SRC TR 88-57

TECHNICAL
RESEARCH
REPORT

Deterministic Codes for Arbitrarily Varying Multiple-Access Channels

by

J.A. Gubner

SYSTEMS RESEARCH CENTER

UNIVERSITY OF MARYLAND

COLLEGE PARK, MARYLAND 20742

ABSTRACT

Title of Dissertation: Deterministic Codes for Arbitrarily Varying Multiple-Access Channels

John Alan Gubner, Doctor of Philosophy, 1988

Dissertation directed by: Prakash Narayan
Associate Professor
Electrical Engineering Department

The arbitrarily varying multiple-access channel (AVMAC) is a model of a multiple-access channel with unknown parameters. In 1981, Jahn characterized the capacity region of the AVMAC, *assuming that the region had a nonempty interior*; however, he did not address the problem of deciding whether or not the capacity region had a nonempty interior. Using the method of *types* and an approach completely different from Jahn's, we have partially solved this problem. We begin by introducing the simple but crucial notion of *symmetrizability* for the two-user AVMAC. We show that if an AVMAC is symmetrizable, then its capacity region has an empty interior. For the two-user AVMAC, this means that at least one (and perhaps both) users cannot reliably transmit information across the channel. More importantly, we show that if the channel is suitably *non*symmetrizable, then the capacity region has a nonempty interior, and both users can reliably transmit information across the channel. In light of these results, it is indeed fortunate that to test a channel for symmetrizability, one simply solves a system of linear equations whose coefficients are the channel transition probabilities.

Our proofs rely heavily on a rather complicated decoding rule. This leads us to seek conditions under which simpler multiple-message decoding techniques might

suffice. In particular, we give conditions under which the universal *maximum mutual information decoding rule* will be effective.

We then consider the situation in which a constraint is imposed on the sequence of "states" in which the channel can reside. We extend our approach to show that in the presence of a state constraint, the capacity region can increase dramatically. A striking example of this effect occurs with the *adder channel.* This channel is symmetrizable, and without a state constraint, neither user can reliably transmit information across the channel. However, if a suitable state constraint is imposed, each user can reliably transmit more than 0.4 bits of information per channel use.

ACKNOWLEDGEMENTS

I am deeply grateful to my advisor, Professor Narayan, for introducing me to the arbitrarily varying channel (AVC), and for suggesting that I investigate the behavior of the multiple-access AVC.

I am also grateful to Professor Imre Csiszár for his helpful suggestions during the initial stages of my analysis of the multiple-access AVC.

I thank Professors Makowski and Krishnaprasad for many technical and non-technical discussions during my studies. Both have always been generous with their time and their ideas. I thank Professor Slud for his careful reading of the dissertation and for his suggestions for improving its presentation. I thank Professor Farvardin for teaching the first course I took in information theory.

For helping me learn to use the graphics capabilities of DELIGHT, I thank Michael Fan and Professor Andre Tits. The graphics of DELIGHT were extremely useful in suggesting the analysis used to prove the inclusion (4.18).

I am very grateful to have been supported during my research by an IEEE Frank A. Cowan Scholarship and by fellowships from the Minta Martin Fund, the University of Maryland Graduate School, and the University of Maryland Systems Research Center.

Finally, I thank my parents for their support, encouragement, and understanding throughout my education.

TABLE OF CONTENTS

Page

List of Figures iv

1 Introduction 1

1.1 Multiple-Access Communication Systems 1

1.2 The Arbitrarily Varying Channel 7

1.3 Summary of Results 9

2 An Introduction to the Theory of Types 13

3 The Arbitrarily Varying Multiple-Access Channel 26

3.1 Introduction 26

3.2 Symmetrizability 30

3.3 Achievable Rates 37

3.4 Alternative Decoding Rules 57

3.5 Decoding Sets and Codeword Properties 62

4 State Constraints for the AVMAC 72

4.1 State Constraints 73

4.2 A Weak Converse 75

4.3 The Additive AVC 82

4.4 Forward Theorems 86

4.4.1 Nonsymmetrizable Channels 86

4.4.2 Symmetrizable Channels 87

5 Conclusions 99

Bibliography 102

LIST OF FIGURES

Number Page

1.1 A Multiple-Access Channel 1

1.2 A Multiple-Access Communication System 3

4.1 The Adder Channel Capacity Region Under a State Constraint 72

CHAPTER 1
INTRODUCTION

1.1 Multiple-Access Communication Systems

A multiple-access communication system is one in which several information sources transmit messages simultaneously over a common channel to a single receiver. We shall restrict our attention to systems with two sources, as our discussion can easily be extended to systems with an arbitrary number of sources.

Consider a situation in which two information sources, referred to as user 1 and user 2, wish to communicate simultaneously with a common receiver by using a *discrete multiple-access channel.* Schematically, a discrete multiple-access channel is a device which takes two n-tuples $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{X}^n$ and $\mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{Y}^n$ as inputs, and generates an output n-tuple, $\mathbf{z} = (z_1, \ldots, z_n) \in \mathcal{Z}^n$, where $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{Z}$ are finite sets, each containing at least two elements, and n is a positive integer (see Figure 1.1).

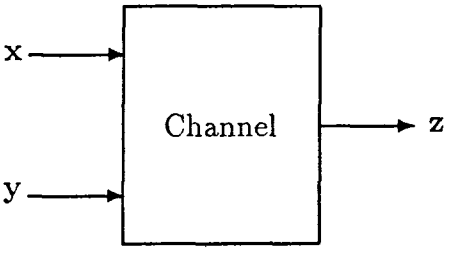

Figure 1.1: A Multiple-Access Channel.

Suppose that user 1 generates messages from the set $\{1, \ldots, N\}$, and that user 2 generates messages from the set $\{1, \ldots, M\}$, where N and M are positive integers. To transmit a message $i \in \{1, \ldots, N\}$, user 1 sends an n-tuple $\mathbf{x}_i \in \mathcal{X}^n$ over the

channel. Similarly, to transmit a message $j \in \{1,\ldots,M\}$, user 2 sends an n-tuple $\mathbf{y}_j \in \mathcal{Y}^n$ over the channel. At the output of the channel, the receiver observes the n-tuple $\mathbf{z}$ and constructs an estimate $(\hat{\imath},\hat{\jmath})$ of the actual messages sent, (i,j). To make these ideas precise, we make the following definition.

Definition 1.1 Let N, M, and n be positive integers. If f, g, and φ are mappings with

$$f : \{1,\ldots,N\} \to \mathcal{X}^n \qquad \text{and} \qquad g : \{1,\ldots,M\} \to \mathcal{Y}^n,$$

and

$$\varphi : \mathcal{Z}^n \to \{1,\ldots,N\} \times \{1,\ldots,M\},$$

then the triple (f,g,φ) is called a *code*. The mapping f is called an *encoder for user* 1; the mapping g is called an *encoder for user* 2, and the mapping φ is called a *decoder*. The *rate pair* of this code is the pair of nonnegative real numbers

$$\left(\frac{\log_2 N}{n}, \frac{\log_2 M}{n}\right). \tag{1.1}$$

Setting $\mathbf{x}_i \triangleq f(i)$, $i = 1;\ldots,N$, and $\mathbf{y}_j \triangleq g(j)$, $j = 1,\ldots,M$, we call $\mathbf{x}_1,\ldots,\mathbf{x}_N$ *codewords for user* 1, and we call $\mathbf{y}_1,\ldots,\mathbf{y}_M$ *codewords for user* 2. There is no requirement that the codewords be distinct. Clearly, knowing f and g is equivalent to knowing the codewords $\mathbf{x}_i$ and $\mathbf{y}_j$ (see Figure 1.2).

Remark. In the literature, (f,g,φ) is called a *deterministic code* in order to distinguish it from more general *random codes*. Random codes are discussed in [4, p. 209].

To model the operation of the channel, we characterize its behavior in terms of a transition probability $P_n(\mathbf{z}|\mathbf{x},\mathbf{y})$. That is, $P_n(\mathbf{z}|\mathbf{x},\mathbf{y})$ denotes the conditional

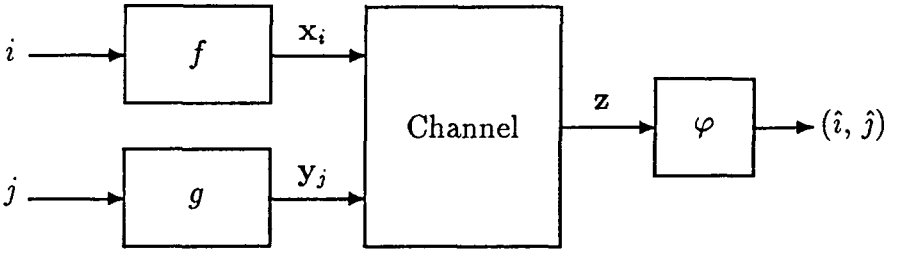

Figure 1.2: A Multiple-Access Communication System.

probability that the channel output is $\mathbf{z}$ given that the channel inputs are $\mathbf{x}$ and $\mathbf{y}$.

Based upon the preceding discussion, we now give a precise mathematical model of a discrete multiple-access communication system. Let $(\Omega, \mathcal{F}, \mathsf{P})$ be a probability space equipped with random variables (RV's) A, B, and $\mathbf{Z}$ as follows. The RV A represents a random message generated by user 1, and the RV B represents a random message generated by user 2. We assume that A and B are statistically independent with A uniformly distributed on $\{1, \ldots, N\}$ and B uniformly distributed on $\{1, \ldots, M\}$. The RV $\mathbf{Z}$ is $\mathcal{Z}^n$-valued and represents the channel output. We assume that $(\Omega, \mathcal{F}, \mathsf{P})$ is constructed so that

$$\mathsf{P}(A = i,\, B = j,\, \mathbf{Z} = \mathbf{z}) \;=\; \frac{1}{N} \cdot \frac{1}{M} \cdot P_n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j). \tag{1.2}$$

Observe that the probability P depends explicitly on the codewords $\mathbf{x}_1, \ldots, \mathbf{x}_N$ and $\mathbf{y}_1, \ldots, \mathbf{y}_M$; in other words, P depends on the encoders f and g. Now, the probability of a decoding error is simply

$$\begin{aligned} \mathsf{P}(\varphi(\mathbf{Z}) \neq (A, B)) \;&=\; \sum_{i=1}^{N} \sum_{j=1}^{M} \mathsf{P}(\varphi(\mathbf{Z}) \neq (i,j),\, A = i,\, B = j) \\ &=\; \sum_{i=1}^{N} \sum_{j=1}^{M} \sum_{\mathbf{z}:\varphi(\mathbf{z}) \neq (i,j)} \mathsf{P}(\mathbf{Z} = \mathbf{z},\, A = i,\, B = j) \end{aligned}$$

$$= \sum_{i=1}^{N}\sum_{j=1}^{M}\sum_{\mathbf{z}:\varphi(\mathbf{z})\neq(i,j)} P_n(\mathbf{z}|\mathbf{x}_i,\mathbf{y}_j)\cdot\frac{1}{N}\cdot\frac{1}{M}$$
$$= \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} P_n(\{\mathbf{z}\in\mathcal{Z}^n:\varphi(\mathbf{z})\neq(i,j)\}|\mathbf{x}_i,\mathbf{y}_j).$$

The subject of information theory is concerned with finding values of N, M, and n for which a code (f,g,φ) with a small probability of a decoding error can be found. Loosely speaking, given a sequence of channel transition probabilities $\{P_n\}_{n=1}^{\infty}$, we would like to characterize the largest set $C\subset\mathbb{R}_+^2$ (called the *capacity region*) for which the following statement can be proved:

> Given any $0<\lambda<1$, for all sufficiently large n, whenever N and M are positive integers such that
>
> $$\left(\frac{\log_2 N}{n},\frac{\log_2 M}{n}\right)\in C,$$
>
> one can find a code (f,g,φ) with
>
> $$\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} P_n(\{\mathbf{z}\in\mathcal{Z}^n:\varphi(\mathbf{z})\neq(i,j)\}|\mathbf{x}_i,\mathbf{y}_j) \leq \lambda. \qquad (1.3)$$

For general sequences of channel transition probabilities, $\{P_n\}$, little is known. However, for the discrete memoryless multiple-access channel defined below in Definition 1.2, the capacity region has been completely characterized [1,11,16].

Remark. Recall that equation (1.2) implies that A and B are independent and uniformly distributed. One way to avoid making this assumption is to replace (1.3) by

$$\max_{i,j} P_n(\{\mathbf{z}\in\mathcal{Z}^n:\varphi(\mathbf{z})\neq(i,j)\}|\mathbf{x}_i,\mathbf{y}_j) \leq \lambda. \qquad (1.4)$$

Clearly, if we had a code satisfying (1.4), then

$$\begin{aligned} \mathsf{P}(\varphi(\mathbf{Z}) \neq (A,B)) &= \sum_{i=1}^{N}\sum_{j=1}^{M} \mathsf{P}(A=i,B=j) P_n(\{\mathbf{z}\in\mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\}|\mathbf{x}_i,\mathbf{y}_j) \\ &\leq \lambda, \end{aligned}$$

regardless of the actual joint distribution of A and B. If we replace (1.3) by (1.4), then the resulting capacity region will be smaller in general. In the literature, the quantity on the left in (1.3) is called the *average* probability of error, and the quantity on the left of (1.4) is called the *maximum* probability of error. To analyze the maximum probability of error is a very difficult problem [4, p. 271], and we shall not attempt it. We shall restrict ourselves to the more tractable analysis of the average probability of error. Hereafter, it will always be understood that the phrase "probability of error" refers to the *average* probability of error.

Definition 1.2 Let $w(\cdot|\cdot,\cdot)$ be a transition probability from $\mathcal{X}\times\mathcal{Y}$ into $\mathcal{Z}$. If

$$P_n(\mathbf{z}|\mathbf{x},\mathbf{y}) = \prod_{k=1}^{n} w(z_k|x_k,y_k),$$

then w is said to be a *discrete memoryless multiple-access channel* (DMMAC). We use the notation

$$w^n(\mathbf{z}|\mathbf{x},\mathbf{y}) \triangleq \prod_{k=1}^{n} w(z_k|x_k,y_k),$$

so that (1.3) becomes

$$\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} w^n(\{\mathbf{z}\in\mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\}|\mathbf{x}_i,\mathbf{y}_j) \leq \lambda. \tag{1.5}$$

The interpretation of the DMMAC is that n-tuples are transmitted component by component. Further, the transition mechanism, characterized by w, is stationary, and its operation on (x_k,y_k) is not influenced by any other components.

Example. Consider a device which in each time unit accepts three $\{0,1\}$-valued inputs, x, y, and s, and generates the output

$$z = x + y + s. \tag{1.6}$$

We claim such a device can be modeled as a DMMAC. Let $\mathbf{S} = (S_1, \ldots, S_n)$ be an n-tuple of independent, identically distributed (i.i.d.), $\mathcal{S}$-valued random variables, where $\mathcal{S} = \{0,1\}$. We call $\mathbf{S}$ the channel noise sequence. We assume that $\mathsf{P}(S_k = 1) = p = 1 - \mathsf{P}(S_k = 0)$ for each $k = 1, \ldots, n$, where $0 < p < 1$ is known to each user and to the receiver. Let $\mathbf{X}$ and $\mathbf{Y}$ denote the random output of the encoders f and g. We assume that the pair $(\mathbf{X}, \mathbf{Y})$ is statistically independent of $\mathbf{S}$. If

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

then for $\mathrm{z} \in \mathcal{Z}^n$, where $\mathcal{Z} = \{0,1,2,3\}$, and for $\mathrm{x} \in \mathcal{X}^n$ and $\mathrm{y} \in \mathcal{Y}^n$,

$$\begin{aligned}
\mathsf{P}(\mathbf{Z} = \mathrm{z} | \mathbf{X} = \mathrm{x}, \mathbf{Y} = \mathrm{y}) &= \mathsf{P}(\mathbf{S} = \mathrm{z} - \mathrm{x} - \mathrm{y} | \mathbf{X} = \mathrm{x}, \mathbf{Y} = \mathrm{y}) \\
&= \mathsf{P}(\mathbf{S} = \mathrm{z} - \mathrm{x} - \mathrm{y}), \\
&\qquad \text{since } \mathbf{S} \text{ and } (\mathbf{X}, \mathbf{Y}) \text{ are independent,} \\
&= \prod_{k=1}^{n} \mathsf{P}(S_k = z_k - x_k - y_k), \\
&\qquad \text{since the RV's } \{S_k\}_{k=1}^n \text{ are i.i.d.}
\end{aligned}$$

By writing $w(z|x,y) = \mathsf{P}(S_1 = z - x - y)$, it follows that we have a DMMAC model of the device described by (1.6).

1.2 The Arbitrarily Varying Channel

From an analytical point of view, the DMMAC provides a very attractive channel model. However, even the simple example above makes several questionable assumptions. Namely,

- we assumed that the $\{S_k\}$ were i.i.d.;
- even if the $\{S_k\}_{k=1}^n$ are i.i.d., is it reasonable to assume that we know or can measure their common distribution?
- we assumed that $\mathbf{S}$ was statistically independent of the pair $(\mathbf{X}, \mathbf{Y})$. If $\mathbf{S}$ represents interference due to other users in a communication network, this independence assumption may not be justified.

It was because we modeled the channel noise as a stochastic process that we found it convenient to make the preceding assumptions. What happens if the channel noise can be characterized only in terms of deterministic, unobservable sequences $\mathbf{s}$? More generally, suppose that the channel transition mechanism operating on (x_k, y_k) depends on an unobservable *state* s_k belonging to a known finite set $\mathcal{S}$. To model this new behavior, let $W(z|x, y, s)$ be a transition probability from $\mathcal{X} \times \mathcal{Y} \times \mathcal{S}$ into $\mathcal{Z}$. That is, $W(z|x, y, s)$ is the conditional probability that the channel output is z given that the channel inputs are x and y, and that the channel state is s. Set

$$W^n(\mathbf{z}|\mathbf{x}, \mathbf{y}, \mathbf{s}) \triangleq \prod_{k=1}^{n} W(z_k|x_k, y_k, s_k),$$

and consider the family of probability measures, $\{\mathsf{P}_\mathbf{s}, \mathbf{s} \in \mathcal{S}^n\}$ on $(\Omega, \mathcal{F})$ determined by (cf. (1.2))

$$\mathsf{P}_\mathbf{s}(A = i, B = j, \mathbf{Z} = \mathbf{z}) = \frac{1}{N} \cdot \frac{1}{M} \cdot W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}).$$

The probability of a decoding error now depends on the unknown state sequence $\mathbf{s}$, and takes the form

$$\mathsf{P}_{\mathbf{s}}(\varphi(\mathbf{Z}) \neq (A,B)) \;=\; \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\{\mathbf{z}\in\mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{s}).$$

Definition 1.3 A transition probability W from $\mathcal{X}\times\mathcal{Y}\times\mathcal{S}$ into $\mathcal{Z}$, is called an *arbitrarily varying multiple-access channel* (AVMAC). For brevity, we usually refer to W as an "AVC."

While a precise definition of the capacity region of an AVC is given in Definitions 3.1 and 3.3, for the present we shall say that the capacity region of an AVC W, denoted $C(W)$, is the largest subset of $\mathbb{R}_+^2$ such that the following statement can be proved:

> Given any $0 < \lambda < 1$, for all sufficiently large n, whenever N and M are positive integers such that
>
> $$\left(\frac{\log_2 N}{n}, \frac{\log_2 M}{n}\right) \in C(W),$$
>
> one can find a code (f,g,φ) with
>
> $$\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\{\mathbf{z}\in\mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{s}) \;\leq \lambda, \qquad \forall \mathbf{s}\in\mathcal{S}^n. \qquad (1.7)$$

What makes the study of the AVC so challenging is that we are now seeking a code (f,g,φ) whose probability of error is bounded above by λ *uniformly* for every $\mathbf{s}\in\mathcal{S}^n$. In other words, the code (f,g,φ) must have a low probability of error no matter what state sequence $\mathbf{s}$ is imposed on the system.

Many interpretations of the state sequence $\mathbf{s}$ are possible. Usually, $\mathbf{s}$ models channel noise or interfering transmissions from other sources. For example, $\mathbf{s}$ might represent unintentional interference from other users in a communication network.

Or, s might represent intentional interference from a jammer. In general, we use s to model interference or noise which is difficult or impractical to characterize statistically.

Returning to the example at the end of the preceding section, if we assume that the channel noise sequence is deterministic, but unobservable, we find that

$$\begin{aligned} \mathsf{P}(\mathbf{Z}=\mathbf{z}|\mathbf{X}=\mathbf{x},\mathbf{Y}=\mathbf{y}) &= \mathsf{P}(\mathbf{X}+\mathbf{Y}+\mathbf{s}=\mathbf{z}|\mathbf{X}=\mathbf{x},\mathbf{Y}=\mathbf{y}) \\ &= \mathsf{P}(\mathbf{z}=\mathbf{x}+\mathbf{y}+\mathbf{s}|\mathbf{X}=\mathbf{x},\mathbf{Y}=\mathbf{y}). \end{aligned} \tag{1.8}$$

The quantity in (1.8) is clearly 0 or 1 according to whether or not the equality $\mathbf{z}=\mathbf{x}+\mathbf{y}+\mathbf{s}$ holds component-wise. Thus,

$$\mathsf{P}(\mathbf{Z}=\mathbf{z}|\mathbf{X}=\mathbf{x},\mathbf{Y}=\mathbf{y}) = \prod_{k=1}^{n} \delta(z_k - x_k - y_k - s_k),$$

where $\delta(t)=1$ if $t=0$ and $\delta(t)=0$ otherwise. Writing

$$W_a(z|x,y,s) \triangleq \delta(z-x-y-s), \tag{1.9}$$

we clearly have an AVMAC model. We call W_a the *adder channel.*

1.3 Summary of Results

In 1981, Jahn [14] characterized the capacity region $C(W)$ of the arbitrarily varying multiple-access channel, *assuming that $C(W)$ had a nonempty interior.* Jahn did not address the question of how one could decide whether or not $C(W)$ had a nonempty interior. In this dissertation we present simple conditions on the channel transition probability W which determine whether or not the capacity region $C(W)$ has a nonempty interior. The techniques used to establish these conditions are also

used to study the case in which the channel state sequences are constrained to lie in a certain subset of $\mathcal{S}^n$. Our work on the multiple-access AVC was motivated by the recent results of Csiszár and Narayan [8] for the single-user AVC. A preliminary study of the multiple-access AVC quickly reveals the far more complex nature of this channel, and clearly indicates that a more intricate approach is required. By combining extensions of the techniques and results of [8] with new ones of our own, we have uncovered some rather intriguing behavior of the AVMAC. We discuss our results below.

Since much of our analysis will rely on combinatorial arguments which employ the method of *types*, Chapter 2 provides a brief introduction to this topic. As an example of the method of types, we give a simple proof of the forward part of Shannon's source coding theorem (Theorem 2.9). Chapter 2 also introduces much of our notation.

In Chapter 3, we introduce the crucial notion of symmetrizability. We show that if W is symmetrizable (in the sense of Definitions 3.6, 3.7, or 3.8), then $C(W)$ has an empty interior. Of considerably more interest is our major result that certain *non*symmetrizability conditions are sufficient to imply that $C(W)$ contains various open rectangles, and thereby possesses a nonempty interior (cf. Theorems 3.15, 3.17, and 3.19). In the proof of Theorem 3.15, we use a rather complicated decoding rule, and so in Section 3.4 we discuss conditions under which a simpler decoding rule might suffice. In particular, Theorem 3.21 gives conditions under which the so-called *maximum mutual information decoding rule* can be used in the proof of Theorem 3.15. The importance of the maximum mutual information (MMI) decoding rule lies in its *universality*. By this we mean that the receiver does not

need to know the channel transition probability W in order to implement the MMI decoding rule.

Recall that in (1.7) we required that the probability of a decoding error be small for *every* $\mathbf{s} \in \mathcal{S}^n$. In practice, this is an overly restrictive requirement. It is often the case that the channel state cannot jump from any state s to any other state s'; i.e., there is some constraint on the permissible state sequences. Such a constraint can be modeled by requiring that (1.7) hold only for those $\mathbf{s}$ belonging to an appropriate subset of $\mathcal{S}^n$. To define such a subset, we proceed as follows. For $s \in \mathcal{S}$, we let $\ell(s)$ denote the "energy" required to put the channel into state s. We assume that the mechanism selecting the channel states can generate only state sequences $\mathbf{s} = (s_1, \ldots, s_n) \in \mathcal{S}^n$ which satisfy

$$\frac{1}{n}\sum_{k=1}^{n} \ell(s_k) \;\leq\; L,$$

where L is a positive number called a *state constraint*. We set

$$\mathcal{S}^n(L) \;\triangleq\; \{\mathbf{s} \in \mathcal{S}^n : \frac{1}{n}\sum_{k=1}^{n} \ell(s_k) \;\leq\; L\}.$$

If we now require that the error probability in (1.7) be less than or equal to λ only when $\mathbf{s} \in \mathcal{S}^n(L)$, rather than for every $\mathbf{s} \in \mathcal{S}^n$, we obtain the *capacity region under state constraint* L, denoted $C(W, L)$. In Chapter 4 we first obtain an "outer bound" on $C(W, L)$ by proving a "weak converse under state constraint L" (cf. Lemma 4.16). Since the techniques used by Jahn [14] do not appear to be useful in proving "inner bounds" on $C(W, L)$, we indicate how our proof of Theorem 3.15 can be extended to show that $C(W, L)$ contains certain open rectangles, *even if* W *is symmetrizable*. Recall that if W is symmetrizable, then the capacity region *without* a state constraint, $C(W)$, has an empty interior. By taking the

closed convex hull of these rectangles, we generate an "inner bound" on $C(W, L)$. To conclude Chapter 4, we prove that for the adder channel, W_a, defined in equation (1.9), our inner and outer bounds coincide, yielding an exact description of $C(W_a, \frac{1}{2})$.

In Chapter 5 we present our conclusions and suggestions for further research.

Clearly, $\mathbf{x} \sim \mathbf{x}' \iff P_{\mathbf{x}} = P_{\mathbf{x}'}$. We denote the equivalence classes induced by $\sim$ by

$$\begin{aligned} \mathcal{T}_{\mathbf{x}} &\triangleq \{\mathbf{x}' \in \mathcal{X}^n : \mathbf{x} \sim \mathbf{x}'\} \\ &= \{\mathbf{x}' \in \mathcal{X}^n : P_{\mathbf{x}} = P_{\mathbf{x}'}\}. \end{aligned} \tag{2.1}$$

In view of (2.1), each equivalence class is uniquely determined by the common probability distribution, or type, of each element in the class. We also point out that given any $\mathbf{x}$ and $\mathbf{x}'$,

CHAPTER 2
AN INTRODUCTION TO THE THEORY OF TYPES

Much of our analysis will rely on combinatorial arguments which employ the method of *types*. This chapter is devoted to an introduction to the method of types as developed by Csiszár, Körner, and Marton [6] and Csiszár and Körner [4]. Our presentation follows that of [4], and additionally includes as an illustration of the method of types, a simple proof of the forward part of Shannon's source coding theorem.

Let $\mathcal{X}$ be a finite set containing at least two elements. Consider the n-fold cartesian product, $\mathcal{X}^n$, where n is a positive integer. If $\mathbf{x} \in \mathcal{X}^n$, for each $a \in \mathcal{X}$, let $N(a|\mathbf{x})$ denote the number of occurrences of a in the sequence $\mathbf{x}$. That is, if $\mathbf{x} = (x_1, \ldots, x_n)$,

$$N(a|\mathbf{x}) \triangleq \sum_{k=1}^{n} \delta_a(x_k),$$

where

$$\delta_a(x) \triangleq \begin{cases} 1, & \text{if } x = a \\ 0, & \text{if } x \neq a. \end{cases}$$

Note that

$$\sum_{a \in \mathcal{X}} N(a|\mathbf{x}) = \sum_{k=1}^{n} \Big(\sum_{a \in \mathcal{X}} \delta_a(x_k) \Big) = \sum_{k=1}^{n} 1 = n.$$

We can define an equivalence relation on $\mathcal{X}^n$, denoted by $\sim$, by declaring

$$\mathbf{x} \sim \mathbf{x}' \iff \forall a \in \mathcal{X},\ N(a|\mathbf{x}) = N(a|\mathbf{x}').$$

Let $\mathcal{D}(\mathcal{X})$ denote the set of all probability distributions on $\mathcal{X}$. For every $\mathbf{x} \in \mathcal{X}^n$, we define the *type* of $\mathbf{x}$ to be the probability distribution $P_{\mathbf{x}} \in \mathcal{D}(\mathcal{X})$ given by

$$P_{\mathbf{x}}(a) \triangleq \frac{N(a|\mathbf{x})}{n}, \qquad a \in \mathcal{X}.$$

Clearly, $\mathbf{x} \sim \mathbf{x}' \iff P_{\mathbf{x}} = P_{\mathbf{x}'}$. We denote the equivalence classes induced by $\sim$ by

$$\begin{aligned} \mathcal{T}_{\mathbf{x}} &\triangleq \{\mathbf{x}' \in \mathcal{X}^n : \mathbf{x} \sim \mathbf{x}'\} \\ &= \{\mathbf{x}' \in \mathcal{X}^n : P_{\mathbf{x}} = P_{\mathbf{x}'}\}. \end{aligned} \tag{2.1}$$

In view of (2.1), each equivalence class is uniquely determined by the common probability distribution, or type, of each element in the class. We also point out that given any $\mathbf{x}$ and $\mathbf{x}'$,

$$\mathcal{T}_{\mathbf{x}} \cap \mathcal{T}_{\mathbf{x}'} \neq \phi \implies \mathcal{T}_{\mathbf{x}} = \mathcal{T}_{\mathbf{x}'}.$$

It then follows that the collection of equivalence classes forms a partition of $\mathcal{X}^n$.

