

# Variations on Information Embedding in Multiple Access and Broadcast Channels

Shivaprasad Kotagiri *Student Member, IEEE*, and  
 J. Nicholas Laneman, *Senior Member, IEEE*

## Abstract

Information embedding (IE) is the transmission of information within a host signal subject to a distortion constraint. There are two types of embedding methods, namely irreversible IE and reversible IE, depending upon whether or not the host, as well as the message, is recovered at the decoder. In irreversible IE, only the embedded message is recovered at the decoder, and in reversible IE, both the message and the host are recovered at the decoder. This paper considers combinations of irreversible and reversible IE in multiple access channels (MAC) and physically degraded broadcast channels (BC).

This paper first considers MAC IE in which separate encoders embed their messages into their host signals subject to distortion constraints. The embedded signals from the two encoders are transmitted to a single decoder across a MAC. This paper study the capacity region in three cases: A) no host recovery at the decoder, B) lossless recovery of one host at the decoder, and C) lossless recovery of both hosts at the decoder. For the cases A and B, inner bounds on the respective capacity regions are developed. For the case C, inner and outer bounds on the capacity region are developed and the capacity region is obtained if the hosts are independent.

This paper also considers BC IE in which two messages intended for separate decoders are embedded into a given host sequence by a single encoder subject to a distortion constraint. This paper study the capacity region for degraded BC in four cases:  $A'$ ) lossless recovery of the host sequence at neither of the decoders,  $B'$ ) lossless recovery of the host sequence at only the better decoder,  $C'$ ) lossless

Manuscript received November 17, 2007.

This work has been supported in part by NSF Career Grant and the State of Indiana through the Twenty-First Century Research and Technology Fund.

Parts of this work were presented at Allerton 2005 and IEEE ISIT 2006.

Shivaprasad Kotagiri and J. Nicholas Laneman are with Department of Electrical Engineering, University of Notre Dame, Notre Dame, IN 46556, Email: {skotagir, jnl}@nd.edu

recovery of the host sequence at both decoders, and  $D'$ ) lossless recovery of the host sequence at only the worse decoder. For the cases  $A'$  and  $B'$ , inner and outer bounds on the respective capacity regions are developed. For the cases  $C'$  and  $D'$ , the respective capacity regions are obtained.

### Index Terms

Information Embedding, Reversible Information Embedding, Multiple Access Channels, Broadcast Channels

## I. INTRODUCTION

Information embedding (IE) is the reliable transmission of information within a host signal subject to a distortion constraint. IE is a recent area of digital media research with many applications including active and passive copyright protection (digital watermarking); steganography; embedding important control, descriptive reference information into a given signal; digital upgrades of communication infrastructure; and covert communications [1], [2], [3], [4]. The main idea of IE is that the host signal can carry different messages at the same time by allowing a small amount of distortion that can be tolerated at the intended receiver for the host signal. It has been observed that IE is closely related to state-dependent channel models with state known non-causally at the encoder [5], [6] [1], [2], [7].

### A. Forms of IE

In IE, a message  $W$  is embedded into a host signal  $S^n$  such that the embedded signal  $X^n$  is close to  $S^n$  under some prescribed distortion measure  $d(\cdot, \cdot)$ , i.e.,  $\mathbb{E}d(X^n, S^n) \leq \Delta$ . The decoder receives  $Y^n$ , which is drawn according a probability law  $p(y^n|x^n, s^n)$  for given  $X^n$  and  $S^n$ . Throughout the paper, we focus on the discrete memoryless case without feedback and denote the channel law by  $p(y|x, s)$ . Based upon whether or not the decoder recovers the host signal in the sense of probability of error going to zero, there are two important types of IE, namely *irreversible* and *reversible* IE.

In irreversible IE, the decoder is only concerned with reliable decoding of the message embedded in the host from the received sequence  $Y^n$  [1], [2], [7], [8]. The irreversible IE capacity of a single-user model is given by

$$C(\Delta) = \max_{p(u, x|s): \mathbb{E}d(X, S) \leq \Delta} [\mathbb{I}(U; Y) - \mathbb{I}(U; S)],$$

where  $\mathbf{U}$  is an auxiliary random variable with  $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{S}|$ . To achieve the capacity, Gel'fand-Pinsker coding [5] is used at the encoder such that the distortion between  $\mathbf{X}^n$  and  $\mathbf{S}^n$  satisfies the constraint  $\Delta$ .

In reversible IE, the decoder is concerned with lossless recovery of the host as well as reliable decoding of the embedded message in the host from the received sequence  $\mathbf{Y}^n$  [9], [10]. Reversible IE is useful for cases in which little or no degradation of the host signal is allowed, with applications in military and medical imagery, and multimedia archives of valuable original works. The reversible IE capacity is given by

$$C(\Delta) = \max_{p(\mathbf{x}|\mathbf{s}): \mathbb{E}d(\mathbf{X},\mathbf{S}) \leq \Delta} [\mathbb{H}(\mathbf{X}, \mathbf{S}; \mathbf{Y}) - \mathbb{H}(\mathbf{S})].$$

To achieve the above capacity expression, superposition coding is used at the encoder such that the distortion constraint is satisfied, i.e.,  $\mathbb{E}[d(\mathbf{X}, \mathbf{S})] \leq \Delta$ .

This paper focuses on IE in multi-user channels such as multiple access channels (MAC) and broadcast channels (BC). We focus on MAC IE with lossless recovery of *some* host sequences at the decoder and BC IE with lossless host recovery at *some* decoders, but the techniques can also be applied to other multi-user scenarios. In single-user IE, substantial results have been developed, but multi-user IE scenarios have not been as extensively studied. Information theoretic study of single-user public and private watermarking systems is studied in [11], [12], [13]. Joint IE and lossy compression is studied in [14], [15] and joint watermarking and encryption is studied in [16]. Multi-user models with state available at the encoders are studied in [17], [18], [19], [20], [21], [22], [23], [24], [25], [26], [27]. As in single-user case, there is a close relationship between multi-user models with non-causal state at the encoders and multi-user IE.

## B. Summary of Results

1) *MAC IE*: In Section II, we consider a two-user MAC IE model shown in Figure 1, but the results can be extended to any number of users. Encoder  $i$  embeds its information  $W_i$  into a host signal  $\mathbf{S}_i^n$ , generated by a host source  $i$ , such that the per-letter distortion between  $\mathbf{S}_i^n$  and  $\mathbf{X}_i^n$  is less than  $\Delta_i$ ,  $i = 1, 2$ .

For this model, we consider the following three cases in recovering, in the sense of probability of error going to zero, the messages and the host sequences at the decoder from the received sequence  $\mathbf{Y}^n$ :

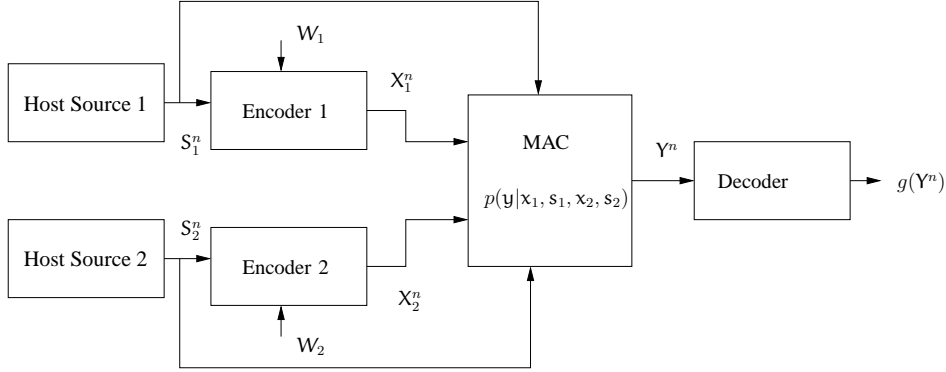


Fig. 1. Block diagram of multiple access channel information embedding model.

- **Case A, Recovery of Neither Host:** The decoder recovers  $(W_1, W_2)$  from  $Y^n$ .
- **Case B, Recovery of One Host:** The decoder recovers  $(W_1, W_2)$  along with the one host from  $Y^n$ . Without loss of generality, we can assume that the host sequence  $S_2^n$  of Encoder 2 is recovered at the decoder.
- **Case C, Recovery of Both Hosts :** The decoder recovers  $(W_1, W_2)$  and  $(S_1^n, S_2^n)$  from  $Y^n$ .

Our general MAC IE model considers scenarios in which the MAC output potentially depends on both the embedded signals and the host signals. For Cases A and B, we develop inner bounds on the respective capacity regions in Sections II-A and II-B, respectively. For Case C, we derive inner and outer bounds on the capacity region if the hosts are correlated in Section II-C, and we show that there is no gap between the inner and the outer bounds if the hosts are independent.

2) *BC IE*: In Section III, we consider IE in a broadcast scenario as shown in Figure 2, which illustrates only two decoders; in principle the model and results can be extended to any number of decoders. In this model, the encoder embeds two independent messages  $(W_1, W_2)$  into a single host sequence  $S^n$  such that the distortion between the embedded signal  $X^n$  and  $S^n$  satisfies a given distortion constraint  $\Delta$ . In this paper, we focus on the case of a degraded broadcast channel, i.e.,  $p(y, z|x, s) = p(y|x, s)p(z|y)$ . Decoder 1, or the *better decoder*, receives the channel output  $Y^n$  which is drawn according to a memoryless probability law  $p(y|x, s)$  for given  $X^n$  and  $S^n$ . Decoder 2, or the *worse decoder*, receives the sequence  $Z^n$  which is corrupted version of  $Y^n$ .

For this model, we consider the following four cases in recovering, in the sense of probability

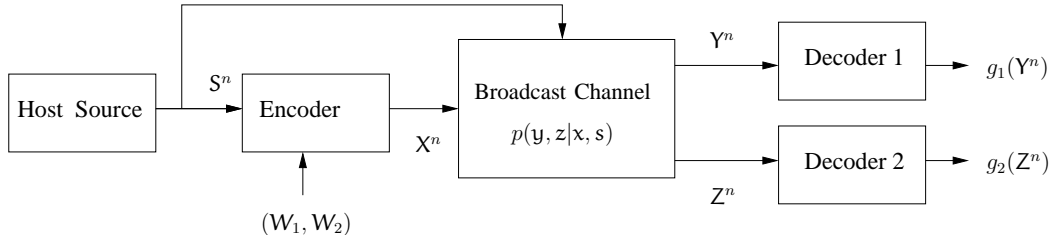


Fig. 2. Block diagram of the broadcast information embedding model.

of error going to zero, the messages and the host sequences at the decoders:

- **Case  $A'$ , No Host Recovery:** Decoder 1 recovers  $(W_1, W_2)$  from  $Y^n$ ; Decoder 2 recovers  $W_2$  from  $Z^n$ .
- **Case  $B'$ , Host Recovery at the Better Decoder:** Decoder 1 recovers  $(W_1, W_2)$  and  $S^n$  from  $Y^n$ ; Decoder 2 recovers  $W_2$  from  $Z^n$ .
- **Case  $C'$ , Host Recovery at Both Decoders:** Decoder 1 recovers  $(W_1, W_2)$  and  $S^n$  from  $Y^n$ ; Decoder 2 recovers  $W_2$  and  $S^n$  from  $Z^n$ .
- **Case  $D'$ , Host Recovery at the Worse Decoder:** Decoder 1 recovers  $(W_1, W_2)$  from  $Y^n$ ; Decoder 2 recovers  $W_2$  and  $S^n$  from  $Z^n$ .

Inner and outer bounds for the BC IE capacity region in Case  $A'$  *without* an encoder distortion constraint are derived in [21]; in this paper, we extend the results to incorporate an encoder distortion constraint in Section III-A. For Case  $B'$ , we develop inner and outer bounds for the BC IE capacity region in Section III-B, and for cases  $C'$  and  $D'$  we derive the BC IE capacity region in Section III-C and Section III-D, respectively. It turns out that the capacity regions in Cases  $C'$  and  $D'$  are identical because the channel output  $Z^n$  is a degraded version of  $Y^n$ . The capacity region for the model considered in Case  $C'$  if compressed hosts are available at the decoders is obtained in [28].

### C. Notation

Throughout the paper, random variables and sample values are denoted in a special font, e.g., random variable  $X$  and sample value  $x$ . Alphabets are denoted in calligraphic font, e.g.,  $\mathcal{X}$ , and are all discrete. The shorthand  $X_1^n$  represents the sequence  $X_{1,1}, X_{1,2}, \dots, X_{1,n}$ , and  $X_{1,i}^n$  represents the

sequence  $X_{1,i}, X_{1,i+1}, \dots, X_{1,n}$ . Finally,  $\mathbb{H}(\cdot)$  and  $\mathbb{I}(\cdot; \cdot)$  denote the standard information-theoretic quantities of (ensemble average) entropy and mutual information, respectively.

## II. MAC IE

In this section, let us formally discuss the model shown in Figure 1. Host source  $i$  generates a sequence  $S_i^n = S_{i1}S_{i2} \dots S_{in}$  of symbols from the discrete alphabet  $\mathcal{S}_i$ ,  $i = 1, 2$ . We assume that the host sequence pair  $(S_1^n, S_2^n)$  is generated by repeated independent drawings of a pair of discrete random variables  $(S_1, S_2)$  from a given joint distribution  $p(s_1, s_2)$ . The host sequence  $S_i^n$  is non-causally known at Encoder  $i$  for  $i = 1, 2$ . The message source at Encoder  $i$  produces the message index  $W_i \in \mathcal{W}_i = \{1, 2, \dots, M_i\}$  with equal probability  $1/M_i$ , for  $i = 1, 2$ . The message index at any encoder is independent of all host sequences and also independent of the messages at all other encoders. The rate at Encoder  $i$ , in bits per channel use, is defined as  $R_i = (1/n) \log_2(M_i)$ .

