence X^n, (6.88) follows from the fact that conditioning reduces entropy, (6.90) follows from the fact that $H(m_X) \leq \log(2^{nH(X|U,V)})$, (6.92) follows from the fact that s_U is the bin index of the sequence U^n, i.e., $s_U \rightarrow U^n \rightarrow X^n$ forms a Markov chain and subsequently using the data processing inequality. To prove (6.93), we define a random variable $\mu(X^n, U^n)$, as follows,

$$\mu(x^n, u^n) = \begin{cases} 1, & \text{if } (x^n, u^n) \in A_\epsilon^{(n)}(p(x, u)); \\ 0, & \text{otherwise.} \end{cases} \tag{6.95}$$

where $A_\epsilon^{(n)}(p(x,u))$ is the set of typical (x^n, u^n) sequences with respect to $p(x,u)$ [14]. We now prove (6.93) as follows,

$$I(X^n;U^n) \leq I(X^n;U^n,\mu(X^n,U^n)) \tag{6.96}$$

$$= I(X^n;\mu(X^n,U^n)) + I(X^n;U^n|\mu(X^n,U^n)) \tag{6.97}$$

$$\leq H(\mu(X^n,U^n)) + I(X^n;U^n|\mu(X^n,U^n)) \tag{6.98}$$

$$\leq 1 + I(X^n;U^n|\mu(X^n,U^n)) \tag{6.99}$$

$$= 1 + \Pr(\mu(X^n,U^n)=0)I(X^n;U^n|\mu(X^n,U^n)=0)+$$

$$\Pr(\mu(X^n,U^n)=1)I(X^n;U^n|\mu(X^n,U^n)=1) \tag{6.100}$$

$$\leq 1 + \Pr(\mu(X^n,U^n)=0)H(X^n)+$$

$$\Pr(\mu(X^n,U^n)=1)I(X^n;U^n|\mu(X^n,U^n)=1) \tag{6.101}$$

$$\leq 1 + n\epsilon H(X) + \Pr(\mu(X^n,U^n)=1)I(X^n;U^n|\mu(X^n,U^n)=1) \tag{6.102}$$

$$\leq 1 + n\epsilon H(X) + I(X^n;U^n|\mu(X^n,U^n)=1) \tag{6.103}$$

$$= 1 + n\epsilon H(X)+$$

$$\sum_{(x^n,u^n)\in A_\epsilon^{(n)}(p(x,u))} p(x^n,u^n)\big[\log(p(x^n,u^n)) - \log(p(x^n)) - \log(p(u^n))\big] \tag{6.104}$$

$$\leq 1 + n\epsilon H(X)+$$

$$\sum_{(x^n,u^n)\in A_\epsilon^{(n)}(p(x,u))} np(x^n,u^n)\big[H(X) + H(U) - H(X,U) + 3\epsilon\big] \tag{6.105}$$

$$= 1 + n\epsilon H(X) + n(I(X;U) + 3\epsilon)\Pr(A_\epsilon^{(n)}(p(x,u))) \tag{6.106}$$

$$\leq 1 + n\epsilon H(X) + n(I(X;U) + 3\epsilon) \tag{6.107}$$

$$= 1 + n(I(X;U) + \epsilon(3 + H(X))) \tag{6.108}$$

where (6.102) follows from the fact that X^n is i.i.d. and (6.105) follows from the property of jointly typical sequences. This implies that,

$$\frac{1}{n} I(X^n;U^n) \leq I(X;U) + \frac{1}{n} + \epsilon(3 + H(X)) \tag{6.109}$$

$$= I(X;U) + \epsilon_n^{'} \tag{6.110}$$

where

$$\epsilon_n^{'} \triangleq \frac{1}{n} + \epsilon(3 + H(X)) \tag{6.111}$$

We therefore have the proof of (6.93). We remark here that this proof is similar to a technique used in equivocation computation for the degraded wiretap channel [68, Lemma 8], and for the interference and broadcast channels with confidential messages [42, Lemma 3].

Continuing from (6.94),

$$\lim_{n\to\infty}\frac{1}{n}H(X^n|s_U,m_X) \geq I(X;V|U) - \lim_{n\to\infty}\epsilon_n^{'} \tag{6.112}$$

$$= I(X;V|U) \tag{6.113}$$

$$\geq \min(I(X;V|U),R_y) \tag{6.114}$$

where in (6.113), we have used the fact that $\epsilon_n^{'} \to 0$ as $n \to \infty$, and (6.114) follows from the fact that $\min(I(X;V|U),R_y) \leq I(X;V|U)$. We therefore have

$$\Delta \leq \min(I(X;V|U),R_y) \tag{6.115}$$

is achievable. This completes the achievability part for the case of two-sided helper.

Converse

The only difference in the converse part for the case of two-sided helper is when deriving an upper bound on the equivocation rate of the eavesdropper:

$$H(X^n|J_x) = H(X^n,J_y|J_x) - H(J_y|X^n,J_x) \tag{6.116}$$

$$= H(J_y|J_x) - H(J_y|X^n,J_x) + H(X^n|J_x,J_y) \tag{6.117}$$

$$\leq I(X^n;J_y|J_x) + n\epsilon_n \tag{6.118}$$

$$= \sum_{i=1}^{n} I(X_i;J_y|J_x,X^{i-1}) + n\epsilon_n \tag{6.119}$$

$$= \sum_{i=1}^{n} I(X_i; J_y, X^{i-1}|J_x, X^{i-1}) + n\epsilon_n \tag{6.120}$$

$$= nI(X; V|U) + n\epsilon_n \tag{6.121}$$

where we have defined

$$V_i = (J_y, X^{i-1}) \tag{6.122}$$

$$U_i = (J_x, X^{i-1}) \tag{6.123}$$

and

$$X = X_Q, \quad Y = Y_Q, \quad V = (Q, V_Q), \quad U = (Q, U_Q) \tag{6.124}$$

We also have,

$$H(X^n|J_x) = H(X^n, J_y|J_x) - H(J_y|X^n, J_x) \tag{6.125}$$

$$= H(J_y|J_x) - H(J_y|X^n, J_x) + H(X^n|J_x, J_y) \tag{6.126}$$

$$\leq H(J_y|J_x) + n\epsilon_n \tag{6.127}$$

$$\leq H(J_y) + n\epsilon_n \tag{6.128}$$

$$\leq nR_y + n\epsilon_n \tag{6.129}$$

This implies

$$\Delta \leq \min(I(X;V|U), R_y) \tag{6.130}$$

The joint distribution of the involved random variables is as follows,

$$p^{out}(x,y,v,u) = p(x,y)p(v|y)p^{out}(u|x,v,y) \tag{6.131}$$

Note that in the achievability proof of Theorem 6.2, joint distributions of the following form are permitted,