Lemma 2.1 (*Type Counting*). *The number of distinct equivalence classes is bounded above by* $(n+1)^{|\mathcal{X}|}$, *where* $|\mathcal{X}|$ *denotes the cardinality of* $\mathcal{X}$.

Proof. Fix $\mathbf{x} \in \mathcal{X}^n$. For each $a \in \mathcal{X}$, the value of $N(a|\mathbf{x})$ must be one of the integers, $0, 1, \ldots, n$. Thus, for each $a \in \mathcal{X}$, there are at most $n+1$ possible values for $N(a|\mathbf{x})$. Since there are $|\mathcal{X}|$ different elements $a \in \mathcal{X}$, the result follows. □

Remark. The bound in the Type Counting Lemma is by no means the best. In fact, the exact number of distinct equivalence classes is [4, Problem 1, p. 39]

$$\binom{n + |\mathcal{X}| - 1}{|\mathcal{X}| - 1}.$$

Obviously, $(n+1)^{|\mathcal{X}|}$ is a polynomial in n. Since we shall always upper bound $(n+1)^{|\mathcal{X}|}$ by an exponential function of n, the exact number of equivalence classes is not important for our results.

Let $\mathcal{D}_n(\mathcal{X})$ denote the subset of $\mathcal{D}(\mathcal{X})$ consisting of probability distributions P which can be expressed as $P(a) = \lambda_n(a)/n, a \in \mathcal{X}$, where $\lambda_n(a)$ is a nonnegative integer. Obviously, there is a one-to-one correspondence between the elements of $\mathcal{D}_n(\mathcal{X})$ and the distinct equivalence classes induced by $\sim$. By the Type Counting Lemma, $\mathcal{D}_n(\mathcal{X})$ is a finite set, and so we can write $\mathcal{X}^n$ as a finite disjoint union,

$$\mathcal{X}^n = \bigcup_{P \in \mathcal{D}_n(\mathcal{X})} \mathcal{T}_P, \tag{2.2}$$

where for $P \in \mathcal{D}_n(\mathcal{X})$, $\mathcal{T}_P \triangleq \{\mathbf{x} \in \mathcal{X}^n : P_{\mathbf{x}} = P\}$.

Throughout this dissertation, log and exp are understood as being to the base 2. We use ln to denote the natural logarithm. Hence,

$$\exp(x) = 2^x = e^{x \ln 2} \qquad \text{and} \qquad \log x = (\log e) \ln x = \frac{\ln x}{\ln 2}.$$

Definition 2.2 For any $P \in \mathcal{D}(\mathcal{X})$, the *entropy* of P, $H(P)$, is given by

$$H(P) \triangleq \sum_a P(a) \log \frac{1}{P(a)},$$

where the sum is understood to be only over those $a \in \mathcal{X}$ such that $P(a) > 0$. We remind the reader that $0 \leq H(P) \leq \log |\mathcal{X}| < \infty$.

Definition 2.3 For all $P, Q \in \mathcal{D}(\mathcal{X})$, the *Kullback-Leibler informational divergence*, $D(P\|Q)$, is defined as follows. If for all $a \in \mathcal{X}$, $P(a) > 0$ implies $Q(a) > 0$ (i.e., $P \ll Q$), then

$$D(P\|Q) \triangleq \sum_a P(a) \log \frac{P(a)}{Q(a)},$$

where the sum is understood to be only over those $a \in \mathcal{X}$ such that $P(a) > 0$. Otherwise, $D(P\|Q) \triangleq \infty$.

For $P \in \mathcal{D}(\mathcal{X})$ and $\mathbf{x} = (x_1, \ldots, x_n)$, we set

$$P^n(\mathbf{x}) \triangleq \prod_{k=1}^{n} P(x_k).$$

We can then state the following result.

Lemma 2.4 *Fix any $Q \in \mathcal{D}(\mathcal{X})$. Then for all $\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{X}^n$, we can write, with the convention that $\exp(-\infty) = 0$,*

$$Q^n(\mathbf{x}) = \exp[-n(D(P_{\mathbf{x}}\|Q) + H(P_{\mathbf{x}}))] \tag{2.3}$$

$$\leq \exp(-nH(P_{\mathbf{x}})). \tag{2.4}$$

Proof. We begin by writing

$$Q^n(\mathbf{x}) = \prod_{k=1}^{n} Q(x_k) = \prod_{a} Q(a)^{N(a|\mathbf{x})},$$

where the second product is understood to be only over those a which occur in $\mathbf{x} = (x_1, \ldots, x_n)$, i.e., those a for which $P_{\mathbf{x}}(a) > 0$. Now, if there is any a with $Q(a) = 0$ but $P_{\mathbf{x}}(a) > 0$, then (2.3) simply asserts that $0 = 0$. So, assume that $P_{\mathbf{x}}(a) > 0$ implies $Q(a) > 0$. We continue with

$$\begin{aligned} -\frac{1}{n}\log Q^n(\mathbf{x}) &= \sum_a \frac{N(a|\mathbf{x})}{n} \log \frac{1}{Q(a)} \\ &= \sum_a P_{\mathbf{x}}(a)\Big(\log \frac{P_{\mathbf{x}}(a)}{Q(a)} + \log \frac{1}{P_{\mathbf{x}}(a)}\Big) \\ &= D(P_{\mathbf{x}}\|Q) + H(P_{\mathbf{x}}). \end{aligned}$$

□

Let Q be any distribution on $\mathcal{X}$. We now make the following crucial observation. Since $\mathbf{x}' \in \mathcal{T}_{\mathbf{x}}$ if and only if $P_{\mathbf{x}} = P_{\mathbf{x}'}$, we see that Q^n is constant on each equivalence class, $\mathcal{T}_{\mathbf{x}}$. In fact, for all $\mathbf{x}' \in \mathcal{T}_{\mathbf{x}}$,

$$Q^n(\mathbf{x}') = Q^n(\mathbf{x}) = \exp[-n(D(P_{\mathbf{x}}\|Q) + H(P_{\mathbf{x}}))].$$

An important consequense of this observation is the following. Taking $Q = P_{\mathbf{x}}$ so that $D(P_{\mathbf{x}}\|Q) = D(P_{\mathbf{x}}\|P_{\mathbf{x}}) = 0$, we get

$$\begin{aligned} 1 \geq P_{\mathbf{x}}^n(\mathcal{T}_{\mathbf{x}}) &= \sum_{\mathbf{x}' \in \mathcal{T}_{\mathbf{x}}} P_{\mathbf{x}}^n(\mathbf{x}') \\ &= \sum_{\mathbf{x}' \in \mathcal{T}_{\mathbf{x}}} \exp(-nH(P_{\mathbf{x}})) \\ &= |\mathcal{T}_{\mathbf{x}}| \cdot \exp(-nH(P_{\mathbf{x}})). \end{aligned}$$

It follows that $|\mathcal{T}_{\mathbf{x}}| \leq \exp(nH(P_{\mathbf{x}}))$. In fact, it can be shown [4, Lemma 2.3, p. 30] that

$$\exp(nH(P_{\mathbf{x}}))(n+1)^{-|\mathcal{X}|} \leq |\mathcal{T}_{\mathbf{x}}| \leq \exp(nH(P_{\mathbf{x}})). \tag{2.5}$$

Further, using (2.3) and (2.5) it is easy to show that

$$Q^n(\mathcal{T}_{\mathbf{x}}) \leq \exp(-nD(P_{\mathbf{x}}\|Q)). \tag{2.6}$$

Definition 2.5 The *variational distance* between any two distributions $P, Q \in \mathcal{D}(\mathcal{X})$, is given by

$$d(P,Q) \triangleq \sum_{x \in \mathcal{X}} |P(x) - Q(x)|,$$

where $|\cdot|$ denotes the usual absolute value.

It is easily seen that d is a metric on $\mathcal{D}(\mathcal{X})$. In fact, $\mathcal{D}(\mathcal{X})$ is compact under d.

Lemma 2.6 (*Continuity of Entropy*). *The entropy, H, regarded as a mapping from the metric space $(\mathcal{D}(\mathcal{X}), d)$ into the metric space $(\mathbb{R}, |\cdot|)$, is uniformly continuous.*

Proof. See [4, Lemma 2.7, p. 33].

Lemma 2.7 (*Pinsker's Inequality*). *For all $P, Q \in \mathcal{D}(\mathcal{X})$,*

$$d(P,Q) \leq \sqrt{(2\ln 2)D(P\|Q)}.$$

Proof. See [4, Problem 17, p. 58].

Observe that Lemmas 2.6 and 2.7 readily yield the following simple result.

Corollary 2.8 *Given $\delta > 0$, there exists an $\eta > 0$ such that for all $P, Q \in \mathcal{D}(\mathcal{X})$, whenever $D(P\|Q) \leq \eta$, we have*

$$|H(P) - H(Q)| \leq \delta/2.$$

We now present, as an illustration of the method of types, a simple proof of the forward part of Shannon's source coding theorem.

Theorem 2.9 *Fix $Q \in \mathcal{D}(\mathcal{X})$. For every $\delta > 0$, there exists an $\varepsilon > 0$ such that for all sufficiently large n, there exists a set $A_n \subset \mathcal{X}^n$ such that*

$$\frac{\log |A_n|}{n} \leq H(Q) + \delta,$$

and

$$Q^n(A_n^c) \leq \exp(-n\varepsilon/2).$$

Proof. Fix $\delta > 0$. By Corollary 2.8, we can choose $\eta > 0$ so small that for all $P \in \mathcal{D}(\mathcal{X})$,

$$D(P\|Q) \leq \eta \implies |H(P) - H(Q)| \leq \delta/2. \tag{2.7}$$

Fix $0 < \varepsilon < \min\{\eta, \delta\}$. Choose n so large that $(n+1)^{|\mathcal{X}|} \leq \exp(n\varepsilon/2)$. Set

$$A_n \triangleq \{\mathbf{x} \in \mathcal{X}^n : D(P_{\mathbf{x}}\|Q) \leq \eta\}.$$

First we shall bound $|A_n|$. Observe that

$$A_n = \bigcup_{P \in \mathcal{D}_n(\mathcal{X}) : D(P\|Q) \leq \eta} \mathcal{T}_P.$$

Now, apply the union bound, the Type Counting Lemma, (2.5) and (2.7) to get

$$\begin{aligned} |A_n| &\leq (n+1)^{|\mathcal{X}|} \exp[n(H(Q) + \delta/2)] \\ &\leq \exp[n(H(Q) + \delta/2 + \varepsilon/2)] \\ &\leq \exp[n(H(Q) + \delta)], \qquad \text{since } \varepsilon < \delta, \end{aligned}$$

or,

$$\frac{\log |A_n|}{n} \leq H(Q) + \delta.$$

We now bound $Q^n(A_n^c)$. Observe that

$$A_n^c = \bigcup_{P \in \mathcal{D}_n(\mathcal{X}) : D(P||Q) > \eta} \mathcal{T}_P.$$

Apply the union bound, the Type Counting Lemma, and (2.6) to get

$$\begin{aligned} Q^n(A_n^c) &\leq (n+1)^{|\mathcal{X}|} \exp(-n\eta) \\ &\leq \exp(n\varepsilon/2) \exp(-n\eta) \\ &= \exp[-n(\eta - \varepsilon/2)] \\ &\leq \exp(-n\varepsilon/2), \qquad \text{since } \eta > \varepsilon. \end{aligned}$$

□

We now generalize the notion of types to the product set $\mathcal{X} \times \mathcal{Y}$, where $\mathcal{Y}$ is another finite set with at least two elements. If

$$\mathbf{x} = (x_1, \ldots, x_n) \in \mathcal{X}^n, \qquad \text{and} \qquad \mathbf{y} = (y_1, \ldots, y_n) \in \mathcal{Y}^n,$$

for $a \in \mathcal{X}$ and $b \in \mathcal{Y}$, we set

$$N(a, b|\mathbf{x}, \mathbf{y}) \triangleq \sum_{k=1}^{n} \delta_a(x_k) \delta_b(y_k),$$

i.e., $N(a, b|\mathbf{x}, \mathbf{y})$ is the number of occurrences of (a, b) in the sequence

$$((x_1, y_1), \ldots, (x_n, y_n)).$$

We then define the *joint type* of $(\mathbf{x}, \mathbf{y})$ as

$$P_{\mathbf{x},\mathbf{y}}(a, b) \triangleq \frac{1}{n} N(a, b|\mathbf{x}, \mathbf{y}), \qquad a \in \mathcal{X},\ b \in \mathcal{Y}.$$

This definition is consistent with that of the type of the sequence $\mathbf{x} \in \mathcal{X}^n$ or $\mathbf{y} \in \mathcal{Y}^n$, since

$$\sum_{b \in \mathcal{Y}} P_{\mathbf{x},\mathbf{y}}(a,b) = P_{\mathbf{x}}(a) \qquad \text{and} \qquad \sum_{a \in \mathcal{X}} P_{\mathbf{x},\mathbf{y}}(a,b) = P_{\mathbf{y}}(b).$$

Now, if[1] $P_{XY} \in \mathcal{D}_n(\mathcal{X} \times \mathcal{Y})$, we write $\mathcal{T}_{XY}$ instead of $\mathcal{T}_{P_{XY}}$, and we say that $(\mathbf{x},\mathbf{y}) \in \mathcal{T}_{XY}$ if and only if $P_{\mathbf{x},\mathbf{y}} = P_{XY}$. Observe that for each $\mathbf{x} \in \mathcal{X}^n$, we can partition $\mathcal{Y}^n$ into equivalence classes as follows. If $P_{XY} \in \mathcal{D}_n(\mathcal{X} \times \mathcal{Y})$ and $\mathbf{x} \in \mathcal{X}^n$,

$$\mathcal{T}_{Y|X}(\mathbf{x}) \triangleq \{\mathbf{y} \in \mathcal{Y}^n : P_{\mathbf{x},\mathbf{y}} = P_{XY}\}.$$

Note that if $P_{\mathbf{x}} \neq P_X$, then $\mathcal{T}_{Y|X}(\mathbf{x}) = \phi$.

Definition 2.10 We denote by $\mathcal{D}_n(\mathcal{Y}|\mathbf{x})$ the set of all $P_{XY} \in \mathcal{D}_n(\mathcal{X} \times \mathcal{Y})$ such that $P_X = P_{\mathbf{x}}$.

Obviously, by the Type Counting Lemma, $|\mathcal{D}_n(\mathcal{Y}|\mathbf{x})| \leq |\mathcal{D}_n(\mathcal{X} \times \mathcal{Y})| \leq (n+1)^{|\mathcal{X}||\mathcal{Y}|}$. Hence, for each fixed $\mathbf{x} \in \mathcal{X}^n$, we can write $\mathcal{Y}^n$ as a finite disjoint union,

$$\mathcal{Y}^n = \bigcup_{P_{XY} \in \mathcal{D}_n(\mathcal{Y}|\mathbf{x})} \mathcal{T}_{Y|X}(\mathbf{x}).$$

Definition 2.11 If $P_{XY} \in \mathcal{D}(\mathcal{X} \times \mathcal{Y})$, $P_{Y|X}$ is the transition probability defined by the equation,

$$P_X(a)P_{Y|X}(b|a) = P_{XY}(a,b), \qquad a \in \mathcal{X},\ b \in \mathcal{Y}.$$

Clearly, for those a with $P(a) > 0$, $P_{Y|X}(\cdot|a)$ is uniquely defined. For those a with $P(a) = 0$, we take $P(\cdot|a)$ to be any arbitrary element of $\mathcal{D}(\mathcal{Y})$.

[1] At this point the subscript XY serves as a place holder indicating that P_{XY} is a distribution on $\mathcal{X} \times \mathcal{Y}$ with marginals P_X and P_Y. Later we will think of P_{XY} as the joint distribution of a pair of RV's, X and Y.

Definition 2.12 If V is a transition probability from $\mathcal{X}$ into $\mathcal{Y}$, and $P \in \mathcal{D}(\mathcal{X})$, then we define the distribution $P \times V \in \mathcal{D}(\mathcal{X} \times \mathcal{Y})$ by

$$(P \times V)(a,b) \triangleq P(a)V(b|a), \qquad a \in \mathcal{X},\ b \in \mathcal{Y},$$

and we define the marginal distribution $PV \in \mathcal{D}(\mathcal{Y})$ by

$$(PV)(b) \triangleq \sum_a (P \times V)(a,b).$$

Definition 2.13 For $P_{XY} \in \mathcal{D}(\mathcal{X} \times \mathcal{Y})$, the *conditional entropy of Y given X* is given by

$$H(Y|X) \triangleq \sum_{a,b} P_X(a)P_{Y|X}(b) \log \frac{1}{P_{Y|X}(b|a)},$$

where the sum is understood to be only over those a, b for which $P_X(a)P_{Y|X}(b) = P_{XY}(a,b) > 0$.

Notation. It is apparent that the conditional entropy is a function which maps $\mathcal{D}(\mathcal{X} \times \mathcal{Y})$ into $[0, \infty)$. To emphasize this point, when discussing two different distributions on $\mathcal{X} \times \mathcal{Y}$, say P and Q, we will sometimes find it convenient to use the notation $H_{\mathcal{Y}|\mathcal{X}}(P)$ and $H_{\mathcal{Y}|\mathcal{X}}(Q)$ to indicate which distribution is being used to compute the conditional entropy.

Lemma 2.14 *Let V be an arbitrary transition probability from $\mathcal{X}$ into $\mathcal{Y}$. Fix any $\mathbf{x} \in \mathcal{X}^n$. Then for every $P_{XY} \in \mathcal{D}_n(\mathcal{Y}|\mathbf{x})$ we have, for all $\mathbf{y} \in \mathcal{T}_{Y|X}(\mathbf{x})$,*

$$V^n(\mathbf{y}|\mathbf{x}) = \exp[-n(D(P_{XY}\|P_X \times V) + H(Y|X))] \tag{2.8}$$

$$\leq \exp(-nH(Y|X)), \tag{2.9}$$

and

$$|\mathcal{T}_{Y|X}(\mathbf{x})| \leq \exp(nH(Y|X)). \tag{2.10}$$

Proof. The proof is analogous to that of Lemma 2.4, and is therefore omitted.

Using (2.8) and (2.10), it is easy to verify the analog of (2.6):

$$V^n(\mathcal{T}_{Y|X}(\mathbf{x})\,|\mathbf{x}) \;\leq\; \exp(-D(P_{XY}\|P_X \times V)). \tag{2.11}$$

Lemma 2.15 (*Projection*). *For every P_{XY} and Q_{XY} in $\mathcal{D}(\mathcal{X} \times \mathcal{Y})$,*

$$d(P_X, Q_X) \;\leq\; d(P_{XY}, Q_{XY}),$$

and

$$D(P_X\|Q_X) \;\leq\; D(P_{XY}\|Q_{XY}).$$

Proof. We omit the straightforward calculations.

We conclude this section with two simple lemmas which together yield the important result that given $P \in \mathcal{D}(\mathcal{X})$, for *all* sufficiently large n, P can be approximated by a *type* $\hat{P} \in \mathcal{D}_n(\mathcal{X})$ with $\hat{P}(x) > 0$ for all $x \in \mathcal{X}$.

Lemma 2.16 *Fix any $P \in \mathcal{D}(\mathcal{X})$. For every $\varepsilon > 0$, there exists a $\hat{P} \in \mathcal{D}(\mathcal{X})$ satisfying*

$$\hat{P}(x) > 0, \quad \forall x \in \mathcal{X} \qquad \textit{and} \qquad \sum_x |P(x) - \hat{P}(x)| \;\leq\; \varepsilon.$$

Proof. Without loss of generality, assume $0 < \varepsilon < 1$. Let c denote the number of $x \in \mathcal{X}$ such that $P(x) = 0$. If $c = 0$, take $\hat{P} \equiv P$. Otherwise, assume $c \geq 1$. Choose any x_0 with $P(x_0) > 0$ (there is one). For $x \neq x_0$ with $P(x) > 0$, set $\hat{P}(x) \triangleq P(x)$. For $x \neq x_0$ with $P(x) = 0$, set

$$\hat{P}(x) \triangleq \frac{\varepsilon}{2c} \cdot P(x_0).$$

Clearly this is a positive quantity. Since $c \geq 1$ and $\epsilon < 1$, it is obvious that

$$\frac{\epsilon}{2c} \cdot P(x_0) \leq \frac{1}{2} < 1.$$

Finally, set

$$\begin{aligned} \hat{P}(x_0) &\triangleq P(x_0) - c \cdot \frac{\epsilon}{2c} P(x_0) \\ &= P(x_0)(1 - \epsilon/2). \end{aligned}$$

Since $0 < \epsilon < 1$, $\hat{P}(x_0)$ satisfies $0 < \frac{1}{2}P(x_0) \leq \hat{P}(x_0) \leq P(x_0) \leq 1$. After verifying that $\sum_x \hat{P}(x) = 1$, the last step is to observe that

$$\begin{aligned} \sum_x |P(x) - \hat{P}(x)| &= \frac{\epsilon}{2} P(x_0) + \frac{\epsilon}{2} P(x_0) \\ &= \epsilon \cdot P(x_0) \leq \epsilon. \end{aligned}$$

□

Lemma 2.17 *Suppose $P \in \mathcal{D}(\mathcal{X})$ satisfies $P(x) > 0$ for all $x \in \mathcal{X}$. Then for every $\epsilon > 0$, there exists an n_0 such that for* each and every $n \geq n_0$, *there exist* positive integers $\lambda_n(x), x \in \mathcal{X}$, *satisfying*

$$\sum_x \lambda_n(x) = n \qquad \textit{and} \qquad \sum_x \left| P(x) - \frac{\lambda_n(x)}{n} \right| \leq \epsilon.$$

Proof. Fix $\epsilon > 0$. Without loss of generality, assume $\frac{\epsilon}{2|\mathcal{X}|} < P(x)$ for all $x \in \mathcal{X}$. Consider the following equivalent statements.

$$\left| P(x) - \frac{\lambda_n(x)}{n} \right| \leq \frac{\epsilon}{2|\mathcal{X}|}$$

$$-\frac{\epsilon}{2|\mathcal{X}|} \leq \frac{\lambda_n(x)}{n} - P(x) \leq \frac{\epsilon}{2|\mathcal{X}|}$$

$$n\left(P(x) - \frac{\epsilon}{2|\mathcal{X}|}\right) \leq \lambda_n(x) \leq n\left(P(x) + \frac{\epsilon}{2|\mathcal{X}|}\right). \tag{2.12}$$

Now, since

$$n\Big(P(x)+\frac{\varepsilon}{2|\mathcal{X}|}\Big)-n\Big(P(x)-\frac{\varepsilon}{2|\mathcal{X}|}\Big) \;=\; \frac{n\varepsilon}{|\mathcal{X}|} \;\geq\; 1$$

when $n \geq |\mathcal{X}|/\varepsilon$, for all sufficiently large n, there exists at least one *positive integer* $\lambda_n(x)$ satisfying (2.12).

Next, fix any $x_0 \in \mathcal{X}$, and set

$$\lambda_n(x) \;\triangleq\; \Big\lceil n\Big(P(x)-\frac{\varepsilon}{2|\mathcal{X}|}\Big)\Big\rceil \;>\; 0, \qquad x \neq x_0,$$

where $\lceil t \rceil$ denotes the smallest integer greater than or equal to t. Since

$$\begin{aligned}
\lambda_n(x) &\leq n\Big(P(x)-\frac{\varepsilon}{2|\mathcal{X}|}\Big)+1, \\
\sum_{x\neq x_0}\lambda_n(x) &\leq n(1-P(x_0))-\frac{n\varepsilon}{2|\mathcal{X}|}(|\mathcal{X}|-1)+(|\mathcal{X}|-1) \\
&= n(1-P(x_0))+(|\mathcal{X}|-1)(1-\frac{n\varepsilon}{2|\mathcal{X}|}).
\end{aligned}$$

Since $1-P(x_0)<1$, it is clear that if $n > 2|\mathcal{X}|/\varepsilon$,

$$\sum_{x\neq x_0}\lambda_n(x) \;<\; n.$$

Thus, we may take $\lambda_n(x_0) = n - \sum_{x\neq x_0}\lambda_n(x)$. Finally, observe that

$$\sum_x\Big|P(x)-\frac{\lambda_n(x)}{n}\Big| \;\leq\; 2\sum_{x\neq x_0}\Big|P(x)-\frac{\lambda_n(x)}{n}\Big|.$$

Since for $x \neq x_0$, $\lambda_n(x)$ satisfies (2.12), we have

$$\sum_x\Big|P(x)-\frac{\lambda_n(x)}{n}\Big| \;\leq\; \varepsilon, \qquad n > 2|\mathcal{X}|/\varepsilon.$$

□

Remark. We point out that the two preceding lemmas combine to say that

$$\bigcup_{n=2}^{\infty}\mathcal{D}_n(\mathcal{X})$$

is dense in $\mathcal{D}(\mathcal{X})$ under the metric d. In fact, since the cardinality of each $\mathcal{D}_n(\mathcal{X})$ is finite (by the Type Counting Lemma), the resulting union is a countable set [17, Prop. 7, p. 21], and thus $(\mathcal{D}(\mathcal{X}), d)$ is a *separable* metric space.

CHAPTER 3

THE ARBITRARILY VARYING MULTIPLE-ACCESS CHANNEL

3.1 Introduction

Let W be a (two-user) AVMAC as described in Definition 1.3. We need the following rather complicated definition.

Definition 3.1 A pair of nonnegative real numbers, (R_1, R_2), is said to be *achievable* for the AVC W if:

> For every $0 < \lambda < 1$, and every $\Delta R > 0$, there exists a positive integer n_0 such that for all $n \geq n_0$, there exist positive integers N and M such that
>
> $$\frac{\log N}{n} > R_1 - \Delta R \qquad \text{and} \qquad \frac{\log M}{n} > R_2 - \Delta R,$$
>
> and such that there exists a code (f, g, φ) (cf. Definition 1.1) with
>
> $$\frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(\{\mathbf{z} \in \mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\} | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \leq \lambda, \qquad \forall \mathbf{s} \in \mathcal{S}^n. \tag{3.1}$$

Remark 3.2 Let $\lfloor t \rfloor$ denote the greatest integer less than or equal to t. Observe that for any $R \geq 0$, $\frac{1}{n} \log \lfloor \exp(nR) \rfloor \leq R$ and in fact converges to R. Hence, in proving that a pair (R_1, R_2) is achievable, we shall find it convenient to take

$$N = \lfloor \exp(nR_1) \rfloor \qquad \text{and} \qquad M = \lfloor \exp(nR_2) \rfloor.$$

Definition 3.3 The *capacity region* of the AVC W, denoted $C(W)$, is defined by

$$C(W) \triangleq \{(R_1, R_2) : (R_1, R_2) \text{ is achievable}\}.$$

A few comments are in order here. First, it is clear from the definition that $C(W)$ is a closed set. Second, by the usual time-sharing principle [4, Lemma 2.2, p. 272], $C(W)$ is also convex. Consequently, if E is any subset of $C(W)$, then the closed convex hull of E is also a subset of $C(W)$.

Before proceeding further, we shall need the following notation. For all $Q_{XYZ} \in \mathcal{D}(\mathcal{X} \times \mathcal{Y} \times \mathcal{Z})$, let

$$\begin{aligned} I_{\mathcal{X}\wedge\mathcal{Z}}(Q_{XYZ}) &\triangleq I(X \wedge Z), \\ I_{\mathcal{Y}\wedge\mathcal{Z}}(Q_{XYZ}) &\triangleq I(Y \wedge Z), \\ I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(Q_{XYZ}) &\triangleq I(X \wedge Z|Y), \\ I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(Q_{XYZ}) &\triangleq I(Y \wedge Z|X), \\ I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(Q_{XYZ}) &\triangleq I(XY \wedge Z), \end{aligned}$$

where the expressions on the right are the usual mutual information quantities computed with the distribution indicated on the left, e.g.,

$$I(X \wedge Z) \triangleq \sum_{x,z} Q_{XZ}(x,z) \log \frac{Q_{XZ}(x,z)}{Q_X(x)Q_Z(z)},$$

$$I(X \wedge Z|Y) \triangleq \sum_{x,y,z} Q_{XYZ}(x,y,z) \log \frac{Q_{XZ|Y}(x,z|y)}{Q_{X|Y}(x|y)Q_{Z|Y}(z|y)},$$

$$I(XY \wedge Z) \triangleq \sum_{x,y,z} Q_{XYZ}(x,y,z) \log \frac{Q_{XYZ}(x,y,z)}{Q_{XY}(x,y)Q_Z(z)}.$$

Suppose $p \in \mathcal{D}(\mathcal{X})$, $q \in \mathcal{D}(\mathcal{Y})$, and $r \in \mathcal{D}(\mathcal{S})$. We can define a probability measure on $\mathcal{X} \times \mathcal{Y} \times \mathcal{S} \times \mathcal{Z}$ by setting

$$(p \times q \times r \times W)(x,y,s,z) \triangleq p(x)q(y)r(s)W(z|x,y,s).$$

We will need to refer to the following conditional probabilities associated with this measure. Let pW, qW, and rW be given by

$$\begin{aligned}(pW)(z|y,s) &\triangleq \sum_x p(x)W(z|x,y,s),\\ (qW)(z|x,s) &\triangleq \sum_y q(y)W(z|x,y,s),\\ (rW)(z|x,y) &\triangleq \sum_s r(s)W(z|x,y,s).\end{aligned}$$

We also need to define

$$(p\times q\times rW)(x,y,z) \triangleq p(x)q(y)(rW)(z|x,y),$$

and set

$$\begin{aligned}I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{X}\wedge\mathcal{Z}}(p\times q\times rW),\\ I^*_{\mathcal{Y}\wedge\mathcal{Z}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW),\\ I^*_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p\times q\times rW),\\ I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW),\\ I^*_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW).\end{aligned} \tag{3.2}$$

Remark. We point out here that if $p,\hat{p}\in\mathcal{D}(\mathcal{X})$ and $q,\hat{q}\in\mathcal{D}(\mathcal{Y})$, then

$$\sum_{x,y,s,z} |(p\times q\times r\times W)(x,y,s,z) - (\hat{p}\times\hat{q}\times r\times W)(x,y,s,z)|$$

is actually independent of both r and W. This expression is easily seen to be equal to

$$\begin{aligned}\sum_{x,y}|p(x)q(y)-\hat{p}(x)\hat{q}(y)| &= \sum_{x,y}|p(x)q(y)-\hat{p}(x)q(y)+\hat{p}(x)q(y)-\hat{p}(x)\hat{q}(y)|\\ &\le d(p,\hat{p})+d(q,\hat{q}).\end{aligned} \tag{3.3}$$

It is then easy to see that if both members of (3.3) are sufficiently small, then all of the quantities, $I^*_{\cdots}(p,q,W)$, are close to the corresponding quantities, $I^*_{\cdots}(\hat{p},\hat{q},W)$.