*Definition 1:* A  $(M_1, M_2, D_1^{(n)}, D_2^{(n)}, n)$  MAC IE code consists of sequences of encoding functions at Encoder 1 and Encoder 2,

$$f_1^n : \mathcal{W}_1 \times \mathcal{S}_1^n \rightarrow \mathcal{X}_1^n, \quad \text{and} \quad f_2^n : \mathcal{W}_2 \times \mathcal{S}_2^n \rightarrow \mathcal{X}_2^n,$$

respectively, and a sequence of decoding functions,

- **Recovery of Neither Host**  $g_A^n : \mathcal{Y}^n \rightarrow (\mathcal{W}_1, \mathcal{W}_2)$
- **Recovery of One Host**  $g_B^n : \mathcal{Y}^n \rightarrow (\mathcal{W}_1, \mathcal{W}_2, \mathcal{S}_2^n)$
- **Recovery of Both Hosts**  $g_C^n : \mathcal{Y}^n \rightarrow (\mathcal{W}_1, \mathcal{S}_1^n, \mathcal{W}_2, \mathcal{S}_2^n)$

The distortions associated with MAC IE code are defined as  $D_i^{(n)} = \mathbb{E}d_i(S_i^n, X_i^n)$  for the additive distortion function

$$d_i(S_i^n, X_i^n) = \frac{1}{n} \sum_{j=1}^n d_i(S_{ij}, X_{ij})$$

for some non-negative bounded distortion functions  $d_i(S_{ij}, X_{ij})$ , where  $i = 1, 2$ .

The embedded signals  $X_1^n$  and  $X_2^n$  from Encoder 1 and Encoder 2, respectively are transmitted across a MAC  $p(\mathbf{y}|\mathbf{x}_1, \mathbf{s}_1, \mathbf{x}_2, \mathbf{s}_2)$  without feedback modeled as a memoryless conditional probability distribution

$$\Pr(\mathbf{y}^n | \mathbf{x}_1^n, \mathbf{s}_1^n, \mathbf{x}_2^n, \mathbf{s}_2^n) = \prod_{j=1}^n p(\mathbf{y}_j | \mathbf{x}_{1j}, \mathbf{s}_{1j}, \mathbf{x}_{2j}, \mathbf{s}_{2j}). \quad (1)$$

*Definition 2:* A rate pair  $(R_1, R_2)$  for a given distortion pair  $(\Delta_1, \Delta_2)$  is said to be *MAC IE achievable* if there exists a sequence of  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D_1^{(n)}, D_2^{(n)}, n)$  MAC IE codes with  $\lim_{n \rightarrow \infty} D_i^{(n)} \leq \Delta_i$ , for  $i = 1, 2$ , and  $\lim_{n \rightarrow \infty} P_e^n = 0$ , where  $P_e^n$  is the probability of error defined appropriately for each case in the sequel of this section.

*Definition 3:* For given  $p(s_1, s_2)$  and  $p(y|x_1, s_1, x_2, s_2)$ , let  $\mathcal{P}_{\text{MAC}}^i(\Delta_1, \Delta_2)$  be the set of all random variable tuples  $(Q, S_1, S_2, (\mathbf{U}_1, \mathbf{X}_1), (\mathbf{U}_2, \mathbf{X}_2), Y)$  taking values in finite alphabets  $\mathcal{Q}, \mathcal{S}, \mathcal{U}_1 \times \mathcal{X}_1, \mathcal{U}_2 \times \mathcal{X}_2$ , and  $\mathcal{Y}$ , respectively, with joint distribution satisfying conditions

- a)  $\sum_{\mathbf{q}, (\mathbf{u}_1, \mathbf{x}_1), (\mathbf{u}_2, \mathbf{x}_2), \mathbf{y}} p(\mathbf{q}, s_1, s_2, (\mathbf{u}_1, \mathbf{x}_1), (\mathbf{u}_2, \mathbf{x}_2), \mathbf{y}) = p(s_1, s_2)$ ,
- b)  $p(\mathbf{q}, s_1, s_2, (\mathbf{u}_1, \mathbf{x}_1), (\mathbf{u}_2, \mathbf{x}_2), \mathbf{y}) = p(\mathbf{q})p(s_1, s_2)p(\mathbf{u}_1, \mathbf{x}_1|s_1, \mathbf{q})p(\mathbf{u}_2, \mathbf{x}_2|s_2, \mathbf{q})p(\mathbf{y}|x_1, s_1, x_2, s_2)$
- c)  $\mathbb{E}d_i(S_i, X_i) \leq \Delta_i$ , for  $i = 1, 2$ .

*Definition 4:* For given  $p(s_1, s_2)$  and  $p(y|x_1, s_1, x_2, s_2)$ , let  $\mathcal{P}_{\text{MAC}}^o(\Delta_1, \Delta_2)$  be the set of all random variable tuples  $(Q, S_1, S_2, X_1, X_2, Y)$  taking values in finite alphabets  $\mathcal{Q}, \mathcal{S}, \mathcal{X}_1, \mathcal{X}_2$ , and  $\mathcal{Y}$ , respectively, with joint distribution satisfying the conditions

- a).  $\sum_{\mathbf{q}, x_1, x_2, \mathbf{y}} p(\mathbf{q}, s_1, s_2, x_1, x_2, \mathbf{y}) = p(s_1, s_2)$ ,
- b).  $p(\mathbf{q}, s_1, s_2, x_1, x_2, \mathbf{y}) = p(\mathbf{q})p(s_1, s_2)p(x_1, x_2|s_1, s_2, \mathbf{q})p(\mathbf{y}|x_1, s_1, x_2, s_2)$ ,
- c).  $\mathbb{E}d_i(S_i, X_i) \leq \Delta_i$ , for  $i = 1, 2$ .

### A. Recovery of Neither Host

In this section, we derive an inner bound on the MAC IE capacity region for Case A, in which the decoder recovers only  $(W_1, W_2)$  from  $Y^n$ . We define the MAC IE capacity region  $\mathcal{C}_{\text{MAC},A}(\Delta_1, \Delta_2)$  as the closure of the set of all MAC IE achievable rates  $(R_1, R_2)$  with  $P_e^{(n)} := \mathbb{P}[(g_A^n(Y^n) \neq (W_1, W_2))] \rightarrow 0$  as  $n \rightarrow \infty$ . The following theorem provides an inner bound on the capacity region.

*Proposition 1:* Let  $\mathcal{R}_{\text{MAC},A}^i(\Delta_1, \Delta_2)$  be the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 \leq \mathbb{I}(\mathbf{U}_1; \mathbf{U}_2, Y|Q) - \mathbb{I}(\mathbf{U}_1; S_1|Q), \quad (2a)$$

$$R_2 \leq \mathbb{I}(\mathbf{U}_2; \mathbf{U}_1, Y|Q) - \mathbb{I}(\mathbf{U}_2; S_2|Q), \quad (2b)$$

$$R_1 + R_2 \leq \mathbb{I}(\mathbf{U}_1, \mathbf{U}_2; Y|Q) - \mathbb{I}(\mathbf{U}_1, \mathbf{U}_2; S_1, S_2|Q) \quad (2c)$$

for some  $(Q, S_1, S_2, (\mathbf{U}_1, \mathbf{X}_1), (\mathbf{U}_2, \mathbf{X}_2), Y) \in \mathcal{P}_{\text{MAC}}^i(\Delta_1, \Delta_2)$ , where  $\mathbf{U}_1$  and  $\mathbf{U}_2$  are auxiliary random variables. Then,  $\mathcal{R}_{\text{MAC},A}^i(\Delta) \subseteq \mathcal{C}_{\text{MAC},A}$ .

### Remarks

- The inner bound in Proposition 1 is similar to that in [29], which considers a Gaussian MAC with no host recovery, but the result here is for the discrete memoryless case. Because the coding procedures, and error events in [29] apply, we do not provide a proof here.
- To achieve the inner bound, distortion-constrained Gel'fand-Pinsker codes can be used to embed  $W_1$  and  $W_2$  into the host sequences  $S_1^n$  and  $S_2^n$  such that the distortion constraints  $\Delta_1$  and  $\Delta_2$  are met, respectively.

### B. Recovery of One Host

In this section, we derive inner and outer bounds on the MAC IE capacity region for Case B, in which the decoder recovers  $(W_1, W_2, S_2^n)$  from  $Y^n$ . We define the MAC IE capacity region  $\mathcal{C}_{\text{MAC},\text{B}}(\Delta_1, \Delta_2)$  as the closure of the set of all MAC IE achievable rates  $(R_1, R_2)$  with  $P_e^{(n)} := \mathbb{P}[(g_B^n(Y^n) \neq (W_1, W_2, S_2^n))] \rightarrow 0$  as  $n \rightarrow \infty$ . The following theorem provides an inner bound for the capacity region.

*Proposition 2:* Let  $\mathcal{R}_{\text{MAC},\text{B}}^i(\Delta_1, \Delta_2)$  be the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 \leq \mathbb{I}(\mathbf{U}_1; Y | \mathbf{X}_2, \mathbf{S}_2, Q) - \mathbb{I}(\mathbf{U}_1; \mathbf{S}_1 | \mathbf{X}_2, \mathbf{S}_2, Q), \quad (3a)$$

$$R_2 \leq \mathbb{I}(\mathbf{X}_2, \mathbf{S}_2; Y | \mathbf{U}_1, Q) - \mathbb{H}(\mathbf{S}_2 | \mathbf{U}_1, Q), \quad (3b)$$

$$R_1 + R_2 \leq \mathbb{I}(\mathbf{U}_1, \mathbf{X}_2, \mathbf{S}_2; Y | Q) - \mathbb{H}(\mathbf{S}_2) - \mathbb{I}(\mathbf{U}_1; \mathbf{S}_1 | \mathbf{X}_2, \mathbf{S}_2, Q) \quad (3c)$$

for some  $(Q, \mathbf{S}_1, \mathbf{S}_2, (\mathbf{U}_1, \mathbf{X}_1), (\mathbf{X}_2, \mathbf{X}_2), Y) \in \mathcal{P}_{\text{MAC}}^i(\Delta_1, \Delta_2)$ , where  $\mathbf{U}_1$  and  $Q$  are auxiliary random variables. Then,  $\mathcal{R}_{\text{MAC},\text{B}}^i(\Delta_1, \Delta_2) \subseteq \mathcal{C}_{\text{MAC},\text{B}}(\Delta_1, \Delta_2)$

### Remarks

- The inner bound in Proposition 2 is a special case of an inner bound in [24], which considers the state-dependent MAC with state known at one encoder and recovery of only messages at the decoder. To obtain the inner bound in Proposition 2, substitute  $(\mathbf{X}_2, \mathbf{S}_2)$  in place of  $\mathbf{X}_2$  into the inner bound in [24].
- To achieve the inner bound, distortion constrained Gel'fand-Pinsker coding is used to embed  $W_1$  into the host sequence  $S_1^n$ , and distortion-constrained superposition coding is used to embed  $W_2$  into the host sequence  $S_2^n$ .

- If we choose  $\mathcal{U}_2 = (X_2, S_2)$  in Proposition 1, we obtain the inner bound in Proposition 2. Thus,  $\mathcal{R}_{\text{MAC},\text{B}}^i(\Delta_1, \Delta_2) \subseteq \mathcal{R}_{\text{MAC},\text{A}}^i(\Delta_1, \Delta_2)$ .

### C. Recovery of Both Hosts

In this section, we derive inner and outer bounds on the MAC IE capacity region for Case C in which the decoder recovers  $(W_1, S_1^n, W_2, S_2^n)$  from  $Y^n$ . We define the MAC IE capacity region  $\mathcal{C}_{\text{MAC},\text{C}}(\Delta_1, \Delta_2)$  as the closure of all MAC IE achievable rates  $(R_1, R_2)$  with  $P_e^{(n)} := \mathbb{P}[(g(Y^n) \neq (W_1, S_1^n, W_2, S_2^n))] \rightarrow 0$  as  $n \rightarrow \infty$ . The following theorem obtains an inner bound for the capacity region.

*Theorem 1:* Let  $\mathcal{R}_{\text{MAC},\text{C}}^i(\Delta_1, \Delta_2)$  be the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 < [\mathbb{I}(X_1, S_1; Y|X_2, S_2, Q) - \mathbb{H}(S_1|S_2)], \quad (4a)$$

$$R_2 < [\mathbb{I}(X_2, S_2; Y|X_1, S_1, Q) - \mathbb{H}(S_2|S_1)], \quad (4b)$$

$$R_1 + R_2 < [\mathbb{I}(X_1, S_1, X_2, S_2; Y|Q) - \mathbb{H}(S_1, S_2)], \quad (4c)$$

for some  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y) \in \mathcal{P}_{\text{MAC}}^i(\Delta_1, \Delta_2)$ . Then,

$$\mathcal{R}_{\text{MAC},\text{C}}^i(\Delta_1, \Delta_2) \subseteq \mathcal{C}_{\text{MAC},\text{C}}(\Delta_1, \Delta_2).$$

**Proof:** See Appendix A

The following theorem gives an outer bound for the capacity region if  $S_1$  and  $S_2$  are correlated.