$$p^{ach}(x,y,v,u) = p(x,y)p(v|y)p^{ach}(u|x,v) \tag{6.132}$$

i.e, we have the Markov chain, $Y \rightarrow (X,V) \rightarrow U$. With the definition of V and U as in (6.122)-(6.123), these random variables do not satisfy this Markov chain. This implies that what we have shown so far is the following,

$$\mathcal{R}_{2-sided} \subseteq \mathcal{R}_{out} \tag{6.133}$$

where

$$\mathcal{R}_{out} = \Big\{(R_x, R_y, \Delta) : R_x \geq H(X|V) \tag{6.134}$$

$$R_y \geq I(Y;V) \tag{6.135}$$

$$\Delta \leq \min(I(X;V|U), R_y)\Big\} \tag{6.136}$$

where the joint distribution of the involved random variables is as given in (6.131).

However, we observe that the term $I(X;V|U)$ depends only on the marginal $p^{out}(u|x,v)$. Similarly, the terms $H(X|V)$ and $I(X;V)$ depend only on the marginal $p(x,v)$. We use these observations to show that the region $\mathcal{R}_{out}$ is the same when it is evaluated using the joint distributions of the form given in (6.132). This is clear by noting that once we are given a distribution of the form given in (6.131), we can construct a new distribution of the form given in (6.132) with the same rate expressions. Consider any distribution $p^{out}(x,y,v,u)$ of the form given in (6.131). Using $p^{out}(x,y,v,u)$, compute the marginal $p^{out}(u|x,v)$ as,

$$p^{out}(u|x,v) = \frac{\sum_y p^{out}(x,y,u,v)}{p(x,v)} \tag{6.137}$$

We now construct a distribution $p^{ach}(x,y,v,u) \in \mathcal{P}_{ach}$ as,

$$p^{ach}(x,y,v,u) = p(x,y)p(v|y)p^{out}(u|x,v) \tag{6.138}$$

such that the terms $I(X;V|U)$, $H(X|V)$ and $I(X;V)$ are the same whether they are evaluated according to $p^{out}(x,y,v,u)$ or according to $p^{ach}(x,y,v,u)$. Therefore, we conclude that it suffices to consider input distributions satisfying the Markov chain $Y \to (X,V) \to U$ when evaluating $\mathcal{R}_{out}$ and hence $\mathcal{R}_{out} = \mathcal{R}_{ach}$. This completes the converse part.

Returning to the remark at the end of Section 6.9.1, we observed that the converse for Theorem 6.1 can be proved by defining V_i as (J_y, X^{i-1}) or as (J_y, Y^{i-1}). On the

other hand, we are only able to prove the converse for Theorem 6.2 by defining $V_i = (J_y, X^{i-1})$. This is same as the definition of V_i as in [59], [47].

We therefore have two similarities with the converse for the rate-distortion function with common coded side information [33], [59], [47]: the first being the definition of V_i, and the second being the equivalence of $\mathcal{R}_{out}$ when evaluated according to (6.131) or according to (6.132).

6.9.3 Proof of Theorem 6.3

Achievability

Fix the distribution $p(x, y, w, z, v_1, v_2, u) = p(x, y)p(w, z|x)p(v_1, v_2|y)p(u|x, v_1, v_2)$.

1. Codebook generation at Helen: From the conditional probability distribution $p(v_1, v_2|y)$ compute $p(v_1) = \sum_{(y,v_2)} p(y)p(v_1, v_2|y)$ and $p(v_2) = \sum_{(y,v_1)} p(y)p(v_1, v_2|y)$. Generate $2^{nI(V_1;Y)}$ sequences $v_1(l)$ independently according to $\prod_{i=1}^{n} p(v_{1i})$, where $l = 1, \ldots, 2^{nI(V_1;Y)}$. Bin these sequences uniformly and independently in $2^{n(I(V_1;Y)-I(V_1;W))}$ bins. Denote the bin index of the sequence $v_1(l)$ as $b_{V_1}(v_1(l))$.

   Next generate $2^{nI(V_2;Y,V_1)}$ sequences $v_2(j)$ independently according to $\prod_{i=1}^{n} p(v_{2i})$, where $j = 1, \ldots, 2^{nI(V_2;Y,V_1)}$. Bin these sequences uniformly and independently in $2^{n(I(V_2;Y,V_1)-I(V_2;W,V_1))}$ bins. Denote the bin index of the sequence $v_2(j)$ as $b_{V_2}(v_2(j))$.

2. Codebook generation at Alice: From the distribution $p(u|x, v_1, v_2)$, compute

$p(u)$. Generate $2^{nI(X,V_1,V_2;U)}$ sequences $u(s)$ independently according to $\prod_{i=1}^{n} p(u_i)$, where $s = 1, \ldots, 2^{nI(X,V_1,V_2;U)}$. Next, bin these sequences uniformly into $2^{n(I(X,V_1,V_2;U)-I(W,V_1,V_2;U))}$ bins.

Also, randomly bin the x^n sequences into $2^{nH(X|U,V_1,V_2,W)}$ bins and index these bins as $m = 1, \ldots, 2^{nH(X|U,V_1,V_2,W)}$.

3. Encoding at Helen: On observing the sequence y^n, Helen tries to find a sequence $v_1(l)$ such that $(v_1(l), y^n)$ are jointly typical. From rate-distortion theory, we know that there exists one such sequence. Helen sends the bin index $b_{V_1}(v_1(l))$ of the sequence $v_1(l)$ on the secure link which is received by Alice and Bob.

   Helen also finds a sequence $v_2(j)$ such that $(v_1(l), v_2(j), y^n)$ are jointly typical. From rate-distortion theory, we know that there exists one such sequence. Helen sends the bin index $b_{V_2}(v_2(j))$ of the sequence $v_2(j)$ on the insecure link which is received by Alice, Bob and Eve.