Definition 3.4 Let

$$\mathcal{R}^*(p,q,W) \triangleq \{(R_1,R_2): \quad 0 \le R_1 < I^*_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W),$$
$$0 \le R_2 < I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W),$$
$$0 \le R_1 + R_2 < I^*_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p,q,W)\},$$

and denote by $\mathcal{R}^*(W)$ the closed convex hull of

$$\bigcup_{p\in\mathcal{P}(\mathcal{X}),\, q\in\mathcal{P}(\mathcal{Y})} \mathcal{R}^*(p,q,W).$$

Theorem 3.5 (*Jahn* (1981) [14]). *For every AVC W, we always have*

$$C(W) \subset \mathcal{R}^*(W), \qquad (\textit{the weak converse}), \tag{3.4}$$

and, if $C(W)$ has a nonempty interior, then

$$\mathcal{R}^*(W) \subset C(W), \qquad (\textit{the forward part}). \tag{3.5}$$

Remark. The weak converse,[1] inclusion (3.4), asserts that all achievable rate pairs must belong to $\mathcal{R}^*(W)$. The forward part, inclusion (3.5), asserts that every rate pair in $\mathcal{R}^*(W)$ is in fact achievable, provided $C(W)$ has a nonempty interior. Obviously, one would like to know exactly when $C(W)$ has a nonempty interior. Below we will give sufficient conditions under which $C(W)$ will have a nonempty interior. In fact, using techniques unrelated to Jahn's, we shall show that under certain conditions, $C(W)$ contains certain open rectangles, proving that $C(W)$ has a nonempty interior. We will also give sufficient conditions under which $C(W)$ will have one of the following forms, each with an empty interior,

$$C(W) = \{(0,0)\},$$

[1] An excellent explanation of the relationship between the weak and the strong converses is given by van der Meulen [19].

$$C(W) = [0, C_1(W)] \times \{0\}, \qquad \text{or} \qquad C(W) = \{0\} \times [0, C_2(W)],$$

where

$$C_1(W) \leq \sup_{p \in \mathcal{D}(\mathcal{X}), q \in \mathcal{D}(\mathcal{Y})} I^*_{\mathcal{X} \wedge \mathcal{Z}|\mathcal{Y}}(p, q, W)$$

and

$$C_2(W) \leq \sup_{p \in \mathcal{D}(\mathcal{X}), q \in \mathcal{D}(\mathcal{Y})} I^*_{\mathcal{Y} \wedge \mathcal{Z}|\mathcal{X}}(p, q, W).$$

3.2 Symmetrizability

The various notions of *symmetrizability* presented below will play a crucial role in determining whether or not $C(W)$ has an empty interior. The definitions below generalize the notion of single-user symmetrizability introduced in [8].

Definition 3.6 The AVC W is said to be *symmetrizable-$\mathcal{X}\mathcal{Y}$* if there exists a transition probability U from $\mathcal{X} \times \mathcal{Y}$ into $\mathcal{S}$ such that

$$\sum_s W(z|x, y, s)U(s|x', y') = \sum_s W(z|x', y', s)U(s|x, y), \qquad \forall x,\ x',\ y,\ y',\ z. \quad (3.6)$$

If no such U exists, we say that W is *nonsymmetrizable-$\mathcal{X}\mathcal{Y}$*.

Definition 3.7 The AVC W is said to be *symmetrizable-$\mathcal{X}$* if there exists a transition probability U from $\mathcal{X}$ into $\mathcal{S}$ such that

$$\sum_s W(z|x, y, s)U(s|x') = \sum_s W(z|x', y, s)U(s|x), \qquad \forall x,\ x',\ y,\ z. \quad (3.7)$$

If no such U exists, we say that W is *nonsymmetrizable-$\mathcal{X}$*.

Definition 3.8 The AVC W is said to be *symmetrizable-$\mathcal{Y}$* if there exists a transition probability U from $\mathcal{Y}$ into $\mathcal{S}$ such that

$$\sum_s W(z|x,y,s)U(s|y') = \sum_s W(z|x,y',s)U(s|y), \qquad \forall x,\, y,\, y',\, z. \tag{3.8}$$

If no such U exists, we say that W is *nonsymmetrizable-$\mathcal{Y}$*.

Example. Let $\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0,1\}$, and let $\mathcal{Z} = \{0,1,2,3\}$. Consider the *adder channel*, W_a, given by (1.9). It is easy to show that if U satisfies (3.6), then $U \equiv 0$. Since $U \equiv 0$ is not a transition probability, the adder channel is nonsymmetrizable-$\mathcal{XY}$. Similarly, it is a simple matter to show that if U satisfies (3.7), then $U(s|x) = \delta_x(s)$, and so the adder channel is symmetrizable-$\mathcal{X}$. Of course, an identical argument shows that the adder channel is symmetrizable-$\mathcal{Y}$.

Theorem 3.9 *If the AVC W is symmetrizable-$\mathcal{XY}$, then*

$$C(W) = \{(0,0)\}.$$

Proof. First observe that since $(0,0)$ is always achievable, $C(W)$ always contains the origin. It remains to show that no other rate pair is achievable. Let n be a positive integer. Let N and M be positive integers with $NM \geq 2$. Suppose $\mathbf{x}_1, \ldots, \mathbf{x}_N$, each in $\mathcal{X}^n$, are codewords for user 1, and suppose $\mathbf{y}_1, \ldots, \mathbf{y}_M$, each in $\mathcal{Y}^n$, are codewords for user 2. Let φ be any decoder. We will show below, by using the same procedure as in [8], that there exists some $\mathbf{s} \in \mathcal{S}^n$ with

$$\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\{\mathbf{z} \in \mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \geq 1/4. \tag{3.9}$$

In other words, if N or M is greater than 1, the code can not have an arbitrarily small probability of error for *every* $\mathbf{s} \in \mathcal{S}^n$.

Suppose $NM \geq 2$. Since W is symmetrizable-$\mathcal{XY}$, let U be a symmetrizing transition probability satisfying (3.6). For each $1 \leq i \leq N$ and $1 \leq j \leq M$, let $\mathbf{S}_{ij} = (S_{ij,1}, \ldots, S_{ij,n})$ be an $\mathcal{S}^n$-valued RV whose components are independent and distributed according to

$$\mathsf{P}(S_{ij,k} = s) \;=\; U(s|x_{i,k}, y_{j,k}), \qquad 1 \leq k \leq n,$$

where $x_{i,k}$ denotes the k'th component of $\mathbf{x}_i$, and $y_{j,k}$ denotes the k'th component of $\mathbf{y}_j$. Observe that for all $\mathbf{z} \in \mathcal{Z}^n$, and all i, i', j, and j',

$$\begin{aligned}
\mathsf{E}[\,W^n(\mathbf{z}|\mathbf{x}_{i'}, \mathbf{y}_{j'}, \mathbf{S}_{ij})\,] \;&=\; \prod_{k=1}^{n} \mathsf{E}[\,W(z_k|x_{i',k}, y_{j',k}, S_{ij,k})\,] \\
&=\; \prod_{k=1}^{n} \sum_{s} W(z_k|x_{i',k}, y_{j',k}, s) U(s|x_{i,k}, y_{j,k}) \\
&=\; \prod_{k=1}^{n} \sum_{s} W(z_k|x_{i,k}, y_{j,k}, s) U(s|x_{i',k}, y_{j',k}) \\
&=\; \mathsf{E}[\,W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{S}_{i'j'})\,], \qquad (3.10)
\end{aligned}$$

where the third equality follows by symmetrizability-$\mathcal{XY}$. Next, let

$$e((i',j'),(i,j)) \;\triangleq\; \mathsf{E}[\,W^n(\{\mathbf{z} : \varphi(\mathbf{z}) \neq (i',j')\}|\mathbf{x}_{i'}, \mathbf{y}_{j'}, \mathbf{S}_{ij})\,].$$

By (3.10),

$$\begin{aligned}
e((i',j'),(i,j)) \;&=\; \sum_{\mathbf{z}:\varphi(\mathbf{z})\neq(i',j')} \mathsf{E}[\,W^n(\mathbf{z}|\mathbf{x}_{i'}, \mathbf{y}_{j'}, \mathbf{S}_{ij})\,] \\
&=\; \sum_{\mathbf{z}:\varphi(\mathbf{z})\neq(i',j')} \mathsf{E}[\,W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{S}_{i'j'})\,] \\
&=\; \mathsf{E}\Big[\sum_{\mathbf{z}:\varphi(\mathbf{z})\neq(i',j')} W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{S}_{i'j'})\Big]. \qquad (3.11)
\end{aligned}$$

Now, if $(i,j) \neq (i',j')$ and $\varphi(\mathbf{z}) = (i,j)$, then $\varphi(\mathbf{z}) \neq (i',j')$. With this fact in mind, we can use (3.11) to write, if $(i,j) \neq (i',j')$,

$$
\begin{aligned}
e((i,j),(i',j')) \;+\; & e((i',j'),(i,j)) \\
&= \mathsf{E}\Big[\sum_{\mathbf{z}:\varphi(\mathbf{z})\neq(i,j)} W^n(\mathbf{z}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{S}_{i'j'}) + \sum_{\mathbf{z}:\varphi(\mathbf{z})\neq(i',j')} W^n(\mathbf{z}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{S}_{i'j'})\Big] \\
&\geq \mathsf{E}\Big[\sum_{\mathbf{z}:\varphi(\mathbf{z})\neq(i,j)} W^n(\mathbf{z}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{S}_{i'j'}) + \sum_{\mathbf{z}:\varphi(\mathbf{z})=(i,j)} W^n(\mathbf{z}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{S}_{i'j'})\Big] \\
&= 1.
\end{aligned} \tag{3.12}
$$

Now, set

$$
e(\mathbf{s}) \;\triangleq\; \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\{\mathbf{z}:\varphi(\mathbf{z})\neq(i,j)\}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{s}). \tag{3.13}
$$

Then

$$
\mathsf{E}[\,e(\mathbf{S}_{i'j'})\,] \;=\; \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} e((i,j),(i',j')).
$$

Next, observe that

$$
\begin{aligned}
\frac{1}{NM}\sum_{i'=1}^{N}\sum_{j'=1}^{M}\mathsf{E}[\,e(\mathbf{S}_{i'j'})\,] \;&=\; \frac{1}{(NM)^2}\sum_{i',j'}\sum_{i,j} e((i,j),(i',j')) \\
&\geq\; \frac{1}{(NM)^2}\,\frac{(NM)[(NM)-1]}{2}, \qquad \text{by (3.12)}, \\
&=\; \frac{(NM)-1}{2(NM)} \\
&\geq\; 1/4, \qquad \text{since } NM \geq 2.
\end{aligned}
$$

From this it follows that for some i', j', $\mathsf{E}[\,e(\mathbf{S}_{i'j'})\,] \geq 1/4$, which in turn implies the existence of at least one $\mathbf{s} \in \mathcal{S}^n$ for which (3.9) holds. □

Lemma 3.10 *If the AVC W is symmetrizable-$\mathcal{X}$, then*

$$
C(W) \;=\; \{0\} \times [0, C_2(W)],
$$

where $C_2(W) \leq \sup_{p,q} I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W)$.

Proof. The proof is similar to that of the previous Theorem. Let n be any positive integer. Let N and M be positive integers. Suppose $\mathbf{x}_1, \ldots, \mathbf{x}_N$, each in $\mathcal{X}^n$, are codewords for user 1, and suppose $\mathbf{y}_1, \ldots, \mathbf{y}_M$, each in $\mathcal{Y}^n$, are codewords for user 2. Let $\varphi(\mathbf{z}) = (\varphi_1(\mathbf{z}), \varphi_2(\mathbf{z}))$ be any decoder such that $\varphi_1 \colon \mathcal{Z}^n \to \{1, \ldots, N\}$ and $\varphi_2 \colon \mathcal{Z}^n \to \{1, \ldots, M\}$. If $N \geq 2$, we will show below, by using a procedure similar to that in [8], that there exists some $\mathbf{s} \in \mathcal{S}^n$ with

$$\frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(\{\mathbf{z} \in \mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\} | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \;\geq\; 1/4. \tag{3.14}$$

In other words, if $N > 1$, the code can not have an arbitrarily small probability of error for *every* $\mathbf{s} \in \mathcal{S}^n$. Since the alternative $N = 1$ implies $\frac{\log N}{n} = 0$, all achievable rate pairs must have the form $(0, R_2)$. Clearly, $C_2(W)$ is the largest value of R_2 such that the pair $(0, R_2)$ is achievable. By Jahn's weak converse (3.4), $C_2(W) \leq \sup_{p,q} I^*_{\mathcal{Y} \wedge \mathcal{Z}|\mathcal{X}}(p, q, W)$.

Suppose $N \geq 2$. Since W is symmetrizable-$\mathcal{X}$, let U be a symmetrizing transition probability satisfying (3.7). For each $1 \leq i \leq N$, let

$$\mathbf{S}_i \;=\; (S_{i,1}, \ldots, S_{i,n})$$

be an $\mathcal{S}^n$-valued RV whose components are independent and distributed according to

$$\mathsf{P}(S_{i,k} = s) \;=\; U(s|x_{i,k}), \qquad 1 \leq k \leq n.$$

Observe that for all $\mathbf{z} \in \mathcal{Z}^n$, and all i, i', and j,

$$\begin{aligned}
\mathsf{E}[\, W^n(\mathbf{z}|\mathbf{x}_{i'}, \mathbf{y}_j, \mathbf{S}_i)\,] \;&=\; \prod_{k=1}^{n} \mathsf{E}[\, W(z_k|x_{i',k}, y_{j,k}, S_{i,k})\,] \\
&=\; \prod_{k=1}^{n} \sum_{s} W(z_k|x_{i',k}, y_{j,k}, s) U(s|x_{i,k}) \\
&=\; \prod_{k=1}^{n} \sum_{s} W(z_k|x_{i,k}, y_{j,k}, s) U(s|x_{i',k}) \\
&=\; \mathsf{E}[\, W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{S}_{i'})\,],
\end{aligned} \tag{3.15}$$

with the third equality following from symmetrizability-$\mathcal{X}$. Next, let

$$e(i',i) \triangleq \frac{1}{M}\sum_{j=1}^{M} \mathsf{E}[\,W^n(\{\mathbf{z}:\varphi_1(\mathbf{z})\neq i'\}|\mathbf{x}_{i'},\mathbf{y}_j,\mathbf{S}_i)\,].$$

By (3.15),

$$\begin{aligned} e(i',i) &= \frac{1}{M}\sum_{j=1}^{M}\sum_{\mathbf{z}:\varphi_1(\mathbf{z})\neq i'} \mathsf{E}[\,W^n(\mathbf{z}|\mathbf{x}_{i'},\mathbf{y}_j,\mathbf{S}_i)\,] \\ &= \frac{1}{M}\sum_{j=1}^{M}\sum_{\mathbf{z}:\varphi_1(\mathbf{z})\neq i'} \mathsf{E}[\,W^n(\mathbf{z}|\mathbf{x}_{i},\mathbf{y}_j,\mathbf{S}_{i'})\,] \\ &= \frac{1}{M}\sum_{j=1}^{M}\mathsf{E}\Big[\sum_{\mathbf{z}:\varphi_1(\mathbf{z})\neq i'} W^n(\mathbf{z}|\mathbf{x}_{i},\mathbf{y}_j,\mathbf{S}_{i'})\Big]. \end{aligned} \tag{3.16}$$

Now, if $i\neq i'$ and $\varphi_1(\mathbf{z})=i$, then $\varphi_1(\mathbf{z})\neq i'$. With this fact in mind, we can use (3.16) to write, if $i\neq i'$,

$$\begin{aligned} e(i,i') &+ e(i',i) \\ &= \frac{1}{M}\sum_{j=1}^{M}\mathsf{E}\Big[\sum_{\mathbf{z}:\varphi_1(\mathbf{z})\neq i} W^n(\mathbf{z}|\mathbf{x}_{i},\mathbf{y}_j,\mathbf{S}_{i'}) + \sum_{\mathbf{z}:\varphi_1(\mathbf{z})\neq i'} W^n(\mathbf{z}|\mathbf{x}_{i},\mathbf{y}_j,\mathbf{S}_{i'})\Big] \\ &\geq \frac{1}{M}\sum_{j=1}^{M}\mathsf{E}\Big[\sum_{\mathbf{z}:\varphi_1(\mathbf{z})\neq i} W^n(\mathbf{z}|\mathbf{x}_{i},\mathbf{y}_j,\mathbf{S}_{i'}) + \sum_{\mathbf{z}:\varphi_1(\mathbf{z})= i} W^n(\mathbf{z}|\mathbf{x}_{i},\mathbf{y}_j,\mathbf{S}_{i'})\Big] \\ &= 1. \end{aligned} \tag{3.17}$$

Now, recalling the definition of $e(\mathbf{s})$ in (3.13), we observe that

$$e(\mathbf{s}) \geq e_{\mathcal{X}}(\mathbf{s}) \triangleq \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\{\mathbf{z}:\varphi_1(\mathbf{z})\neq i\}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{s}).$$

Then

$$\mathsf{E}[\,e_{\mathcal{X}}(\mathbf{S}_{i'})\,] = \frac{1}{N}\sum_{i=1}^{N} e(i,i').$$

Next, observe that

$$\begin{aligned}
\frac{1}{N}\sum_{i'=1}^{N}\mathsf{E}[e_{\mathcal{X}}(\mathbf{S}_{i'})] &= \frac{1}{N^2}\sum_{i'}\sum_{i}e(i,i') \\
&\geq \frac{1}{N^2}\frac{N(N-1)}{2}, \qquad \text{by (3.17)}, \\
&= \frac{N-1}{2N} \\
&\geq 1/4, \qquad \text{since } N \geq 2.
\end{aligned}$$

From this it follows that for some i', $\mathsf{E}[e_{\mathcal{X}}(\mathbf{S}_{i'})] \geq 1/4$, which in turn implies the existence of some $\mathbf{s} \in \mathcal{S}^n$ with $e(\mathbf{s}) \geq e_{\mathcal{X}}(\mathbf{s}) \geq 1/4$ so that (3.14) holds. □

By interchanging the roles of $\mathcal{X}$ and $\mathcal{Y}$, we have the obvious analog of the preceding lemma.

Lemma 3.11 *If the AVC W is symmetrizable-$\mathcal{Y}$, then*

$$C(W) = [0, C_1(W)] \times \{0\},$$

where $C_1(W) \leq \sup_{p,q} I^*_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W)$.

Corollary 3.12 *If the AVC W is symmetrizable-$\mathcal{X}$ and symmetrizable-$\mathcal{Y}$, then*

$$C(W) = \{(0,0)\}.$$

Clearly, the three kinds of symmetrizability defined above give simple conditions under which $C(W)$ will have an empty interior. While we conjecture that if W is nonsymmetrizable-$\mathcal{XY}$, nonsymmetrizable-$\mathcal{X}$, and nonsymmetrizable-$\mathcal{Y}$, then every pair $(R_1, R_2) \in \mathcal{R}^*(W)$ is achievable, we have been unable to prove this. In order to state what we can prove, we need the following two definitions.

Definition 3.13 For any $q \in \mathcal{D}(\mathcal{Y})$, we say qW is *symmetrizable-$\mathcal{X}$* if there exists a transition probability U from $\mathcal{X}$ into $\mathcal{S}$ such that

$$\sum_s (qW)(z|x,s)U(s|x') = \sum_s (qW)(z|x',s)U(s|x), \qquad \forall x, x', z. \tag{3.18}$$

If no such U exists, we say that qW is *nonsymmetrizable-$\mathcal{X}$*.

Remark. If W is symmetrizable-$\mathcal{X}\mathcal{Y}$ and U satisfies (3.6), and if q is any element of $\mathcal{D}(\mathcal{Y})$, then multiplying both sides by $q(y)q(y')$ and summing over all y, y' shows that qW is symmetrizable-$\mathcal{X}$. Similarly, if W is symmetrizable-$\mathcal{X}$ and U satisfies (3.7), multiplying both sides by $q(y)$ and summing over all y shows that qW is symmetrizable-$\mathcal{X}$ for every $q \in \mathcal{D}(\mathcal{Y})$.

Definition 3.14 For any $p \in \mathcal{D}(\mathcal{X})$, we say pW is *symmetrizable-$\mathcal{Y}$* if there exists a transition probability U from $\mathcal{Y}$ into $\mathcal{S}$ such that

$$\sum_s (pW)(z|y,s)U(s|y') \;=\; \sum_s (pW)(z|y',s)U(s|y), \qquad \forall y,\, y',\, z. \tag{3.19}$$

If no such U exists, we say that pW is *nonsymmetrizable-$\mathcal{Y}$*.

3.3 Achievable Rates

In this section we prove that there are nonempty, open rectangles of achievable rate pairs for the AVC W, provided certain nonsymmetrizability conditions are satisfied.

Theorem 3.15 *Suppose W is nonsymmetrizable-$\mathcal{Y}$. Fix any $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$. Further, suppose qW is nonsymmetrizable-$\mathcal{X}$. If*

$$0 \;<\; R_1 \;<\; I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) \tag{3.20}$$

and

$$0 \;<\; R_2 \;<\; I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W), \tag{3.21}$$

then (R_1, R_2) is achievable in the sense of Definition 3.1.

Remark 3.16 Suppose $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$ are strictly positive. If qW is nonsymmetrizable-$\mathcal{X}$, and if W is nonsymmetrizable-$\mathcal{Y}$, then $I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W)$ and $I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W)$ are both strictly positive. To see this, suppose $I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) = 0$. Then there is some $r \in \mathcal{D}(\mathcal{S})$ with $I_{\mathcal{X}\wedge\mathcal{Z}}(p \times q \times rW) = 0$. This implies $\sum_s (qW)(z|x,s)r(s)$ is not a function of x. But then taking $U(s|x) = r(s)$ will symmetrize qW. Similarly, if $I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W) = 0$, there is some $r \in \mathcal{D}(\mathcal{S})$ with $I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p \times q \times rW) = 0$. This implies $\sum_s W(z|x,y,s)r(s)$ is not a function of y. Taking $U(s|y) = r(s)$ shows that W is symmetrizable-$\mathcal{Y}$. An analogous observation for single-user AVC's was made in [8].

Upon proving Theorem 3.15 we must also have the following analog obtained by interchanging the roles of $\mathcal{X}$ and $\mathcal{Y}$.

Theorem 3.17 *Suppose W is nonsymmetrizable-$\mathcal{X}$. Fix any $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$. Further, suppose pW is nonsymmetrizable-$\mathcal{Y}$. If*

$$0 < R_1 < I^*_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W) \quad \text{and} \quad 0 < R_2 < I^*_{\mathcal{Y}\wedge\mathcal{Z}}(p,q,W),$$

then (R_1, R_2) is achievable in the sense of Definition 3.1.

Before proceeding with the proof of Theorem 3.15, we need to introduce two auxiliary functions and an associated lemma. Observe that W is symmetrizable-$\mathcal{Y}$ if and only if for some transition probability U from $\mathcal{Y}$ into $\mathcal{S}$ we have

$$F^W_{\mathcal{Y}}(U) = 0,$$

where

$$F^W_{\mathcal{Y}}(U) \triangleq \max_{x,y,y',z} \left| \sum_s W(z|x,y,s)U(s|y') - \sum_s W(z|x,y',s)U(s|y) \right|. \tag{3.22}$$

Now, let

$$\xi_{\mathcal{Y}}(W) \triangleq \inf_U F_{\mathcal{Y}}^W(U). \tag{3.23}$$

Since $F_{\mathcal{Y}}^W$ is a continuous function on the compact set of transition probabilities from $\mathcal{Y}$ into $\mathcal{S}$, the infimum in (3.23) is always achieved. It follows that W is symmetrizable-$\mathcal{Y}$ if and only if $\xi_{\mathcal{Y}}(W) = 0$. Similarly, if $q \in \mathcal{D}(\mathcal{Y})$, and if U is any transition probability from $\mathcal{X}$ into $\mathcal{S}$, we let

$$F_{\mathcal{X}}^W(q,U) \triangleq \max_{x,x',z} \Big| \sum_s (qW)(z|x,s)U(s|x') - \sum_s (qW)(z|x',s)U(s|x) \Big|, \tag{3.24}$$

and we set

$$\xi_{\mathcal{X}}(q,W) \triangleq \inf_U F_{\mathcal{X}}^W(q,U). \tag{3.25}$$

The following lemma says that $\xi_{\mathcal{X}}(q,W)$ is a uniformly continuous function of $q \in \mathcal{D}(\mathcal{Y})$.

Lemma 3.18 *For any q, $\hat{q} \in \mathcal{D}(\mathcal{Y})$,*

$$|\xi_{\mathcal{X}}(q,W) - \xi_{\mathcal{X}}(\hat{q},W)| \leq d(q,\hat{q}).$$

Proof. Fix any transition probability U from $\mathcal{X}$ into $\mathcal{S}$. We appeal to the inequality $||a| - |b|| \leq |a - b|$ with

$$a = \sum_s (qW)(z|x,s)U(s|x') - \sum_s (qW)(z|x',s)U(s|x),$$

and

$$b = \sum_s (\hat{q}W)(z|x,s)U(s|x') - \sum_s (\hat{q}W)(z|x',s)U(s|x).$$

Now,

$$\begin{aligned} a - b &= \sum_y [q(y) - \hat{q}(y)] \sum_s W(z|x,y,s)U(s|x') \\ &\qquad + \sum_y [\hat{q}(y) - q(y)] \sum_s W(z|x',y,s)U(s|x) \\ &= \sum_y [q(y) - \hat{q}(y)] \Big(\sum_s W(z|x,y,s)U(s|x') - \sum_s W(z|x',y,s)U(s|x) \Big). \end{aligned}$$

So, $||a| - |b|| \leq |a - b| \leq d(q, \hat{q}) F_X^W(U) \leq d(q, \hat{q})$. Hence, we can write

$$|a| \leq |b| + d(q, \hat{q}) \qquad \text{and} \qquad |b| \leq |a| + d(q, \hat{q}).$$

It now follows that

$$F_X^W(q, U) \leq F_X^W(\hat{q}, U) + d(q, \hat{q}) \qquad \text{and} \qquad F_X^W(\hat{q}, U) \leq F_X^W(q, U) + d(q, \hat{q}),$$

and that

$$\xi_X(q, W) \leq \xi_X(\hat{q}, W) + d(q, \hat{q}) \qquad \text{and} \qquad \xi_X(\hat{q}, W) \leq \xi_X(q, W) + d(q, \hat{q}).$$

□

Theorem 3.19 *If W is nonsymmetrizable-$\mathcal{Y}$ and there exists a $q \in \mathcal{D}(\mathcal{Y})$ such that qW is nonsymmetrizable-$\mathcal{X}$, or if W is nonsymmetrizable-$\mathcal{X}$ and there exists a $p \in \mathcal{D}(\mathcal{X})$ such that pW is nonsymmetrizable-$\mathcal{Y}$, then $C(W) = \mathcal{R}^*(W)$.*

Proof. By Jahn's weak converse, inclusion (3.4), $C(W) \subset \mathcal{R}^*(W)$. Now, suppose that W is nonsymmetrizable-$\mathcal{Y}$ and that for some q, qW is nonsymmetrizable-$\mathcal{X}$. By combining the preceding lemma with Lemma 2.16, we may assume that q is strictly positive. Choose any positive $p \in \mathcal{D}(\mathcal{X})$. By Remark 3.16, $I^*_{\mathcal{X} \wedge \mathcal{Z}}(p, q, W)$ and $I^*_{\mathcal{Y} \wedge \mathcal{Z}|\mathcal{X}}(p, q, W)$ are both positive. By Theorem 3.15, $C(W)$ has a nonempty interior, and by Jahn's forward result, inclusion (3.5), $\mathcal{R}^*(W) \subset C(W)$. □

Proof of Theorem 3.15. Let us first state explicitly what we shall prove.