*Theorem 2:* Let  $\mathcal{R}_{\text{MAC},\text{C}}^o(\Delta_1, \Delta_2)$  be the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 < [\mathbb{I}(X_1, S_1; Y|X_2, S_2, Q) - \mathbb{H}(S_1|S_2)], \quad (5a)$$

$$R_2 < [\mathbb{I}(X_2, S_2; Y|X_1, S_1, Q) - \mathbb{H}(S_2|S_1)], \quad (5b)$$

$$R_1 + R_2 < [\mathbb{I}(X_1, S_1, X_2, S_2; Y|Q) - \mathbb{H}(S_1, S_2)], \quad (5c)$$

for some  $(Q, S_1, S_2, X_1, X_2, Y) \in \mathcal{P}_{\text{MAC}}^o(\Delta_1, \Delta_2)$ . If the host random variables  $S_1$  and  $S_2$  are correlated, then

$$\mathcal{C}_{\text{MAC},\text{C}}(\Delta_1, \Delta_2) \subseteq \mathcal{R}_{\text{MAC},\text{C}}^o(\Delta_1, \Delta_2).$$

If the host random variables  $S_1$  and  $S_2$  are independent, then

$$\mathcal{C}_{\text{MAC},\text{C}}(\Delta_1, \Delta_2) \subseteq \mathcal{R}_{\text{MAC},\text{C}}^i(\Delta_1, \Delta_2).$$

**Proof:** See Appendix B

The following corollary of Theorem 1 and Theorem 2 states the MAC IE capacity region for a given pair of distortion constraints  $(\Delta_1, \Delta_2)$  if the host random variables  $S_1$  and  $S_2$  are independent.

*Corollary 1:* If the host random variables  $S_1$  and  $S_2$  are independent, then the capacity region  $\mathcal{C}_{\text{MAC,C}}(\Delta_1, \Delta_2)$  is the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 < [\mathbb{I}(\mathbf{X}_1, \mathbf{S}_1; \mathbf{Y} | \mathbf{X}_2, \mathbf{S}_2, \mathbf{Q}) - \mathbb{H}(\mathbf{S}_1 | \mathbf{S}_2)], \quad (6a)$$

$$R_2 < [\mathbb{I}(\mathbf{X}_2, \mathbf{S}_2; \mathbf{Y} | \mathbf{X}_1, \mathbf{S}_1, \mathbf{Q}) - \mathbb{H}(\mathbf{S}_2 | \mathbf{S}_1)], \quad (6b)$$

$$R_1 + R_2 < [\mathbb{I}(\mathbf{X}_1, \mathbf{S}_1, \mathbf{X}_2, \mathbf{S}_2; \mathbf{Y} | \mathbf{Q}) - \mathbb{H}(\mathbf{S}_1, \mathbf{S}_2)], \quad (6c)$$

for some  $(\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, (\mathbf{X}_1, \mathbf{X}_1), (\mathbf{X}_2, \mathbf{X}_2), \mathbf{Y}) \in \mathcal{P}_{\text{MAC}}^i(\Delta_1, \Delta_2)$ .

*Remarks*

- To compute either (4) or (5), it is sufficient to consider time-sharing random variable  $\mathbf{Q}$  with  $|\mathcal{Q}| \leq 4$  by Caratheodory's theorem [30].
- In most communication scenarios, message transmission rates of zero are achievable. However, in this model, message transmission rates of zero can be unachievable if the host source pair  $p(s_1, s_2)$  is such that the upper bounds on  $R_1$ ,  $R_2$  and  $R_1 + R_2$  in (6) are negative. This is because we require host recovery at the decoder as well.

### III. DEGRADED BC IE

In this section, let us formally define the BC IE model shown in Figure 2. A host sequence  $S^n = (S_1, S_2, \dots, S_n)$  is an independent and identically distributed (i.i.d.) discrete random sequence whose elements are drawn with probability mass function  $p(s)$ ,  $s \in \mathcal{S}$ . All alphabets are discrete. We assume that the host sequence  $S^n$  is non-causally known at the encoder. The encoder embeds a message pair  $(W_1, W_2)$  into the host sequence  $S^n$  such that the average distortion between  $S^n$  and the embedded sequence  $X^n$  satisfies a given distortion constraint  $\Delta$ . The messages  $W_1 \in \{1, 2, \dots, M_1\}$  and  $W_2 \in \{1, 2, \dots, M_2\}$  are drawn equally likely with probabilities  $1/M_1$  and  $1/M_2$ , respectively. Then the rate of message  $W_i$  is given by  $R_i = (1/n) \log_2 M_i$  bits per channel use, for  $i = 1, 2$ . It is also assumed that the message  $W_i$  is independent of the other message and the host sequence for  $i = 1, 2$ .

*Definition 5:* A  $(M_1, M_2, D^{(n)}, n)$  BC IE code consists of a sequence of encoding functions at the encoder

$$f^n : \mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}^n \rightarrow \mathcal{X}^n,$$

and a sequence of decoding functions at Decoder 1 and Decoder 2

- **No Host Recovery**  $g_{1,A'}^n : \mathcal{Y}^n \rightarrow (\mathcal{W}_1, \mathcal{W}_2)$  and  $g_{2,A'}^n : \mathcal{Z}^n \rightarrow \mathcal{W}_2$
- **Host Recovery at the Better Decoder**  $g_{1,B'}^n : \mathcal{Y}^n \rightarrow (\mathcal{W}_1, \mathcal{W}_2, \mathcal{S}^n)$  and  $g_{2,B'}^n : \mathcal{Z}^n \rightarrow \mathcal{W}_2$
- **Host Recovery at Both Decoders**  $g_{1,C'}^n : \mathcal{Y}^n \rightarrow (\mathcal{W}_1, \mathcal{W}_2, \mathcal{S}^n)$  and  $g_{2,C'}^n : \mathcal{Z}^n \rightarrow (\mathcal{W}_2, \mathcal{S}^n)$
- **Host Recovery at the Worse Decoder**  $g_{1,D'}^n : \mathcal{Y}^n \rightarrow (\mathcal{W}_1, \mathcal{W}_2)$  and  $g_{2,D'}^n : \mathcal{Z}^n \rightarrow (\mathcal{W}_2, \mathcal{S}^n)$ ,

respectively. The associated distortion is defined as  $D^{(n)} = \mathbb{E}d(\mathcal{S}^n, \mathcal{X}^n)$ , where  $d(\mathcal{S}^n, \mathcal{X}^n) = (1/n) \sum_{j=1}^n d(S_j, X_j)$  for given non-negative bounded distortion measure  $d(\cdot, \cdot)$ .

The embedded signal  $\mathcal{X}^n$  is transmitted across a discrete memoryless degraded broadcast channel (DMDBC) with state,  $p(y|x, s)p(z|y)$ , modeled as a memoryless conditional probability distribution

$$\Pr(\mathcal{Y}^n = \mathbf{y}^n, \mathcal{Z}^n = \mathbf{z}^n | \mathcal{X}^n = \mathbf{x}^n, \mathcal{S}^n = \mathbf{s}^n) = \prod_{j=1}^n p(y_j | x_j, s_j) p(z_j | y_j). \quad (7)$$

*Definition 6:* A rate pair  $(R_1, R_2)$  for a given distortion  $\Delta$  is said to be BC IE achievable if there exists a sequence of  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D^{(n)}, n)$  BC IE codes with  $\lim_{n \rightarrow \infty} D^{(n)} \leq \Delta$  and  $\lim_{n \rightarrow \infty} P_e^n = 0$ , where  $P_e^n$  is the probability of error defined appropriately for each case in the sequel of the paper.

*Definition 7:* For a given  $p(s)$  and  $p(y|x, s)p(z|y)$ , let  $\mathcal{P}(\Delta)$  be the collection of random variables  $(\mathcal{T}, \mathcal{S}, \mathcal{X}, \mathcal{Y}, \mathcal{Z})$  with joint probability mass function satisfying the following conditions

- a)  $p(\mathbf{t}, \mathbf{s}, \mathbf{x}, \mathbf{y}, \mathbf{z}) = p(\mathbf{t}, \mathbf{s}, \mathbf{x})p(\mathbf{y}|\mathbf{x}, \mathbf{s})p(\mathbf{z}|\mathbf{y})$
- b)  $\sum_{\mathbf{t} \in \mathcal{T}, \mathbf{x} \in \mathcal{X}} p(\mathbf{t}, \mathbf{x}, \mathbf{s}) = p(\mathbf{s})$
- c)  $\mathbb{E}d(\mathcal{S}, \mathcal{X}) \leq \Delta$ ,

where  $\mathcal{T}$  is an auxiliary random variable.

#### A. No Host Recovery

In this section, we state inner and outer bounds for the BC IE capacity region in Case  $A'$ , in which Decoder 1 recovers  $(\mathcal{W}_1, \mathcal{W}_2)$  from  $\mathcal{Y}^n$  and Decoder 2 recovers  $\mathcal{W}_2$  from  $\mathcal{Z}^n$ . The BC IE capacity region  $\mathcal{C}_{A'}(\Delta)$  is the closure of all BC IE achievable rates  $(R_1, R_2)$  with  $P_e^{(n)} := \Pr[(g_{1,A'}^n(\mathcal{Y}^n) \neq (\mathcal{W}_1, \mathcal{W}_2) \text{ or } g_{2,A'}^n(\mathcal{Z}^n) \neq \mathcal{W}_2] \rightarrow 0$  as  $n \rightarrow \infty$ .

*Proposition 3:* Let  $\mathcal{R}_{A'}^i(\Delta)$  be the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 \leq \mathbb{I}(\mathbf{V}; \mathbf{Y}|\mathbf{U}) - \mathbb{I}(\mathbf{V}; \mathbf{S}|\mathbf{U}), \quad (8a)$$

$$R_2 \leq \mathbb{I}(\mathbf{U}; \mathbf{Z}) - \mathbb{I}(\mathbf{U}; \mathbf{S}), \quad (8b)$$

for some  $((\mathbf{U}, \mathbf{V}), \mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{P}(\Delta)$ , where  $\mathbf{U}$  and  $\mathbf{V}$  are auxiliary random variables with alphabet sizes satisfying  $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{S}| + 1$  and  $|\mathcal{V}| \leq |\mathcal{X}||\mathcal{S}|(|\mathcal{X}||\mathcal{S}| + 1)$ , respectively. Let  $\mathcal{R}_{A'}^o(\Delta)$  be the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 \leq \mathbb{I}(\mathbf{V}; \mathbf{Y}|\mathbf{U}, \mathbf{W}) - \mathbb{I}(\mathbf{V}; \mathbf{S}|\mathbf{U}, \mathbf{W}), \quad (9a)$$

$$R_2 \leq \mathbb{I}(\mathbf{U}; \mathbf{Z}) - \mathbb{I}(\mathbf{U}; \mathbf{S}), \quad (9b)$$

$$R_1 + R_2 \leq \mathbb{I}(\mathbf{U}, \mathbf{V}, \mathbf{W}; \mathbf{Y}) - \mathbb{I}(\mathbf{U}, \mathbf{V}, \mathbf{W}; \mathbf{S}), \quad (9c)$$

for some  $((\mathbf{U}, \mathbf{V}, \mathbf{W}), \mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{P}(\Delta)$ , where  $\mathbf{U}$ ,  $\mathbf{W}$ , and  $\mathbf{V}$  are auxiliary random variables with alphabet sizes satisfying  $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{S}| + 2$ ,  $|\mathcal{V}| \leq |\mathcal{X}||\mathcal{S}|(|\mathcal{X}||\mathcal{S}| + 2) + 1$ , and  $|\mathcal{W}| \leq (|\mathcal{X}||\mathcal{S}|(|\mathcal{X}||\mathcal{S}| + 2) + 1)(|\mathcal{X}||\mathcal{S}| + 2)|\mathcal{X}||\mathcal{S}| + 1$ , respectively. Then,  $\mathcal{R}_{A'}^i(\Delta) \subseteq \mathcal{C}_{A'}(\Delta) \subseteq \mathcal{R}_{A'}^o(\Delta)$ .

#### *Remarks*

The inner and outer bounds in Proposition 3 are slightly different from those in [21], which does not consider an encoder distortion constraint. Although essentially the same proofs in [21] apply, here there is an additional constraint on the joint probability mass functions  $\mathcal{P}(\Delta)$  to limit the average distortion between the host  $\mathbf{S}$  and the channel input  $\mathbf{X}$  to be at most  $\Delta$ . To achieve the inner bound, Gel'fand-Pinsker codes can be used to embed the messages  $(W_1, W_2)$  into the host sequence  $S^n$ .

#### *B. Host Recovery at the Better Decoder*

In this section, we derive inner and outer bounds on the BC IE capacity region in Case  $B'$ , in which Decoder 1 recovers  $(W_1, W_2)$  and  $S^n$  from  $Y^n$  and Decoder 2 recovers only  $W_2$  from  $Z^n$ . We define the BC IE capacity region  $\mathcal{C}_{B'}(\Delta)$  as the closure of all BC IE achievable rates  $(R_1, R_2)$  with  $P_e^{(n)} := \Pr[(g_{1,B'}^n(Y^n) \neq (W_1, W_2, \hat{S}^n) \text{ or } g_{2,B'}^n(Z^n) \neq W_2] \rightarrow 0$  as  $n \rightarrow \infty$ . The following two theorems give inner and outer bounds for the capacity region in this case.