4. Encoding at Alice: On observing the sequence x^n, Alice first finds the bin index m_X in which the sequence x^n falls. Alice also receives the bin indices $b_{V_1}(v_1(l))$ and $b_{V_2}(v_2(j))$ from Helen. She first looks for a unique $\hat{v}_1(l)$ in the bin $b_{V_1}(v_1(l))$ such that $(x^n, \hat{v}_1(l))$ are jointly typical. Alice can estimate the correct sequence $v_1(l)$ as long as the number of sequences in each bin is less than $2^{nI(X;V_1)}$. Note from the codebook generation step at Helen, that the number of v_1 sequences in each bin is approximately $2^{nI(V_1;Y)}/2^{n(I(V_1;Y)-I(V_1;W))} = 2^{nI(V_1;W)}$. Since $V_1 \to X \to W$ forms a Markov chain, we have $I(V_1;W) \leq I(V_1;X)$ and therefore the number of v_1 sequences in each bin is less than $2^{nI(X;V_1)}$ and

consequently Alice can estimate the correct sequence $v_1(l)$.

Using x^n and $\hat{v}_1(l)$, Alice looks for a unique $\hat{v}_2(j)$ in the bin $b_{V_2}(v_2(j))$ such that $(x^n, \hat{v}_1(l), \hat{v}_2(j))$ are jointly typical. Alice can estimate the correct sequence $v_2(j)$ as long as the number of sequences in each bin is less than $2^{nI(X,V_1;V_2)}$. The number of $v_2(j)$ sequences in each bin is $2^{nI(W,V_1;V_2)}$. From the Markov chain $W \rightarrow X \rightarrow (V_1, V_2)$, we have $I(W, V_1; V_2) \leq I(X, V_1; V_2)$ and therefore Alice can correctly estimate the sequence $v_2(j)$.

She next finds a sequence u such that $(u, \hat{v}_1(l), \hat{v}_2(j), x^n)$ are jointly typical. Let the bin index of this resulting u sequence be s_U.

Alice transmits the pair (s_U, m_X) which is received by Bob and Eve. The total rate used by Alice is $I(X; U|V_1, V_2, W) + H(X|U, V_1, V_2, W) = H(X|V_1, V_2, W)$.

5. Decoding at Bob: On receiving the pair (s_U, m_X) from Alice and the bin indices $b_{V_1}(v_1(l))$ and $b_{V_2}(v_2(j))$ from Helen, Bob looks for a unique $\hat{v}_1(l)$ in the bin $b_V(v_1(l))$ such that $(w^n, \hat{v}_1(l))$ are jointly typical. He can estimate the correct sequence $v_1(l)$ with high probability since the number of v_1 sequences in each bin is approximately $2^{nI(V_1;W)}$. Using the estimate $\hat{v}_1(l)$ and w^n, he looks for a unique $\hat{v}_2(j)$ in the bin $b_{V_2}(v_2(j))$ such that $(w^n, \hat{v}_1(l)), \hat{v}_2(j))$ are jointly typical. With high probability, the correct sequence $v_2(j)$ can be decoded by Bob since the number of v_2 sequences in each bin is approximately $2^{nI(V_2;W|V_1)}$.

He next searches the bin s_U for a sequence $\hat{u}$ such that $(\hat{u}, \hat{v}_1(l), \hat{v}_2(j), w^n)$ are jointly typical. Since the number of u sequences in each auxiliary bin is approximately $2^{nI(X,V_1,V_2;U)}/2^{n(I(X,V_1,V_2;U)-I(W,V_1,V_2;U))}$ which is $2^{nI(W,V_1,V_2;U)}$, with high

probability, Bob will be able to obtain the correct u sequence.

Using the estimates $\hat{u}$, $\hat{v}_1(l)$, and $\hat{v}_2(j)$, Bob searches for a unique x^n sequence in the bin m_X such that $(\hat{u}, \hat{v}_1(l), \hat{v}_2(j), w^n, x^n)$ are jointly typical. This is possible since the number of x^n sequences in each bin is approximately $2^{nH(X)}/2^{nH(X|U,V_1,V_2,W)}$, i.e., $2^{nI(U,V_1,V_2,W;X)}$. Therefore, Bob can correctly decode the x^n sequence with high probability.

6. Equivocation:

$$H(X^n|s_U, m_X, b_{V_2}, Z^n) = H(X^n, m_X, s_U, b_{V_2}|Z^n) - H(m_X, s_U, b_{V_2}|Z^n) \tag{6.139}$$

$$= H(X^n|Z^n) + H(m_X, s_U, b_{V_2}|X^n, Z^n) - H(m_X, s_U, b_{V_2}|Z^n) \tag{6.140}$$

$$= H(X^n|Z^n) + H(s_U, b_{V_2}|X^n, Z^n) - H(m_X, s_U, b_{V_2}|Z^n) \tag{6.141}$$

$$\geq H(X^n|Z^n) + H(s_U, b_{V_2}|X^n, Z^n) - H(m_X|Z^n) - H(s_U, b_{V_2}|Z^n) \tag{6.142}$$

$$\geq H(X^n|Z^n) + H(s_U, b_{V_2}|X^n, Z^n) - H(m_X) - H(s_U, b_{V_2}|Z^n) \tag{6.143}$$

$$\geq H(X^n|Z^n) + H(s_U, b_{V_2}|X^n, Z^n) - nH(X|U, V_1, V_2, W) - H(s_U, b_{V_2}|Z^n) \tag{6.144}$$

$$= H(X^n|Z^n) - I(s_U, b_{V_2}; X^n|Z^n) - nH(X|U, V_1, V_2, W) \tag{6.145}$$

$$\geq H(X^n|Z^n) - I(U^n, V_2^n; X^n|Z^n) - nH(X|U, V_1, V_2, W) \tag{6.146}$$

$$\geq H(X^n|Z^n) - nI(U, V_2; X|Z) - nH(X|U, V_1, V_2, W) - n\epsilon_n^{'} \tag{6.147}$$

$$= nH(X|Z) - nI(U, V_2; X|Z) - nH(X|U, V_1, V_2, W) - n\epsilon_n^{'} \tag{6.148}$$

$$= n(H(X|U, V_2, Z) - H(X|U, V_1, V_2, W)) - n\epsilon_n^{'} \tag{6.149}$$

$$= n(I(X; V_1|U, V_2, W) + I(X; W|U, V_2) - I(X; Z|U, V_2)) - n\epsilon_n^{'} \tag{6.150}$$

where (6.141) follows from the fact that m_X is the bin index of the sequence X^n, (6.142) and (6.143) follow from the fact that conditioning reduces entropy, (6.144) follows from the fact that $H(m_X) \leq \log(2^{nH(X|U,V_1,V_2,W)})$, (6.146) follows from the fact that s_U is the bin index of the sequence U^n and b_{V_2} is the bin index of the sequence V_2^n. We will prove (6.147) as follows. Let us define a random variable $\mu(X^n, Z^n, U^n, V_2^n)$, as follows,