> Provided that the hypotheses of the theorem hold, we shall prove that there exists an $\varepsilon > 0$ such that for all sufficiently large n, if we take $N = \lfloor \exp(nR_1) \rfloor$ and $M = \lfloor \exp(nR_2) \rfloor$, then there exist codewords $\mathbf{x}_1, \ldots, \mathbf{x}_N$ for user 1, each in $\mathcal{X}^n$, and there exist codewords $\mathbf{y}_1, \ldots, \mathbf{y}_M$ for user 2, each in $\mathcal{Y}^n$, and there exists a decoder φ with

$$\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\{\mathbf{z}\in\mathcal{Z}^n:\varphi(\mathbf{z})\neq(i,j)\}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{s}) \;\leq\; \exp(-n\epsilon/8), \qquad \forall \mathbf{s}\in\mathcal{S}^n. \tag{3.26}$$

Now, suppose that R_1 satisfies (3.20) and R_2 satisfies (3.21). Then we can choose $\delta > 0$ so small that (cf. (3.23) and (3.25))

$$\begin{aligned} 0 \;<\; 2\delta \;&<\; \min\{\xi_{\mathcal{X}}(q,W),\xi_{\mathcal{Y}}(W)\}, \\ 0 \;<\; R_1 \;&<\; I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W)-2\delta, \\ 0 \;<\; R_2 \;&<\; I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W)-2\delta. \end{aligned} \tag{3.27}$$

Next, observe that we can always find $\hat{p}\in\mathcal{D}(\mathcal{X})$ and $\hat{q}\in\mathcal{D}(\mathcal{Y})$ such that for all $x\in\mathcal{X}$, $\hat{p}(x)>0$, and for all $y\in\mathcal{Y}$, $\hat{q}(y)>0$, and such that $d(p,\hat{p})$ and $d(q,\hat{q})$ are both sufficiently small so that

$$\begin{aligned} \xi_{\mathcal{X}}(q,W) \;&\leq\; \xi_{\mathcal{X}}(\hat{q},W)+\delta/2, \\ I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) \;&\leq\; I^*_{\mathcal{X}\wedge\mathcal{Z}}(\hat{p},\hat{q},W)+\delta/2, \\ I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W) \;&\leq\; I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(\hat{p},\hat{q},W)+\delta/2. \end{aligned}$$

Let $\beta \triangleq \frac{1}{2}\min\{\min_x \hat{p}(x), \min_y \hat{q}(y)\} > 0$. Choose η with

$$0 \;<\; \eta \;<\; \min\left\{\frac{\delta}{2}, \frac{\beta^4\delta^2}{16\ln 2}, \frac{\beta^6\delta^2}{16\ln 2}\right\}, \tag{3.28}$$

and so small that if $P^{(1)}$ and $P^{(2)}$ are any two distributions on $\mathcal{X}\times\mathcal{Z}$ or on $\mathcal{X}\times\mathcal{Y}\times\mathcal{Z}$ with $D(P^{(1)}\|P^{(2)})\leq\eta$, then

$$|I_{\mathcal{X}\wedge\mathcal{Z}}(P^{(1)}) - I_{\mathcal{X}\wedge\mathcal{Z}}(P^{(2)})| \;<\; \delta/2 \tag{3.29}$$

and

$$|I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P^{(1)}) - I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P^{(2)})| \;<\; \delta/2. \tag{3.30}$$

Now, for fixed $\mathbf{s} \in \mathcal{S}^n$, let

$$e(\mathbf{s}) \triangleq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(\{\mathbf{z} \in \mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\} | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}).$$

Clearly, applying the union bound followed by (3.40) and (3.44) yields,

$$\begin{aligned} e(\mathbf{s}) &\leq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(F_i^c \cup G_{ij}^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\leq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(F_i^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\quad + \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(G_{ij}^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\leq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(J_i^0(\mathbf{s})^c \cup J_i^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\quad + \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(K_{ij}^0(\mathbf{s})^c \cup K_{ij}^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}). \end{aligned}$$

Next, observe that

$$K_{ij}^0(\mathbf{s}) \subset J_i^0(\mathbf{s}) \implies J_i^0(\mathbf{s})^c \subset K_{ij}^0(\mathbf{s})^c,$$

and apply the union bound again to obtain

$$\begin{aligned} e(\mathbf{s}) \leq \frac{2}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} & W^n(K_{ij}^0(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &+ \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(J_i^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &+ \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(K_{ij}^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}). \end{aligned} \tag{3.45}$$

We now turn to the task of bounding $e(\mathbf{s})$ uniformly for $\mathbf{s} \in \mathcal{S}^n$. Each of the three preceding sums will be treated separately. To begin, let

$$e_0(\mathbf{s}) \triangleq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(K_{ij}^0(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}). \tag{3.46}$$

Set

$$A(\mathbf{s}) \triangleq \{i : I(\mathbf{x}_i \wedge \mathbf{s}) > \varepsilon\},$$

In the remainder of this proof we drop the underscore from $\underline{R}_1$ and $\underline{R}_2$; hence, from here until the end of the proof, references to R_1, R_2, (3.32), and (3.33) are actually references to $\underline{R}_1$, $\underline{R}_2$, (3.35), and (3.36). Also note that this convention means that instead of (3.34), we can write

$$N = \exp(nR_1) \qquad \text{and} \qquad M = \exp(nR_2).$$

Regard n as fixed so large that we have found $P \in \mathcal{P}_n(\mathcal{X})$ and $Q \in \mathcal{P}_n(\mathcal{Y})$ satisfying (3.32) and (3.33). Now, assuming n is large enough,[2] we select codewords for user 1, $\mathrm{x}_1, \ldots, \mathrm{x}_N$, *each of type* $P \in \mathcal{P}_n(\mathcal{X})$, and we select codewords for user 2, $\mathrm{y}_1, \ldots, \mathrm{y}_M$, *each of type* $Q \in \mathcal{P}_n(\mathcal{Y})$, such that the codeword properties we use below in the proof will hold. The fact that we can do this is the subject of Theorem 3.22. Since the properties that we need seem quite strange at first, we will not introduce them until they appear naturally in the course of the proof. The reader is referred to Theorem 3.22 for a complete description of these properties.

We now define the decoding rule. To do this, we shall use the following subsets of $\mathcal{Z}^n$. For $\mathrm{s} \in \mathcal{S}^n$, and $i = 1, \ldots, N$, let

$$J_i^0(\mathrm{s}) \triangleq \{\mathrm{z} \in \mathcal{Z}^n : D(P_{\mathrm{x}_i,\mathrm{s},\mathrm{z}} \| P \times P_{\mathrm{s}} \times QW) \leq \eta\}. \tag{3.37}$$

Next, let

$$J_i^0 \triangleq \bigcup_{\mathrm{s}'' \in \mathcal{S}^n} J_i^0(\mathrm{s}'').$$

If $\mathrm{z} \in J_i^0(\mathrm{s})$, then we say that $(\mathrm{x}_i, \mathrm{s}, \mathrm{z})$ is *jointly typical.* Thus, if $\mathrm{z} \in J_i^0$, there must be some $\mathrm{s}'' \in \mathcal{S}^n$ with $(\mathrm{x}_i, \mathrm{s}'', \mathrm{z})$ jointly typical. What we would like to do is use a decoder which decides message i was sent whenever $\mathrm{z} \in J_i^0$ and $\mathrm{z} \notin J_{i'}^0$ for all $i' \neq i$. In other words, if there is a unique i such that $\mathrm{z} \in J_i^0$, then we

[2]How large depends only on ε and on the cardinalities of the sets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{S}$.

would decide message i was sent. Unfortunately, this approach, sometimes called *typicality decoding*, will not suffice for a general AVC. We need a stronger decoding rule. To help us decide between i and i' when $\mathbf{z}$ belongs to both J_i^0 and $J_{i'}^0$, we will use the set

$$J_i^1(\mathbf{s}) \triangleq \{\mathbf{z} \in \mathcal{Z}^n : \forall i' \neq i, \mathbf{z} \in J_{i'}^0 \Longrightarrow I(\mathbf{x}_i\mathbf{z} \wedge \mathbf{x}_{i'}|\mathbf{s}) \leq \eta\}, \tag{3.38}$$

where $I(\mathbf{x}_i\mathbf{z} \wedge \mathbf{x}_{i'}|\mathbf{s})$ denotes $I(XZ \wedge X'|S)$ computed using $P_{XX'SZ} = P_{\mathbf{x}_i,\mathbf{x}_{i'},\mathbf{s},\mathbf{z}}$. Let

$$F_i \triangleq \bigcup_{\mathbf{s}' \in \mathcal{S}^n} [J_i^0(\mathbf{s}') \cap J_i^1(\mathbf{s}')]. \tag{3.39}$$

We note that this definition implies that for any fixed $\mathbf{s} \in \mathcal{S}^n$,

$$F_i^c = \bigcap_{\mathbf{s}' \in \mathcal{S}^n} [J_i^0(\mathbf{s}')^c \cup J_i^1(\mathbf{s}')^c] \subset [J_i^0(\mathbf{s})^c \cup J_i^1(\mathbf{s})^c]. \tag{3.40}$$

We claim that $F_1, \ldots, F_N$ are pairwise disjoint. This is a consequence of the assumption that qW is nonsymmetrizable-$\mathcal{X}$; see Section 3.5. Let φ_1 be any mapping defined on $\mathcal{Z}^n$ such that for each i,

$$\mathbf{z} \in F_i \Longrightarrow \varphi_1(\mathbf{z}) = i, \tag{3.41}$$

i.e., $F_i \subset \mathcal{Z}^n$ is the *decoding set* for message i. Note that in general, $\bigcup_{i=1}^{N} F_i$ is a proper subset of $\mathcal{Z}^n$; however, it will turn out that any φ_1 satisfying (3.41) will suffice. To summarize, the mapping φ_1 will assign message i to the output $\mathbf{z}$ if for some $\mathbf{s}'$, $(\mathbf{x}_i, \mathbf{s}', \mathbf{z})$ is jointly typical *and*, whenever $i' \neq i$ is such that $(\mathbf{x}_{i'}, \mathbf{s}'', \mathbf{z})$ is jointly typical for some $\mathbf{s}''$, then $I(\mathbf{x}_i\mathbf{z} \wedge \mathbf{x}_{i'}|\mathbf{s}') \leq \eta$. It remains to define the decoding rule for the messages of user 2. To this end, for each $i = 1, \ldots, N$ and each $j = 1, \ldots, M$, let

$$K_{ij}^0(\mathbf{s}) \triangleq \{\mathbf{z} \in \mathcal{Z}^n : D(P_{\mathbf{x}_i,\mathbf{y}_j,\mathbf{s},\mathbf{z}} \| P \times Q \times P_{\mathbf{s}} \times W) \leq \eta\}, \tag{3.42}$$

$$K_{ij}^0 \triangleq \bigcup_{\mathbf{s}'' \in \mathcal{S}^n} K_{ij}^0(\mathbf{s}''),$$

$$K_{ij}^1(\mathbf{s}) \triangleq \{\mathbf{z} \in \mathcal{Z}^n : \forall j' \neq j, \mathbf{z} \in K_{ij'}^0 \Longrightarrow I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{y}_{j'}|\mathbf{s}) \leq \eta\}.$$

Now let

$$G_{ij} \triangleq \bigcup_{\mathbf{s}' \in \mathcal{S}^n} [K_{ij}^0(\mathbf{s}') \cap K_{ij}^1(\mathbf{s}')]. \tag{3.43}$$

Clearly, for any fixed $\mathbf{s} \in \mathcal{S}^n$,

$$G_{ij}^c \subset [K_{ij}^0(\mathbf{s})^c \cup K_{ij}^1(\mathbf{s})^c]. \tag{3.44}$$

We claim that for each i, $G_{i1}, \ldots, G_{iM}$ are pairwise disjoint. This is a consequence of the assumption that W is nonsymmetrizable-$\mathcal{Y}$; we establish this claim in Section 3.5. Let φ_2 be any mapping defined on $\mathcal{Z}^n$ such that for all i, j,

$$\mathbf{z} \in F_i \cap G_{ij} \Longrightarrow \varphi_2(\mathbf{z}) = j.$$

Let

$$\varphi(\mathbf{z}) \triangleq (\varphi_1(\mathbf{z}), \varphi_2(\mathbf{z}$$

In other words, we first try to decode message i from user 1, and only then do we try to decode message j from user 2. (The idea of first decoding message i and then decoding message j also appears in the context of source coding; see Slepian and Wolf [18].) It is now easy to see that

$$\varphi(\mathbf{z}) \neq (i,j) \Longrightarrow \varphi_1(\mathbf{z}) \neq i \quad \text{or} \quad \varphi_2(\mathbf{z}) \neq j,$$

or, in terms of the decoding sets,

$$\varphi(\mathbf{z}) \neq (i,j) \Longrightarrow \mathbf{z} \in F_i^c \cup [F_i^c \cup G_{ij}^c] = F_i^c \cup G_{ij}^c.$$

Now, for fixed $\mathbf{s} \in \mathcal{S}^n$, let

$$e(\mathbf{s}) \triangleq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(\{\mathbf{z} \in \mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i,j)\} | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}).$$

Clearly, applying the union bound followed by (3.40) and (3.44) yields,

$$\begin{aligned} e(\mathbf{s}) &\leq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(F_i^c \cup G_{ij}^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\leq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(F_i^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\quad + \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(G_{ij}^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\leq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(J_i^0(\mathbf{s})^c \cup J_i^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\quad + \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(K_{ij}^0(\mathbf{s})^c \cup K_{ij}^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}). \end{aligned}$$

Next, observe that

$$K_{ij}^0(\mathbf{s}) \subset J_i^0(\mathbf{s}) \implies J_i^0(\mathbf{s})^c \subset K_{ij}^0(\mathbf{s})^c,$$

and apply the union bound again to obtain

$$\begin{aligned} e(\mathbf{s}) &\leq \frac{2}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(K_{ij}^0(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\quad + \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(J_i^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\quad + \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(K_{ij}^1(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}). \end{aligned} \tag{3.45}$$

We now turn to the task of bounding $e(\mathbf{s})$ uniformly for $\mathbf{s} \in \mathcal{S}^n$. Each of the three preceding sums will be treated separately. To begin, let

$$e_0(\mathbf{s}) \triangleq \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(K_{ij}^0(\mathbf{s})^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}). \tag{3.46}$$

Set

$$A(\mathbf{s}) \triangleq \{i : I(\mathbf{x}_i \wedge \mathbf{s}) > \epsilon\},$$

and

$$B(\mathrm{s},\mathrm{x}_i) \triangleq \{j : I(\mathrm{y}_j \wedge \mathrm{x}_i\mathrm{s}) > \varepsilon\}.$$

Then

$$e_0(\mathrm{s}) \leq \frac{1}{N}|A(\mathrm{s})| + \frac{1}{N}\sum_{i\notin A(\mathrm{s})}\frac{1}{M}\sum_{j=1}^{M} W^n(K_{ij}^0(\mathrm{s})^c|\mathrm{x}_i,\mathrm{y}_j,\mathrm{s}).$$

Continuing,

$$\begin{aligned} e_0(\mathrm{s}) &\leq \frac{1}{N}|A(\mathrm{s})| + \frac{1}{N}\sum_{i\notin A(\mathrm{s})}\Big(\frac{1}{M}|B(\mathrm{s},\mathrm{x}_i)| + \frac{1}{M}\sum_{j\notin B(\mathrm{s},\mathrm{x}_i)} W^n(K_{ij}^0(\mathrm{s})^c|\mathrm{x}_i,\mathrm{y}_j,\mathrm{s})\Big) \\ &\leq \frac{1}{N}|A(\mathrm{s})| + \frac{1}{M}\max_i |B(\mathrm{s},\mathrm{x}_i)| \\ &\quad + \frac{1}{NM}\sum_{i\notin A(\mathrm{s})}\Big(\sum_{j\notin B(\mathrm{s},\mathrm{x}_i)} W^n(K_{ij}^0(\mathrm{s})^c|\mathrm{x}_i,\mathrm{y}_j,\mathrm{s})\Big). \end{aligned} \tag{3.47}$$

Fix $i \notin A(\mathrm{s})$ and $j \notin B(\mathrm{s},\mathrm{x}_i)$ and observe that if $P_{XYSZ} \in \mathcal{D}_n(\mathcal{Z}|\mathrm{x}_i,\mathrm{y}_j,\mathrm{s})$, then $I(X \wedge S) \leq \varepsilon$ and $I(Y \wedge XS) \leq \varepsilon$. Now, write

$$K_{ij}^0(\mathrm{s})^c = \bigcup_{P_{XYSZ}\in\mathcal{D}_n(\mathcal{Z}|\mathrm{x}_i,\mathrm{y}_j,\mathrm{s}):\, D(P_{XYSZ}\|P\times Q\times P_S\times W)>\eta} \mathcal{T}_{Z|XYS}(\mathrm{x}_i,\mathrm{y}_j,\mathrm{s}).$$

Then using (2.11), the union bound, and the Type Counting Lemma (see Notes following (3.48) below),

$$\begin{aligned} W^n(K_{ij}^0(\mathrm{s})^c|\mathrm{x}_i,\mathrm{y}_j,\mathrm{s}) &\leq \sum \exp(-nD(P_{XYSZ}\|P_{XYS}\times W)) \\ &= \sum \exp[-n(D(P_{XYSZ}\|P\times Q\times P_S\times W) \\ &\qquad - I(X\wedge S) - I(Y\wedge XS))] \\ &\leq \sum \exp[-n(\eta-2\varepsilon)] \\ &\leq (n+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}||\mathcal{Z}|}\exp[-n(\eta-2\varepsilon)] \\ &\leq \exp[-n(\eta-3\varepsilon)] \\ &\leq \exp(-2n\varepsilon), \qquad \text{since } \eta \geq 5\varepsilon. \end{aligned} \tag{3.48}$$

Notes. (i) The summations are understood to be over all

$$P_{XYSZ} \in \mathcal{D}_n(\mathcal{Z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \text{ such that } D(P_{XYSZ}\|P \times Q \times P_S \times W) > \eta.$$

(ii) We assume n is so large that $(n+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}||\mathcal{Z}|} \leq \exp(n\varepsilon)$. We caution the reader that we will make similar assumptions as needed below without comment.

Now, it is a property of our codewords (Theorem 3.22, inequalities (3.81) and (3.82)) that for all $\mathbf{s} \in \mathcal{S}^n$, and all $\mathbf{x} \in \mathcal{X}^n$,

$$\frac{1}{N}|A(\mathbf{s})| \leq \exp(-n\varepsilon/2) \qquad \text{and} \qquad \frac{1}{M}|B(\mathbf{s},\mathbf{x})| \leq \exp(-n\varepsilon/2).$$

Putting these inequalities along with (3.48) into (3.47) yields

$$e_0(\mathbf{s}) \leq 3\exp(-n\varepsilon/4). \tag{3.49}$$

We now bound the third sum in (3.45). The second sum is treated similarly. Let

$$e_1(\mathbf{s}) \triangleq \frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(K_{ij}^1(\mathbf{s})^c|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}). \tag{3.50}$$

For each i, j, and $\mathbf{s}$, write

$$K_{ij}^1(\mathbf{s})^c = \bigcup_{j' \neq j} [\, K_{ij'}^0 \cap \{\mathbf{z} : I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{y}_{j'}|\mathbf{s}) > \eta\}\,].$$

We claim that

$$K_{ij'}^0 \subset \{\mathbf{z} : I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i) > R_2 + \eta\}.$$

This is easily seen as follows. Suppose that $\mathbf{z} \in K_{ij'}^0$. Then there is some $\mathbf{s}'' \in \mathcal{S}^n$ such that $\mathbf{z} \in K_{ij'}^0(\mathbf{s}'')$. This means that

$$D(P_{\mathbf{x}_i,\mathbf{y}_{j'},\mathbf{s}'',\mathbf{z}}\|P \times Q \times P_{\mathbf{s}''} \times W) \leq \eta.$$

Applying the Projection Lemma 2.15,

$$D(P_{\mathbf{x}_i,\mathbf{y}_{j'},\mathbf{z}} \| P \times Q \times P_{\mathbf{s}''}W) \leq \eta. \tag{3.51}$$

By (3.51) and the definition of η in regard to (3.30), we can write

$$\begin{aligned} I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i) &= I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P_{\mathbf{x}_i,\mathbf{y}_{j'},\mathbf{z}}) > I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P \times Q \times P_{\mathbf{s}''}W) - \delta/2 \\ &> I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P, Q, W) - \delta/2. \end{aligned}$$

Using (3.33), followed by the fact that we chose $\eta < \delta/2$,

$$\begin{aligned} I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i) &> (R_2 + \delta) - \delta/2 \\ &> R_2 + \eta. \end{aligned}$$

Having established our claim, we then see that

$$K^1_{ij}(\mathbf{s})^c \subset \bigcup_{j' \neq j} \{\mathbf{z} : I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i) > R_2 + \eta \text{ and } I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{y}_{j'}|\mathbf{s}) > \eta\}. \tag{3.52}$$

The next step is to write

$$\begin{aligned} \{j' \neq j\} &= \{j' \neq j\} \cap \bigcup_{P_{XYY'S}} \{j' : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}\} \\ &= \bigcup_{P_{XYY'S}} \{j' \neq j : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}\}, \end{aligned}$$

where the union is over *all* joint types $P_{XYY'S} \in \mathcal{D}_n(\mathcal{X} \times \mathcal{Y} \times \mathcal{Y} \times \mathcal{S})$. So, we can write

$$K^1_{ij}(\mathbf{s})^c \subset \bigcup_{P_{XYY'S}} \Big(\bigcup_{j' \neq j : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}} \{\mathbf{z} : I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i) > R_2 + \eta \text{ and } I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{y}_{j'}|\mathbf{s}) > \eta\} \Big).$$

We use this inclusion as follows. By setting

$$\theta_{ij}(\mathbf{s}) \triangleq \bigcup_{j' \neq j : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}} \{\mathbf{z} : I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i) > R_2 + \eta \text{ and } I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{y}_{j'}|\mathbf{s}) > \eta\}, \tag{3.53}$$

Then note that since

$$\gamma \subset \mathcal{T}_{Z|XYY'S}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \subset \mathcal{T}_{Z|XYS}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}),$$

we have, by Lemma 2.14, inequality (2.9)

$$\mathbf{z} \in \gamma \implies W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \leq \exp[-nH(Z|XYS)].$$

We can now write

$$\begin{aligned} W^n(\gamma|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) &= \sum_{\mathbf{z}\in\gamma} W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\leq |\gamma| \exp[-nH(Z|XYS)] \\ &\leq \exp[nH(Z|XYY'S)] \cdot \exp[-nH(Z|XYS)] \\ &= \exp[-nI(Y' \wedge Z|XYS)], \end{aligned} \tag{3.61}$$

where the distribution $P_{XYY'SZ}$ satisfies both (3.59) and (3.60). We must still lower bound $I(Y' \wedge Z|XYS)$ independently of Z. There are four cases to consider:

1. $R_2 \geq I(Y' \wedge XYS)$
2. $I(Y' \wedge XYS) \geq R_2 \geq I(Y' \wedge XS)$
3. $I(Y' \wedge XS) \geq R_2 \geq I(Y' \wedge S)$
4. $I(Y' \wedge S) \geq R_2$.

In the first three cases, we will use the inequality

$$\begin{aligned} I(Y' \wedge Z|XYS) &= I(Y' \wedge YSZ|X) - I(Y' \wedge YS|X) \\ &= I(Y' \wedge YSZ|X) - I(Y' \wedge XYS) + I(Y' \wedge X) \\ &\geq I(Y' \wedge YSZ|X) - I(Y' \wedge XYS) \\ &\geq I(Y' \wedge Z|X) - I(Y' \wedge XYS). \end{aligned} \tag{3.62}$$

where

$$\zeta_{j'} \triangleq \{\mathbf{z} : I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i) > R_2 + \eta \text{ and } I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{y}_{j'}|\mathbf{s}) > \eta\}.$$

We would like to apply the union bound to $W^n(\theta_{ij}(\mathbf{s})|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s})$. Before doing so, we bound the quantity $W^n(\zeta_{j'}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s})$ uniformly for j' such that $(\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}$. To do this, write

$$\begin{aligned}
\zeta_{j'} &= \zeta_{j'} \cap \mathcal{Z}^n \\
&= \zeta_{j'} \cap \bigcup_{P_{XYY'SZ} \in \mathcal{D}_n(\mathcal{Z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})} \mathcal{T}_{Z|XYY'S}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \\
&= \bigcup_{P_{XYY'SZ} \in \mathcal{D}_n(\mathcal{Z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})} [\zeta_{j'} \cap \mathcal{T}_{Z|XYY'S}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})]. \qquad (3.58)
\end{aligned}$$

Now, consider a set of the form

$$\gamma = \zeta_{j'} \cap \mathcal{T}_{Z|XYY'S}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})$$

for some joint type $P_{XYY'SZ} \in \mathcal{D}_n(\mathcal{Z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})$. The first step is to bound $W^n(\gamma|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s})$ independently of the particular type $P_{XYY'SZ} \in \mathcal{D}_n(\mathcal{Z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})$. In other words, we need a bound that depends only on $P_{XYY'S} = P_{\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}}$. Now, if $\mathbf{z} \in \gamma$, then $P_{\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}, \mathbf{z}} = P_{XYY'SZ}$ and

$$I(Y' \wedge Z|X) > R_2 + \eta, \qquad (3.59)$$

and

$$I(XYZ \wedge Y'|S) > \eta. \qquad (3.60)$$

In other words, either $\gamma = \phi$ or (3.59) and (3.60) both hold. Now, observe that by Lemma 2.14, inequality (2.10),

$$|\gamma| \leq |\mathcal{T}_{Z|XYY'S}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})| \leq \exp[nH(Z|XYY'S)].$$

Then note that since

$$\gamma \subset \mathcal{T}_{Z|XYY'S}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \subset \mathcal{T}_{Z|XYS}(\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}),$$

we have, by Lemma 2.14, inequality (2.9)

$$\mathbf{z} \in \gamma \implies W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \leq \exp[-nH(Z|XYS)].$$

We can now write

$$\begin{aligned} W^n(\gamma|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) &= \sum_{\mathbf{z}\in\gamma} W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\ &\leq |\gamma| \exp[-nH(Z|XYS)] \\ &\leq \exp[nH(Z|XYY'S)] \cdot \exp[-nH(Z|XYS)] \\ &= \exp[-nI(Y' \wedge Z|XYS)], \end{aligned} \tag{3.61}$$

where the distribution $P_{XYY'SZ}$ satisfies both (3.59) and (3.60). We must still lower bound $I(Y' \wedge Z|XYS)$ independently of Z. There are four cases to consider:

1. $R_2 \geq I(Y' \wedge XYS)$
2. $I(Y' \wedge XYS) \geq R_2 \geq I(Y' \wedge XS)$
3. $I(Y' \wedge XS) \geq R_2 \geq I(Y' \wedge S)$
4. $I(Y' \wedge S) \geq R_2$.