*Theorem 3:* Let  $\mathcal{R}_{B'}^i(\Delta)$  be the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 \leq \mathbb{I}(\mathbf{X}, \mathbf{S}; \mathbf{Y}|\mathbf{U}) - \mathbb{H}(\mathbf{S}|\mathbf{U}), \quad (10a)$$

$$R_2 \leq \mathbb{I}(\mathbf{U}; \mathbf{Z}) - \mathbb{I}(\mathbf{U}; \mathbf{S}), \quad (10b)$$

for some  $(\mathbf{U}, \mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{P}(\Delta)$ , where  $\mathbf{U}$  is an auxiliary random variable with alphabet size satisfying  $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{S}| + 1$ . Then  $\mathcal{R}_{B'}^i(\Delta) \subseteq \mathcal{C}_{B'}(\Delta)$ .

**Proof:** See C .

*Theorem 4:* Let  $\mathcal{R}_{B'}^o(\Delta)$  be the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 \leq \mathbb{I}(\mathbf{X}, \mathbf{S}; \mathbf{Y}|\mathbf{U}) - \mathbb{H}(\mathbf{S}|\mathbf{U}), \quad (11a)$$

$$R_2 \leq \mathbb{I}(\mathbf{U}, \mathbf{V}; \mathbf{Z}) - \mathbb{I}(\mathbf{U}, \mathbf{V}; \mathbf{S}), \quad (11b)$$

for some  $((\mathbf{U}, \mathbf{V}), \mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{P}(\Delta)$ , where  $\mathbf{U}$  and  $\mathbf{V}$  are auxiliary random variables with alphabet sizes satisfying  $|\mathcal{U}| \leq |\mathcal{X}||\mathcal{S}| + 1$  and  $|\mathcal{V}| \leq |\mathcal{X}||\mathcal{S}|(|\mathcal{X}||\mathcal{S}| + 1)$ , respectively. Then  $\mathcal{C}_{B'}(\Delta) \subseteq \mathcal{R}_{B'}^o(\Delta)$ .

**Proof:** See Appendix D.

*Remarks*

To obtain the above inner bound, the message  $W_2$  is embedded into the host sequence  $S^n$  using Gel'fand-Pinsker coding, and the message  $W_1$  is embedded into the host sequence using superposition coding such that the distortion constraint is satisfied. The above inner and outer bounds are already convex regions. So, there is no need to introduce time-sharing auxiliary random variables. Let us write the constraint on  $R_2$  in the outer bound given in (11) as follows

$$\mathbb{I}(\mathbf{U}, \mathbf{V}; \mathbf{Z}) - \mathbb{I}(\mathbf{U}, \mathbf{V}; \mathbf{S}) = \mathbb{I}(\mathbf{U}; \mathbf{Z}) - \mathbb{I}(\mathbf{U}; \mathbf{S}) + \{\mathbb{I}(\mathbf{V}; \mathbf{Z}|\mathbf{U}) - \mathbb{I}(\mathbf{V}; \mathbf{S}|\mathbf{U})\}.$$

This term  $\mathbb{I}(\mathbf{V}; \mathbf{Z}|\mathbf{U}) - \mathbb{I}(\mathbf{V}; \mathbf{S}|\mathbf{U})$  is the difference between the inner and outer bounds. If  $\mathbf{V}$  is a deterministic function of  $\mathbf{U}$ , both inner and outer bounds coincide. This clearly shows that  $\mathcal{R}_{B'}^i(\Delta) \subseteq \mathcal{R}_{B'}^o(\Delta)$ .

### C. Host Recovery at Both Decoders

This section derives the BC IE capacity region in Case  $C'$ , in which Decoder 1 recovers  $(W_1, W_2)$  and  $S^n$  from  $Y^n$  and Decoder 2 recovers  $W_2$  and  $S^n$  from  $Z^n$ . We define the BC IE capacity region  $\mathcal{C}_{C'}(\Delta)$  as the closure of all BC IE achievable rates  $(R_1, R_2)$  with  $P_e^{(n)} := \Pr[(g_{1,C'}^n(Y^n) \neq (W_1, W_2, S^n) \text{ or } g_{2,C'}^n(Z^n) \neq (W_2, S^n))] \rightarrow 0$  as  $n \rightarrow \infty$ .

*Theorem 5:*  $\mathcal{C}_{C'}(\Delta)$  is the closure of the set of all rate pairs  $(R_1, R_2)$  such that

$$R_1 \leq \mathbb{I}(\mathbf{X}; \mathbf{Y}|\mathbf{U}, \mathbf{S}), \quad (12a)$$

$$R_2 \leq \mathbb{I}(\mathbf{X}, \mathbf{S}; \mathbf{Z}) - \mathbb{H}(\mathbf{S}), \quad (12b)$$

for some  $(U, S, X, Y, Z) \in \mathcal{P}(\Delta)$ , where  $U$  is an auxiliary random variable with  $|U| \leq |\mathcal{X}||S|$ .

**Proof:** See Appendix E

*Remarks*

To achieve the BC IE capacity region, the messages  $(W_1, W_2)$  are embedded into the host sequence using distortion-constrained superposition coding as in the previous cases because lossless recovery, i.e., reversible embedding, of the host sequence  $S^n$  is required in Case  $C'$ .

#### D. Host Recovery at the Worse Decoder

This section derives the BC IE capacity region in Case  $D'$ , in which Decoder 1 recovers  $(W_1, W_2)$  from  $Y^n$  and Decoder 2 recovers  $W_2$  and  $S^n$  from  $Z^n$ . We define the broadcast IE capacity region  $\mathcal{C}_{D'}(\Delta)$  as the closure of all BC IE achievable rates  $(R_1, R_2)$  with  $P_e^{(n)} := \Pr[(g_{1,D'}^n(Y^n) \neq (W_1, W_2) \text{ or } g_{2,D'}^n(Z^n) \neq (W_2, S^n)] \rightarrow 0$  as  $n \rightarrow \infty$ .

*Corollary 2:*  $\mathcal{C}_{D'}(\Delta) = \mathcal{C}_{C'}(\Delta)$ .

**Proof:** Since  $Z^n$  is a degraded version of  $Y^n$ , and  $(W_2, S^n)$  must be reliably decoded from  $Z^n$ ,  $(W_2, S^n)$  can also be decoded from  $Y^n$ . This implies that the BC IE capacity region in Case  $D'$  is the same as in Case  $C'$ .

## APPENDIX

We present definitions related to strong typicality [30], [31], [32] and important theorems based on strong typicality which will be used throughout the section.

*Definition 8:* A sequence  $\mathbf{x}^n \in \mathcal{X}^n$  is said to be  $\epsilon$ -strongly typical with respect to a distribution  $p(\mathbf{x})$  on  $\mathcal{X}$  or  $\mathbf{x}^n \in T_\epsilon^n(\mathcal{X})$  if

$$\left| \frac{1}{n} N(\mathbf{a}|\mathbf{x}^n) - p(\mathbf{a}) \right| < \frac{\epsilon}{|\mathcal{X}|},$$

for all  $\mathbf{a} \in \mathcal{X}$  with  $p(\mathbf{a}) > 0$ , and  $N(\mathbf{a}|\mathbf{x}^n) = 0$  for all  $\mathbf{a} \in \mathcal{X}$  with  $p(\mathbf{a}) = 0$ , where  $N(\mathbf{a}|\mathbf{x}^n)$  is the number of occurrences of the symbol  $\mathbf{a}$  in the sequence  $\mathbf{x}^n$ .

*Definition 9:* A pair of sequences  $(\mathbf{x}^n, \mathbf{y}^n) \in \mathcal{X}^n \times \mathcal{Y}^n$  is said to be jointly  $\epsilon$ -strongly typical with respect to a distribution  $p(\mathbf{x}, \mathbf{y})$  on  $\mathcal{X} \times \mathcal{Y}$  or  $(\mathbf{x}^n, \mathbf{y}^n) \in T_\epsilon^n(\mathbf{x}, \mathbf{y})$  if

$$\left| \frac{1}{n} N(\mathbf{a}, \mathbf{b}|\mathbf{x}^n, \mathbf{y}^n) - p(\mathbf{a}, \mathbf{b}) \right| < \frac{\epsilon}{|\mathcal{X}||\mathcal{Y}|},$$

for all  $(a, b) \in \mathcal{X} \times \mathcal{Y}$  with  $p(a, b) > 0$ , and  $N(a, b|x^n, y^n) = 0$  for all  $(a, b) \in \mathcal{X} \times \mathcal{Y}$  with  $p(a, b) = 0$ , where  $N(a, b|x^n, y^n)$  is the number of occurrences of the symbol  $(a, b)$  in the pair of sequences  $(x^n, y^n)$ .

For completeness, we recall theorems on strong typicality [30], [31], [32] which will be used throughout this section.

*Lemma 1:* Suppose  $X^n$  is generated from a discrete memoryless source (DMS)  $p(x)$  and  $X^n \in T_\epsilon^n(\mathcal{X})$ . Then, we have the following

$$2^{-n[\mathbb{H}(\mathcal{X})+\epsilon_1]} < P^n(x^n) < 2^{-n[\mathbb{H}(\mathcal{X})-\epsilon_1]} \quad (13)$$

$$(1 - \epsilon_2) 2^{n[\mathbb{H}(\mathcal{X})-\epsilon_1]} < |T_\epsilon^n(\mathcal{X})| < 2^{n[\mathbb{H}(\mathcal{X})+\epsilon_1]} \quad (14)$$

$$(1 - \epsilon_2) \leq \Pr[X^n \in T_\epsilon^n(\mathcal{X})] \leq 1 \quad (15)$$

where  $\epsilon_1 \rightarrow 0$  as  $\epsilon \rightarrow 0$ , and  $\epsilon_2 \rightarrow 0$  as  $n \rightarrow \infty$  for fixed  $\epsilon$ .

*Lemma 2:* Suppose  $(X^n, Y^n)$  is generated from a discrete memoryless source (DMS)  $p(x, y)$  and  $(x^n, y^n) \in T_\epsilon^n(\mathcal{X}, \mathcal{Y})$  and Then, we have the following

$$2^{-n[\mathbb{H}(\mathcal{X}, \mathcal{Y})+\epsilon'_1]} < P^n(x^n, y^n) < 2^{-n[\mathbb{H}(\mathcal{X}, \mathcal{Y})-\epsilon'_1]} \quad (16)$$

$$(1 - \epsilon'_2) 2^{n[\mathbb{H}(\mathcal{X}, \mathcal{Y})-\epsilon'_1]} < |T_\epsilon^n(\mathcal{X}, \mathcal{Y})| < 2^{n[\mathbb{H}(\mathcal{X}, \mathcal{Y})+\epsilon'_1]} \quad (17)$$

$$(1 - \epsilon'_2) \leq \Pr[(X^n, Y^n) \in T_\epsilon^n(\mathcal{X}, \mathcal{Y})] \leq 1 \quad (18)$$

where  $\epsilon'_1 \rightarrow 0$  as  $\epsilon \rightarrow 0$ , and  $\epsilon'_2 \rightarrow 0$  as  $n \rightarrow \infty$  for fixed  $\epsilon$ .

*Lemma 3:* Suppose  $(X^n, Y^n)$  is generated from a discrete memoryless source (DMS)  $p(x, y)$  and  $(X^n, Y^n) \in T_\epsilon^n(\mathcal{X}, \mathcal{Y})$ . Then, we have the following

$$2^{-n[\mathbb{H}(\mathcal{Y}|\mathcal{X})+\epsilon''_1]} < P^n(y^n|x^n) < 2^{-n[\mathbb{H}(\mathcal{Y}|\mathcal{X})-\epsilon''_1]} \quad (19)$$

$$(1 - \epsilon''_2) 2^{n[\mathbb{H}(\mathcal{Y}|\mathcal{X})-\epsilon''_1]} < |T_\epsilon^n(\mathcal{X}, \mathcal{Y}|x^n)| < 2^{n[\mathbb{H}(\mathcal{Y}|\mathcal{X})+\epsilon''_1]} \quad (20)$$

$$(1 - \epsilon''_2) \leq \Pr[(x^n, Y^n) \in T_\epsilon^n(\mathcal{X}, \mathcal{Y})] \leq 1 \quad (21)$$

where  $\epsilon''_1 \rightarrow 0$  as  $\epsilon \rightarrow 0$ , and  $\epsilon''_2 \rightarrow 0$  as  $n \rightarrow \infty$  for fixed  $\epsilon$ , and  $T_\epsilon^n(\mathcal{X}, \mathcal{Y}|x^n) = \{y^n : (x^n, y^n) \in T_\epsilon^n(\mathcal{X}, \mathcal{Y})\}$ .

### A. Proof of Theorem 1

In this section, we demonstrate existence of a sequence of MAC IE codes  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D_1^{(n)}, D_2^{(n)}, n)$  with  $\lim_{n \rightarrow \infty} P_e^n = 0$ , and  $\lim_{n \rightarrow \infty} D_i^{(n)} \leq \Delta_i$  for  $i = 1, 2$  if the rate pair  $(R_1, R_2)$  satisfying (4). Fix  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y) \in \mathcal{P}_{\text{MAC}}^i(\Delta_1, \Delta_2)$  and  $n$ . We construct a MAC IE code  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D_1^{(n)}, D_2^{(n)}, n)$  as follows.