$$\mu(x^n, z^n, u^n, v_2^n) = \begin{cases} 1, & \text{if } (x^n, z^n, u^n, v_2^n) \in A_\epsilon^{(n)}(p(x, z, u, v_2)); \\ 0, & \text{otherwise.} \end{cases} \tag{6.151}$$

where $A_\epsilon^{(n)}(p(x, z, u, v_2))$ is the set of typical (x^n, z^n, u^n, v_2^n) sequences with respect to $p(x, z, u, v_2)$ [14]. We now prove (6.147) as follows,

$$I(X^n; U^n, V_2^n|Z^n) \leq I(X^n; U^n, V_2^n, \mu(X^n, Z^n, U^n, V_2^n)|Z^n) \tag{6.152}$$

$$= I(X^n; \mu(X^n, Z^n, U^n, V_2^n)|Z^n) +$$

$$I(X^n; U^n, V_2^n|Z^n, \mu(X^n, Z^n, U^n, V_2^n)) \tag{6.153}$$

$$\leq H(\mu(X^n, Z^n, U^n, V_2^n)) + I(X^n; U^n, V_2^n|Z^n, \mu(X^n, Z^n, U^n, V_2^n)) \tag{6.154}$$

$$\leq 1 + I(X^n; U^n, V_2^n|Z^n, \mu(X^n, Z^n, U^n, V_2^n)) \tag{6.155}$$

$$= 1 + \Pr(\mu = 0) I(X^n; U^n, V_2^n|Z^n, \mu = 0) +$$

$$\Pr(\mu = 1) I(X^n; U^n, V_2^n|Z^n, \mu = 1) \tag{6.156}$$

$$\leq 1 + \Pr(\mu = 0) H(X^n|Z^n) +$$

$$\Pr(\mu = 1) I(X^n; U^n, V_2^n|Z^n, \mu = 1) \tag{6.157}$$

$$\leq 1 + n\epsilon H(X|Z) + \Pr(\mu = 1) I(X^n; U^n, V_2^n|Z^n, \mu = 1) \tag{6.158}$$

$$\leq 1 + n\epsilon H(X|Z) + I(X^n; U^n, V_2^n|Z^n, \mu = 1) \tag{6.159}$$

$$= 1 + n\epsilon H(X|Z) +$$

$$\sum_{(x^n, z^n, u^n, v_2^n) \in A_\epsilon^{(n)}(p(x,u,v_2|z))} p(x^n, u^n, v_2^n, z^n) \big[\log(p(x^n, u^n, v_2^n|z^n)) -$$

$$\log(p(x^n|z^n)) - \log(p(u^n, v_2^n|z^n))\big] \tag{6.160}$$

$$\leq 1 + n\epsilon H(X|Z) +$$

$$\sum_{(x^n, z^n, u^n, v_2^n) \in A_\epsilon^{(n)}(p(x,u,v_2|z))} np(x^n, u^n, v_2^n, z^n) \big[H(X|Z) +$$

$$H(U, V_2|Z) - H(X, U, V_2|Z) + 3\epsilon\big] \tag{6.161}$$

$$= 1 + n\epsilon H(X|Z) + n(I(X; U, V_2|Z) + 3\epsilon) \Pr(A_\epsilon^{(n)}(p(x, z, u, v_2))) \tag{6.162}$$

$$\leq 1 + n\epsilon H(X|Z) + n(I(X; U, V_2|Z) + 3\epsilon) \tag{6.163}$$

$$= 1 + n(I(X; U, V_2|Z) + \epsilon(3 + H(X|Z))) \tag{6.164}$$

where (6.158) follows from the fact that the pair (X^n, Z^n) is i.i.d. and (6.161) follows from the property of jointly typical sequences. This implies that,

$$\frac{1}{n} I(X^n; s_U, b_{V_2} | Z^n) \leq I(X; U, V_2 | Z) + \frac{1}{n} + \epsilon(3 + H(X|Z)) \tag{6.165}$$

$$= I(X; U, V_2 | Z) + \epsilon_n^{'} \tag{6.166}$$

where

$$\epsilon_n^{'} \triangleq \frac{1}{n} + \epsilon(3 + H(X|Z)) \tag{6.167}$$

This completes the proof of (6.147).

Continuing from (6.150), we have,

$$\lim_{n\to\infty} \frac{1}{n} H(X^n | s_U, m_X, b_{V_2}, Z^n) \geq I(X; V_1 | U, V_2, W) + I(X; W|U, V_2) - I(X; Z|U, V_2) - \lim_{n\to\infty} \epsilon_n^{'} \tag{6.168}$$

$$= I(X; V_1 | U, V_2, W) + I(X; W|U, V_2) - I(X; Z|U, V_2) \tag{6.169}$$

$$\geq \min(R_{sec}, I(X; V_1 | U, V_2, W)) + I(X; W|U, V_2) - I(X; Z|U, V_2) \tag{6.170}$$

This completes the achievability part.

Converse

Let the coded outputs of the helper be denoted as (J_{sec}, J_{ins}), where J_{sec} denotes the coded output of the secure link, J_{ins} denotes the coded output of the insecure link, and the output of Alice be denoted as J_x, i.e.,

$$(J_{sec}, J_{ins}) = f_y(Y^n) \qquad \text{and} \qquad J_x = f_x(X^n, J_{sec}, J_{ins}) \tag{6.171}$$

First note that, for noiseless reconstruction of the sequence X^n at Bob, we have by Fano's inequality

$$H(X^n|J_x, J_{sec}, J_{ins}, W^n) \leq n\epsilon_n \tag{6.172}$$

We start by obtaining a lower bound on R_x, the rate of Alice, as follows,

$$\begin{aligned}
nR_x &\geq H(J_x) && (6.173)\\
&\geq H(J_x|J_{sec}, J_{ins}, W^n) && (6.174)\\
&= H(X^n, J_x|J_{sec}, J_{ins}, W^n) - H(X^n|J_x, J_{sec}, J_{ins}, W^n) && (6.175)\\
&\geq H(X^n, J_x|J_{sec}, J_{ins}, W^n) - n\epsilon_n && (6.176)\\
&\geq H(X^n|J_{sec}, J_{ins}, W^n) - n\epsilon_n && (6.177)\\
&= \sum_{i=1}^{n} H(X_i|X^{i-1}, J_{sec}, J_{ins}, W^n) - n\epsilon_n && (6.178)\\
&= \sum_{i=1}^{n} H(X_i|J_{sec}, J_{ins}, X^{i-1}, W_{i+1}^n, W_i) - n\epsilon_n && (6.179)
\end{aligned}$$

$$\geq \sum_{i=1}^{n} H(X_i|J_{sec}, J_{ins}, Y^{i-1}, X^{i-1}, W_{i+1}^n, W_i) - n\epsilon_n \tag{6.180}$$

$$= \sum_{i=1}^{n} H(X_i|V_{1i}, V_{2i}, W_i) - n\epsilon_n \tag{6.181}$$

$$= nH(X|V_1, V_2, W) - n\epsilon_n \tag{6.182}$$

where (6.176) follows by (6.172) and (6.179) follows from the following Markov chain,

$$W^{i-1} \rightarrow (J_{sec}, J_{ins}, X^{i-1}, W_{i+1}^n, W_i) \rightarrow X_i \tag{6.183}$$