In the first three cases, we will use the inequality

$$\begin{aligned} I(Y' \wedge Z|XYS) &= I(Y' \wedge YSZ|X) - I(Y' \wedge YS|X) \\ &= I(Y' \wedge YSZ|X) - I(Y' \wedge XYS) + I(Y' \wedge X) \\ &\geq I(Y' \wedge YSZ|X) - I(Y' \wedge XYS) \\ &\geq I(Y' \wedge Z|X) - I(Y' \wedge XYS). \end{aligned} \tag{3.62}$$

By (3.59),

$$I(Y' \wedge Z|XYS) \;\geq\; R_2 + \eta - I(Y' \wedge XYS).$$

Substituting this into (3.61) yields

$$W^n(\gamma|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \;\leq\; \exp[-n(\eta + R_2 - I(Y' \wedge XYS))],$$

independently of $P_{XYY'SZ} \in \mathcal{D}_n(\mathcal{Z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s})$. Applying the Type Counting Lemma to (3.58), we get

$$W^n(\zeta_{j'}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \;\leq\; \exp[-n(\eta - \varepsilon + R_2 - I(Y' \wedge XYS))].$$

By another property of our codewords (Theorem 3.22, inequality (3.85)),

$$|\{j' : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}\}| \;\leq\; \exp[n(|R_2 - I(Y' \wedge XYS)|^+ + \varepsilon)]. \qquad (3.63)$$

Thus

$$W^n(\theta_{ij}(\mathbf{s})|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \;=\; W^n\Big(\bigcup_{j' \neq j : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}} \zeta_{j'}\,|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}\Big)$$

is bounded above by

$$\exp[-n(\eta - 2\varepsilon + R_2 - I(Y' \wedge XYS) - |R_2 - I(Y' \wedge XYS)|^+)].$$

In case 1 we get

$$W^n(\theta_{ij}(\mathbf{s})|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \;\leq\; \exp[-n(\eta - 2\varepsilon)].$$

In case 2 we use the fact that the inequality in (3.57) fails. This leads to

$$I(Y \wedge XY'S) \;\leq\; R_2 - I(Y' \wedge XS) + \varepsilon.$$

Rewriting this as

$$I(Y \wedge XY'S) + I(Y' \wedge XS) \;\leq\; R_2 + \varepsilon,$$

or equivalently as

$$I(Y' \wedge XYS) + I(Y \wedge XS) \leq R_2 + \varepsilon,$$

we obtain $I(Y' \wedge XYS) \leq R_2 + \varepsilon$. Thus in case 2,

$$W^n(\theta_{ij}(\mathbf{s})|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \leq \exp[-n(\eta - 3\varepsilon)].$$

In case 3 we use the fact that both inequalities, (3.56) and (3.57), fail. So,

$$I(Y \wedge XY'S) \leq \varepsilon,$$

and

$$I(X \wedge Y'S) + I(Y' \wedge S) \leq R_2 + \varepsilon.$$

Write

$$\begin{aligned} I(Y' \wedge XYS) &= I(Y \wedge XY'S) + I(X \wedge Y'S) + I(Y' \wedge S) \\ &\quad - [H(X) + H(Y) + H(S) - H(XYS)] \\ &\leq R_2 + 2\varepsilon. \end{aligned}$$

So, in case 3,

$$W^n(\theta_{ij}(\mathbf{s})|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \leq \exp[-n(\eta - 4\varepsilon)].$$

Since the bounds for the first two cases imply the third, in the first three cases, we may use the preceding inequality. Now, in case 4 use (3.60) to write

$$\begin{aligned} I(Y' \wedge Z|XYS) &= I(XYZ \wedge Y'|S) - I(XY \wedge Y'|S) \\ &\geq \eta - I(XY \wedge Y'|S). \end{aligned}$$

We claim that $I(XY \wedge Y'|S) \leq 2\varepsilon$. Since the inequalities in (3.56) and (3.57) fail,

$$I(X \wedge Y'S) \leq \varepsilon \quad \text{and} \quad I(Y \wedge XY'S) \leq \varepsilon.$$

Writing

$$
\begin{aligned}
I(XY \wedge Y'|S) &= I(Y \wedge XY'S) + I(X \wedge Y'S) \\
&\quad - [H(X) + H(Y) + H(S) - H(XYS)] \\
&\leq 2\varepsilon,
\end{aligned}
$$

we have $I(Y' \wedge Z|XYS) \geq \eta - 2\varepsilon$. Combining this with (3.61), and applying the Type Counting Lemma to (3.58) yields

$$
W^n(\zeta_{j'}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \leq \exp[-n(\eta - 3\varepsilon)].
$$

Since in case 4, the upper bound in (3.63) reduces to $\exp(n\varepsilon)$, we have

$$
\begin{aligned}
W^n(\theta_{ij}(\mathbf{s})|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) &= W^n\Big(\bigcup_{j' \neq j : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}} \zeta_{j'} |\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \\
&\leq \exp[-n(\eta - 4\varepsilon)].
\end{aligned}
$$

We then have, in all four cases, when (3.56) and (3.57) both fail,

$$
\begin{aligned}
W^n(\theta_{ij}(\mathbf{s})|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) &\leq \exp[-n(\eta - 4\varepsilon)] \\
&\leq \exp(-n\varepsilon), \qquad \text{since } \eta > 5\varepsilon, \\
&\leq \exp(-n\varepsilon/2).
\end{aligned}
$$

To summarize, regardless of (3.56) and (3.57), we always have the quantity in (3.55) bounded above by $\exp(-n\varepsilon/2)$. By (3.54) we have

$$
\begin{aligned}
e_1(\mathbf{s}) &\leq \sum_{P_{XYY'S}} \exp(-n\varepsilon/2) \\
&\leq (n+1)^{|\mathcal{X}||\mathcal{Y}|^2|\mathcal{S}|} \exp(-n\varepsilon/2) \\
&\leq \exp(n\varepsilon/4) \exp(-n\varepsilon/2) \\
&= \exp(-n\varepsilon/4). \qquad (3.64)
\end{aligned}
$$

Finally, by using a similar procedure, whose main difference is that instead of (3.62) we use the fact that

$$\begin{aligned} I(X' \wedge Z|XYS) &= I(X' \wedge XYSZ) - I(X' \wedge XYS) \\ &\geq I(X' \wedge Z) - I(X' \wedge XYS), \end{aligned}$$

and also the fact that

$$\begin{aligned} I(X' \wedge Z|XYS) &= I(XYZ \wedge X'|S) - I(XY \wedge X'|S) \\ &\geq I(XZ \wedge X'|S) - I(XY \wedge X'|S), \end{aligned}$$

we can bound the middle term in (3.45) by $\exp(-n\varepsilon/4)$. Combining this with (3.49) and (3.64), we have, for every $\mathbf{s} \in \mathcal{S}^n$,

$$e(\mathbf{s}) \leq 8\exp(-n\varepsilon/4).$$

Since for all sufficiently large n, $8 \leq \exp(n\varepsilon/8)$, we see that (3.26) holds. □

Remark. Before arriving at the decoding rule described in the preceding proof, we tried the following. Let

$$K_{ij}^2(\mathbf{s}) \triangleq \{\mathbf{z} \in \mathcal{Z}^n : \forall i' \neq i, \mathbf{z} \in K_{i'j}^0 \Longrightarrow I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{x}_{i'}|\mathbf{s}) \leq \eta\},$$

$$K_{ij}^3(\mathbf{s}) \triangleq \{\mathbf{z} \in \mathcal{Z}^n : \forall i' \neq i, \forall j' \neq j, \mathbf{z} \in K_{i'j'}^0 \Longrightarrow I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{x}_{i'}\mathbf{y}_{j'}|\mathbf{s}) \leq \eta\},$$

and set

$$E_{ij} \triangleq \bigcup_{\mathbf{s}' \in \mathcal{S}^n} [K_{ij}^0(\mathbf{s}') \cap K_{ij}^1(\mathbf{s}') \cap K_{ij}^2(\mathbf{s}') \cap K_{ij}^3(\mathbf{s}')].$$

Then with only a little extra care, one can show that the $\{E_{ij}\}$ are pairwise disjoint, provided that W is nonsymmetrizable-$\mathcal{XY}$, nonsymmetrizable-$\mathcal{X}$, and nonsymmetrizable-$\mathcal{Y}$. One would then like to use any decoder φ with the property that

$$\mathbf{z} \in E_{ij} \Longrightarrow \varphi(\mathbf{z}) = (i, j).$$

Our problem with this approach is that we have been unable to find a *useful* bound on (compare (3.63))

$$|\{(i',j') : (\mathbf{x}_i, \mathbf{x}_{i'}, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XX'YY'S}\}|.$$

3.4 Alternative Decoding Rules

In the proof of Theorem 3.15, the decoder φ was described in terms of the sets $\{F_i\}$ and $\{G_{ij}\}$ defined by (3.39) and (3.43). For a given $\mathbf{z} \in \mathcal{Z}^n$, determining which F_i and G_{ij} that $\mathbf{z}$ belongs to would be a complicated and demanding task. Consider the following *maximum mutual information decoder* (MMI decoder). Let

$$\hat{F}_i \triangleq \{\mathbf{z} \in \mathcal{Z}^n : I(\mathbf{x}_i \wedge \mathbf{z}) > I(\mathbf{x}_{i'} \wedge \mathbf{z}), \forall i' \neq i\} \tag{3.65}$$

and

$$\hat{G}_{ij} \triangleq \{\mathbf{z} \in \mathcal{Z}^n : I(\mathbf{y}_j \wedge \mathbf{z}|\mathbf{x}_i) > I(\mathbf{y}_{j'} \wedge \mathbf{z}|\mathbf{x}_i), \forall j' \neq j\}. \tag{3.66}$$

Obviously, the $\{\hat{F}_i\}_{i=1}^N$ are disjoint, as are the $\{\hat{G}_{ij}\}_{j=1}^M$ for each i. If $\hat{\varphi}(\mathbf{z}) = (\hat{\varphi}_1(\mathbf{z}), \hat{\varphi}_2(\mathbf{z}))$ has the property that

$$\mathbf{z} \in \hat{F}_i \implies \hat{\varphi}_1(\mathbf{z}) = i \tag{3.67}$$

and

$$\mathbf{z} \in \hat{F}_i \cap \hat{G}_{ij} \implies \hat{\varphi}_2(\mathbf{z}) = j, \tag{3.68}$$

then we say $\hat{\varphi}$ is an MMI decoder. Clearly, the decoder $\hat{\varphi}$ is much simpler than the decoder φ used in the proof of Theorem 3.15. More importantly, $\hat{\varphi}$ is *universal* in the sense that the definition of the sets $\{\hat{F}_i\}$ and $\{\hat{G}_{ij}\}$ does not depend in any way on W. Below we will present a theorem that gives sufficient conditions under

which $\hat{\varphi}$ can be used instead of φ in the proof of Theorem 3.15. We first need the following general lemma.

Lemma 3.20 *Let $\{\hat{F}_i\}$ and $\{\hat{G}_{ij}\}$ be arbitrary subsets of $\mathcal{Z}^n$, not necessarily given by* (3.65) *and* (3.66). *Suppose that the $\{\hat{F}_i\}_{i=1}^N$ are disjoint and that the $\{\hat{G}_{ij}\}_{j=1}^M$ are disjoint for each i. Let $\hat{\varphi}$ satisfy* (3.67) *and* (3.68). *Let $J_i^0(\mathbf{s})$ and $K_{ij}^0(\mathbf{s})$ be given by* (3.37) *and* (3.42) *respectively. If*

$$\hat{F}_i^c \cap J_i^0(\mathbf{s}) \subset \bigcup_{i' \neq i} \{\mathbf{z} : I(\mathbf{x}_{i'} \wedge \mathbf{z}) > R_1 + \eta \text{ and } I(\mathbf{x}_i \mathbf{z} \wedge \mathbf{x}_{i'} | \mathbf{s}) > \eta\}, \quad \forall \mathbf{s} \in \mathcal{S}^n, \tag{3.69}$$

and if

$$\hat{G}_{ij}^c \cap K_{ij}^0(\mathbf{s}) \subset \bigcup_{j' \neq j} \{\mathbf{z} : I(\mathbf{y}_{j'} \wedge \mathbf{z} | \mathbf{x}_i) > R_2 + \eta \text{ and } I(\mathbf{x}_i \mathbf{y}_j \mathbf{z} \wedge \mathbf{y}_{j'} | \mathbf{s}) > \eta\}, \quad \forall \mathbf{s} \in \mathcal{S}^n, \tag{3.70}$$

then we can use $\hat{\varphi}$ instead of φ in the proof of Theorem 3.15.

Proof. Observe that

$$\hat{\varphi}(\mathbf{z}) \neq (i,j) \implies \mathbf{z} \in \hat{F}_i^c \cup \hat{G}_{ij}^c.$$

Hence

$$\frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M W^n(\{\mathbf{z} \in \mathcal{Z}^n : \hat{\varphi}(\mathbf{z}) \neq (i,j)\} | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \leq \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M W^n(\hat{F}_i^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) + \frac{1}{NM} \sum_{i=1}^N \sum_{j=1}^M W^n(\hat{G}_{ij}^c | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}).$$

We consider only the second term. The first is treated similarly. Write

$$\begin{aligned} \hat{G}_{ij}^c &= [\hat{G}_{ij}^c \cap K_{ij}^0(\mathbf{s})^c] \cup [\hat{G}_{ij}^c \cap K_{ij}^0(\mathbf{s})] \\ &\subset K_{ij}^0(\mathbf{s})^c \cup [\hat{G}_{ij}^c \cap K_{ij}^0(\mathbf{s})]. \end{aligned}$$

By (3.70),

$$\hat{G}_{ij}^c \subset K_{ij}^0(\mathbf{s})^c \cup \bigcup_{j' \neq j} \{\mathbf{z} : I(\mathbf{y}_{j'} \wedge \mathbf{z} | \mathbf{x}_i) > R_2 + \eta \text{ and } I(\mathbf{x}_i \mathbf{y}_j \mathbf{z} \wedge \mathbf{y}_{j'} | \mathbf{s}) > \eta\}.$$

A review of the proof of Theorem 3.15 giving special attention to equations (3.46) and (3.49) as well as (3.50), (3.52), and (3.64) shows that

$$\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\hat{G}_{ij}^c|\mathbf{x}_i,\mathbf{y}_j,\mathbf{s}) \;\le\; 4\exp(-n\varepsilon/4).$$

□

We now give sufficient conditions under which an MMI decoder can be used in the proof of Theorem 3.15.

Theorem 3.21 *If $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$ are such that*

$$I_{\mathcal{X}\wedge\mathcal{Z}}(p\times q\times r\times W) \;>\; I_{\mathcal{S}\wedge\mathcal{Z}}(p\times q\times r\times W), \qquad \forall r\in\mathcal{D}(\mathcal{S}), \tag{3.71}$$

and

$$I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times r\times W) \;>\; I_{\mathcal{S}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times r\times W), \qquad \forall r\in\mathcal{D}(\mathcal{S}), \tag{3.72}$$

then for

$$0 \;<\; R_1 \;<\; I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) \qquad \text{and} \qquad 0 \;<\; R_2 \;<\; I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W),$$

there exists an $\varepsilon>0$ such that for all sufficiently large n, if $N \triangleq \lfloor\exp(nR_1)\rfloor$ and $M \triangleq \lfloor\exp(nR_2)\rfloor$, then there exist codewords for user 1, $\mathbf{x}_1,\ldots,\mathbf{x}_N$, each in $\mathcal{X}^n$, and there exist codewords for user 2, $\mathbf{y}_1,\ldots,\mathbf{y}_M$, each in $\mathcal{Y}^n$, and there exists an MMI decoder $\hat{\varphi}$ *with*

$$\frac{1}{NM}\sum_{i=1}^{N}\sum_{j=1}^{M} W^n(\{\mathbf{z}\in\mathcal{Z}^n : \hat{\varphi}(\mathbf{z})\neq(i,j)\}|\mathbf{x}_i,\mathbf{y}_j,\mathbf{s}) \;\le\; \exp(-n\varepsilon)$$

holding uniformly *for every $\mathbf{s}\in\mathcal{S}^n$.*

Interpretation. Observe that no explicit assumptions concerning nonsymmetrizability have been made. Recall that the proof of Theorem 3.15 used the nonsymmetrizability assumptions only to show that the $\{F_i\}$ and the $\{G_{ij}\}$ were disjoint.

For the MMI decoder, the $\{\hat{F}_i\}_{i=1}^N$ and the $\{\hat{G}_{ij}\}_{j=1}^M$ are obviously disjoint. We also point out that while no knowledge of W is required to define $\hat{\varphi}$, the conditions (3.71) and (3.72) obviously depend on W. The point is this. Suppose that one knows only that W belongs to a certain class of channels. If one can show that for some p and q, every channel in this class satisfies (3.71) and (3.72), then one can confidently implement $\hat{\varphi}$ without a complete knowledge of W.

Proof. Assume $\delta > 0$ has been chosen small enough that

$$I_{\mathcal{X}\wedge\mathcal{Z}}(p \times q \times r \times W) - I_{\mathcal{S}\wedge\mathcal{Z}}(p \times q \times r \times W) \ > \ 2\delta, \qquad \forall r \in \mathcal{D}(\mathcal{S}),$$

and

$$I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p \times q \times r \times W) - I_{\mathcal{S}\wedge\mathcal{Z}|\mathcal{X}}(p \times q \times r \times W) \ > \ 2\delta, \qquad \forall r \in \mathcal{D}(\mathcal{S}).$$

Then as in the proof of Theorem 3.15, we can assume that $\hat{p}$ and $\hat{q}$ and P and Q have been chosen so that

$$I_{\mathcal{X}\wedge\mathcal{Z}}(P \times Q \times r \times W) - I_{\mathcal{S}\wedge\mathcal{Z}}(P \times Q \times r \times W) \ > \ \delta, \qquad \forall r \in \mathcal{D}(\mathcal{S}), \quad (3.73)$$

and

$$I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P \times Q \times r \times W) - I_{\mathcal{S}\wedge\mathcal{Z}|\mathcal{X}}(P \times Q \times r \times W) \ > \ \delta, \qquad \forall r \in \mathcal{D}(\mathcal{S}). \quad (3.74)$$

Let $\mathbf{x}_1, \ldots, \mathbf{x}_N$ be the codewords for user 1, all of type P, and let $\mathbf{y}_1, \ldots, \mathbf{y}_M$ be the codewords for user 2, all of type Q and having the properties listed in Theorem 3.22. With $\hat{F}_i$ and $\hat{G}_{ij}$ given by (3.65) and (3.66) respectively, we have $\mathbf{z} \in \hat{F}_i^c \cap J_i^0(\mathbf{s})$ if and only if

$$\mathbf{z} \in \bigcup_{i' \neq i} \{\mathbf{z} : I(\mathbf{x}_{i'} \wedge \mathbf{z}) \geq I(\mathbf{x}_i \wedge \mathbf{z}) \text{ and } D(P_{\mathbf{x}_i,\mathbf{s},\mathbf{z}} \| P \times P_{\mathbf{s}} \times QW) \leq \eta\}.$$

By the Projection Lemma 2.15, $D(P_{\mathbf{x}_i,\mathbf{s},\mathbf{z}}\|P\times P_{\mathbf{s}}\times QW)\le\eta$ implies $D(P_{\mathbf{x}_i,\mathbf{z}}\|P\times QP_{\mathbf{s}}W)\le\eta$, and so by (3.29), (3.32), and the fact that $\eta<\delta/2$, if $\mathbf{z}\in\hat{F}_i^c\cap J_i^0(\mathbf{s})$, then there is some $i'\neq i$ with

$$\begin{aligned} I(\mathbf{x}_{i'}\wedge\mathbf{z}) \;\ge\; I(\mathbf{x}_i\wedge\mathbf{z}) &\ge I_{\mathcal{X}\wedge\mathcal{Z}}(P\times Q\times P_{\mathbf{s}}W)-\delta/2 \\ &\ge I^*_{\mathcal{X}\wedge\mathcal{Z}}(P,Q,W)-\delta/2 \\ &> R_1+\eta. \end{aligned}$$

We claim that $I(\mathbf{x}_i\mathbf{z}\wedge\mathbf{x}_{i'}|\mathbf{s})>\eta$ as well. Observe that

$$\begin{aligned} I(\mathbf{x}_i\mathbf{z}\wedge\mathbf{x}_{i'}|\mathbf{s}) &\ge I(\mathbf{z}\wedge\mathbf{x}_{i'}|\mathbf{s}) \\ &= I(\mathbf{x}_{i'}\mathbf{s}\wedge\mathbf{z})-I(\mathbf{s}\wedge\mathbf{z}) \\ &\ge I(\mathbf{x}_{i'}\wedge\mathbf{z})-I(\mathbf{s}\wedge\mathbf{z}) \\ &\ge I(\mathbf{x}_i\wedge\mathbf{z})-I(\mathbf{s}\wedge\mathbf{z}) \\ &\ge [I_{\mathcal{X}\wedge\mathcal{Z}}(P\times P_{\mathbf{s}}\times QW)-I_{\mathcal{S}\wedge\mathcal{Z}}(P\times P_{\mathbf{s}}\times QW)]-\delta/2, \\ &\qquad\qquad \text{since } \mathbf{z}\in J_i^0(\mathbf{s}) \text{ (see Note below)}, \\ &\ge \delta/2 \;>\; \eta, \qquad \text{by (3.73)}. \end{aligned}$$

Note. We assume η was chosen so small that not only do we have (3.29) and (3.32), but also if $P^{(1)}$ and $P^{(2)}$ are any two distributions on $\mathcal{X}\times\mathcal{S}\times\mathcal{Z}$ or on $\mathcal{X}\times\mathcal{Y}\times\mathcal{S}\times\mathcal{Z}$ with $D(P^{(1)}\|P^{(2)})\le\eta$, then

$$\left|[I_{\mathcal{X}\wedge\mathcal{Z}}(P^{(1)})-I_{\mathcal{S}\wedge\mathcal{Z}}(P^{(1)})]-[I_{\mathcal{X}\wedge\mathcal{Z}}(P^{(2)})-I_{\mathcal{S}\wedge\mathcal{Z}}(P^{(2)})]\right| \;<\; \delta/2$$

and

$$\left|[I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P^{(1)})-I_{\mathcal{S}\wedge\mathcal{Z}|\mathcal{X}}(P^{(1)})]-[I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(P^{(2)})-I_{\mathcal{S}\wedge\mathcal{Z}|\mathcal{X}}(P^{(2)})]\right| \;<\; \delta/2.$$

Thus $\hat{F}_i^c \cap J_i^0(\mathbf{s}) \subset \bigcup_{i' \neq i} \{\mathbf{z} : I(\mathbf{x}_{i'} \wedge \mathbf{z}) > R_1 + \eta \text{ and } I(\mathbf{x}_i \mathbf{z} \wedge \mathbf{x}_{i'} | \mathbf{s}) > \eta\}$. The proof of (3.70) follows similarly if one observes that

$$\begin{aligned} I(\mathbf{x}_i \mathbf{y}_j \mathbf{z} \wedge \mathbf{y}_{j'} | \mathbf{s}) &\geq I(\mathbf{x}_i \mathbf{z} \wedge \mathbf{y}_{j'} | \mathbf{s}) \\ &= I(\mathbf{x}_i \mathbf{z} \wedge \mathbf{y}_{j'} \mathbf{s}) - I(\mathbf{x}_i \mathbf{z} \wedge \mathbf{s}) \\ &= [I(\mathbf{x}_i \wedge \mathbf{y}_{j'} \mathbf{s}) + I(\mathbf{z} \wedge \mathbf{y}_{j'} \mathbf{s} | \mathbf{x}_i)] - [I(\mathbf{x}_i \wedge \mathbf{s}) + I(\mathbf{z} \wedge \mathbf{s} | \mathbf{x}_i)] \\ &= [I(\mathbf{y}_{j'} \mathbf{s} \wedge \mathbf{z} | \mathbf{x}_i) - I(\mathbf{s} \wedge \mathbf{z} | \mathbf{x}_i)] + [I(\mathbf{x}_i \wedge \mathbf{y}_{j'} \mathbf{s}) - I(\mathbf{x}_i \wedge \mathbf{s})] \\ &\geq I(\mathbf{y}_{j'} \wedge \mathbf{z} | \mathbf{x}_i) - I(\mathbf{s} \wedge \mathbf{z} | \mathbf{x}_i). \end{aligned}$$

□

3.5 Decoding Sets and Codeword Properties

In this section we prove our claim that for each i, the decoding sets $\{G_{ij}\}_{j=1}^M$ defined in equation (3.43) are pairwise disjoint. Based on this proof, it can easily be shown that the sets $\{F_i\}$ defined in equation (3.39) are also pairwise disjoint. The last part of this section is devoted to giving a complete list of the codeword properties which we assumed in the proof of Theorem 3.15.

We first establish that for each i, the $\{G_{ij}\}_{j=1}^M$ are pairwise disjoint. Suppose that for some pair $j \neq j'$, $\mathbf{z} \in G_{ij} \cap G_{ij'}$. Since $\mathbf{z} \in G_{ij}$, there must be some $\mathbf{s} \in \mathcal{S}^n$ with

$$\mathbf{z} \in K_{ij}^0(\mathbf{s}) \cap K_{ij}^1(\mathbf{s}).$$

Similarly, since $\mathbf{z} \in G_{ij'}$, there must be some $\mathbf{s}' \in \mathcal{S}^n$ with

$$\mathbf{z} \in K_{ij'}^0(\mathbf{s}') \cap K_{ij'}^1(\mathbf{s}').$$

Now, since $\mathbf{z} \in K^0_{ij'}(\mathbf{s}')$, $\mathbf{z} \in K^0_{ij'}$. Since we also have $\mathbf{z} \in K^1_{ij}(\mathbf{s})$, we conclude that

$$I(\mathbf{x}_i\mathbf{y}_j\mathbf{z} \wedge \mathbf{y}_{j'}|\mathbf{s}) \ \leq \ \eta. \tag{3.75}$$

Arguing similarly, since $\mathbf{z} \in K^0_{ij}(\mathbf{s})$, $\mathbf{z} \in K^0_{ij}$. Since we also have

$$\mathbf{z} \in K^1_{ij'}(\mathbf{s}') \ = \ \{\mathbf{z} \in \mathcal{Z}^n : \forall j \neq j', \mathbf{z} \in K^0_{ij} \Longrightarrow I(\mathbf{x}_i\mathbf{y}_{j'}\mathbf{z} \wedge \mathbf{y}_j|\mathbf{s}') \leq \eta\},$$

we conclude that

$$I(\mathbf{x}_i\mathbf{y}_{j'}\mathbf{z} \wedge \mathbf{y}_j|\mathbf{s}') \ \leq \ \eta. \tag{3.76}$$

We also obviously have

$$D(P_{\mathbf{x}_i,\mathbf{y}_j,\mathbf{s},\mathbf{z}}\|P \times Q \times P_{\mathbf{s}} \times W) \ \leq \eta \quad \text{and} \quad D(P_{\mathbf{x}_i,\mathbf{y}_{j'},\mathbf{s}',\mathbf{z}}\|P \times Q \times P_{\mathbf{s}'} \times W) \ \leq \ \eta. \tag{3.77}$$

Let $P_{XYY'SS'Z} = P_{\mathbf{x}_i,\mathbf{y}_j,\mathbf{y}_{j'},\mathbf{s},\mathbf{s}',\mathbf{z}}$. Note that $P_Y = P_{Y'} = Q$ and $P_X = P$. Thus,

$$D(P_{XYSZ}\|P \times Q \times P_S \times W) \ \leq \ \eta \quad \text{and} \quad I(XYZ \wedge Y'|S) \ \leq \ \eta \tag{3.78}$$

and

$$D(P_{XY'S'Z}\|P \times Q \times P_{S'} \times W) \ \leq \ \eta \quad \text{and} \quad I(XY'Z \wedge Y|S') \ \leq \ \eta. \tag{3.79}$$

We can rewrite the two inequalities in (3.79) as

$$\sum_{x,y,y',s,z} P_{XYY'S'Z}(x,y,y',s,z) \log \frac{P_{XY'S'Z}(x,y',s,z)}{P(x)Q(y')P_{S'}(s)W(z|x,y',s)} \ \leq \ \eta$$

and

$$\sum_{x,y,y',s,z} P_{XYY'S'Z}(x,y,y',s,z) \log \frac{P_{XYY'S'Z}(x,y,y',s,z)P_{S'}(s)}{P_{XY'S'Z}(x,y',s,z)P_{YS'}(y,s)} \ \leq \ \eta.$$

Adding these two inequalities yields

$$\sum_{x,y,y',s,z} P_{XYY'S'Z}(x,y,y',s,z) \log \frac{P_{XYY'S'Z}(x,y,y',s,z)}{P(x)Q(y)Q(y')W(z|x,y',s)P_{S'|Y'}(s|y)} \ \leq \ 2\eta.$$

We recognize the preceding expression as an informational divergence. If we let

$$V'(z|x,y,y') \triangleq \sum_s W(z|x,y',s)P_{S'|Y}(s|y),$$

then applying the Projection Lemma 2.15 yields

$$D(P_{XYY'Z}\|P \times Q \times Q \times V') \leq 2\eta.$$

By Pinsker's Inequality (Lemma 2.7),

$$d(P_{XYY'Z}, P \times Q \times Q \times V') \leq \sqrt{(2\ln 2)(2\eta)} = 2\sqrt{\eta \ln 2}.$$

Next, starting with (3.78) and proceeding as above, we arrive at

$$d(P_{XYY'Z}, P \times Q \times Q \times V) \leq 2\sqrt{\eta \ln 2},$$

where

$$V(z|x,y,y') \triangleq \sum_s W(z|x,y,s)P_{S|Y'}(s|y').$$

Since d is a metric, we can use the triangle inequality to get

$$\sum_{x,y,y',z} P(x)Q(y)Q(y')|V(z|x,y,y') - V'(z|x,y,y')| \leq 4\sqrt{\eta \ln 2}.$$

Recalling that $P(x) \geq \beta > 0$ and $Q(y) \geq \beta > 0$,

$$\max_{x,y,y',z} |V(z|x,y,y') - V'(z|x,y,y')| \leq \frac{4\sqrt{\eta \ln 2}}{\beta^3} < \delta,$$

since we chose $\eta < \beta^6\delta^2/(16 \ln 2)$. Now, observe that the preceding maximum does not change if we interchange y and y' and then interchange V and V'. Hence, we also have

$$\max_{x,y,y',z} |V'(z|x,y',y) - V(z|x,y',y)| < \delta.$$

It is then easy to show that

$$\max_{x,y,y',z}\left|\tfrac{1}{2}[V(z|x,y,y')+V'(z|x,y',y)]-\tfrac{1}{2}[V'(z|x,y,y')+V(z|x,y',y)]\right| \;<\; \delta.$$

If we set $U(s|y) \triangleq \frac{1}{2}[P_{S'|Y}(s|y)+P_{S|Y'}(s|y)]$, this becomes

$$\max_{x,y,y',z}\left|\sum_s W(z|x,y,s)U(s|y')-\sum_s W(z|x,y',s)U(s|y)\right| \;<\; \delta. \tag{3.80}$$

In other words (cf. (3.22)) $F_{\mathcal{Y}}^{W}(U) < \delta$, and so we must have (cf. (3.23))

$$\xi_{\mathcal{Y}}(W) \;<\; \delta,$$

contradicting (3.27).

Having established that for each i, $G_{i1},\ldots,G_{iM}$ are pairwise disjoint, it can be similarly established that $F_1,\ldots,F_N$ are pairwise disjoint; simply contradict (3.31) instead of (3.27).

We conclude this section with a theorem which establishes that for all sufficiently large n, we can always find a set of codewords for each user such that the properties used in the proof the Theorem 3.15 will hold.