- Code construction:** Throughout the achievability proof, let  $i \in \mathcal{J} = \{1, 2\}$ . Generate time sharing sequence  $Q^n = (Q_1, Q_2, \dots, Q_n)$  whose elements are i.i.d. with distribution  $p(q)$ . At Encoder  $i$ , for each  $s_i^n \in \mathcal{S}_i^n$ , generate  $\lceil 2^{nR_i} \rceil$   $X_i^n$  sequence drawn according to  $\prod_{j=1}^n p(x_{ij}|s_{ij}, q_j)$ . Call these sequences  $X_i^n(Q^n, S_i^n, m_i)$  where  $m_i \in \{1, 2, \dots, 2^{nR_i}\}$ ,  $i = 1, 2$ . In this way, the codebooks are generated at each encoder and revealed to the decoder.
- Since the sequence  $Q^n$  serves as time sharing sequence, it can be assumed that the sequence  $Q^n$  is known at both the encoders and at the decoder without loss of generality.
- Encoding:** Encoder  $i$ , upon observing  $S_i^n$  at the output of host source  $i$  and time sharing random sequence  $Q^n$ , sends message  $W_i \in \{1, 2, \dots, \lceil 2^{nR_i} \rceil\}$  by transmitting the codeword  $X_i^n(Q^n, S_i^n, W_i)$ . In this way, the codeword  $X_i^n$  is chosen and transmitted from Encoder  $i$  for a given time sharing sequence  $Q^n$ , a given host sequence  $S_i^n$ , and a message  $W_i$ .
- Decoding:** Fix  $0 < \epsilon_1 < \epsilon$ . Since the decoder knows the time sharing sequence  $Q^n = q^n$ , the decoder, upon receiving the channel output  $Y^n$ , looks for a tuple  $(X_1^n(q^n, s_1^n, m_1), X_2^n(q^n, s_2^n, m_2))$  such that  $(X_1^n(q^n, s_1^n, m_1), X_2^n(q^n, s_2^n, m_2), Y^n) \in T_{\epsilon_1}^n[Q, S_1, S_2, X_1, X_2, Y|q^n, s_1^n, s_2^n]$  for all  $(s_1^n, s_2^n) \in T_{\epsilon_1}^n[S_1, S_2]$ . If a unique vector of sequences exists, the decoder declares that  $(\hat{W}_1, \hat{W}_2, \hat{S}_1^n, \hat{S}_2^n) = (m_1, m_2, s_1^n, s_2^n)$ . Otherwise, the decoder declares an error. In this way, the messages and the host sequences are decoded at the decoder.
- Probability of error:** The average probability of error is given by the following

$$\begin{aligned}
 P_e^n &= \sum_{(s_1^n, s_2^n, q^n) \in \mathcal{S}_1^n \times \mathcal{S}_2^n \times \mathcal{Q}^n} p(q^n) p(s_1^n, s_2^n) \Pr[\text{error} | (s_1^n, s_2^n, q^n)] \\
 &\leq \sum_{(q^n, s_1^n, s_2^n) \notin T_{\epsilon_1}^n[Q, S_1, S_2]} p(q^n) p(s_1^n, s_2^n) \\
 &+ \sum_{(q^n, s_1^n, s_2^n) \in T_{\epsilon_1}^n[Q, S_1, S_2]} p(s_1^n, s_2^n) p(q^n) \Pr[\text{error} | (s_1^n, s_2^n, q^n)] \quad (22)
 \end{aligned}$$

The first term,  $\Pr[(q^n, s_1^n, s_2^n) \notin T_{\epsilon_1}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2]]$ , in the right hand side expression of (22) goes to zero as  $n \rightarrow \infty$  by Lemma 2.

Without loss of generality, it can be assumed that the time-sharing sequence is  $q^n$ , the output of the host source  $i$  is  $\tilde{s}_i^n$ , and  $W_i = 1$  is being transmitted from Encoder  $i$ . Hence, the codeword  $X_i^n(q^n, \tilde{s}_i^n, 1)$  is transmitted from Encoder  $i$ . It is also assumed that the time-sharing random sequence  $Q^n = q^n$  is known at both the encoders and the decoder. Let  $F$  be the event that  $(\tilde{s}_1^n, \tilde{s}_2^n)$  and  $q^n$  are the output of the host source pair and time sharing sequence, respectively and  $(q^n, s_1^n, s_2^n) \in T_{\epsilon_1}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2]$ .

The following error events are considered to compute  $\Pr[\text{error}|F]$  and can be made to approach zero as  $n \rightarrow \infty$ .

- 1)  $E_1: (X_1^n(q^n, \tilde{s}_1^n, 1), X_2^n(q^n, \tilde{s}_2^n, 1), Y^n) \notin T_{\epsilon}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}|q^n, \tilde{s}_1^n, \tilde{s}_2^n]$  under the event  $F$ . By using Lemma 2, we can show that  $\Pr[E_1|F] \rightarrow 0$  as  $n \rightarrow \infty$ .
- 2)  $E_2: (X_1^n(q^n, \tilde{s}_1^n, m_1), X_2^n(q^n, \tilde{s}_2^n, 1), Y^n) \in T_{\epsilon}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}|q^n, \tilde{s}_1^n, \tilde{s}_2^n]$  under the event  $F$  for all  $m_1 \neq 1$ . It can be shown that  $\Pr(E_2|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_1 < \mathbb{I}(\mathbf{X}_1; \mathbf{Y}|\mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_2, \mathbf{Q})$ .
- 3)  $E_3: (X_1^n(q^n, s_1^n, m_1), X_2^n(q^n, \tilde{s}_2^n, 1), Y^n) \in T_{\epsilon}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}|q^n, s_1^n, \tilde{s}_2^n]$  under the event  $F$  for all  $m_1 \in M_1$  and for all  $s_1^n \neq \tilde{s}_1^n$  and  $s_1^n \in T_{\epsilon_1}^n[\mathbf{S}_1, \mathbf{S}_2|\tilde{s}_2^n]$ . It can be shown that  $\Pr(E_3|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_1 < \mathbb{I}(\mathbf{S}_1, \mathbf{X}_1; \mathbf{Y}|\mathbf{S}_2, \mathbf{X}_2, \mathbf{Q}) - \mathbb{H}(\mathbf{S}_1|\mathbf{S}_2)$ .
- 4)  $E_4: (X_1^n(q^n, \tilde{s}_1^n, 1), X_2^n(q^n, \tilde{s}_2^n, m_2), Y^n) \in T_{\epsilon}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}|q^n, \tilde{s}_1^n, \tilde{s}_2^n]$  under the event  $F$  for all  $m_2 \neq 1$ . It can be shown that  $\Pr(E_4|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_2 < \mathbb{I}(\mathbf{X}_2; \mathbf{Y}|\mathbf{S}_1, \mathbf{X}_1, \mathbf{S}_2, \mathbf{Q})$ .
- 5)  $E_5: (X_1^n(q^n, \tilde{s}_1^n, 1), X_2^n(q^n, s_2^n, m_2), Y^n) \in T_{\epsilon}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}|q^n, \tilde{s}_1^n, s_2^n]$  under the event  $F$  for all  $m_2 \in M_2$ ,  $s_2^n \neq \tilde{s}_2^n$ , and  $s_2^n \in T_{\epsilon_1}^n[\mathbf{S}_1, \mathbf{S}_2|\tilde{s}_1^n]$ . It can be shown that  $\Pr(E_5|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_2 < \mathbb{I}(\mathbf{X}_2, \mathbf{S}_2; \mathbf{Y}|\mathbf{S}_1, \mathbf{X}_1, \mathbf{S}_2, \mathbf{Q}) - \mathbb{H}(\mathbf{S}_2|\mathbf{S}_1)$ .
- 6)  $E_6: (X_1^n(q^n, \tilde{s}_1^n, m_1), X_2^n(q^n, s_2^n, m_2), Y^n) \in T_{\epsilon}^n[\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_1, \mathbf{X}_2, \mathbf{Y}|q^n, \tilde{s}_1^n, s_2^n]$  under the event  $F$  for all  $m_1 \in M_1$ ,  $m_2 \in M_2$ ,  $s_2^n \neq \tilde{s}_2^n$  and  $s_2^n \in T_{\epsilon_1}^n[\mathbf{S}_1, \mathbf{S}_2|\tilde{s}_1^n]$ . It can be shown that  $\Pr(E_6|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $R_1 + R_2 < \mathbb{I}(\mathbf{X}_1, \mathbf{S}_2, \mathbf{X}_2; \mathbf{Y}|\mathbf{S}_1, \mathbf{Q}) - \mathbb{H}(\mathbf{S}_2|\mathbf{S}_1)$ .

- 7)  $E_7 : (X_1^n(q^n, s_1^n, m_1), X_2^n(q^n, s_2^n, m_2), Y^n) \in T_\epsilon^n[\mathcal{Q}, \mathcal{S}_1, \mathcal{S}_2, \mathcal{X}_1, \mathcal{X}_2, \mathcal{Y} | q^n, \tilde{s}_1^n, \tilde{s}_2^n]$  under the event  $F$  for all  $m_1 \in M_1$ ,  $m_2 \in M_2$ ,  $(s_1^n, s_2^n) \neq (\tilde{s}_1^n, \tilde{s}_2^n)$ , and  $(s_1^n, s_2^n) \in T_{\epsilon_1}^n[\mathcal{S}_1, \mathcal{S}_2]$ . It can be shown that  $\Pr(E_7|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_1 + R_2 < \mathbb{I}(\mathcal{S}_1, \mathcal{X}_1, \mathcal{S}_2, \mathcal{X}_2; \mathcal{Y} | \mathcal{Q}) - \mathbb{H}(\mathcal{S}_1, \mathcal{S}_2)$ .
- 8)  $E_8 : (X_1^n(q^n, s_1^n, m_1), X_2^n(q^n, \tilde{s}_2^n, m_2), Y^n) \in T_\epsilon^n[\mathcal{Q}, \mathcal{S}_1, \mathcal{X}_1, \mathcal{S}_2, \mathcal{X}_2, \mathcal{Y} | q^n, s_1^n, \tilde{s}_2^n]$  under the event  $F$  for all  $m_1 \neq 1$ ,  $m_2 \in M_2$ ,  $s_1^n \neq \tilde{s}_1^n$ , and  $s_1^n \in T_{\epsilon_1}^n[\mathcal{S}_1, \mathcal{S}_2 | \tilde{s}_2^n]$ . It can be shown that  $\Pr(E_8|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_1 + R_2 < \mathbb{I}(\mathcal{S}_1, \mathcal{X}_1, \mathcal{X}_2; \mathcal{Y} | \mathcal{S}_2, \mathcal{Q}) - \mathbb{H}(\mathcal{S}_1 | \mathcal{S}_2)$ .
- 9)  $E_9 : (X_1^n(q^n, \tilde{s}_1^n, m_1), X_2^n(q^n, \tilde{s}_2^n, m_2), Y^n) \in T_\epsilon^n[\mathcal{Q}, \mathcal{S}_1, \mathcal{S}_2, \mathcal{X}_1, \mathcal{X}_2, \mathcal{Y} | q^n, \tilde{s}_1^n, \tilde{s}_2^n]$  under the event  $F$  for all  $m_1 \neq 1$ , and  $m_2 \neq M_2$ . It can be shown that  $\Pr(E_9|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_1 + R_2 < \mathbb{I}(\mathcal{X}_1, \mathcal{X}_2; \mathcal{Y} | \mathcal{S}_1, \mathcal{S}_2, \mathcal{Q})$ .

Then by using the union bound,  $\Pr[\text{error}|F] \leq \sum_{j=1}^9 \Pr[E_j|F]$ .  $\Pr[\text{error}|F]$  goes to zero as  $n \rightarrow \infty$  since  $\Pr(E_j) \rightarrow 0$ , where  $j = 1$  to  $9$ , as  $n \rightarrow \infty$  if rate pair  $(R_1, R_2)$  satisfies (4). It can be concluded that  $P_e^n \rightarrow 0$  as  $n \rightarrow \infty$  if rate pair  $(R_1, R_2)$  satisfies (4).

- **Average distortions:** We consider two cases in calculating the average distortion between the host sequence  $S_i^n$  and the codeword  $X_i^n$  for any given message  $m_i$  and  $q^n \in T_\epsilon^n[\mathcal{Q}]$ . If  $X_i^n(q^n, S_i^n, m_i) \in T_\epsilon^n(X_i | q^n, S_i^n)$  for any  $(q^n, S_1^n, S_2^n) \in T_{\epsilon_1}^n[\mathcal{Q}, \mathcal{S}_1, \mathcal{S}_2]$ , then the distortion between  $S_i^n$  and  $X_i^n$  is given by

$$\begin{aligned}
d_i(S_i^n, X_i^n) &= \frac{1}{n} \sum_{\mathbf{x}_i, \mathbf{s}_i} N(\mathbf{x}_i, \mathbf{s}_i | S_i^n, X_i^n) d_i(\mathbf{s}_i, \mathbf{x}_i), \\
&\leq \sum_{\mathbf{x}_i, \mathbf{s}_i} p(\mathbf{s}_i, \mathbf{x}_i) d_i(\mathbf{s}_i, \mathbf{x}_i) + \epsilon d_{i, \max} \\
&\leq \Delta + \epsilon d_{i, \max}
\end{aligned} \tag{23}$$

where  $d_{i, \max}$  is the maximum distortion over the set  $\mathcal{S}_i \times \mathcal{X}_i$ . If  $X_i^n(q^n, S_i^n, m_i) \in T_\epsilon^n(X_i | q^n, S_i^n)$  for any  $(q^n, S_1^n, S_2^n) \in T_{\epsilon_1}^n[\mathcal{Q}, \mathcal{S}_1, \mathcal{S}_2]$ , the distortion  $d_i(S_i^n, X_i^n)$  can be upper bounded by  $d_{i, \max}$ . From error event  $E_1$  given  $F$ , we can show that  $\Pr[X_i^n(q^n, S_i^n, m_i) \in T_\epsilon^n(X_i | q^n, S_i^n)]$  goes to zero as  $n \rightarrow \infty$ . We can then conclude that  $\lim_{n \rightarrow \infty} \mathbb{E} d_i(S_i^n, f^n(S_i^n, W_i)) \leq \Delta_i$  by letting  $\epsilon \rightarrow 0$  and  $n \rightarrow \infty$ .