In (6.181), we have defined

$$V_{1i} = (J_{sec}, Y^{i-1}, X^{i-1}, W_{i+1}^n) \tag{6.184}$$

$$V_{2i} = J_{ins} \tag{6.185}$$

We next obtain a lower bound on R_{sec}, the rate of the secure link,

$$nR_{sec} \geq H(J_{sec}) \tag{6.186}$$

$$\geq H(J_{sec}|W^n) \tag{6.187}$$

$$\geq I(J_{sec}; Y^n|W^n) \tag{6.188}$$

$$= \sum_{i=1}^{n} I(J_{sec}, Y^{i-1}, W^{i-1}, W_{i+1}^n; Y_i|W_i) \tag{6.189}$$

$$= \sum_{i=1}^{n} I(J_{sec}, Y^{i-1}, W_{i+1}^n; Y_i|W_i) \tag{6.190}$$

$$= \sum_{i=1}^{n} I(J_{sec}, Y^{i-1}, X^{i-1}, W_{i+1}^n; Y_i|W_i) \tag{6.191}$$

$$= \sum_{i=1}^{n} I(V_{1i}; Y_i|W_i) \tag{6.192}$$

$$= nI(V_1; Y|W) \tag{6.193}$$

where (6.190) and (6.191) follow from the Markov chain

$$(X^{i-1}, W^{i-1}) \rightarrow (J_{sec}, Y^{i-1}, W_{i+1}^n) \rightarrow Y_i \tag{6.194}$$

Next, we provide a lower bound on R_{ins}, the rate of the insecure link,

$$nR_{ins} \geq H(J_{ins}) \tag{6.195}$$

$$\geq H(J_{ins}|J_{sec}, W^n) \tag{6.196}$$

$$\geq H(J_{ins}|J_{sec}, W^n) - H(J_{ins}|J_{sec}, Y^n) \tag{6.197}$$

$$= I(J_{ins}; Y^n|J_{sec}) - I(J_{ins}; W^n|J_{sec}) \tag{6.198}$$

$$= \sum_{i=1}^{n} I(J_{ins}; Y_i|J_{sec}, Y^{i-1}, W_{i+1}^n) - I(J_{ins}; W_i|J_{sec}, Y^{i-1}, W_{i+1}^n) \tag{6.199}$$

$$= \sum_{i=1}^{n} I(J_{ins}; Y_i|J_{sec}, Y^{i-1}, X^{i-1}W_{i+1}^n) - I(J_{ins}; W_i|J_{sec}, Y^{i-1}, X^{i-1}, W_{i+1}^n) \tag{6.200}$$

$$= \sum_{i=1}^{n} I(V_{2i}; Y_i|V_{1i}) - I(V_{2i}; W_i|V_{1i}) \tag{6.201}$$

$$= \sum_{i=1}^{n} I(V_{2i}; Y_i|W_i, V_{1i}) \tag{6.202}$$

$$= nI(V_2; Y|W, V_1) \tag{6.203}$$

where (6.199) follows from the Csiszar's sum lemma [16], and (6.200) follows from

the following Markov chain,

$$X^{i-1} \rightarrow (J_{sec}, Y^{i-1}, W_{i+1}^n) \rightarrow (J_{ins}, Y_i, W_i) \tag{6.204}$$

We now have the main step, i.e., an upper bound on the equivocation rate of the eavesdropper,

$$H(X^n|J_x, J_{ins}, Z^n) = H(X^n, Z^n|J_x, J_{ins}) - H(Z^n|J_x, J_{ins}) \tag{6.205}$$

$$= H(X^n, W^n, J_{sec}, Z^n|J_x, J_{ins}) - H(Z^n|J_x, J_{ins})$$

$$- H(W^n, J_{sec}|X^n, Z^n, J_x, J_{ins}) \tag{6.206}$$

$$= H(W^n, J_{sec}|J_x, J_{ins}) + H(X^n|W^n, J_x, J_{sec}, J_{ins}) + H(Z^n|X^n, W^n)$$

$$- H(Z^n|J_x, J_{ins}) - H(W^n|X^n, Z^n) - H(J_{sec}|X^n, J_x, J_{ins}, W^n) \tag{6.207}$$

$$= (H(W^n|J_x, J_{ins}) - H(Z^n|J_x, J_{ins})) - (H(W^n|X^n, Z^n)$$

$$- H(Z^n|X^n, W^n)) + I(J_{sec}; X^n|J_x, J_{ins}, W^n)$$

$$+ H(X^n|W^n, J_x, J_{sec}, J_{ins}) \tag{6.208}$$

$$\leq (H(W^n|J_x, J_{ins}) - H(Z^n|J_x, J_{ins})) - (H(W^n|X^n, Z^n)$$

$$- H(Z^n|X^n, W^n)) + I(J_{sec}; X^n|J_x, J_{ins}, W^n) + n\epsilon_n \tag{6.209}$$

where (6.207) follows from the Markov chain $Y^n \rightarrow X^n \rightarrow (W^n, Z^n)$ and (6.209)

follows by (6.172). Now, using Csiszar's sum lemma [16], we have

$$H(W^n|J_x, J_{ins}) - H(Z^n|J_x, J_{ins}) = \sum_{i=1}^{n} H(W_i|Z^{i-1}, W_{i+1}^n, J_x, J_{ins}) - \sum_{i=1}^{n} H(Z_i|Z^{i-1}, W_{i+1}^n, J_x, J_{ins}) \quad (6.210)$$