Theorem 3.22 (*Codeword Properties*). *Given $\varepsilon > 0$, there exists an n_0 depending only on ε, $|\mathcal{X}|$, $|\mathcal{Y}|$, and $|\mathcal{S}|$, such that for every $n \geq n_0$, if $P \in \mathcal{D}_n(\mathcal{X})$ and $Q \in \mathcal{D}_n(\mathcal{Y})$, and if N and M are positive integers with*

$$\varepsilon \;\leq\; R_1 = \frac{\log N}{n} \quad \textit{and} \quad \varepsilon \;\leq\; R_2 = \frac{\log M}{n},$$

then there exist codewords, $\mathbf{x}_1,\ldots,\mathbf{x}_N$, each of type P, and there exist codewords, $\mathbf{y}_1,\ldots,\mathbf{y}_M$, each of type Q such that (3.81) – (3.90) *all hold simultaneously:*

$$\frac{1}{N}|\{i : I(\mathbf{x}_i \wedge \mathbf{s}) > \varepsilon\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{s} \in \mathcal{S}^n, \tag{3.81}$$

$$\frac{1}{M}|\{j : I(\mathbf{y}_j \wedge \mathbf{x}\mathbf{s}) > \varepsilon\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{x} \in \mathcal{X}^n, \mathbf{s} \in \mathcal{S}^n, \tag{3.82}$$

$$\frac{1}{M}|\{j : I(\mathbf{y}_j \wedge \mathbf{s}) > \varepsilon\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{s} \in \mathcal{S}^n, \tag{3.83}$$

$$\frac{1}{N}|\{i : I(\mathbf{x}_i \wedge \mathbf{y}\mathbf{s}) > \varepsilon\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{y} \in \mathcal{Y}^n, \mathbf{s} \in \mathcal{S}^n. \tag{3.84}$$

For every type $P_{XX'YY'S} \in \mathcal{D}_n(\mathcal{X} \times \mathcal{X} \times \mathcal{Y} \times \mathcal{Y} \times \mathcal{S})$,

$$|\{j' : (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}\}| \leq \exp[n(|R_2 - I(Y' \wedge XYS)|^+ + \varepsilon)], \quad \forall \mathbf{s} \in \mathcal{S}^n, \tag{3.85}$$

and

$$|\{i' : (\mathbf{x}_i, \mathbf{x}_{i'}, \mathbf{y}_j, \mathbf{s}) \in \mathcal{T}_{XX'YS}\}| \leq \exp[n(|R_1 - I(X' \wedge XYS)|^+ + \varepsilon)], \quad \forall \mathbf{s} \in \mathcal{S}^n; \tag{3.86}$$

if $I(X \wedge Y'S) > |R_2 - I(Y' \wedge S)|^+ + \varepsilon$,

$$\frac{1}{N}|\{i : \exists j' \text{ with } (\mathbf{x}_i, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XY'S}\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{s} \in \mathcal{S}^n; \tag{3.87}$$

if $I(Y \wedge XY'S) > |R_2 - I(Y' \wedge XS)|^+ + \varepsilon$,

$$\frac{1}{M}|\{j : \exists j' \neq j \text{ with } (\mathbf{x}_i, \mathbf{y}_j, \mathbf{y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{s} \in \mathcal{S}^n; \tag{3.88}$$

if $I(Y \wedge X'S) > |R_1 - I(X' \wedge S)|^+ + \varepsilon$,

$$\frac{1}{M}|\{j : \exists i' \text{ with } (\mathbf{x}_{i'}, \mathbf{y}_j, \mathbf{s}) \in \mathcal{T}_{X'YS}\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{s} \in \mathcal{S}^n; \tag{3.89}$$

if $I(X \wedge X'YS) > |R_1 - I(X' \wedge YS)|^+ + \varepsilon$,

$$\frac{1}{N}|\{i : \exists i' \neq i \text{ with } (\mathbf{x}_i, \mathbf{x}_{i'}, \mathbf{y}_j, \mathbf{s}) \in \mathcal{T}_{XX'YS}\}| \leq \exp(-n\varepsilon/2), \quad \forall \mathbf{s} \in \mathcal{S}^n. \tag{3.90}$$

Proof. Observe that if $P_{\mathbf{x}_i} = P$ and $P_{\mathbf{y}_j} = Q$ for all i and j respectively, then in order that all of the bounds (3.85) - (3.90) be nonvacuous, it is necessary that $P_X = P_{X'} = P$ and $P_Y = P_{Y'} = Q$. Most of the properties follow easily from their single-user counterparts proved in the appendix of [8]. The exceptions are (3.87) and (3.89); for these, a proof is required. It will suffice to prove (3.87).

Let $\{\mathbf{X}_1, \ldots, \mathbf{X}_N\}$ and $\{\mathbf{Y}_1, \ldots, \mathbf{Y}_M\}$ be two independent families of i.i.d. RV's such that each member of the family $\{\mathbf{X}_1, \ldots, \mathbf{X}_N\}$ is uniformly distributed on $\mathcal{T}_P$, and each member of the family $\{\mathbf{Y}_1, \ldots, \mathbf{Y}_M\}$ is uniformly distributed on $\mathcal{T}_Q$.

Let $t \stackrel{\Delta}{=} \exp(-n\varepsilon/2)$, and and define the events

$$A(\mathbf{s}, \mathcal{T}_{XY'S}) \stackrel{\Delta}{=} \left\{\frac{1}{N}|\{i : \exists j' \text{ with } (\mathbf{X}_i, \mathbf{Y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XY'S}\}| \leq t\right\},$$

and

$$A \stackrel{\Delta}{=} \bigcap A(\mathbf{s}, \mathcal{T}_{XY'S}),$$

where the intersection is over all $\mathbf{s} \in \mathcal{S}^n$ and all types $P_{XY'S}$ such that

$$I(X \wedge Y'S) > |R_2 - I(Y' \wedge S)|^+ + \varepsilon.$$

The assertion in (3.87) will be proved if $\mathsf{P}(A) > 0$, or equivalently, $\mathsf{P}(A^c) < 1$. Now, we will show below that, *uniformly* for every $\mathbf{s} \in \mathcal{S}^n$ and every set $\mathcal{T}_{XY'S}$,

$$\mathsf{P}(A(\mathbf{s}, \mathcal{T}_{XY'S})^c) \leq 2\exp[-\tfrac{1}{2}\exp(n\varepsilon/4)]. \tag{3.91}$$

It will then follow that

$$\begin{aligned}\mathsf{P}(A^c) &\leq |\mathcal{S}|^n(n+1)^{|\mathcal{X}||\mathcal{Y}||\mathcal{S}|} \cdot 2\exp[-\tfrac{1}{2}\exp(n\varepsilon/4)] \\ &= 2\exp[\,n\log|\mathcal{S}| + |\mathcal{X}||\mathcal{Y}||\mathcal{S}|\log(n+1) - \tfrac{1}{2}\exp(n\varepsilon/4)\,].\end{aligned}$$

Clearly, if n is sufficiently large (obviously, how large depends only on ε, $|\mathcal{X}|$, $|\mathcal{Y}|$, and $|\mathcal{S}|$),

$$\mathsf{P}(A^c) < 1.$$

In order to prove (3.91), we will prove and employ the following: *uniformly* for every $\mathbf{s} \in \mathcal{S}^n$ and every set $\mathcal{T}_{Y'S}$,

$$\mathsf{P}(G(\mathbf{s}, \mathcal{T}_{Y'S})^c) \;\leq\; \exp[-\tfrac{1}{2}\exp(n\varepsilon/4)], \tag{3.92}$$

where

$$G(\mathbf{s}, \mathcal{T}_{Y'S}) \;\triangleq\; \Big\{|\{j' : (\mathbf{Y}_{j'}, \mathbf{s}) \in \mathcal{T}_{Y'S}\}| \;\leq\; t'\Big\},$$

and $t' \triangleq \exp[\,n(|R_2 - I(Y' \wedge S)|^+ + \varepsilon/4)\,]$. To prove (3.92), let

$$g_{j'} \;\triangleq\; \begin{cases} 1, & \text{if } \mathbf{Y}_{j'} \in \mathcal{T}_{Y'|S}(\mathbf{s}) \\ 0, & \text{otherwise.} \end{cases}$$

Observe that

$$|\{j' : (\mathbf{Y}_{j'}, \mathbf{s}) \in \mathcal{T}_{Y'S}\}| \;=\; \sum_{j'=1}^{M} g_{j'}.$$

So, using Markov's inequality, followed by the independence of the RV's $\{g_{j'}\}$,

$$\begin{aligned} \mathsf{P}(G(\mathbf{s}, \mathcal{T}_{Y'S})^c) \;&=\; \mathsf{P}\Big(\sum_{j'=1}^{M} g_{j'} > t'\Big) \\ &=\; \mathsf{P}\Big(\exp\Big(\sum_{j'=1}^{M} g_{j'}\Big) > \exp(t')\Big) \\ &\leq\; \exp(-t') \cdot \mathsf{E}[\exp\Big(\sum_{j'=1}^{M} g_{j'}\Big)\,] \\ &=\; \exp(-t') \cdot \prod_{j'=1}^{M} \mathsf{E}[\exp(g_{j'})\,]. \end{aligned}$$

Now, since exp's are to the base 2, and since

$$2^x \;\leq\; 1 + x, \qquad \text{when } x \in [0,1],$$

we can write

$$\mathsf{E}[\exp(g_{j'})\,] \;\leq\; \mathsf{E}[\,1 + g_{j'}\,]$$

$$
\begin{aligned}
&= 1 + \mathsf{E}[\,g_{j'}\,] \\
&\leq e^{\mathsf{E}[g_{j'}]} \\
&= \exp(\,\mathsf{E}[\,g_{j'}\,]\log e\,).
\end{aligned}
$$

To upper bound $\mathsf{E}[\,g_{j'}\,]$, we appeal to (2.5) and (2.10), and then assume that n is so large that $(n+1)^{|\mathcal{Y}|} \leq \exp(n\varepsilon/4)/(2\log e)$. This yields

$$
\begin{aligned}
\mathsf{E}[\,g_{j'}\,] &= \mathsf{P}(\mathbf{Y}_{j'} \in \mathcal{T}_{Y'|S}(\mathrm{s})) \\
&= \frac{1}{|\mathcal{T}_Q|}|\mathcal{T}_{Y'|S}(\mathrm{s})| \\
&\leq \exp(nH(Y'|S))/[\exp(nH(Y'))(n+1)^{-|\mathcal{Y}|}] \\
&\leq \exp[\,-n(I(Y'\wedge S)-\varepsilon/4)\,]/2\log e.
\end{aligned}
$$

With this upper bound,

$$
\begin{aligned}
\mathsf{P}(G(\mathrm{s},\mathcal{T}_{Y'S})^c) &\leq \exp[\,-t' + M\mathsf{E}[g_1]\log e\,] \\
&\leq \exp[\,-(t' - \tfrac{1}{2}\exp[n((R_2 - I(Y'\wedge S)) + \varepsilon/4)])\,] \\
&\leq \exp[\,-\tfrac{1}{2}\exp(n\varepsilon/4)\,].
\end{aligned}
$$

Having established (3.92), we proceed to verify (3.91). Write

$$
\begin{aligned}
\mathsf{P}(A(\mathrm{s},\mathcal{T}_{XY'S})^c) &= \mathsf{P}(A(\mathrm{s},\mathcal{T}_{XY'S})^c \cap G(\mathrm{s},\mathcal{T}_{Y'S})) + \mathsf{P}(A(\mathrm{s},\mathcal{T}_{XY'S})^c \cap G(\mathrm{s},\mathcal{T}_{Y'S})^c) \\
&\leq \mathsf{P}(A(\mathrm{s},\mathcal{T}_{XY'S})^c \cap G(\mathrm{s},\mathcal{T}_{Y'S})) + \exp[\,-\tfrac{1}{2}\exp(n\varepsilon/4)\,]. \qquad (3.93)
\end{aligned}
$$

Keeping in mind that

$$
\dot{\mathbf{X}}_i \in \mathcal{T}_{X|Y'S}(\mathbf{Y}_{j'},\mathrm{s}) \iff \mathbf{X}_i \in \mathcal{T}_{X|Y'S}(\mathbf{Y}_{j'},\mathrm{s}) \text{ and } \mathbf{Y}_{j'} \in \mathcal{T}_{Y'|S}(\mathrm{s}),
$$

let

$$
f_i \triangleq \begin{cases} 1, & \text{if } \mathbf{X}_i \in \bigcup\limits_{j':\mathbf{Y}_{j'}\in\mathcal{T}_{Y'|S}(\mathrm{s})} \mathcal{T}_{X|Y'S}(\mathbf{Y}_{j'},\mathrm{s}) \\ 0, & \text{otherwise.} \end{cases}
$$

Let g denote the indicator function of the event $G(\mathbf{s}, \mathcal{T}_{Y'|S})$. Then

$$\begin{aligned} \mathsf{P}(A(\mathbf{s}, \mathcal{T}_{XY'|S})^c \cap G(\mathbf{s}, \mathcal{T}_{Y'|S})) &= \mathsf{P}\Big(\Big\{\frac{1}{N}\sum_{i=1}^{N} f_i > t\Big\} \cap G(\mathbf{s}, \mathcal{T}_{Y'|S})\Big) \\ &\leq \exp[-Nt] \cdot \mathsf{E}[g \cdot \exp\Big(\sum_{i=1}^{N} f_i\Big)]. \end{aligned} \tag{3.94}$$

To upper bound the preceding expectation, we need the following σ-fields. Let

$$\mathcal{F}_0 \triangleq \sigma(\mathbf{Y}_1, \ldots, \mathbf{Y}_M),$$

and for $i = 1, \ldots, N$, let

$$\mathcal{F}_i \triangleq \sigma(\mathbf{Y}_1, \ldots, \mathbf{Y}_M, \mathbf{X}_1, \ldots, \mathbf{X}_i).$$

Write

$$\mathsf{E}[g \cdot \exp\Big(\sum_{i=1}^{N} f_i\Big)] = \mathsf{E}[\mathsf{E}[\exp(f_N) \mid \mathcal{F}_{N-1}]\, g \exp\Big(\sum_{i=1}^{N-1} f_i\Big)]. \tag{3.95}$$

First, observe that by independence,

$$\mathsf{E}[f_N \mid \mathcal{F}_{N-1}] \cdot g = g \cdot \frac{1}{|\mathcal{T}_P|} \Big| \bigcup_{j': \mathbf{Y}_{j'} \in \mathcal{T}_{Y'|S}(\mathbf{s})} \mathcal{T}_{X|Y'S}(\mathbf{Y}_{j'}, \mathbf{s}) \Big|.$$

If $g = 0$ in the preceding equation, the left-hand side is 0, and any nonnegative number will be an upper bound. If $g = 1$, we have

$$|\{j' : \mathbf{Y}_{j'} \in \mathcal{T}_{Y'|S}(\mathbf{s})\}| \leq t'.$$

If n is sufficiently large,

$$\begin{aligned} \mathsf{E}[f_N \mid \mathcal{F}_{N-1}] \cdot g &\leq g \cdot t' \cdot \exp[-n(I(X \wedge Y'S) - \varepsilon/4)]/2\log e \\ &= g \cdot \exp[n(|R_2 - I(Y' \wedge S)|^+ - I(X \wedge Y'S) + \varepsilon/2)]/2\log e. \end{aligned}$$

So, if $I(X \wedge Y'S) > |R_2 - I(Y' \wedge S)|^+ + \varepsilon$,

$$\mathsf{E}[f_N \mid \mathcal{F}_{N-1}] \cdot g \leq g \cdot \exp(-n\varepsilon/2)/2\log e.$$

Invoking the inequality $2^x \leq 1 + x$, we then get

$$\begin{aligned} \mathsf{E}[\exp(f_N) \mid \mathcal{F}_{N-1}] \cdot g &\leq (1 + \mathsf{E}[f_N \mid \mathcal{F}_{N-1}]) \cdot g \\ &\leq (1 + \exp(-n\varepsilon/2)/2\log e) \cdot g \\ &\leq g \cdot \exp[\tfrac{1}{2}\exp(-n\varepsilon/2)]. \end{aligned}$$

Applying the preceding analysis inductively to (3.95),

$$\mathsf{E}[g \cdot \exp\Big(\sum_{i=1}^{N} f_i\Big)] \leq \mathsf{E}[g] \cdot \exp[\tfrac{1}{2}N\exp(-n\varepsilon/2)].$$

Since $\mathsf{E}[g] = \mathsf{P}(g = 1) \leq 1$,

$$\mathsf{E}[g \cdot \exp\Big(\sum_{i=1}^{N} f_i\Big)] \leq \exp[\tfrac{1}{2}N\exp(-n\varepsilon/2)].$$

Combining this with (3.94),

$$\begin{aligned} \mathsf{P}(A(\mathbf{s}, \mathcal{T}_{XY'S})^c \cap G(\mathbf{s}, \mathcal{T}_{Y'S})) &\leq \exp[-N(t - \tfrac{1}{2}\exp(-n\varepsilon/2))] \\ &= \exp[-N(\tfrac{1}{2}\exp(-n\varepsilon/2))] \\ &= \exp[-\tfrac{1}{2}\exp[n(R_1 - \varepsilon/2)]] \\ &\leq \exp[-\tfrac{1}{2}\exp(n\varepsilon/2)], \end{aligned} \tag{3.96}$$

where the last step follows because $R_1 \geq \varepsilon$. Combining (3.93) with (3.96) yields (3.91). □

Remark. We point out that the procedure that established (3.92) also shows that with positive probability we can find $\mathbf{Y}_1, \ldots, \mathbf{Y}_M$, each of type Q, such that for all $P_{XYY'S}$,

$$|\{j' : (\mathbf{x}, \mathbf{y}, \mathbf{Y}_{j'}, \mathbf{s}) \in \mathcal{T}_{XYY'S}\}| \leq \exp[n(|R_2 - I(Y' \wedge XYS)|^+ + \varepsilon)], \quad \forall \mathbf{x}, \mathbf{y}, \mathbf{s}.$$

Thus we have also proved (3.85). Since (3.88) and (3.90) are more intricate, we refer the reader to the appendix in [8].

CHAPTER 4
STATE CONSTRAINTS FOR THE AVMAC

In this chapter we assume that the state-selection mechanism can generate only those state sequences which satisfy a certain time-average constraint. We will show how this assumption can increase the capacity region. A striking example of this phenomenon occurs with the *adder channel.* This channel is symmetrizable-$\mathcal{X}$, symmetrizable-$\mathcal{Y}$, and nonsymmetrizable-$\mathcal{XY}$. By Corollary 3.12, its capacity region consists only of the origin. However, when a *state constraint* is imposed, the capacity region has the form shown in Figure 4.1.

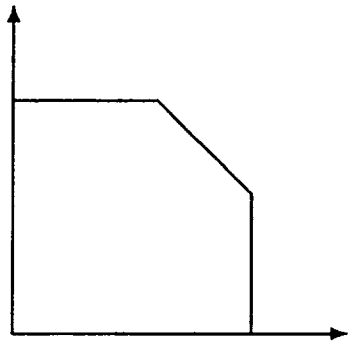

Figure 4.1: The Adder Channel Capacity Region Under a State Constraint.

This chapter is organized as follows. We first prove a new "weak converse" theorem to give an outer bound on the capacity region under a state constraint. We then apply this result to the *additive AVC*, and then to the *group adder AVC.* To derive inner bounds on the capacity region under a state constraint, we use Lemma 4.16. To prove this result, we modify the proof of Theorem 3.15 to handle state constraints, *even for symmetrizable channels.* To conclude the chapter, we use our inner and outer bounds to find the capacity region of the adder channel under a state constraint.

4.1 State Constraints

Fix any function $\ell: \mathcal{S} \to [0, \infty)$ such that $\min_{s \in \mathcal{S}} \ell(s) = 0$. Set $\ell_{\max} \triangleq \max_{s \in \mathcal{S}} \ell(s)$. Next, for any $\mathrm{s} = (s_1, \ldots, s_n) \in \mathcal{S}^n$, let

$$\ell_n(\mathrm{s}) \triangleq \frac{1}{n} \sum_{k=1}^{n} \ell(s_k).$$

Example. If $\mathcal{S} = \{0, 1\}$ and $\ell(s) = s$, then $\ell_n(\mathrm{s})$ is the normalized Hamming weight of s, i.e., the fraction of 1's in s.

Definition 4.1 For any *state constraint*, $L \geq 0$, let

$$\mathcal{S}^n(L) \triangleq \{\mathrm{s} \in \mathcal{S}^n : \ell_n(\mathrm{s}) \leq L\}.$$

Of course, if $L \geq \ell_{\max}$, then $\mathcal{S}^n(L) = \mathcal{S}^n$.

Consider the following modification of Definition 3.1.

Definition 4.2 A pair of nonnegative real numbers, (R_1, R_2), is said to be *achievable under state constraint* L for the AVC W if:

> For every $0 < \lambda < 1$, and every $\Delta R > 0$, there exists a positive integer n_0 such that for all $n \geq n_0$, there exist positive integers N and M such that
>
> $$\frac{\log N}{n} > R_1 - \Delta R \qquad \text{and} \qquad \frac{\log M}{n} > R_2 - \Delta R,$$
>
> and such that there exists a code (f, g, φ) (cf. Definition 1.1) with
>
> $$\frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(\{\mathrm{z} \in \mathcal{Z}^n : \varphi(\mathrm{z}) \neq (i, j)\} | \mathrm{x}_i, \mathrm{y}_j, \mathrm{s}) \leq \lambda, \qquad \forall \mathrm{s} \in \mathcal{S}^n(L).$$

Definition 4.3 The *capacity region under state constraint* L, denoted $C(W, L)$, is defined by

$$C(W, L) \triangleq \{(R_1, R_2) : (R_1, R_2) \text{ is achievable under state constraint } L\}.$$

Clearly, if a pair (R_1, R_2) is achievable in the sense of Definition 3.1, it is achievable in the sense Definition 4.2. Thus, we always have

$$C(W) \subset C(W, L).$$

Even though it is a slight abuse of notation, for $r \in \mathcal{D}(\mathcal{S})$, we set $\ell(r) \triangleq \sum_s \ell(s) r(s)$. If we let

$$\mathcal{D}^L(\mathcal{S}) \triangleq \{r \in \mathcal{D}(\mathcal{S}) : \ell(r) \leq L\},$$

then we can write the following analog of (3.2):

$$\begin{aligned}
I^L_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}^L(\mathcal{S})} I_{\mathcal{X}\wedge\mathcal{Z}}(p\times q\times rW),\\
I^L_{\mathcal{Y}\wedge\mathcal{Z}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}^L(\mathcal{S})} I_{\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW),\\
I^L_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}^L(\mathcal{S})} I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p\times q\times rW),\\
I^L_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}^L(\mathcal{S})} I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW),\\
I^L_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}^L(\mathcal{S})} I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW).
\end{aligned}$$

Note that if $L \geq \ell_{\max}$, then $\mathcal{D}^L(\mathcal{S}) = \mathcal{D}(\mathcal{S})$, and the preceding definitions reduce to (3.2). Further, in analogy with Definition 3.4, we set

$$\begin{aligned}
\mathcal{R}^L(p,q,W) \triangleq \{(R_1,R_2): \quad & 0 \leq R_1 < I^L_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W),\\
& 0 \leq R_2 < I^L_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W),\\
& 0 \leq R_1+R_2 < I^L_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p,q,W)\},
\end{aligned}$$

and we take $\mathcal{R}^L(W)$ to be the closed convex hull of

$$\bigcup_{p\in\mathcal{D}(\mathcal{X}),\, q\in\mathcal{D}(\mathcal{Y})} \mathcal{R}^L(p,q,W).$$

4.2 A Weak Converse

We now proceed to establish a weak converse, $C(W,L) \subset \mathcal{R}^L(W)$. It is easy to see that if $L_1 \leq L_2$, then $\mathcal{R}^{L_2}(p,q,W) \subset \mathcal{R}^{L_1}(p,q,W)$, and so $\mathcal{R}^{L_2}(W) \subset \mathcal{R}^{L_1}(W)$. This observation leads us to the following lemma.

Lemma 4.4 *For* $0 < L < \ell_{\max}$,

$$\bigcap_{0<\delta<L} \mathcal{R}^{L-\delta}(W) = \mathcal{R}^L(W). \tag{4.1}$$

Proof. First, we clearly have $\bigcap_{0<\delta<L} \mathcal{R}^{L-\delta}(W) \supset \mathcal{R}^L(W)$. It remains to prove the reverse inclusion. Lemmas 4.5 and 4.6 below will establish that for every $\varepsilon > 0$, there exists a $\delta > 0$ such that for all p and q,

$$\begin{aligned} R^{L-\delta}(p,q,W) \subset \{(R_1,R_2): \quad & 0 \leq R_1 < I^L_{X\wedge Z|Y}(p,q,W) + \varepsilon, \\ & 0 \leq R_2 < I^L_{Y\wedge Z|X}(p,q,W) + \varepsilon, \\ & 0 \leq R_1 + R_2 < I^L_{XY\wedge Z}(p,q,W) + \varepsilon\}. \end{aligned} \tag{4.2}$$

Let $\mathcal{R}^L_\varepsilon(p,q,W)$ denote the set on the right-hand side of (4.2). Let $\mathcal{R}^L_\varepsilon(W)$ denote the closed convex hull of

$$\bigcup_{p\in\mathcal{D}(\mathcal{X}),q\in\mathcal{D}(\mathcal{Y})} \mathcal{R}^L_\varepsilon(p,q,W).$$

Clearly, for every $\varepsilon > 0$, there exists a $0 < \delta < L$ with $\mathcal{R}^{L-\delta}(W) \subset \mathcal{R}^L_\varepsilon(W)$. It follows that

$$\bigcap_{0<\delta<L} \mathcal{R}^{L-\delta}(W) \subset \bigcap_{\varepsilon>0} \mathcal{R}^L_\varepsilon(W).$$

Now, it is easy to see that every point in $\mathcal{R}^L_\varepsilon(W)$ is within distance ε of $\mathcal{R}^L(W)$. Since $\mathcal{R}^L(W)$ is closed set, $\bigcap_{\varepsilon>0} R^L_\varepsilon(W) \subset \mathcal{R}^L(W)$, and so

$$\bigcap_{0<\delta<L} \mathcal{R}^{L-\delta}(W) \subset \bigcap_{\varepsilon>0} \mathcal{R}^L_\varepsilon(W) \subset \mathcal{R}^L(W).$$

□

Lemma 4.5 *For every $\eta > 0$, there exists a δ, $0 < \delta < L$, such that for all $r \in \mathcal{D}^L(\mathcal{S})$, there exists an $\hat{r} \in \mathcal{D}^{L-\delta}(\mathcal{S})$ with $d(r, \hat{r}) < \eta$.*

Proof. Recall our assumption that $\min_s \ell(s) = 0$. Hence, there is some $s_0 \in \mathcal{S}$ with $\ell(s_0) = 0$. Let $\eta > 0$ be given. Choose $0 < \delta < L$ such that

$$2(1 - \frac{L-\delta}{L}) \ < \ \eta.$$

For $s \neq s_0$, set $\hat{r}(s) = r(s) \cdot (L-\delta)/L$. Since

$$\sum_{s \neq s_0} \hat{r}(s) = (1 - r(s_0)) \frac{L-\delta}{L} < 1,$$

we can set $\hat{r}(s_0) = 1 - \sum_{s \neq s_0} \hat{r}(s)$. Observe that since $\ell(s_0) = 0$,

$$\sum_s \ell(s)\hat{r}(s) = \frac{L-\delta}{L} \sum_s \ell(s) r(s) \leq L - \delta.$$

Finally, note that

$$d(r, \hat{r}) \leq 2 \sum_{s \neq s_0} |r(s) - \hat{r}(s)| = 2(1 - \frac{L-\delta}{L}) \sum_{s \neq s_0} r(s) < \eta.$$

□

Lemma 4.6 *For every $\varepsilon > 0$, there exists a $\delta > 0$ such that for all $p \in \mathcal{D}(\mathcal{X})$ and all $q \in \mathcal{D}(\mathcal{Y})$,*

$$\begin{aligned} I^{L-\delta}_{\mathcal{X} \wedge \mathcal{Z}|\mathcal{Y}}(p, q, W) \ &< \ I^{L}_{\mathcal{X} \wedge \mathcal{Z}|\mathcal{Y}}(p, q, W) + \varepsilon, \\ I^{L-\delta}_{\mathcal{Y} \wedge \mathcal{Z}|\mathcal{X}}(p, q, W) \ &< \ I^{L}_{\mathcal{Y} \wedge \mathcal{Z}|\mathcal{X}}(p, q, W) + \varepsilon, \\ I^{L-\delta}_{\mathcal{X}\mathcal{Y} \wedge \mathcal{Z}}(p, q, W) \ &< \ I^{L}_{\mathcal{X}\mathcal{Y} \wedge \mathcal{Z}}(p, q, W) + \varepsilon. \end{aligned}$$

Proof. It suffices to prove the first inequality. Let $\varepsilon > 0$ be given. Choose $\eta > 0$ such that $d(r, \hat{r}) < \eta$ implies

$$|I_{\mathcal{X} \wedge \mathcal{Z}|\mathcal{Y}}(p \times q \times \hat{r}W) - I_{\mathcal{X} \wedge \mathcal{Z}|\mathcal{Y}}(p \times q \times rW)| \ < \ \varepsilon.$$

Let $\delta > 0$ be as in the previous lemma. Let $r \in \mathcal{D}^L(\mathcal{S})$ be such that

$$I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p \times q \times rW) \;=\; I^L_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p, q, W).$$

By the previous lemma, there exists an $\hat{r} \in \mathcal{D}^{L-\delta}(\mathcal{S})$ with $d(r, \hat{r}) < \eta$, and so

$$\begin{aligned} I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p \times q \times \hat{r}W) \;&<\; I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p \times q \times rW) + \varepsilon \\ &=\; I^L_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p, q, W) + \varepsilon, \end{aligned}$$

from which the desired result follows immediately. □

Having established (4.1), we can now prove the following result.