This concludes that  $\mathcal{R}_{\text{MAC}, C}^i(\Delta_1, \Delta_2) \subseteq C_{\text{MAC}, C}(\Delta_1, \Delta_2)$ .

### B. Proof of Theorem 2

We prove the following lemmas which will be used in the proof of Theorem 2.

**Lemma 4:** Let  $(Q_j, S_1, S_2, (X_{1j}, X_{1j}), (X_{2j}, X_{2j}), Y_j) \in \mathcal{P}_{MAC}^i(\Delta_{1j}, \Delta_{2j})$ , let  $\sum_{j=1}^n \lambda_j = 1$ ,  $\lambda_j > 0$  for  $j \in \{1, 2, \dots, n\}$ , and let  $\Delta_i = \sum_{j=1}^n \lambda_j \Delta_{ij}$  for  $i \in \{1, 2\}$ . Then, there exists

$$(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y) \in \mathcal{P}_{MAC}^i(\Delta_1, \Delta_2)$$

such that

$$\sum_{j=1}^n \lambda_j [\mathbb{I}(S_1, X_{1j}; Y_j | X_{2j}, S_2, Q_j)] = \mathbb{I}(S_1, X_1; Y | X_2, S_2, Q) \quad (24a)$$

$$\sum_{j=1}^n \lambda_j [\mathbb{I}(S_2, X_{2j}; Y_j | S_1, X_{1j}, Q_j)] = \mathbb{I}(S_2, X_2; Y | X_1, S_1, Q) \quad (24b)$$

$$\sum_{j=1}^n \lambda_j [\mathbb{I}(S_1, X_{1j}, S_2, X_{2j}; Y_j | Q_j)] = \mathbb{I}(S_1, X_1, S_2, X_2; Y | Q) \quad (24c)$$

**Proof:** If we prove the lemma for  $n = 2$ , then we can easily extend it to any value of  $n$ . Let  $n = 2$  and let  $\lambda_1 + \lambda_2 = 1$ ,  $\lambda_j > 0$  for  $j = 1, 2$ . Let  $\beta$  be a binary random variable such that  $\Pr(Z = j) = \lambda_j$  for  $j = 1, 2$ . Let

$$(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y) = ((Z, Q_z), S_1, S_2, (X_{1z}, X_{1z}), (X_{2z}, X_{2z}), Y_z).$$

$$(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y) = \begin{cases} ((Q_1, 1), S_1, S_2, (X_{11}, X_{11}), (X_{21}, X_{21}), Y_1), & \text{if } Z = 1; \\ ((Q_2, 2), S_1, S_2, (X_{12}, X_{12}), (X_{22}, X_{22}), Y_2) & \text{if } Z = 2; \end{cases}$$

To show that  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y) \in \mathcal{P}_{MAC}^i(\Delta_1, \Delta_2)$ , we have to check the conditions in Definition (3). We can easily show that  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y)$  satisfies the first condition. To check the second condition, we observe that the  $X_1 \leftrightarrow (S_1, S_2, Q) \leftrightarrow X_2$  follows as consequence of

$$\mathbb{I}(X_1, X_2 | S_1, S_2, Q) = \lambda_1 \mathbb{I}(X_{11}, X_{21} | S_1, S_2, Q_1) + \lambda_2 \mathbb{I}(X_{12}, X_{22} | S_1, S_2, Q_2) = 0$$

Similarly,  $X_1 \leftrightarrow (S_1, Q) \leftrightarrow S_2$  and  $S_1 \leftrightarrow (S_2, Q) \leftrightarrow X_2$ . We can easily verify that  $\mathbb{E}d_i(S_i, X_i) < \lambda_1 \Delta_{i1} + \lambda_2 \Delta_{i2}$ , for  $i = 1, 2$  using the distribution on  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y)$ . Since the distribution on  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y)$  satisfies the conditions in Definition (3), we can conclude that  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y) \in \mathcal{P}_{MAC}^i(\Delta_1, \Delta_2)$ . We can easily derive the equations (24) by using the distribution on  $(Q, S_1, S_2, (X_1, X_1), (X_2, X_2), Y)$ . This completes the proof of Lemma.

*Lemma 5:* Let  $(Q_j, S_1, S_2, X_{1j}, X_{2j}, Y_j) \in \mathcal{P}_{\text{MAC}}^o(\Delta_{1j}, \Delta_{2j})$ , let  $\sum_{j=1}^n \lambda_j = 1$ ,  $\lambda_j > 0$  for  $j \in \{1, 2, \dots, n\}$ , and let  $\Delta_i = \sum_{j=1}^n \lambda_j \Delta_{ij}$  for  $i \in \{1, 2\}$ . Then, there exists  $(Q, S_1, S_2, X_1, X_2, Y) \in \mathcal{P}_{\text{MAC}}^o(\Delta_1, \Delta_2)$  such that

$$\sum_{j=1}^n \lambda_j [\mathbb{I}(X_{1j}, S_1; Y_j | X_{2j}, S_2, Q_j)] = \mathbb{I}(X_1, S_1; Y | X_2, S_2, Q) \quad (25a)$$

$$\sum_{j=1}^n \lambda_j [\mathbb{I}(X_{2j}, S_2; Y_j | X_{1j}, S_{1j}, Q_j)] = \mathbb{I}(X_2, S_2; Y | X_1, S_1, Q) \quad (25b)$$

$$\sum_{j=1}^n \lambda_j [\mathbb{I}(X_{1j}, S_{1j}, X_{2j}, S_{2j}; Y_j | Q_j)] = [\mathbb{I}(X_1, S_1, X_2, S_2; Y | Q)] \quad (25c)$$

**Proof:** We do not prove the lemma because proof is similar to the proof of Lemma 4.

*Lemma 6:*  $\mathcal{R}_{\text{MAC}, C}^i(\Delta_1, \Delta_2) \subseteq \mathcal{R}_{\text{MAC}, C}^i(\Delta'_1, \Delta'_2)$  and  $\mathcal{R}_{\text{MAC}, C}^o(\Delta_1, \Delta_2) \subseteq \mathcal{R}_{\text{MAC}, C}^o(\Delta'_1, \Delta'_2)$  for any  $\Delta_1 \leq \Delta'_1$  and  $\Delta'_2 \leq \Delta_2$ .

**Proof:** This lemma can be directly proved from the fact that  $\mathcal{P}_{\text{MAC}}^i(\Delta_1, \Delta_2) \subseteq \mathcal{P}_{\text{MAC}}^i(\Delta'_1, \Delta'_2)$  and  $\mathcal{P}_{\text{MAC}}^o(\Delta_1, \Delta_2) \subseteq \mathcal{P}_{\text{MAC}}^o(\Delta'_1, \Delta'_2)$ .

We are now ready to prove the Theorem 2, i.e., prove that for any sequence of MAC IE codes  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D_1^{(n)}, D_2^{(n)}, n)$  with  $\lim_{n \rightarrow \infty} P_e^n = 0$  and  $\lim_{n \rightarrow \infty} D_i^{(n)} \leq \Delta_i$ , for  $i = 1, 2$ , the rates must satisfy (6).

Consider a given code of block length  $n$ . The joint distribution on  $\mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}_1^n \times \mathcal{S}_2^n \times \mathcal{X}_1^n \times \mathcal{X}_2^n \times \mathcal{Y}^n$  is given by

$$p(w_1, w_2, s_1^n, s_2^n, x_1^n, x_2^n, y^n) = \frac{1}{2^{nR_1}} \frac{1}{2^{nR_2}} \left( \prod_{j=1}^n p(s_{1j}, s_{2j}) \right) p(x_1^n | w_1, s_1^n) p(x_2^n | w_2, s_2^n) \prod_{i=1}^n p(y_j | x_{1j}, x_{2j}, s_{1j}, s_{2j}),$$

where,  $p(x_i^n | w_i, s_i^n)$  is 1 if  $x_i^n = f_i^n(w_i, s_i^n)$  and 0 otherwise, for  $i = 1, 2$ . By Fano's inequality [30], the conditional entropy of  $(W_1, W_2, S_1^n, S_2^n)$  given  $Y^n$  is bounded as

$$\mathbb{H}(W_1, W_2, S_1^n, S_2^n | Y^n) \leq n(R_1 + R_2 + \log_2(|\mathcal{S}_1| |\mathcal{S}_2|)) P_e^n + 1 \triangleq n\epsilon_n, \quad (26)$$

for  $i = 1, 2$ , where  $\epsilon_n \rightarrow 0$  as  $P_e^n \rightarrow 0$ . We can now bound the rate  $R_1$  as

$$\begin{aligned} nR_1 &\leq \mathbb{H}(W_1) = \mathbb{H}(W_1 | W_2) \\ &\stackrel{(a)}{=} \mathbb{H}(W_1, S_1^n | W_2, S_2^n) - \mathbb{H}(S_1^n | S_2^n) \\ &= \mathbb{H}(W_1, S_1^n | W_2, S_2^n) - \mathbb{H}(W_1, S_1^n | W_2, S_2^n, Y^n) \end{aligned}$$

$$\begin{aligned}
& + \mathbb{H}(W_1, S_1^n | W_2, S_2^n Y^n) - \mathbb{H}(S_1^n | S_2^n) \\
& \stackrel{(b)}{\leq} \mathbb{H}(W_1, S_1^n | W_2, S_2^n) - \mathbb{H}(W_1, S_1^n | W_2, S_2^n, Y^n) - \mathbb{H}(S_1^n | S_2^n) + n\epsilon_n \\
& \stackrel{(c)}{=} \mathbb{H}(W_1, S_1^n | W_2, X_2^n, S_2^n) - \mathbb{H}(W_1, S_1^n | Y^n, W_2, X_2^n, S_2^n) - \mathbb{H}(S_1^n | S_2^n) + n\epsilon_n \\
& = \mathbb{H}(W_1, S_1^n; Y^n | W_2, X_2^n, S_2^n) - \mathbb{H}(S_1^n | S_2^n) + n\epsilon_n \\
& = \mathbb{H}(Y^n | W_2, X_2^n, S_2^n) - \mathbb{H}(Y^n | W_2, X_2^n, S_2^n, W_1, S_1^n) - \mathbb{H}(S_1^n | S_2^n) + n\epsilon_n \\
& \stackrel{(d)}{=} \mathbb{H}(Y^n | W_2, X_2^n, S_2^n) - \mathbb{H}(Y^n | W_2, X_2^n, S_2^n, W_1, S_1^n, X_1^n) - \mathbb{H}(S_1^n | S_2^n) + n\epsilon_n \\
& \stackrel{(e)}{=} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, X_2^n, S_2^n, Y^{j-1}) - \mathbb{H}(Y_j | W_2, X_2^n, S_2^n, W_1, S_1^n, X_1^n, Y^{j-1}) \\
& \quad - \mathbb{H}(S_{1j} | S_2^n, S_1^{j-1})] + n\epsilon_n \\
& \stackrel{(f)}{=} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, X_2^n, S_2^n, Y^{j-1}) - \mathbb{H}(Y_j | X_{1j}, S_{1j}, X_{2j}, S_{2j}) - \mathbb{H}(S_{1j} | S_{2j})] + n\epsilon_n \\
& \stackrel{(g)}{\leq} \sum_{j=1}^n [\mathbb{H}(Y_j | X_{2j}, S_{2j}) - \mathbb{H}(Y_j | X_{1j}, S_{1j}, X_{2j}, S_{2j}) - \mathbb{H}(S_{1j} | S_{2j})] + n\epsilon_n \\
& = \sum_{j=1}^n [\mathbb{H}(X_{1j}, S_{1j}; Y_j | X_{2j}, S_{2j}) - \mathbb{H}(S_{1j} | S_{2j})] + n\epsilon_n,
\end{aligned}$$

where:

(a) follows from the fact that  $W_1$  is independent of each other; and  $(W_1, W_2)$  is independent of  $(S_1^n, S_2^n)$ .

(b) follows from Fano's inequality,

(c) follows from the fact that  $X_2^n$  is a function of  $(W_1, S_1^n)$ ,

(d) follows from the fact that  $X_1^n$  is a function of  $(W_1, S_1^n)$ ,

(e) follows from the chain rule of mutual information and entropy,

(f) follows from the fact that  $Y_j$  depends only on  $X_{1j}, X_{2j}, S_{1j}$ , and  $S_{2j}$  by the memoryless property of the channel and  $S_{1j} \leftrightarrow S_{2j} \leftrightarrow (S_1^{j-1}, S_2^{j-1}, S_{2,j+1}^n)$ ,

(g) follows from removing conditioning.