and we also have,

$$H(W^n|X^n, Z^n) - H(Z^n|X^n, W^n) = H(W^n|X^n) - H(Z^n|X^n) \quad (6.211)$$

$$= \sum_{i=1}^{n} H(W_i|X_i) - \sum_{i=1}^{n} H(Z_i|X_i) \quad (6.212)$$

$$= \sum_{i=1}^{n} H(W_i|X_i, Z^{i-1}, W_{i+1}^n, J_x, J_{ins}) - \sum_{i=1}^{n} H(Z_i|X_i, Z^{i-1}, W_{i+1}^n, J_x, J_{ins}) \quad (6.213)$$

where (6.212) follows from the memorylessness of the sources and (6.213) follows from the Markov chain $Y^n \to X^n \to (W^n, Z^n)$. Now, defining,

$$U_i = (J_x, Z^{i-1}, W_{i+1}^n) \quad (6.214)$$

and

$$X = X_Q, \quad Y = Y_Q, \quad Z = Z_Q, \quad W = W_Q \quad (6.215)$$

$$V_1 = (Q, V_{1Q}), \quad V_2 = (Q, V_{2Q}), \quad U = (Q, U_Q) \quad (6.216)$$

we have from (6.210) and (6.213),

$$H(W^n|J_x, J_{ins}) - H(Z^n|J_x, J_{ins}) = n(H(W|U, V_2) - H(Z|U, V_2)) \tag{6.217}$$

$$H(W^n|X^n, Z^n) - H(Z^n|X^n, W^n) = n(H(W|X, U, V_2) - H(Z|X, U, V_2)) \tag{6.218}$$

Now consider,

$$\begin{aligned}
I(J_{sec}; X^n|J_x, J_{ins}, W^n) &= \sum_{i=1}^{n} I(J_{sec}; X_i|J_x, J_{ins}, W^n, X^{i-1}) && (6.219)\\
&= \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, W^n, X^{i-1}) \\
&\quad - \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, J_{sec}, W^n, X^{i-1}) && (6.220)\\
&= \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, W_i, X^{i-1}, W_{i+1}^n) \\
&\quad - \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, J_{sec}, W_i, X^{i-1}, W_{i+1}^n) && (6.221)\\
&= \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, W_i, X^{i-1}, Z^{i-1}, W_{i+1}^n) \\
&\quad - \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, J_{sec}, W_i, X^{i-1}, Z^{i-1}, W_{i+1}^n) && (6.222)\\
&\leq \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, W_i, Z^{i-1}, W_{i+1}^n) \\
&\quad - \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, J_{sec}, W_i, X^{i-1}, Z^{i-1}, W_{i+1}^n) && (6.223)\\
&\leq \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, W_i, Z^{i-1}, W_{i+1}^n) \\
&\quad - \sum_{i=1}^{n} H(X_i|J_x, J_{ins}, J_{sec}, W_i, X^{i-1}, Y^{i-1}, Z^{i-1}, W_{i+1}^n) \\
& && (6.224)
\end{aligned}$$

$$= \sum_{i=1}^{n} H(X_i|U_i, W_i, V_{2i}) - \sum_{i=1}^{n} H(X_i|U_i, W_i, V_{2i}, V_{1i}) \tag{6.225}$$

$$= \sum_{i=1}^{n} I(X_i; V_{1i}|W_i, U_i, V_{2i}) \tag{6.226}$$

$$= nI(X; V_1|W, U, V_2) \tag{6.227}$$

We also have

$$I(J_{sec}; X^n|J_x, J_{ins}, W^n) \leq H(J_{sec}) \tag{6.228}$$

$$\leq nR_{sec} \tag{6.229}$$

Therefore, we have

$$I(J_{sec}; X^n|J_x, J_{ins}, W^n) \leq n \min(R_{sec}, I(X; V_1|W, U, V_2)) \tag{6.230}$$

Finally, on substituting (6.217), (6.218) and (6.230) in (6.209), we arrive at

$$H(X^n|J_x, J_{ins}, Z^n) \leq n(\min(R_{sec}, I(X; V_1|W, U, V_2)) + I(X; W|U, V_2)$$

$$- I(X; Z|U, V_2) + \epsilon_n) \tag{6.231}$$

This implies

$$\Delta \leq \min(R_{sec}, I(X; V_1|W, U, V_2)) + I(X; W|U, V_2) - I(X; Z|U, V_2) \tag{6.232}$$

Also note that the following is a Markov chain,

$$(V_1, V_2) \rightarrow Y \rightarrow X \rightarrow (W, Z) \tag{6.233}$$

Therefore, the joint distribution of the involved random variables is

$$p^{out}(x, y, w, z, v_1, v_2, u) = p(x, y)p(w, z|x)p(v_1, v_2|y)p(u|x, v_1, v_2, y) \tag{6.234}$$

On the other hand, the joint distribution of the involved random variables in the achievability proof of Theorem 6.3 is in the following form,

$$p^{ach}(x, y, w, z, v_1, v_2, u) = p(x, y)p(w, z|x)p(v_1, v_2|y)p(u|x, v_1, v_2) \tag{6.235}$$

i.e., they satisfy the Markov chain $Y \rightarrow (X, V_1, V_2) \rightarrow U$. Now using the observation that $I(X; W|U, V_1, V_2)$ depends on the marginal $p(x, w, u, v_1, v_2)$ and $I(X; Z|U, V_1, V_2)$ depends on the marginal $p(x, z, u, v_1, v_2)$ and using similar arguments used in the converse proof of Theorem 6.2, it can be shown that it suffices to consider distributions of the form given in (6.235) when evaluating our outer bound. This completes the proof of the converse part.

Chapter 7

Conclusions

In this dissertation, we studied three important aspects of wireless networks, namely feedback, relaying and cooperation. Feedback and user cooperation are two important phenomena which need to be investigated to obtain performance limits for wireless networks. For this purpose, we studied the multiple access channel and the interference channel with generalized feedback and developed new outer bounds on the respective capacity regions. We focused on several forms of feedback, namely, noiseless feedback, noisy feedback and user cooperation. For the Gaussian multi-user channels with feedback and cooperation, we proposed a new approach to deal with auxiliary random variables. Our approach sheds light on the shortcomings of the maximum entropy theorem when dealing with noisy feedback and user cooperation models. Furthermore, we believe that this approach can be useful for other problems in multi-user information theory.

We studied the effects of relaying by first considering a special class of primitive relay channels. We focused on the state-dependent channel, where a relay can observe the channel state and help in data transmission by communicating the channel state through an orthogonal finite-capacity link to the receiver. We obtained a new outer

bound on the capacity of this channel and showed that this bound also yields a new capacity result. We studied another variation of this problem, where the channel state information is available to the transmitter in a rate-limited manner.