Theorem 4.7 (*Weak Converse Under State Constraint L*).

$$C(W, L) \;\subset\; \mathcal{R}^L(W).$$

Proof. It suffices to prove that for every $0 < \delta < L$,

$$C(W, L) \;\subset\; \mathcal{R}^{L-\delta}(W).$$

Fix $0 < \delta < L$. Let $0 < \lambda < 1$ and $\Delta R > 0$ be arbitrary. Suppose that $(R_1, R_2) \in C(W, L)$. Then by Definition 4.2, for all $n \geq n_0$, there exist positive integers N and M such that

$$\frac{\log N}{n} \;>\; R_1 - \Delta R \qquad \text{and} \qquad \frac{\log M}{n} \;>\; R_2 - \Delta R, \tag{4.3}$$

and such that there exist codewords $\mathbf{x}_1, \ldots, \mathbf{x}_N$ for user 1; codewords $\mathbf{y}_1, \ldots, \mathbf{y}_M$ for user 2; and a decoder $\varphi(\mathbf{z}) = (\varphi_1(\mathbf{z}), \varphi_2(\mathbf{z}))$ with

$$e(\mathbf{s}) \;\triangleq\; \frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(\{\mathbf{z} \in \mathcal{Z}^n : \varphi(\mathbf{z}) \neq (i, j)\} | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \;\leq\; \frac{\lambda}{2}, \quad \forall \mathbf{s} \in \mathcal{S}^n(L). \tag{4.4}$$

Now, let $r_1, \ldots, r_n$ be any elements of $\mathcal{D}^{L-\delta}(\mathcal{S})$, and set

$$r(\mathbf{s}) \triangleq \prod_{k=1}^{n} r_k(s_k), \qquad \mathbf{s} = (s_1, \ldots, s_n) \in \mathcal{S}^n.$$

Let A be a $\{1, \ldots, N\}$-valued RV, and B a $\{1, \ldots, M\}$-valued RV. Let

$$\mathbf{X} = (X_1, \ldots, X_n), \quad \mathbf{Y} = (Y_1, \ldots, Y_n), \quad \mathbf{S} = (S_1, \ldots, S_n), \text{ and } \mathbf{Z} = (Z_1, \ldots, Z_n)$$

be $\mathcal{X}^n$, $\mathcal{Y}^n$, $\mathcal{S}^n$, and $\mathcal{Z}^n$-valued RV's, respectively, whose joint distribution is given by

$$\begin{aligned} &\mathsf{P}(\mathbf{Z} = \mathbf{z}, \mathbf{X} = \mathbf{x}, \mathbf{Y} = \mathbf{y}, \mathbf{S} = \mathbf{s}, B = j, A = i) \\ &\qquad = W^n(\mathbf{z}|\mathbf{x}, \mathbf{y}, \mathbf{s}) r(\mathbf{s}) \delta_{\mathbf{x}_i}(\mathbf{x}) \delta_{\mathbf{y}_j}(\mathbf{y}) \tfrac{1}{M} \cdot \tfrac{1}{N}. \end{aligned} \tag{4.5}$$

Clearly, since $\mathsf{P}(\mathbf{S} = \mathbf{s}) = \prod_{k=1}^{n} r_k(s_k)$, the $\{S_k\}$ are independent. Now, observe that by Markov's inequality, the independence of the $\{S_k\}$, and the fact that

$$\mathsf{E}[\,|\ell(S_k) - \mathsf{E}[\,\ell(S_k)\,]|^2\,] \le \ell_{\max}^2,$$

we have

$$\begin{aligned} \mathsf{P}(\ell_n(\mathbf{S}) > L) &= \mathsf{P}\Big(\frac{1}{n}\sum_{k=1}^{n}\Big[\ell(S_k) - \mathsf{E}[\,\ell(S_k)\,]\Big] > L - \frac{1}{n}\sum_{k=1}^{n}\mathsf{E}[\,\ell(S_k)\,]\Big) \\ &\le \mathsf{P}\Big(\frac{1}{n}\sum_{k=1}^{n}\Big[\ell(S_k) - \mathsf{E}[\,\ell(S_k)\,]\Big] > \delta\Big) \\ &\le \frac{\ell_{\max}^2}{n\delta^2} \le \lambda/2, \qquad \text{assuming } n \ge \ell_{\max}^2/[\delta^2(\lambda/2)]. \end{aligned} \tag{4.6}$$

Note that if $L \ge \ell_{\max}$, $\mathsf{P}(\ell_n(\mathbf{S}) > L) = 0$. Next, observe that (4.5) also implies

$$\mathsf{P}(A = i, B = j, \mathbf{Z} = \mathbf{z}) = \frac{1}{NM}\sum_{\mathbf{s}\in\mathcal{S}^n} W^n(\mathbf{z}|\mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) r(\mathbf{s}).$$

By (4.4) and (4.6), for all $n \ge \max\{n_0, \ell_{\max}^2/[\delta^2(\lambda/2)]\}$,

$$
\begin{aligned}
\mathsf{P}(\varphi(\mathbf{Z}) \neq (A,B)) &= \sum_{i,j} \mathsf{P}(\varphi(\mathbf{Z}) \neq (i,j), A=i, B=j) \\
&= \sum_{\mathbf{s}\in\mathcal{S}^n} r(\mathbf{s}) \Big(\frac{1}{NM} \sum_{i=1}^{N} \sum_{j=1}^{M} W^n(\{\mathbf{z} : \varphi(\mathbf{z}) \neq (i,j)\} | \mathbf{x}_i, \mathbf{y}_j, \mathbf{s}) \Big) \\
&= \mathsf{E}[\, e(\mathbf{S}) \,] \\
&\leq \max_{\mathbf{s}\in\mathcal{S}^n(L)} e(\mathbf{s}) + \mathsf{P}(\ell_n(\mathbf{S}) > L) \\
&\leq \lambda/2 + \lambda/2 \;=\; \lambda. \qquad (4.7)
\end{aligned}
$$

The remainder of the proof is almost identical to Jahn's proof [14] of the weak converse (without state constraint L, of course). Clearly, (4.7) implies

$$
\mathsf{P}(\varphi_1(\mathbf{Z}) \neq A) \;\leq\; \lambda \quad \text{and} \quad \mathsf{P}(\varphi_2(\mathbf{Z}) \neq B) \;\leq\; \lambda.
$$

Now, using Fano's inequality [4, p. 53], if $\tau \triangleq \mathsf{P}(\varphi(\mathbf{Z}) \neq (A,B))$,

$$
H(AB|\varphi(\mathbf{Z})) \;\leq\; \tau \log(NM-1) + h(\tau),
$$

where $h(t) \triangleq -[t\log t + (1-t)\log(1-t)]$, $t \in (0,1)$, and $h(0) = h(1) \triangleq 0$. Since $h(\cdot) \leq 1$ and $\tau \leq \lambda$, and since $H(AB|\mathbf{Z}) \leq H(AB|\varphi(\mathbf{Z}))$ [4, Problem 1(b), p. 56],

$$
H(AB|\mathbf{Z}) \;\leq\; \lambda \log(NM) + 1.
$$

Similarly,

$$
H(A|\mathbf{Z}) \;\leq\; \lambda \log N + 1 \qquad \text{and} \qquad H(B|\mathbf{Z}) \;\leq\; \lambda \log M + 1.
$$

From (4.5), $H(A) = \log N$, $H(B) = \log M$, and $H(AB) = \log NM$. Hence,

$$
\begin{aligned}
(1-\lambda)\log NM &\leq H(AB) - H(AB|\mathbf{Z}) + 1 \;=\; I(AB \wedge \mathbf{Z}) + 1, \\
(1-\lambda)\log N &\leq H(A) - H(A|\mathbf{Z}) + 1 \;=\; I(A \wedge \mathbf{Z}) + 1, \qquad (4.8) \\
(1-\lambda)\log M &\leq H(B) - H(B|\mathbf{Z}) + 1 \;=\; I(B \wedge \mathbf{Z}) + 1.
\end{aligned}
$$

From (4.5) we also see that

$$\mathsf{P}(\mathbf{Z}=\mathbf{z}|(\mathbf{X},\mathbf{Y})=(\mathbf{x},\mathbf{y}),(A,B)=(i,j))=\sum_{\mathbf{s}\in\mathcal{S}^n} r(\mathbf{s})W^n(\mathbf{z}|\mathbf{x},\mathbf{y},\mathbf{s})$$

does not depend on (i,j). Hence, by the Data Processing Inequality [13, p. 26, inequality (2.3.19b)],

$$I(AB\wedge\mathbf{Z}) \;\leq\; I(\mathbf{XY}\wedge\mathbf{Z}).$$

Similarly, (4.5) implies

$$\mathsf{P}(\mathbf{Z}=\mathbf{z}|\mathbf{X}=\mathbf{x},A=i) \;=\; \sum_{\mathbf{s}\in\mathcal{S}^n} r(\mathbf{s})\Big(\frac{1}{M}\sum_{j=1}^{M} W^n(\mathbf{z}|\mathbf{x},\mathbf{y}_j,\mathbf{s})\Big)$$

does not depend on i. Therefore, by the Data Processing Inequality,

$$\begin{aligned} I(A\wedge\mathbf{Z}) &\leq I(\mathbf{X}\wedge\mathbf{Z}) \\ &\leq I(\mathbf{X}\wedge\mathbf{YZ}) \\ &= I(\mathbf{X}\wedge\mathbf{Y})+I(\mathbf{X}\wedge\mathbf{Z}|\mathbf{Y}) \\ &= I(\mathbf{X}\wedge\mathbf{Z}|\mathbf{Y}), \end{aligned}$$

where the last step follows because (4.5) implies $\mathbf{X}$ and $\mathbf{Y}$ are independent. An analogous argument will establish that

$$I(B\wedge\mathbf{Z}) \;\leq\; I(\mathbf{Y}\wedge\mathbf{Z}|\mathbf{X}).$$

Recalling (4.8), we have

$$\begin{aligned} (1-\lambda)\log NM &\leq I(\mathbf{XY}\wedge\mathbf{Z})+1, \\ (1-\lambda)\log N &\leq I(\mathbf{X}\wedge\mathbf{Z}|\mathbf{Y})+1, \\ (1-\lambda)\log M &\leq I(\mathbf{Y}\wedge\mathbf{Z}|\mathbf{X})+1. \end{aligned}$$

Now, we use (4.5) to see that

$$\begin{aligned}
\mathsf{P}(\mathbf{Z}=\mathbf{z}|\mathbf{X}=\mathbf{x},\mathbf{Y}=\mathbf{y}) &= \sum_{\mathbf{s}\in\mathcal{S}^n} r(\mathbf{s})W^n(\mathbf{z}|\mathbf{x},\mathbf{y},\mathbf{s}) \\
&= \sum_{s_1,\ldots,s_n}\prod_{k=1}^{n} r_k(s_k)W(z_k|x_k,y_k,s_k) \\
&= \prod_{k=1}^{n}(r_kW)(z_k|x_k,y_k).
\end{aligned}$$

It follows that

$$H(\mathbf{Z}|\mathbf{XY}) = \sum_{k=1}^{n} H(Z_k|X_kY_k),$$

and hence,

$$\begin{aligned}
I(\mathbf{XY}\wedge\mathbf{Z}) &= H(\mathbf{Z}) - H(\mathbf{Z}|\mathbf{XY}) \\
&\le \sum_{k=1}^{n} H(Z_k) - H(\mathbf{Z}|\mathbf{XY}) \\
&= \sum_{k=1}^{n} I(X_kY_k\wedge Z_k) \\
&= \sum_{k=1}^{n} I_{\mathcal{XY}\wedge\mathcal{Z}}(p_k\times q_k\times r_kW),
\end{aligned}$$

where $p_k(x) \triangleq \mathsf{P}(X_k=x)$, $q_k(y) \triangleq \mathsf{P}(Y_k=y)$, and the last step follows because (4.5) implies X_k and Y_k are independent. Similarly, we can write

$$\begin{aligned}
I(\mathbf{X}\wedge\mathbf{Z}|\mathbf{Y}) &= H(\mathbf{Z}|\mathbf{Y}) - H(\mathbf{Z}|\mathbf{XY}) \\
&\le \sum_{k=1}^{n} H(Z_k|\mathbf{Y}) - H(\mathbf{Z}|\mathbf{XY}) \\
&\le \sum_{k=1}^{n} H(Z_k|Y_k) - H(\mathbf{Z}|\mathbf{XY}) \\
&= \sum_{k=1}^{n} I(X_k\wedge Z_k|Y_k) \\
&= \sum_{k=1}^{n} I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p_k\times q_k\times r_kW),
\end{aligned}$$

and, of course,

$$I(\mathbf{Y}\wedge\mathbf{Z}|\mathbf{X}) \le \sum_{k=1}^{n} I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p_k\times q_k\times r_kW).$$

We conclude that

$$\begin{aligned}
\frac{\log N}{n} + \frac{\log M}{n} &\leq \frac{1}{1-\lambda}\Big(\frac{1}{n}\sum_{k=1}^{n} I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p_k \times q_k \times r_k W) + \frac{1}{n}\Big), \\
\frac{\log N}{n} &\leq \frac{1}{1-\lambda}\Big(\frac{1}{n}\sum_{k=1}^{n} I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p_k \times q_k \times r_k W) + \frac{1}{n}\Big), \\
\frac{\log M}{n} &\leq \frac{1}{1-\lambda}\Big(\frac{1}{n}\sum_{k=1}^{n} I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p_k \times q_k \times r_k W) + \frac{1}{n}\Big).
\end{aligned}$$

Since the k'th term in each of the preceeding sums depends on r only through r_k, if we take the infimum over all r such that each $r_k \in \mathcal{D}^{L-\delta}(\mathcal{S})$, we get

$$\begin{aligned}
\frac{\log N}{n} + \frac{\log M}{n} &\leq \frac{1}{1-\lambda}\Big(\frac{1}{n}\sum_{k=1}^{n} I^{L-\delta}_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p_k, q_k, W) + \frac{1}{n}\Big), \\
\frac{\log N}{n} &\leq \frac{1}{1-\lambda}\Big(\frac{1}{n}\sum_{k=1}^{n} I^{L-\delta}_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p_k, q_k, W) + \frac{1}{n}\Big), \\
\frac{\log M}{n} &\leq \frac{1}{1-\lambda}\Big(\frac{1}{n}\sum_{k=1}^{n} I^{L-\delta}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p_k, q_k, W) + \frac{1}{n}\Big).
\end{aligned}$$

This combined with (4.3) shows that $(R_1, R_2) \in \mathcal{R}^{L-\delta}(W)$. □

4.3 The Additive AVC

Having established a weak converse in Theorem 4.7, we now compute $\mathcal{R}^L(W)$ for the two-user *additive AVC*. We also consider the special case of the two-user *group adder AVC*. We begin with a few preliminaries. Let $\mathcal{G}$ denote a finite commutative group under $+$, and let $\mathcal{S}$ denote an arbitrary finite set. Suppose X, Y, and N are $\mathcal{G}$-valued RV's on some probability space, $(\Omega, \mathcal{F}, \mathsf{P}_s)$, where $s \in \mathcal{S}$ is unknown. Set

$$Z = X + Y + N. \tag{4.9}$$

Here X and Y represent channel input symbols, while N represents the channel noise. We assume that for every $s \in \mathcal{S}$, N and (X, Y) are independent under P_s.

Suppose that the marginal distribution of N can be written as

$$\mathsf{P}_s(N = n) = V(n|s)$$

for some transition probability V from $\mathcal{S}$ into $\mathcal{G}$. Then

$$\begin{aligned} \mathsf{P}_s(Z = z|X = x, Y = y) &= \mathsf{P}_s(N = z - x - y|X = x, Y = y) \\ &= \mathsf{P}_s(N = z - x - y) \\ &= V(z - x - y|s). \end{aligned}$$

In light of the preceding paragraph, let $\mathcal{X} = \mathcal{Y} = \mathcal{Z} = \mathcal{G}$.

Definition 4.8 We say W is an *additive AVC* if

$$W(z|x, y, s) = V(z - x - y|s) \tag{4.10}$$

for some transition probability V from $\mathcal{S}$ into $\mathcal{G}$. We also write $(rW)(z|x, y) = (rV)(z - x - y)$, where $(rV)(t) \triangleq \sum_s r(s)V(t|s)$.

We shall need the following lemma before proceeding further.

Lemma 4.9 *Let W be an additive AVC given by* (4.10). *Then*

$$H_{Z|X\mathcal{Y}}(p \times q \times rW) = H(rV),$$

independently of p and q.

Proof. Recall that if X, Y, and Z are discrete RV's with joint distribution P_{XYZ}, then

$$H(Z|XY) = \sum_{x,y} P_{XY}(x, y)H(Z|X = x, Y = y),$$

where for fixed x, y, $H(Z|X = x, Y = y)$ denotes the entropy of $P_{Z|XY}(\cdot|x, y)$. Since $(rW)(z|x, y) = (rV)(z - x - y)$, and since $\mathcal{G}$ is a group,

$$-\sum_{z\in\mathcal{G}}(rV)(z - x - y)\log(rV)(z - x - y)$$

does not depend on x, y, and is simply $H(rV)$. □

We next consider the following definition.

Definition 4.10 For $p, q \in \mathcal{D}(\mathcal{G})$, the *convolution* of p and q is given by

$$(p * q)(t) \triangleq \sum_{b \in \mathcal{G}} p(t-b)q(b).$$

Observe that convolution is both commutative and associative. Next, if $p(\tau) = 1/|\mathcal{G}|$ for all $\tau \in \mathcal{G}$, then $(p * q)(t) = 1/|\mathcal{G}|$ for all $t \in \mathcal{G}$. In other words, the convolution of the uniform distribution with any distribution is again the uniform distribution. Now, use the fact that

$$\begin{aligned}(pqrW)(z) &\triangleq \sum_{x,y,s} p(x)q(y)r(s)W(z|x,y,s) \\ &= (p * q * rV)(z)\end{aligned}$$

in order to write $H_Z(p \times q \times rW) = H(p * q * rV)$. It then follows that

$$I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p \times q \times rW) = H(p * q * rV) - H(rV).$$

We recall here that the maximum value of H is $\log|\mathcal{G}|$, and is achieved by the uniform distribution. Let u denote the uniform distribution on $\mathcal{G}$; $u(t) \triangleq 1/|\mathcal{G}|, t \in \mathcal{G}$. By the minimax theorem [15, Theorem 1.5.1, p. 14] or [12, Theorem 2, p. 44],

$$\begin{aligned}&\sup_{p \in \mathcal{D}(\mathcal{X}), q \in \mathcal{D}(\mathcal{Y})} I^L_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p, q, rW) \\ &\qquad = \max_{p \in \mathcal{D}(\mathcal{X})} \max_{q \in \mathcal{D}(\mathcal{Y})} \min_{r \in \mathcal{D}^L(\mathcal{S})} H(p * q * rV) - H(rV) \\ &\qquad = \max_{p \in \mathcal{D}(\mathcal{X})} \min_{r \in \mathcal{D}^L(\mathcal{S})} \left[\left(\max_{q \in \mathcal{D}(\mathcal{Y})} H(p * q * rV) \right) - H(rV) \right] \\ &\qquad = \log|\mathcal{G}| - \max_{r \in \mathcal{D}^L(\mathcal{S})} H(rV).\end{aligned}$$

By writing

$$I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p \times q \times rW) = H(p * rV) - H(rV)$$

and

$$I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW) \;=\; H(q*rV)-H(rV),$$

we see that

$$\sup_{p,q} I^L_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W)=\sup_{p,q} I^L_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W)=\log|\mathcal{G}|-\max_{r\in\mathcal{D}^L(\mathcal{S})} H(rV) \qquad (4.11)$$

as well. Since each of the three suprema is achieved by $p=q=u$, it follows that for an additive AVC, $\mathcal{R}^L(W)$ has the shape of a 45° triangle:

$$\mathcal{R}^L(W) \;=\; \{(R_1,R_2): 0\le R_1+R_2\le \log|\mathcal{G}|-\max_{r\in\mathcal{D}^L(\mathcal{S})} H(rV)\}. \qquad (4.12)$$

A special case of the additive AVC is the *group adder channel.* In this model, $\mathcal{S}=\mathcal{G}$, and V has the special form

$$V(t|s) \;=\; V_0(t-s)$$

for some $V_0\in\mathcal{D}(\mathcal{G})$. The motivation for this model is similar to that of the additive AVC. We consider a fixed probability space $(\Omega,\mathcal{F},\mathsf{P})$, and instead of (4.9), we set

$$Z \;=\; X+Y+N+s,$$

where s is unknown, and $\mathsf{P}(N=n)=V_0(n)$. It then follows that if (X,Y) and N are independent under P,

$$\begin{aligned}\mathsf{P}(Z=z|X=x,Y=y) &= \mathsf{P}(N=z-x-y-s|X=x,Y=y)\\ &= \mathsf{P}(N=z-x-y-s)\\ &= V_0(z-x-y-s).\end{aligned}$$

Now, for the group adder channel,

$$(rV)(t) \;=\; (r*V_0)(t).$$

We see immediately that if r or V_0 is uniform, $r * V_0 = u$, and $H(r * V_0) = \log|\mathcal{G}|$. Thus, if $u \in \mathcal{D}^L(\mathcal{S})$, or if $V_0 = u$, then (4.12) reduces to $\mathcal{R}^L(W) = \{(0,0)\}$. Note that $u \in \mathcal{D}^L(\mathcal{S})$ if and only if

$$\frac{1}{|\mathcal{G}|}\sum_{s\in\mathcal{G}}\ell(s) \;\leq\; L. \tag{4.13}$$

We can further specialize the group adder AVC to a *noiseless* group adder channel by setting $\mathsf{P}(N = 0) = 1$. In other words, $V_0(t) = \delta(t)$, where $\delta(t) = 1$ if $t = 0$, and $\delta(t) = 0$ otherwise. In this case, $r * V_0 = r * \delta = r$, and

$$\mathcal{R}^L(W) \;=\; \{(R_1, R_2) : 0 \leq R_1 + R_2 \leq \log|\mathcal{G}| - \max_{r\in\mathcal{D}^L(\mathcal{S})} H(r)\}.$$

Thus, for the *noiseless* group adder AVC, $\mathcal{R}^L(W) = \{(0,0)\}$ if and only if (4.13) holds.

4.4 Forward Theorems

In this section, we prove forward theorems which provide inner bounds on the capacity region under state constraint L.

4.4.1 Nonsymmetrizable Channels

The following theorem is an obvious analog of Theorem 3.15 when the permissible state sequences are constrained to lie in $\mathcal{S}^n(L)$. We prove the existence of nonempty, open rectangles of achievable rate pairs, provided that certain nonsymmetrizability conditions are satisfied.

Theorem 4.11 *Suppose W is nonsymmetrizable-$\mathcal{Y}$. Fix any $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$. Further, suppose qW is nonsymmetrizable-$\mathcal{X}$. If*

$$0 < R_1 < I^L_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) \quad \text{and} \quad 0 < R_2 < I^L_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W), \tag{4.14}$$

then (R_1, R_2) is achievable under state constraint L (cf. Definition 4.2).

Remark. It trivially follows from Remark 3.16 that if $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$ are strictly positive, then the mutual information quantities in (4.14) are strictly positive under the preceding nonsymmetrizability assumptions.

Proof. The proof of this result is easily obtained by repeating the proof of Theorem 3.15, providing that every occurrence of $\mathcal{D}(\mathcal{S})$ is changed to $\mathcal{D}^L(\mathcal{S})$, and every occurrence of $\mathcal{S}^n$ is changed to $\mathcal{S}^n(L)$. □

Analogous modifications can be made to Lemma 3.20 and to Theorem 3.21.

4.4.2 Symmetrizable Channels

Recall that by Theorem 3.9, Lemma 3.10, and Lemma 3.11, if W is symmetrizable-$\mathcal{X}\mathcal{Y}$, symmetrizable-$\mathcal{Y}$, or symmetrizable-$\mathcal{X}$, then $C(W)$ has an empty interior. We now show that if one imposes a state constraint L on such a channel, it is possible that $C(W,L)$ will have a nonempty interior.

We begin with the following example. Let $\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0,1\}$, and let $\mathcal{Z} = \{0,1,2,3\}$. Let W_a denote the adder channel given by (1.9). This channel has a very interesting property. When viewed as a single-user AVC with channel input symbols $(x,y) \in \mathcal{X} \times \mathcal{Y}$, the capacity of W_a is 1 (under the average probability of error criterion without constraints). This is easy to see; simply observe that

$(x,y) = (0,0)$ implies $z = 0$ or $z = 1$ and $(x,y) = (1,1)$ implies $z = 2$ or $z = 3$. Obviously, error-free transmission results if the transmitter sends only the symbols $(0,0)$ and $(1,1)$. Now, when a two-user channel is viewed as a single-user channel, the following result is proved in [8]: The multiple-access AVC treated as a single-user AVC has a positive capacity if and only if it is nonsymmetrizable-$\mathcal{XY}$. Hence, the channel W_a in (1.9) is nonsymmetrizable-$\mathcal{XY}$. (This fact is also easy to verify from the definition of symmetrizability-$\mathcal{XY}$. Suppose there is a transition probability U satisfying (3.6). Then a simple calculation shows that $U \equiv 0$. But $U \equiv 0$ is *not* a transition probability.) Next, it is a simple matter to show that W_a is symmetrizable-$\mathcal{X}$ and that the only transition probability satisfying (3.7) is $U(s|x) = \delta_x(s)$. Similarly, W_a is symmetrizable-$\mathcal{Y}$ and the only transition probability satisfying (3.8) is $U(s|y) = \delta_y(s)$. Further, for all $p \in \mathcal{D}(\mathcal{X})$ and all $q \in \mathcal{D}(\mathcal{Y})$, $U(s|x) = \delta_x(s)$ and $U(s|y) = \delta_y(s)$ are the only solutions of (3.18) and (3.19) respectively. This last fact would not have been true if we had taken $z = x + y + s \pmod 2$ and $\mathcal{Z} = \{0,1\}$. In that case, if $q(y) = 1/2$, $y = 0$, 1, every U satisfies (3.18). If $q(y) \neq 1/2$, the only solutions of (3.18) are the solutions of (3.7).

Definition 4.12 Let $\mathcal{U}_{\mathcal{Y}}(W)$ denote the set of all transition probabilities from $\mathcal{Y}$ into $\mathcal{S}$ such that (3.8) holds.

Definition 4.13 If U is a transition probability from $\mathcal{Y}$ into $\mathcal{S}$, and if $q \in \mathcal{D}(\mathcal{Y})$, we set $(qU)(s) \triangleq \sum_y U(s|y)q(y)$. We let

$$\ell_{\mathcal{Y}}^{W}(q) \triangleq \inf_{U \in \mathcal{U}_{\mathcal{Y}}(W)} \ell(qU).$$

If $\mathcal{U}_{\mathcal{Y}}(W) = \phi$, we take $\ell_{\mathcal{Y}}^{W}(q) = \infty$.

Definition 4.14 For $q \in \mathcal{D}(\mathcal{Y})$, let $\mathcal{U}_{\mathcal{X}}(q, W)$ denote the set of all transition probabilities from $\mathcal{X}$ into $\mathcal{S}$ which satisfy (3.18).

Observe that for the adder channel, $\mathcal{U}_{\mathcal{X}}(q, W_a) = \mathcal{U}_{\mathcal{X}}(W_a)$, and does not depend on q.

Definition 4.15 If U is a transition probability from $\mathcal{X}$ into $\mathcal{S}$, and if $p \in \mathcal{D}(\mathcal{X})$, we set $(pU)(s) \triangleq \sum_x U(s|x)p(x)$. We let

$$\ell_{\mathcal{X}}^{W}(p, q) \triangleq \inf_{U \in \mathcal{U}_{\mathcal{X}}(q,W)} \ell(pU).$$

If $\mathcal{U}_{\mathcal{X}}(q, W) = \phi$, we take $\ell_{\mathcal{X}}^{W}(p, q) = \infty$.

For the adder channel, $\ell_{\mathcal{X}}^{W_a}(p, q) = \ell_{\mathcal{X}}^{W_a}(p)$, and does not depend on q.

The following lemma is the major result of this section. Its importance lies in the fact that no nonsymmetrizability assumptions are made.

Lemma 4.16 *Assume that $U_{\mathcal{X}}(q, W)$ does not depend on q. Fix any $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$. If*

$$L < \ell_{\mathcal{X}}^{W}(p, q) \qquad \text{and} \qquad L < \ell_{\mathcal{Y}}^{W}(q), \tag{4.15}$$

and if

$$0 < R_1 < I_{\mathcal{X} \wedge \mathcal{Z}}^{L}(p, q, W) \qquad \text{and} \qquad 0 < R_2 < I_{\mathcal{Y} \wedge \mathcal{Z}|\mathcal{X}}^{L}(p, q, W), \tag{4.16}$$

then (R_1, R_2) is achievable under state constraint L (cf. Definition 4.2).