Hence, we have

$$R_1 \leq \frac{1}{n} \sum_{j=1}^n [\mathbb{H}(X_{1j}, S_{1j}; Y_j | X_{2j}, S_{2j}) - \mathbb{H}(S_{1j} | S_{2j})] + \epsilon_n$$

Similarly, we can bound  $R_2$  and  $R_1 + R_2$  as

$$R_2 \leq \frac{1}{n} \sum_{j=1}^n [\mathbb{I}(\mathbf{X}_{2j}, \mathbf{S}_2; \mathbf{Y}_j | \mathbf{X}_{1j}, \mathbf{S}_1)] - \mathbb{H}(\mathbf{S}_1 | \mathbf{S}_2) + \epsilon_n,$$

$$R_1 + R_2 \leq \frac{1}{n} \sum_{j=1}^n [\mathbb{I}(\mathbf{X}_{1j}, \mathbf{S}_{1j}, \mathbf{X}_{2j}, \mathbf{S}_2; \mathbf{Y}_j)] - \mathbb{H}(\mathbf{S}_1 | \mathbf{S}_2) + \epsilon_n.$$

If the host random variables  $\mathbf{S}_1$  and  $\mathbf{S}_2$  are correlated, we can clearly see that the random vector  $(\mathbf{Q}_j, \mathbf{S}_1, \mathbf{S}_2, \mathbf{X}_{1j}, \mathbf{X}_{2j}, \mathbf{Y}_j)$  with  $p(\mathbf{q}_j = j) = 1$  belongs to set

$\mathcal{P}_{\text{MAC}}^o(\mathbb{E}[d_1(\mathbf{S}_{1j}, \mathbf{X}_{1j})], \mathbb{E}[d_2(\mathbf{S}_{2j}, \mathbf{X}_{1j})])$  for  $j \in \{1, 2, \dots, n\}$ . According to Lemma 5, there exists a random vector  $(\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, \tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_2, \tilde{\mathbf{Y}}) \in \mathcal{P}_{\text{MAC}}^o(\frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_1(\mathbf{S}_{1j}, \mathbf{X}_{1j})], \frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_2(\mathbf{S}_{1j}, \mathbf{X}_{1j})])$  such that the following is true

$$\frac{1}{n} \sum_{j=1}^n [\mathbb{I}(\mathbf{X}_{1j}, \mathbf{S}_1; \mathbf{Y}_j | \mathbf{X}_{2j}, \mathbf{S}_2)] = \mathbb{I}(\tilde{\mathbf{X}}_1, \mathbf{S}_1; \tilde{\mathbf{Y}} | \tilde{\mathbf{X}}_2, \mathbf{S}_2, \mathbf{Q})$$

$$\frac{1}{n} \sum_{j=1}^n [\mathbb{I}(\mathbf{X}_{2j}, \mathbf{S}_2; \mathbf{Y}_j | \mathbf{X}_{1j}, \mathbf{S}_1)] = \mathbb{I}(\tilde{\mathbf{X}}_2, \mathbf{S}_2; \tilde{\mathbf{Y}} | \tilde{\mathbf{X}}_1, \mathbf{S}_1, \mathbf{Q})$$

$$\frac{1}{n} \sum_{j=1}^n [\mathbb{I}(\mathbf{X}_{1j}, \mathbf{S}_{1j}, \mathbf{X}_{2j}, \mathbf{S}_2; \mathbf{Y}_j)] = \mathbb{I}(\tilde{\mathbf{X}}_1, \mathbf{S}_1, \tilde{\mathbf{X}}_2, \mathbf{S}_2; \tilde{\mathbf{Y}} | \mathbf{Q})$$

As  $n \rightarrow \infty$ , we can conclude the following

$$\mathcal{C}_{\text{MAC}, \mathbf{C}}(\Delta_1, \Delta_2) \subseteq \mathcal{R}_{\text{MAC}, \mathbf{C}}^o \left( \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_1(\mathbf{S}_{1j}, \mathbf{X}_{1j})], \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_2(\mathbf{S}_{1j}, \mathbf{X}_{1j})] \right)$$

$$\stackrel{(a)}{\subseteq} \mathcal{R}_{\text{MAC}, \mathbf{C}}^o(\Delta_1, \Delta_2) \quad (29)$$

where (a) follows from the Lemma 6.

If the host random variables  $\mathbf{S}_1$  and  $\mathbf{S}_1$  are independent, we can obtain the following from the condition that the messages  $W_1$  and  $W_2$  are independent.

$$p(\mathbf{x}_{1j}, \mathbf{x}_{2j} | \mathbf{s}_{1j}, \mathbf{s}_{2j}) = p(\mathbf{x}_{1j} | \mathbf{s}_{1j}) p(\mathbf{x}_{2j} | \mathbf{s}_{2j}).$$

Then, we can clearly see that the random variable tuple  $(\mathbf{Q}_j, \mathbf{S}_1, \mathbf{S}_2, (\mathbf{X}_{1j}, \mathbf{X}_{1j}), (\mathbf{X}_{2j}, \mathbf{X}_{2j}), \mathbf{Y}_j)$  with  $p(\mathbf{q}_j = j) = 1$  belongs to set  $\mathcal{P}_{\text{MAC}}^i(\mathbb{E}[d_1(\mathbf{S}_{1j}, \mathbf{X}_{1j})], \mathbb{E}[d_2(\mathbf{S}_{2j}, \mathbf{X}_{1j})])$  for  $j \in \{1, 2, \dots, n\}$ .

According to Lemma 4, there exists a random vector

$$(\mathbf{Q}, \mathbf{S}_1, \mathbf{S}_2, (\tilde{\mathbf{X}}_1, \tilde{\mathbf{X}}_1), (\tilde{\mathbf{X}}_2, \tilde{\mathbf{X}}_2), \tilde{\mathbf{Y}}) \in \mathcal{P}_{\text{MAC}}^i \left( \frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_1(\mathbf{S}_{1j}, \mathbf{X}_{1j})], \frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_2(\mathbf{S}_{1j}, \mathbf{X}_{1j})] \right)$$

such that (28) is true. As  $n \rightarrow \infty$ , we can conclude the following

$$\begin{aligned} \mathcal{C}_{\text{MAC},\text{C}}(\Delta_1, \Delta_2) &\subseteq \mathcal{R}_{\text{MAC},\text{C}}^i \left( \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_1(\mathbf{S}_{1j}, \mathbf{X}_{1j})], \lim_{n \rightarrow \infty} \frac{1}{n} \sum_{j=1}^n \mathbb{E}[d_2(\mathbf{S}_{1j}, \mathbf{X}_{1j})] \right) \\ &\stackrel{(a)}{\subseteq} \mathcal{R}_{\text{MAC},\text{C}}^i(\Delta_1, \Delta_2) \end{aligned} \quad (30)$$

where (a) follows from the Lemma 6. This completes the proof of Theorem 2.

### C. Proof of Theorem 3

In this section, we show that  $\mathcal{R}_{B'}^i(\Delta) \subseteq \mathcal{C}_{B'}(\Delta)$ . Fix the random vector  $(\mathbf{U}, \mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{P}(\Delta)$ . For each  $n$ , we construct a  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D^{(n)}, n)$  BC IE code as follows.

- **Code construction :** Generate  $\lceil 2^{nR_2} \rceil 2^{n(\mathbb{I}(\mathbf{U};\mathbf{S})+\epsilon)}$   $\mathbf{U}^n$  sequences drawn according to  $\prod_{j=1}^n p(\mathbf{u}_j)$ . Distribute these sequences randomly into  $\lceil 2^{nR_2} \rceil$  bins such that each bin has  $2^{n(\mathbb{I}(\mathbf{U};\mathbf{S})+\epsilon)}$  sequences. Label all sequences  $\mathbf{U}_1^n$  in bin  $m_2 \in \{1, 2, \dots, \lceil 2^{nR_2} \rceil\}$  as  $\mathbf{U}_1^n(m_2)$ . For each  $(\mathbf{S}^n, \mathbf{U}^n) \in T_\epsilon^n[\mathbf{S}, \mathbf{U}]$ , generate  $\lceil 2^{nR_1} \rceil$   $\mathbf{X}^n$  sequences according to  $\prod_{j=1}^n p(x_j|u_j, s_j)$ . Label these sequences as  $\mathbf{X}^n(\mathbf{S}^n, \mathbf{U}^n, m_1)$ , where  $(\mathbf{S}^n, \mathbf{U}^n) \in T_\epsilon^n[\mathbf{S}, \mathbf{U}]$  and  $m_1 \in \{1, 2, \dots, \lceil 2^{nR_1} \rceil\}$ . These codebooks are revealed to the encoder and both the decoders.
- **Encoder :** The encoder, upon observing  $\mathbf{S}^n \in T_\epsilon^n[\mathbf{S}]$  at the output of the host source, embeds message  $W_2 \in \{1, 2, \dots, \lceil 2^{nR_2} \rceil\}$  into the host sequence by looking for a  $\mathbf{U}^n$  in bin  $W_2$  such that  $\mathbf{U}^n(W_2) \in T_\epsilon^n[\mathbf{S}, \mathbf{U}|\mathbf{S}^n]$ . If such a sequence  $\mathbf{U}^n(W_2)$  does not exist, the encoder declares an error; otherwise, the encoder embeds message  $W_1 \in \{1, 2, \dots, \lceil 2^{nR_1} \rceil\}$  into the host sequence  $\mathbf{S}^n$  by choosing the codeword  $\mathbf{X}^n(\mathbf{S}^n, \mathbf{U}^n(W_2), W_1)$ .
- **Decoder 1:** Decoder 1, upon receiving  $\mathbf{Y}^n$ , which is a distorted or attacked version of the embedded sequence  $\mathbf{X}^n$ , looks for  $\mathbf{U}^n(m_2)$ ,  $m_2 \in \{1, 2, \dots, \lceil 2^{nR_2} \rceil\}$  such that  $(\mathbf{U}^n(m_2), \mathbf{Y}^n) \in T_\epsilon^n[\mathbf{U}, \mathbf{Y}]$ . If a unique codeword  $\mathbf{U}^n(m_2)$  does not exist, Decoder 1 declares an error; otherwise, Decoder 1 declares that  $\hat{W}_2 = m_2$ . Upon decoding the sequence  $\mathbf{U}^n(\hat{W}_2)$ , Decoder 1 looks for  $\mathbf{X}^n(s^n, \mathbf{U}^n(\hat{W}_2), m_1)$  such that  $(\mathbf{X}^n(s^n, \mathbf{U}^n(\hat{W}_2), m_1), \mathbf{Y}^n) \in T_\epsilon^n[\mathbf{S}, \mathbf{U}, \mathbf{X}, \mathbf{Y}|s^n, \mathbf{U}^n(\hat{W}_2)]$  for each  $s^n \in T_\epsilon^n[\mathbf{U}, \mathbf{S}|\mathbf{U}^n(\hat{W}_2)]$  and  $m_1 \in \{1, 2, \dots, \lceil 2^{nR_1} \rceil\}$ . If a unique codeword  $\mathbf{X}^n(s^n, \mathbf{U}^n(\hat{W}_2), m_1)$  exists, Decoder 1 declares that  $(\hat{W}_1, \hat{S}_2^n) = (m_1, s^n)$ ; otherwise, it declares an error.
- **Decoder 2:** Decoder 2, up on receiving  $\mathbf{Z}^n$ , which is a degraded version of  $\mathbf{Y}^n$ , looks for  $\mathbf{U}^n(m_2)$ ,  $m_2 \in \{1, 2, \dots, \lceil 2^{nR_2} \rceil\}$  such that  $(\mathbf{U}^n(m_2), \mathbf{Z}^n) \in T_\epsilon^n[\mathbf{U}, \mathbf{Z}]$ . If a unique codeword

$\mathcal{U}^n(m_2)$  exists, Decoder 2 declares that  $\hat{W}_2 = m_2$ ; otherwise, Decoder 2 declares an error.

- **Probability of error:** The average probability of error is given by

$$\begin{aligned} P_e^n &= \sum_{s^n \in \mathcal{S}^n} p(s^n) \Pr[\text{error}|s^n] \\ &\leq \sum_{s^n \notin T_\epsilon^n[\mathcal{S}]} p(s^n) + \sum_{s^n \in T_\epsilon^n[\mathcal{S}]} p(s^n) \Pr[\text{error}|s^n], \end{aligned} \quad (31)$$

where the first term,  $\Pr[s^n \notin T_\epsilon^n[\mathcal{S}]]$ , goes to zero as  $n \rightarrow \infty$  by the strong asymptotic equipartition property (AEP). Without loss of generality, it can be assumed that the output of the host source is  $\tilde{s}^n$ , and the message pair  $(W_1, W_2) = (1, 1)$  is to be embedded in to the host sequence  $\tilde{s}^n$ . Let  $F$  be the event that the host source output is  $\tilde{s}^n$ . To compute  $\Pr[\text{error}|F]$ , let us write the error event as  $E_0 \cup E_1 \cup E_2 \cup E_3$ , where:

- 1)  $E_0$  is the event that there is no  $\mathcal{U}^n(1)$  such that  $\mathcal{U}^n(1) \in T_\epsilon^n[\mathcal{U}, \mathcal{S}|\tilde{s}^n]$ . Using well-known rate-distortion arguments, the probability of this event approaches zero as  $n$  goes to infinity since each bin has  $2^{n(\mathbb{I}(\mathcal{U}; \mathcal{S}) + \epsilon)}$   $\mathcal{U}^n$  sequences.

Conditioned on the event  $F \cap E_0^c$ , it can also be assumed that  $\tilde{\mathcal{U}}^n(1)$  is jointly strongly typical with the host sequence  $\tilde{s}^n$ . Hence, the embedded sequence  $X^n(\tilde{s}^n, \tilde{\mathcal{U}}^n(1), 1)$  is generated and transmitted from the encoder.