In several communication scenarios, it might be the case that there is no direct link between the transmitter and the receiver. Therefore, any communication between them is possible only through the help of intermediate relay nodes. This scenario is modelled by the parallel relay network or the diamond channel. We studied the class of diamond channels, where the source is connected to the relays through an arbitrary memoryless broadcast channel and the relays communicate to the destination through an orthogonal multiple access channel. For this model, we established the capacity when the broadcast channel is deterministic. We also studied the model where the relays are partially separated from each other and established the capacity for two sub-classes of such channels. Using this result, we showed that feedback from the destination to the relays can strictly increase the capacity of the diamond channel.

In several sensor network scenarios, involving distributed compression of sources, there might be adversarial nodes. The goal is to transmit the source reliably to the legitimate nodes but leak as little information as possible to the adversarial nodes. To take this into account, we considered information theoretic secrecy, where we aim to limit the information leakage to the eavesdropper. For this purpose, we considered a secure source coding problem with coded side information from a helper to the legitimate user. We first provided the characterization of the rate-equivocation region for this problem. We generalized this result for two different models with increasing complexity. We characterized the rate-equivocation region for the case of two-sided

helper. For this model, we showed that Slepian-Wolf binning alone is insufficient and using our achievable scheme, one attains strictly larger equivocation at the eavesdropper than the case of one-sided helper. We also considered the situation when there are both secure and insecure rate-limited links from the helper and characterized the rate-equivocation region.

BIBLIOGRAPHY

[1] R. Ahlswede. Multi-way communication channels. In *Proc. 2nd Int. Symp. Inform. Theory*, Tsahkadsor, Armenian, S.S.R., 1971.

[2] R. Ahlswede and T. S. Han. On source coding with side information via a multiple-access channel and related problems in multi-user information theory. *IEEE Trans. on Information Theory*, 29(3):396–412, May 1983.

[3] R. Ahlswede and J. Korner. Source coding with side information and a converse for degraded broadcast channels. *IEEE Trans. on Information Theory*, 21(6):629–637, Nov 1975.

[4] M. Aleksic, P. Razaghi, and W. Yu. Capacity of a class of modulo-sum relay channels. *IEEE Trans. on Information Theory*, 55(3):921–930, March 2009.

[5] S. Boyd and L. Vandenberghe. *Convex Optimization*. Cambridge University Press, 2004.

[6] S. I. Bross and A. Lapidoth. An improved achievable rate region for the discrete memoryless two-user multiple-access channel with noiseless feedback. *IEEE Trans. on Information Theory*, 51(3):811–833, March 2005.

[7] S. I. Bross, A. Lapidoth, and M. Wigger. The Gaussian MAC with conferencing encoders. In *IEEE International Symposium on Information Theory*, July 2008.

[8] A. B. Carleial. Multiple-access channels with different genaralized feedback signals. *IEEE Trans. on Information Theory*, 28(6):841–850, November 1982.

[9] M. H. M. Costa. Writing on dirty paper. *IEEE Trans. on Information Theory*, 29(3):439–441, May 1983.

[10] M. H. M. Costa. A new entropy power inequality. *IEEE Trans. on Information Theory*, 31(6):751–760, Nov. 1985.

[11] T. M. Cover. The capacity of the relay channel. In *Open Problems in Communication and Computation*, pages 72–73, 1987.

[12] T. M. Cover and A. El Gamal. Capacity theorems for the relay channel. *IEEE Trans. on Information Theory*, 25(5):572–584, September 1979.

[13] T. M. Cover and C. S. K. Leung. An achievable rate region for the multiple access channel with feedback. *IEEE Trans. on Information Theory*, 27(3):292–298, May 1981.

[14] T. M. Cover and J. A. Thomas. *Elements of Information Theory*. New York:Wiley, 1991.

[15] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. on Information Theory*, 24(3):339–348, May 1978.

[16] I. Csiszar and J. Korner. *Information Theory: Coding Theorems for Discrete Memoryless Systems*. Academic Press, 1981.

[17] I. Csiszar and P. Narayan. Common randomness and secret key generation with a helper. *IEEE Trans. on Information Theory*, 46(2):344–366, March 2000.

[18] T. Ericson and J. Korner. Successive encoding of correlated sources. *IEEE Trans. on Information Theory*, 29(3):390–395, May 1983.

[19] N. Gaarder and J. Wolf. The capacity region of a multiple-access discrete memoryless channel can increase with feedback. *IEEE Trans. on Information Theory*, 21(1):100–102, Jan 1975.

[20] M. Gastpar and G. Kramer. On cooperation via noisy feedback. In *Int. Zurich Seminar on Communications (IZS)*, pages 146–149, February 2006.

[21] M. Gastpar and G. Kramer. On noisy feedback for interference channels. In *Proc. Asilomar Conf. on Signals, Systems, and Computers, Pacific Grove, CA, USA*, Oct. 29-Nov. 1 2006.

[22] S. I. Gelfand and M. S. Pinsker. Capacity of a broadcast channel with one deterministic component. *Problemy Peredachi Informatsii*, 16(1):24–34, 1980.

[23] S. I. Gelfand and M. S. Pinsker. Coding for channel with random parameters. *Problems of Control and Information Theory*, 9(1):19–31, 1980.

[24] L. Grokop, A. Sahai, and M. Gastpar. Discriminatory source coding for a noiseless broadcast channel. In *IEEE International Symposium on Information Theory*, 2005.

[25] D. Gunduz, E. Erkip, and H. V. Poor. Lossless compression with security constraints. In *IEEE International Symposium on Information Theory*, 2008.

[26] D. Gunduz, E. Erkip, and H. V. Poor. Secure lossless compression with side information. In *IEEE Information Theory Workshop*, 2008.

[27] T. S. Han. The capacity region for the deterministic broadcast channel with a common message. *IEEE Trans. on Information Theory*, 27(1):122–125, January 1981.

[28] T. S. Han and K. Kobayashi. A new achievable rate region for the interference channel. *IEEE Trans. on Information Theory*, 27(1):49–60, January 1981.

[29] C. Heegard and A. El Gamal. On the capacity of computer memory with defects. *IEEE Trans. on Information Theory*, 29(5):731–739, Sep. 1983.

[30] A. P. Hekstra and F. M. J. Willems. Dependence balance bounds for single output two-way channels. *IEEE Trans. on Information Theory*, 35(1):44–53, January 1989.

[31] A. Host-Madsen. Capacity bounds for cooperative diversity. *IEEE Trans. on Information Theory*, 52(4):1522–1544, April 2006.