Proof. Choose $\alpha > 0$ so small that

$$L < \ell_{\mathcal{X}}^{W}(p, q) - 2\alpha \qquad \text{and} \qquad L < \ell_{\mathcal{Y}}^{W}(q) - 2\alpha.$$

Let (cf. equation (3.23))

$$\xi^{\alpha}_{\mathcal{X}}(q,W) \triangleq \inf_{(p,U):\ell(pU)\le \ell^{W}_{\mathcal{X}}(p,q)-\alpha} F^{W}_{\mathcal{X}}(q,U)$$

and (cf. equation (3.25))

$$\xi^{\alpha}_{\mathcal{Y}}(W) \triangleq \inf_{(q,U):\ell(qU)\le \ell^{W}_{\mathcal{Y}}(q)-\alpha} F^{W}_{\mathcal{Y}}(U).$$

We claim $\xi^{\alpha}_{\mathcal{X}}(q,W)$ and $\xi^{\alpha}_{\mathcal{Y}}(W)$ are strictly positive. We treat only $\xi^{\alpha}_{\mathcal{X}}(q,W)$. First note that since $U_{\mathcal{X}}(q,W)$ does not depend on q, neither does $\ell^{W}_{\mathcal{X}}(p,q)$. It is then easy to see that $\xi^{\alpha}_{\mathcal{X}}(q,W)$ is a continuous function of q. Suppose $\xi^{\alpha}_{\mathcal{X}}(q,W)=0$. Since $\xi^{\alpha}_{\mathcal{X}}(q,W)$ is the infimum of a continuous function over the compact set of pairs (p,U) satisfying $\ell(pU)\le \ell^{W}_{\mathcal{X}}(p,q)-\alpha$, there is some (p^*,U^*) satisfying

$$\ell(p^*U^*) \le \ell^{W}_{\mathcal{X}}(p^*,q)-\alpha \qquad \text{and} \qquad F^{W}_{\mathcal{X}}(q,U^*)=0.$$

Hence $U^* \in U_{\mathcal{X}}(q,W)$, and so we must have $\ell(p^*U^*) \ge \ell^{W}_{\mathcal{X}}(p^*,q)$, which is a contradiction. Thus, $\xi^{\alpha}_{\mathcal{X}}(q,W)>0$.

Choose $\delta>0$ so small that

$$\begin{aligned} 0 < 2\delta &< \min\{\xi^{\alpha}_{\mathcal{X}}(q,W),\xi^{\alpha}_{\mathcal{Y}}(W)\}, \qquad (4.17)\\ 0 < R_1 &< I^{L}_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W)-2\delta,\\ 0 < R_2 &< I^{L}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W)-2\delta. \end{aligned}$$

Choose $\hat{p}\in\mathcal{D}(\mathcal{X})$ and $\hat{q}\in\mathcal{D}(\mathcal{Y})$, both strictly positive with $d(p,\hat{p})$ and $d(q,\hat{q})$ both so small that

$$\begin{aligned} \ell^{W}_{\mathcal{X}}(p,q) &\le \ell^{W}_{\mathcal{X}}(\hat{p},\hat{q})+\alpha/2,\\ \ell^{W}_{\mathcal{Y}}(q) &\le \ell^{W}_{\mathcal{Y}}(\hat{q})+\alpha/2,\\ \xi^{\alpha}_{\mathcal{X}}(q,W) &\le \xi^{\alpha}_{\mathcal{X}}(\hat{q},W)+\delta/2, \end{aligned}$$

$$I^L_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W) \;\le\; I^L_{\mathcal{X}\wedge\mathcal{Z}}(\hat{p},\hat{q},W)+\delta/2,$$
$$I^L_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W) \;\le\; I^L_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(\hat{p},\hat{q},W)+\delta/2.$$

(Since we have assumed that $U_{\mathcal{X}}(q,W)$ does not depend on q, it is easy to see that $\ell^W_{\mathcal{X}}(p,q)$ is a continuous function of p, and does not depend on q.) The remainder of the proof is almost identical to the proof of Theorem 3.15 except as detailed below.

The first step is to replace $\mathcal{S}^n$ by $\mathcal{S}^n(L)$ and $\mathcal{D}(\mathcal{S})$ by $\mathcal{D}^L(\mathcal{S})$. In particular, (3.43) becomes

$$G_{ij} \;\triangleq\; \bigcup_{\mathbf{s}'\in\mathcal{S}^n(L)} [\,K^0_{ij}(\mathbf{s}')\cap K^1_{ij}(\mathbf{s}')\,].$$

To show that for each i, $G_{i1},\ldots,G_{iM}$ are pairwise disjoint, we proceed as in Section 3.5, where $P_{XX'YY'SS'} = P_{\mathbf{x}_i,\mathbf{x}_{i'},\mathbf{y}_j,\mathbf{y}_{j'},\mathbf{s},\mathbf{s}'}$. Write

$$\begin{aligned}
\ell_n(\mathbf{s}) &= \frac{1}{n}\sum_{k=1}^{n}\ell(s_k)\\
&= \sum_{s}\ell(s)P_S(s)\\
&= \mathsf{E}[\,\ell(S)\,]\\
&= \mathsf{E}[\,\mathsf{E}[\,\ell(S)\mid Y'\,]\,]\\
&= \sum_{y,s}\ell(s)P_{S|Y'}(s|y)Q(y)\\
&= \ell(QP_{S|Y'}).
\end{aligned}$$

Similarly, $\ell_n(\mathbf{s}') = \ell(QP_{S'|Y})$. Since $\mathbf{s}$ and $\mathbf{s}'$ belong to $\mathcal{S}^n(L)$,

$$\ell(QP_{S|Y'}) \;\le\; L \;<\; \ell^W_{\mathcal{Y}}(Q)-\alpha \quad\text{and}\quad \ell(QP_{S'|Y}) \;\le\; L \;<\; \ell^W_{\mathcal{Y}}(Q)-\alpha.$$

By multiplying $1/2$ times the sum of these two inequalities and setting $U(s|y)\triangleq \frac{1}{2}[P_{S'|Y}(s|y)+P_{S|Y'}(s|y)]$, we must have

$$\ell(QU) \;\le\; \ell^W_{\mathcal{Y}}(Q)-\alpha.$$

This combined with the fact that $F_{\mathcal{Y}}^{W}(U) < \delta$ as in (3.80) implies $\xi_{\mathcal{Y}}^{a}(W) < \delta$, contradicting (4.17).

In all other respects, the proof of this lemma is nearly identical to the proof of Theorem 3.15. □

Definition 4.17 Let

$$\mathcal{R}_{\mathcal{X}}^{L}(p,q,W) \triangleq \{(R_1,R_2) : 0 < R_1 < I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}^{L}(p,q,W),\ 0 < R_2 < I_{\mathcal{Y}\wedge\mathcal{Z}}^{L}(p,q,W)\},$$

and

$$\mathcal{R}_{\mathcal{Y}}^{L}(p,q,W) \triangleq \{(R_1,R_2) : 0 < R_1 < I_{\mathcal{X}\wedge\mathcal{Z}}^{L}(p,q,W),\ 0 < R_2 < I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}^{L}(p,q,W)\}.$$

Observe that if $\mathcal{U}_{\mathcal{X}}(q,W) = \mathcal{U}_{\mathcal{X}}(W)$, then $\ell_{\mathcal{X}}^{W}(p,q) = \ell_{\mathcal{X}}^{W}(p)$. Hence, we have the following theorem.

Theorem 4.18 *If for every $q \in \mathcal{D}(\mathcal{Y})$, $\mathcal{U}_{\mathcal{X}}(q,W) = \mathcal{U}_{\mathcal{X}}(W)$, and if for every $p \in \mathcal{D}(\mathcal{X})$, $\mathcal{U}_{\mathcal{Y}}(p,W) = \mathcal{U}_{\mathcal{Y}}(W)$, then $C(W,L)$ contains the closed convex hull of*

$$\bigcup_{p\in\mathcal{D}(\mathcal{X}):\,L\le\ell_{\mathcal{X}}^{W}(p),\ q\in\mathcal{D}(\mathcal{Y}):\,L\le\ell_{\mathcal{Y}}^{W}(q)} [\mathcal{R}_{\mathcal{X}}^{L}(p,q,W) \cup \mathcal{R}_{\mathcal{Y}}^{L}(p,q,W)].$$

To conclude our discussion of state constraints, we return to the adder channel given by (1.9). We take $\ell(s) = s$ so that $\ell_n(\mathbf{s})$ is the average number of 1's in the sequence $\mathbf{s}$. We claim that

$$C(W_a,\tfrac{1}{2}) = \{(R_1,R_2) : 0 \le R_1 \le \tfrac{1}{2},\ 0 \le R_2 \le \tfrac{1}{2},\ 0 \le R_1 + R_2 \le 2 - \tfrac{3}{4}\log 3\}.$$

To establish our claim, we proceed as follows. Let $p^*(0) = p^*(1) = \frac{1}{2}$ and $q^*(0) = q^*(1) = \frac{1}{2}$. Below we will prove that for all $p \in \mathcal{D}(\mathcal{X})$ and all $q \in \mathcal{D}(\mathcal{Y})$,

$$\mathcal{R}^{\frac{1}{2}}(p,q,W_a) \subset \mathcal{R}^{\frac{1}{2}}(p^*,q^*,W_a). \tag{4.18}$$

From (4.18) it then follows that

$$\bigcup_{p\in\mathcal{D}(\mathcal{X}),\,q\in\mathcal{D}(\mathcal{Y})} \mathcal{R}^{\frac{1}{2}}(p,q,W_a) \;=\; \mathcal{R}^{\frac{1}{2}}(p^*,q^*,W_a). \tag{4.19}$$

Since $\mathcal{R}^{\frac{1}{2}}(p^*,q^*,W_a)$ is obviously convex, upon taking the closure of both sides in (4.19), we have

$$\begin{aligned}\mathcal{R}^{\frac{1}{2}}(W_a) \;=\; \{(R_1,R_2):\quad & 0\le R_1\le I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p^*,q^*,W_a),\\ & 0\le R_2\le I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p^*,q^*,W_a),\\ & 0\le R_1+R_2\le I^{\frac{1}{2}}_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p^*,q^*,W_a)\}.\end{aligned} \tag{4.20}$$

Now, let $r^*(0)=r^*(1)=\frac{1}{2}$. Since $\ell(s)=s$, it is clear that $r^*\in\mathcal{D}^{\frac{1}{2}}(\mathcal{S})$. Using notation introduced below in (4.24)–(4.26), it is an easy calculation to show that

$$\begin{aligned} I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p^*,q^*,W_a) &\triangleq \inf_{r\in\mathcal{D}^{\frac{1}{2}}(\mathcal{S})} I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p^*\times q^*\times rW_a)\\ &= I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p^*\times q^*\times r^*W_a)\\ &= \frac{1}{2},\\ I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p^*,q^*,W_a) &\triangleq \inf_{r\in\mathcal{D}^{\frac{1}{2}}(\mathcal{S})} I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p^*\times q^*\times rW_a)\\ &= I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p^*\times q^*\times r^*W_a)\\ &= \frac{1}{2}, \end{aligned}$$

and

$$\begin{aligned} I^{\frac{1}{2}}_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p^*,q^*,W_a) &\triangleq \inf_{r\in\mathcal{D}^{\frac{1}{2}}(\mathcal{S})} I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p^*\times q^*\times rW_a)\\ &= I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p^*\times q^*\times r^*W_a)\\ &= 2-\frac{3}{4}\log 3 \;\approx\; 0.81. \end{aligned}$$

Hence, (4.20) simplifies to

$$\mathcal{R}^{\frac{1}{2}}(W_a) \;=\; \{(R_1,R_2): 0\le R_1\le\tfrac{1}{2},\, 0\le R_2\le\tfrac{1}{2},\, 0\le R_1+R_2\le 2-\tfrac{3}{4}\log 3\}.$$

By Theorem 4.7, the weak converse under state constraint L, $C(W_a, \frac{1}{2}) \subset \mathcal{R}^{\frac{1}{2}}(W_a)$. To prove that $\mathcal{R}^{\frac{1}{2}}(W_a) \subset C(W_a, \frac{1}{2})$, we proceed as follows. First, it is easy to compute

$$I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}}(p^*, q^*, W_a) \;=\; I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}}(p^*, q^*, W_a) \;=\; \frac{3}{2} - \frac{3}{4}\log 3 \;\approx\; 0.31. \tag{4.21}$$

The key point is to observe that since

$$2 - \frac{3}{4}\log 3 \;=\; \left(\frac{3}{2} - \frac{3}{4}\log 3\right) + \frac{1}{2},$$

we can write

$$I^{\frac{1}{2}}_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p^*, q^*, W_a) \;=\; I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}}(p^*, q^*, W_a) + I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p^*, q^*, W_a) \tag{4.22}$$

and

$$I^{\frac{1}{2}}_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p^*, q^*, W_a) \;=\; I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}}(p^*, q^*, W_a) + I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p^*, q^*, W_a). \tag{4.23}$$

From (4.22) and (4.23), it now follows that $\mathcal{R}^{\frac{1}{2}}(W_a)$, that is, the set on the right in equation (4.20), is equal to the closed convex hull of the union of the open rectangles (cf. Definition 4.17)

$$\mathcal{R}^{\frac{1}{2}}_{\mathcal{X}}(p^*, q^*, W_a)$$
$$= \{(R_1, R_2) : 0 < R_1 < I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p^*, q^*, W_a),\, 0 < R_2 < I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}}(p^*, q^*, W_a)\}$$

and

$$\mathcal{R}^{\frac{1}{2}}_{\mathcal{Y}}(p^*, q^*, W_a)$$
$$= \{(R_1, R_2) : 0 < R_1 < I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}}(p^*, q^*, W_a),\, 0 < R_2 < I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p^*, q^*, W_a)\}.$$

By Theorem 4.18, it follows that $\mathcal{R}^{\frac{1}{2}}(W_a) \subset C(W_a, \frac{1}{2})$. This proves our claim, provided that we can establish (4.18).

In order to establish (4.18), we first agree that if p is a probability distribution on $\{0,1\}$, then we also write p as shorthand for the value $p(1)$. With this convention, a little tedious calculation shows that

$$I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p\times q\times rW_a)$$

$$= H((1-p)(1-r),(1-p)r+p(1-r),pr)-h(r), \tag{4.24}$$

$$I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW_a)$$

$$= H((1-q)(1-r),(1-q)r+q(1-r),qr)-h(r), \tag{4.25}$$

$$I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW_a)$$

$$= H((1-p)(1-q)(1-r),$$

$$(1-p)(1-q)r+(1-p)q(1-r)+p(1-q)(1-r),$$

$$(1-p)qr+p(1-q)r+pq(1-r),pqr)-h(r), \tag{4.26}$$

where $H(t_1,\ldots,t_m)\triangleq -\sum_{k=1}^{m} t_k\log t_k$, and $h(r)\triangleq H(r,1-r)$. We also point out that (4.24)–(4.26) can be used to simplify

$$I_{\mathcal{X}\wedge\mathcal{Z}}(p\times q\times rW_a) \;=\; I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW_a)-I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW_a)$$

and

$$I_{\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW_a) \;=\; I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW_a)-I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p\times q\times rW_a)$$

for use in verifying (4.21). Now, (4.18) will be established if we can show that

$$\sup_{(p,q)\in[0,1]\times[0,1]} I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W_a) \;=\; I^{\frac{1}{2}}_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p^*,q^*,W_a), \tag{4.27}$$

$$\sup_{(p,q)\in[0,1]\times[0,1]} I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W_a) \;=\; I^{\frac{1}{2}}_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p^*,q^*,W_a), \tag{4.28}$$

and

$$\sup_{(p,q)\in[0,1]\times[0,1]} I^{\frac{1}{2}}_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p,q,W_a) \;=\; I^{\frac{1}{2}}_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p^*,q^*,W_a). \tag{4.29}$$

To establish (4.27)–(4.29), we first note that

$$\sup_{(p,q)\in[0,1]\times[0,1]} I^{\frac{1}{2}}_{\cdots}(p,q,W_a) \;=\; \sup_{(p,q)\in[0,1]\times[0,1]} \inf_{r\in\mathcal{D}^{\frac{1}{2}}(\mathcal{S})} I_{\cdots}(p\times q\times rW_a).$$

Hence, (4.27)–(4.29) will be established if we can show that $((p^*,q^*),r^*)$ is a *saddle point* in each case. Recall that if F is a real-valued function of two variables, say u and v, then (u^*,v^*) is a saddle point for F if for all u and v,

$$F(u,v^*) \;\le\; F(u^*,v^*) \;\le\; F(u^*,v). \tag{4.30}$$

If (4.30) holds, it is trivial to show that

$$\sup_u \inf_v F(u,v) \;=\; F(u^*,v^*).$$

To establish (4.30), one shows that v^* is a *global* minimum of $F(u^*,v)$ regarded as a function of v, and that u^* is a *global* maximum of $F(u,v^*)$ regarded as a function of u. Now, it is not too difficult to establish (4.27) and (4.28) since (4.24) implies $I_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p\times q\times rW_a)$ does not depend on q, and (4.25) implies $I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW_a)$ does not depend on p. To establish (4.29) is extemely tedious, and we only sketch the derivation:

Let

$$F(p,q,r) \;\triangleq\; I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW_a).$$

Using (4.26), it is straightforward to show that $F(p^*,q^*,r^*)\le F(p^*,q^*,r)$ for all $r\in[0,1]$. To show that $F(p,q,r^*)\le F(p^*,q^*,r^*)$ for all $(p,q)\in[0,1]\times[0,1]$, we proceed as follows. Let

$$f(p,q) \;\triangleq\; F(p,q,r^*).$$

Then for $(p,q)\in(0,1)\times(0,1)$,

$$\left.\frac{\partial f}{\partial p}\right|_{(p,q)} \;=\; -(\log e)\Big[q\ln\frac{pq}{1-pq}+(1-q)\ln\frac{1-(1-p)(1-q)}{(1-p)(1-q)}\Big], \tag{4.31}$$

and

$$\left.\frac{\partial f}{\partial q}\right|_{(p,q)} = -(\log e)\left[p \ln \frac{pq}{1-pq} + (1-p)\ln \frac{1-(1-p)(1-q)}{(1-p)(1-q)}\right].$$

Clearly, $\frac{\partial f}{\partial p} = \frac{\partial f}{\partial q} = 0$ at $(p,q) = (\frac{1}{2}, \frac{1}{2})$. Also, it is not hard to show that the second derivative matrix of f is negative definite at $(\frac{1}{2}, \frac{1}{2})$, and hence this point is a *local* maximum for f. To show that $(\frac{1}{2}, \frac{1}{2})$ is a *global* maximum for f on $(0,1) \times (0,1)$, we proceed as follows. Letting

$$a = \ln \frac{pq}{1-pq} \qquad \text{and} \qquad b = \ln \frac{1-(1-p)(1-q)}{(1-p)(1-q)},$$

we see that if

$$\left.\frac{\partial f}{\partial p}\right|_{(p,q)} = 0 \qquad \text{and} \qquad \left.\frac{\partial f}{\partial q}\right|_{(p,q)} = 0, \tag{4.32}$$

then

$$qa + (1-q)b = 0 \qquad \text{and} \qquad pq + (1-p)b = 0.$$

Rewriting this as

$$q(a-b) = -b \qquad \text{and} \qquad p(a-b) = -b,$$

we see that if $a \neq b$, we must have $p = q$. We remark that we cannot have $a = b$ if $0 < p, q < 1$. Thus, the only solutions of (4.32) must be of the form (p,p). Now, according to (4.31), $\frac{\partial f}{\partial p}|_{(p,p)} = 0$ if and only if

$$m(p) \triangleq p[\ln p^2 - \ln(1-p^2)] + (1-p)[\ln(1-(1-p)^2) - \ln(1-p)^2] = 0.$$

Clearly, $m(\frac{1}{2}) = 0$. To show that $p = \frac{1}{2}$ is the only possible solution, it is sufficient to show that m is a strictly increasing function on $(0,1)$. This can be accomplished by showing that $m' > 0$ on $(0,1)$. In fact, we show that m' has a unique minimum at $p = \frac{1}{2}$, and that $m'(\frac{1}{2}) > 0$. To show that m' has a unique minimum at $p = \frac{1}{2}$,

we show that the only solution of $m''(p) = 0$ is $p = \frac{1}{2}$, and that $m'''(\frac{1}{2}) > 0$. Showing that $m''(p) = 0$ has the unique solution $p = \frac{1}{2}$ is the tedious part of the task. Having done all of the above, it follows that f has a *unique* maximum on $(0,1) \times (0,1)$. With only a little more work, it is easy to verify that $(\frac{1}{2}, \frac{1}{2})$ maximizes f on $[0,1] \times [0,1]$. □

CHAPTER 5
CONCLUSIONS

In 1981, Jahn [14] characterized the capacity region $C(W)$ of the arbitrarily varying multiple-access channel, *assuming that $C(W)$ had a nonempty interior.* Jahn did not address the question of how one could decide *a priori* whether or not $C(W)$ had a nonempty interior. In Chapter 3 we showed that if W is symmetrizable in the sense of Definitions 3.6, 3.7, or 3.8, then $C(W)$ has an empty interior. We then gave sufficient *non*symmetrizability conditions under which $C(W)$ contains various open rectangles, and thereby possesses a nonempty interior (cf. Theorems 3.15 and 3.17). However, we still have the following open problem. If W is nonsymmetrizable-$\mathcal{X}$, nonsymmetrizable-$\mathcal{Y}$, and nonsymmetrizable-$\mathcal{X}\mathcal{Y}$, does it follow that $C(W)$ has a nonempty interior? We conjecture that this is the case. One approach to proving this might be to show that if W is nonsymmetrizable-$\mathcal{X}$, -$\mathcal{Y}$, and -$\mathcal{X}\mathcal{Y}$, then there exists a $p \in \mathcal{D}(\mathcal{X})$ such that pW is nonsymmetrizable-$\mathcal{Y}$, or there exists a $q \in \mathcal{D}(\mathcal{Y})$ such that qW is nonsymmetrizable-$\mathcal{X}$.

In proving Theorem 3.19, we appealed to Jahn's forward result, inclusion (3.5), to show that if W is nonsymmetrizable-$\mathcal{Y}$ and qW is nonsymmetrizable-$\mathcal{X}$, then $\mathcal{R}^*(W) \subset C(W)$. To see why we took this approach, suppose that W is nonsymmetrizable-$\mathcal{X}$ and nonsymmetrizable-$\mathcal{Y}$, and suppose that for some $p \in \mathcal{D}(\mathcal{X})$ and $q \in \mathcal{D}(\mathcal{Y})$, pW is nonsymmetrizable-$\mathcal{Y}$ and qW is nonsymmetrizable-$\mathcal{X}$. Then Theorem 3.15 and Theorem 3.17 do not in general combine even to show that $C(W)$ contains the region

$$\{(R_1, R_2) : 0 \le R_1 \le I^*_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p, q, W), \quad 0 \le R_2 \le I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p, q, W), \quad 0 \le R_1 + R_2 \le I^*_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p, q, W)\}. \tag{5.1}$$

This can be seen by considering the inequalities

$$\begin{aligned} I^*_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p,q,W) &\triangleq \inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p\times q\times rW) \\ &= \inf_{r\in\mathcal{D}(\mathcal{S})}\Big[I_{\mathcal{X}\wedge\mathcal{Z}}(p\times q\times rW)+I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW)\Big] \\ &\geq \inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{X}\wedge\mathcal{Z}}(p\times q\times rW)+\inf_{r\in\mathcal{D}(\mathcal{S})} I_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p\times q\times rW) \\ &= I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W)+I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W) \end{aligned} \tag{5.2}$$

and

$$I^*_{\mathcal{X}\mathcal{Y}\wedge\mathcal{Z}}(p,q,W) \geq I^*_{\mathcal{Y}\wedge\mathcal{Z}}(p,q,W)+I^*_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W). \tag{5.3}$$

If either inequality is strict, then the closed convex hull of the union of the open rectangles

$$\{(R_1,R_2): 0<R_1<I^*_{\mathcal{X}\wedge\mathcal{Z}|\mathcal{Y}}(p,q,W),\ 0<R_2<I^*_{\mathcal{Y}\wedge\mathcal{Z}}(p,q,W)\}$$

and

$$\{(R_1,R_2): 0<R_1<I^*_{\mathcal{X}\wedge\mathcal{Z}}(p,q,W),\ 0<R_2<I^*_{\mathcal{Y}\wedge\mathcal{Z}|\mathcal{X}}(p,q,W)\}$$

will be a proper subset of the region in (5.1). It follows that in general, our approach cannot give a direct proof that $\mathcal{R}^*(W)\subset C(W)$. As a possible topic of future research, we suggest that a more complicated decoding rule might overcome this difficulty (cf. the Remark at the end of Section 3.3). Of course, in the special case that for every $p\in\mathcal{D}(\mathcal{X})$ and every $q\in\mathcal{D}(\mathcal{Y})$, one can show that each of the five different infima in (5.3) and (5.2) is achieved by the same $\hat{r}\in\mathcal{D}(\mathcal{S})$ ($\hat{r}$ depending on p and q), Theorems 3.15 and 3.17 can be combined with a time-sharing argument to give a proof that $\mathcal{R}^*(W)\subset C(W)$ without appealing to Jahn's result.

A very important part of our proof of Theorem 3.15 was the decoding rule defined in terms of the decoding sets F_i and G_{ij} (cf. (3.39) and (3.43)). As we pointed

out, this decoding rule is significantly more powerful than the so-called typicality decoding rule. However, as seen from the definition of the sets F_i and G_{ij}, our decoding rule is quite complicated. Consequently, we discussed the effectiveness of alternative decoding rules in Section 3.4. Our main result there, Theorem 3.21, gave conditions under which the universal maximum mutual information decoding rule could be used in the proof of Theorem 3.15. One direction of further research would be to analyze the effectiveness of other universal decoding rules such as the minimum (Hamming) distance decoding rule (for binary inputs and outputs), the independence decoding rule (for the additive AVC), and the maximum likelihood decoding rule.

In Chapter 4 we applied state constraints to the AVMAC. Our main results were an outer bound on $C(W, L)$ in the form of a weak converse (Theorem 4.7), and an inner bound on $C(W, L)$ given by Theorem 4.18. The key to proving Theorem 4.18 was the assumption that $\mathcal{U}_{\mathcal{X}}(q, W)$ did not depend on q. For the adder channel, this assumption is satisfied, and in fact we showed that our inner and outer bounds coincide to determine $C(W_a, \frac{1}{2})$. Note that for the adder channel, the analogs of (5.2) and (5.3) hold with equality (cf. (4.22) and (4.23)). The case in which $\mathcal{U}_{\mathcal{X}}(q, W)$ varies with q remains unsolved.

In studying the additive AVC and the group adder AVC, we computed $\mathcal{R}^L(W)$. Can one show that $\mathcal{R}^L(W) \subset C(W, L)$? Observe that since $\mathcal{R}^L(W)$ is a triangular region, it is equal to the convex hull of its two legs. Unfortunately, these legs have no interior points. This makes a straightforward application of Lemma 4.16 impossible. However, we do not know if it is possible to approximate the legs of $\mathcal{R}^L(W)$ with open rectangles of the form $\mathcal{R}^L_{\mathcal{X}}(p, q, W)$ and $\mathcal{R}^L_{\mathcal{Y}}(p, q, W)$.

BIBLIOGRAPHY

[1] R. Ahlswede, "Multi-way communication channels," in *Proc. 2nd Int. Symp. Inform. Theory* (Tsahkadsor, Armenian S.S.R.), pp. 23-52, 1971. (Publishing House of the Hungarian Academy of Sciences, 1973.)

[2] R. Ahlswede, "An elementary proof of the strong converse theorem for the multiple-access channel," *J. Comb., Inform. Syst. Sci.*, vol. 7, no. 3, pp. 216-230, 1982.

[3] P. Billingsley, *Probability and Measure.* New York: Wiley, 1979.

[4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems.* New York: Academic, 1981.

[5] I. Csiszár and J. Körner, "On the capacity of the arbitrarily varying channel for the maximum probability of error," *Z. Wahrscheinlichkeitstheorie verw. Geb.*, vol. 57, pp. 87-101, 1981.

[6] I. Csiszár, J. Körner, and K. Marton, "A new look at the error exponent of discrete memoryless channels," preprint, presented at the IEEE Int. Symp. Information Theory, Cornell University, Ithaca, NY, 1977.

[7] I. Csiszár and P. Narayan, "Arbitrarily varying channels with constrained inputs and states," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 27-34, Jan. 1988.

[8] I. Csiszár and P. Narayan, "The capacity of the arbitrarily varying channel revisited: Positivity, constraints," *IEEE Trans. Inform. Theory*, vol. IT-34, pp. 181-193, Mar. 1988.

[9] I. Csiszár and P. Narayan, "Capacity and decoding rules for classes of arbitrarily varying channels," submitted to *IEEE Trans. Inform. Theory.*

[10] G. Dueck, "The strong converse of the coding theorem for the multiple access-channel," *J. Comb., Inform. Syst. Sci.*, vol. 6, no. 3, pp. 187-196, 1981.

[11] A. El Gamal and T. M. Cover, "Multiple user information theory," *Proc. IEEE*, vol. 68, no. 12, pp. 1466-1483, Dec. 1980.

[12] K. Fan, "Minimax theorems," *Proc. N. A. S.*, vol. 39, pp. 42-47, 1953.

[13] R. G. Gallager, *Information Theory and Reliable Communication.* New York: Wiley, 1968.

[14] J.-H. Jahn, "Coding of arbitrarily varying multiuser channels," *IEEE Trans. Inform. Theory*, vol. IT-27, pp. 212-226, Mar. 1981.

[15] S. Karlin, *Mathematical Methods and Theory in Games, Programming, and Economics, Volume II The Theory of Infinite Games.* Reading, MA: Addison-Wesley, 1959.

[16] H. Liao, "A coding theorem for multiple access communications," presented at the Int. Symp. Information Theory, Asilomar, 1972. Also Ph.D. dissertation, "Multiple Access Channels," Dep. Eng., Univ. Hawaii, Honolulu, 1972.

[17] H. L. Royden, *Real Analysis, 2nd ed.* New York: MacMillan, 1968.

[18] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. IT-19, pp. 471-480, July 1973.

[19] E. C. van der Meulen, "Recent coding theorems and converses for multi-way channels. Part II: The multiple-access channel (1976-1985)," preprint.

[20] J. van Tiel, *Convex Analysis, An Introductory Text.* Chichester: Wiley, 1984.