[32] W. Kang and S. Ulukus. Capacity of a class of diamond channels. *Submitted to IEEE Trans. on Information Theory*, July 2008.

[33] A. Kaspi and T. Berger. Rate-distortion for correlated sources with partially separated encoders. *IEEE Trans. on Information Theory*, 28(6):828–840, Nov 1982.

[34] G. Keshet, Y. Steinberg, and N. Merhav. Channel coding in the presence of side information: subject review. *Foundations and Trends in Communications and Information Theory, NOW Publishers*, June 2008.

[35] Y-H. Kim. Coding techniques for primitive relay channels. In *Proc. Annual Allerton Conference on Communication, Control and Computing*, pages 129–135, 2007.

[36] Y-H. Kim. Capacity of a class of deterministic relay channels. *IEEE Trans. on Information Theory*, 54(3):1328–1329, Mar. 2008.

[37] G. Kramer. *Directed Information for Channels with Feedback*. Ph.D. dissertation, Swiss Federal Institute of Technology (ETH), Zurich, Switzerland, 1998.

[38] G. Kramer. Feedback strategies for a class of two-user multiple access channels. *IEEE Trans. on Information Theory*, 45(6):2054–2059, September 1999.

[39] G. Kramer. Capacity results for the discrete memoryless network. *IEEE Trans. on Information Theory*, 49(1):4–21, Jan. 2003.

[40] N. V. Kuznetsov and B. S. Tsybakov. Coding in memories with defective cells. *Problemy Peredachi Informatsii*, 10(2):52–60, 1974.

[41] H. Liao. *Multiple Access Channels*. Ph.D. Thesis, University of Hawaii, 1972.

[42] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy capacity regions. *IEEE Trans. on Information Theory*, 54(6):2493–2507, June 2008.

[43] W. Luh and D. Kundur. Distributed keyless secret sharing over noiseless channels. In *IEEE Global Communications Conference*, 2007.

[44] K. Marton. A coding theorem for the discrete memoryless broadcast channel. *IEEE Trans. on Information Theory*, 25:306–311, May 1979.

[45] L. Ozarow. The capacity of the white Gaussian multiple access channel with feedback. *IEEE Trans. on Information Theory*, 30(4):623–629, July 1984.

[46] M. Payaro and D. Palomar. A multivariate generalization of Costa's entropy power inequality. In *IEEE International Symposium on Information Theory*, July 2008.

[47] H. Permuter, Y. Steinberg, and T. Weissman. Problems we can solve with a helper. In *IEEE Information Theory Workshop*, 2009.

[48] V. Prabhakaran and K. Ramchandran. On secure distributed source coding. In *IEEE Information Theory Workshop*, 2007.

[49] I. Sason. On achievable rate regions for the Gaussian interference channel. *IEEE Trans. on Information Theory*, 50(6):1345–1356, June 2004.

[50] H. Sato. The capacity of the Gaussian interference channel under strong interference. *IEEE Trans. on Information Theory*, 27:786–788, November 1981.

[51] J. P. M. Schalkwijk and T. Kailath. A coding scheme for additive noise channels with feedback-Part I: No bandwidth constraint. *IEEE Trans. on Information Theory*, 12:172–182, April 1966.

[52] B. E. Schein. *Distributed Coordination in Network Information Theory.* Ph.D. Thesis, MIT, 2001.

[53] A. Sendonaris, E. Erkip, and B. Aazhang. User cooperation diversity–part I: System description. *IEEE Trans. on Communications*, 51(11):1927–1938, November 2003.

[54] C. E. Shannon. Communication theory of secrecy systems. *Bell System Technical Journal*, 28(4):656–715, October 1949.

[55] C. E. Shannon. Channels with side information at the transmitter. *IBM Journal Research and Development*, 2:289–293, 1958.

[56] C. E. Shannon. Two-way communication channels. In *Proc. 4th Berkeley Symp. Math. Stat. Prob.*, pages 611–644. University of California Press, Berkeley, 1961.

[57] D. Tuninetti. On interference channels with generalized feedback. In *IEEE International Symposium on Information Theory*, June 2007.

[58] E. C. van der Meulen. A survey of multi-way channels in information theory: 1961-1976. *IEEE Trans. on Information Theory*, 23(1):1–37, January 1977.

[59] D. Vasudevan and E. Perron. Cooperative source coding with encoder breakdown. In *IEEE International Symposium on Information Theory*, 2007.

[60] V. Venkatesan. Optimality of Gaussian inputs for a multi-access achievable rate region. *Semester Thesis, ETH Zurich, Switzerland*, June 2007.

[61] A. J. Vinck, W. L. M. Hoeks, and K. A. Post. On the capacity of the two-user M-ary multiple-access channel with feedback. *IEEE Trans. on Information Theory*, 31(4):540–543, July 1985.

[62] F. M. J. Willems. The feedback capacity region of a class of discrete memoryless multiple access channels. *IEEE Trans. on Information Theory*, 28(1):93–95, January 1982.

[63] F. M. J. Willems. On multiple access channels with feedback. *IEEE Trans. on Information Theory*, 30(6):842–845, November 1984.

[64] F. M. J. Willems and E. C. van der Meulen. The discrete memoryless multiple access channel with cribbing encoders. *IEEE Trans. on Information Theory*, 31:313 –327, May 1985.

[65] F. M. J. Willems, E. C. van der Meulen, and J. P. M. Schalkwijk. Achievable rate region for the multiple access channel with generalized feedback. In *Proc. Annual Allerton Conference on Communication, Control and Computing*, pages 284–292, 1983.

[66] H. S. Witsenhausen and A. D. Wyner. A conditional entropy bound for a pair of discrete random variables. *IEEE Trans. on Information Theory*, 21(5):493–501, September 1975.

[67] A. D. Wyner. On source coding with side information at the decoder. *IEEE Trans. on Information Theory*, 21(3):294–300, May 1975.

[68] A. D. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1335–1387, January 1975.

[69] A. D. Wyner and J. Ziv. A theorem on the entropy of certain binary sequences and applications-I. *IEEE Trans. on Information Theory*, 19(6):769–772, Nov 1973.

[70] Z. Zhang. Partial converse for the relay channel. *IEEE Trans. on Information Theory*, 34(5):1106–1110, September 1988.

[71] Z. Zhang, T. Berger, and J. P. M. Schalkwijk. New outer bounds to capacity regions of two-way channels. *IEEE Trans. on Information Theory*, 32(3):383–386, May 1986.