- 2)  $E_1$  is the event that

$$(\tilde{\mathcal{U}}^n(1), X^n(\tilde{s}^n, \tilde{\mathcal{U}}^n(1), 1), Y^n, Z^n) \notin T_\epsilon^n[\mathcal{S}, \mathcal{U}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}|\tilde{s}^n].$$

By the strong AEP, we can show that  $\Pr[E_1|F \cap E_0^c] \rightarrow 0$  as  $n \rightarrow \infty$ .

- 3)  $E_2 := E_{2,1} \cup (E_{2,1}^c \cap E_{2,2})$ , where  $E_{2,1}$  is the event that  $(\mathcal{U}^n, Y^n) \in T_\epsilon^n[\mathcal{U}, \mathcal{Y}]$  for  $\mathcal{U}^n \neq \tilde{\mathcal{U}}^n(1)$ , and  $E_{2,2}$  is the event that  $(X^n(s^n, \tilde{\mathcal{U}}^n(1), m_1), Y^n) \in T_\epsilon^n[\mathcal{S}, \mathcal{U}, \mathcal{X}, \mathcal{Y}|\mathcal{S}^n, \tilde{\mathcal{U}}^n(1)]$  for  $m_1 \neq 1$  or  $s^n \in \{s^n : s^n \neq \tilde{s}^n, s^n \in T_\epsilon^n[\mathcal{U}, \mathcal{S}|\tilde{\mathcal{U}}^n(1)]\}$ . It can be shown that  $\Pr[E_{2,1}|F \cap E_0^c] \rightarrow 0$  as  $n \rightarrow \infty$  if  $R_2 \leq \mathbb{I}(\mathcal{U}; \mathcal{Y}) - \mathbb{I}(\mathcal{U}; \mathcal{S})$  and that  $\Pr(E_{2,2}|F \cap E_0^c \cap E_{2,1}^c) \rightarrow 0$  as  $n \rightarrow \infty$  if  $R_1 \leq \mathbb{I}(\mathcal{S}, \mathcal{X}; \mathcal{Y}|\mathcal{U}) - \mathbb{H}(\mathcal{S}|\mathcal{U})$ .

- 4)  $E_3$  is the event that  $(\mathcal{U}^n, Z^n) \in T_\epsilon^n[\mathcal{U}, \mathcal{Z}]$  for  $\mathcal{U}^n \neq \tilde{\mathcal{U}}^n(1)$ . Using Gel'fand-Pinsker arguments, it can be shown that  $\Pr[E_3|F \cap E_0^c] \rightarrow 0$  as  $n \rightarrow \infty$  if  $R_2 \leq \mathbb{I}(\mathcal{U}; \mathcal{Z}) - \mathbb{I}(\mathcal{U}; \mathcal{S})$ . Because the broadcast channel is degraded, this constraint on  $R_2$  is more restrictive than the previous constraint.

Thus, by the union bound, it can be shown that  $P_e^n$  goes to zero as  $n \rightarrow \infty$  if  $(R_1, R_2) \in \mathcal{R}_{B'}^i$ .

- **Average distortion:** Since  $(X^n, \tilde{s}^n)$  is jointly strongly typical with high probability and the distribution belongs to  $\mathcal{P}(\Delta)$ , it can be shown that the average distortion  $D^{(n)}$  associated with the generated code satisfies the distortion constraint  $\Delta$  as  $n \rightarrow \infty$  as in the Proof of Theorem 1.

#### D. Proof of Theorem 4

In this section, we show that  $\mathcal{C}_{B'}(\Delta) \subseteq \mathcal{R}_{B'}^o(\Delta)$ . If we are given a sequence of  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D^{(n)}, n)$  BC IE codes, i.e.,  $X^n = f(W_1, W_2, S^n)$ ,  $g_{1,B'}^n(Y^n) = (\hat{W}_1, \hat{W}_2, \hat{S}^n)$ , and  $g_{2,B'}^n(Z^n) = \hat{W}_2$ , with  $\lim_{n \rightarrow \infty} P_e^n = 0$  and  $\lim_{n \rightarrow \infty} D^{(n)} \leq \Delta$ , then we show that the rate pair  $(R_1, R_2)$  must satisfy (11) for some  $((U, V), S, X, Y, Z) \in \mathcal{P}(\Delta)$ . Consider a given code of block length  $n$ . The joint distribution on  $\mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}^n \times \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$  induced by the code is given by

$$\begin{aligned} p(w_1, w_2, s^n, x^n, y^n, z^n) &= \\ &= \frac{1}{\lceil 2^{nR_1} \rceil \lceil 2^{nR_2} \rceil} p(s^n) p(x^n | w_1, w_2, s^n) \\ &\quad \times \prod_{j=1}^n p(y_j | x_j, s_j) p(z_j | y_j), \end{aligned}$$

where,  $p(x^n | w_1, w_2, s^n)$  is 1 if  $x^n = f^n(w_1, w_2, s^n)$  and 0 otherwise. We can bound the rate  $R_1$  as follows:

$$\begin{aligned} nR_1 &\leq \mathbb{H}(W_1) \\ &\stackrel{(a)}{=} \mathbb{H}(W_1, S^n | W_2) - \mathbb{H}(S^n | W_2) \\ &= \mathbb{H}(W_1, S^n | W_2) - \mathbb{H}(W_1, S^n | W_2, Y^n) \\ &\quad + \mathbb{H}(W_1, S^n | W_2, Y^n) - \mathbb{H}(S^n | W_2) \\ &\stackrel{(b)}{\leq} \mathbb{I}(W_1, S^n; Y^n | W_2) - \mathbb{H}(S^n | W_2) + n\epsilon_n \\ &\stackrel{(c)}{=} \sum_{j=1}^n [\mathbb{I}(W_1, S^n; Y_j | W_2, Y^{j-1}) - \mathbb{H}(S_j | W_2)] + n\epsilon_n \\ &\stackrel{(d)}{=} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, Y^{j-1}) - \mathbb{H}(Y_j | W_2, Y^{j-1}, W_1, S^n, X^n) \\ &\quad - \mathbb{H}(S_j | W_2)] + n\epsilon_n \end{aligned}$$

$$\begin{aligned}
& \stackrel{(e)}{=} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, Y^{j-1}, Z^{j-1}) - \mathbb{H}(Y_j | S_j, X_j) \\
& \quad - \mathbb{H}(S_j | W_2)] + n\epsilon_n \\
& \stackrel{(f)}{\leq} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, Z^{j-1}) - \mathbb{H}(Y_j | S_j, X_j, W_2, Z^{j-1}) \\
& \quad - \mathbb{H}(S_j | W_2, Z^{j-1})] + n\epsilon_n \\
& = \sum_{j=1}^n \mathbb{I}(S_j, X_j; Y_j | W_2, Z^{j-1}) - \mathbb{H}(S_j | W_2, Z^{j-1}) + n\epsilon_n
\end{aligned} \tag{32}$$

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

- (a) follows from the fact that  $W_1$ ,  $W_2$  and  $S^n$  are mutually independent,
- (b) follows from Fano's inequality,
- (c) follows from the chain rule and the fact that  $S^n$  is i.i.d. and independent of  $W_2$ ,
- (d) follows from the fact that  $X^n$  is a deterministic function of  $(W_1, W_2, S^n)$ ,
- (e) follows from degraded and memoryless properties of the broadcast channel, and
- (f) follows from removing conditioning in the positive term and introducing conditioning in the negative term.

We can also bound the rate  $R_2$  as follows:

$$\begin{aligned}
nR_2 & \leq \mathbb{H}(W_2) \\
& \stackrel{(a)}{\leq} \mathbb{I}(W_2; Z^n) + n\epsilon_n \\
& = \sum_{j=1}^n [\mathbb{I}(W_2, S_{j+1}^n; Z^j) - \mathbb{I}(W_2, S_j^n; Z^{j-1})] + n\epsilon_n \\
& \stackrel{(b)}{\leq} \sum_{j=1}^n [\mathbb{I}(W_2, S_{j+1}^n; Z^{j-1}) + \mathbb{I}(W_2, S_{j+1}^n; Z_j | Z^{j-1}) \\
& \quad - \mathbb{I}(W_2, S_{j+1}^n; Z^{j-1}) - \mathbb{I}(S_j; Z^{j-1} | W_2, S_{j+1}^n)] + n\epsilon_n \\
& = \sum_{j=1}^n [\mathbb{I}(W_2, S_{j+1}^n; Z_j | Z^{j-1}) - \mathbb{I}(S_j; Z^{j-1} | W_2, S_{j+1}^n)] + n\epsilon_n \\
& = \sum_{j=1}^n [\mathbb{H}(Z_j | Z^{j-1}) - \mathbb{H}(Z_j | W_2, Z^{j-1}, S_{j+1}^n)]
\end{aligned}$$

$$\begin{aligned}
& - \mathbb{H}(S_j | W_2, S_{j+1}^n) + \mathbb{H}(S_j | W_2, Z^{j-1}, S_{j+1}^n)] + n\epsilon_n \\
\stackrel{(c)}{\leq} & \sum_{j=1}^n [\mathbb{H}(Z_j) - \mathbb{H}(Z_j | W_2, Z^{j-1}, S_{j+1}^n) \\
& - \mathbb{H}(S_j) + \mathbb{H}(S_j | W_2, Z^{j-1}, S_{j+1}^n)] + n\epsilon_n \\
= & \sum_{j=1}^n [\mathbb{I}(W_2, Z^{j-1}, S_{j+1}^n; Z_j) - \mathbb{I}(W_2, Z^{j-1}, S_{j+1}^n; S_j)] + n\epsilon_n \tag{33}
\end{aligned}$$

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

(a) follows from Fano's inequality,

(b) follows from applying the chain rule on  $(Z^{j-1}, Z_j)$  and  $(S_{j+1}^n, S_j)$  in the first and second mutual information expressions, respectively, and

(c) follows from removing conditioning and the fact that  $S^n$  is i.i.d. and independent of  $W_2$ .

Let  $\tilde{U}_j := \{W_2, Z^{j-1}\}$  and  $V_j := \{S_{j+1}^n\}$  for  $j = 1, 2, \dots, n$ . We can then write (32) and (33) as

$$R_1 \leq \mathbb{I}(S, X; Y | Q, \tilde{U}) - \mathbb{H}(S | Q, \tilde{U}) + \epsilon_n, \tag{34a}$$

$$R_2 \leq \mathbb{I}(\tilde{U}, V; Z | Q) - \mathbb{I}(\tilde{U}, V; S | Q) + \epsilon_n, \tag{34b}$$

where  $Q$  takes values in the set  $\mathcal{Q} \in \{1, 2, \dots, n\}$  with equal probability and the joint probability distribution on  $(S, Q, \tilde{U}, V, X, Y, Z)$  is  $p(S = s, Q = q, \tilde{U} = \tilde{u}, V = v, X = x)p(y|x, s)p(z|y)$ , with

$$\begin{aligned}
p(S = s, Q = q, \tilde{U} = \tilde{u}, V = v, X = x) = \\
p(s)p(q)p(\mathbf{U}_q = \tilde{u}, V_q = v | s, q)p(\mathbf{X}_q = x | s, q, \tilde{u}, v).
\end{aligned}$$

Finally, we can write (34) as

$$R_1 \leq \mathbb{I}(S, X; Y | U) - \mathbb{H}(S | U) + n\epsilon_n,$$

$$R_2 \leq \mathbb{I}(U, V; Z) - \mathbb{I}(U, V; S) + n\epsilon_n,$$

where  $U := (Q, \tilde{U})$ , since  $\mathbb{I}(\tilde{U}, V; Z | Q) \leq \mathbb{I}(Q, \tilde{U}, V; Z)$  and  $\mathbb{I}(Q; S) = 0$ .

Given any  $\delta > 0$ , the associated distortion  $D^{(n)}$ , for sufficiently large  $n$ , satisfies

$$\begin{aligned}
\Delta + \delta & \geq D^{(n)} \\
& = \mathbb{E}d(\mathbf{X}^n, \mathbf{S}^n)
\end{aligned}$$

$$\begin{aligned}
&= \frac{1}{n} \sum_{j=1}^n \sum_{\mathbf{x}, \mathbf{s}} p(X_j = x, S_j = s) d(\mathbf{x}, \mathbf{s}) \\
&= \sum_{\mathbf{x}, \mathbf{s}} p(\mathbf{X} = \mathbf{x}, \mathbf{S} = \mathbf{s}) d(\mathbf{x}, \mathbf{s}) \\
&= \mathbb{E}d(\mathbf{X}, \mathbf{S}).
\end{aligned}$$

As  $n \rightarrow \infty$  and  $\delta \rightarrow 0$ ,  $((\mathbf{U}, \mathbf{V}), \mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{P}(\Delta)$  and  $(R_1, R_2) \in \mathcal{R}_{B'}^o$ . Thus,  $\mathcal{C}_{B'}(\Delta) \subseteq \mathcal{R}_{B'}^o$ .

### E. Proof of Theorem 5

1) *Achievability:* In this section, we show that  $\mathcal{R}_{C'}^i(\Delta) \subseteq \mathcal{C}_{C'}(\Delta)$ . Fix the random vector  $(\mathbf{U}, \mathbf{S}, \mathbf{X}, \mathbf{Y}, \mathbf{Z}) \in \mathcal{P}(\Delta)$ . For each  $n$ , we construct a  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D^{(n)}, n)$  BC IE code as follows.

- **Code construction:** At Encoder, for each  $s^n \in \mathcal{S}^n$ , generate  $2^{nR_2}$   $\mathbf{U}^n$  sequences drawn according to  $\prod_{j=1}^n p(\mathbf{u}_j | s_j)$ . Denote these sequences as  $\mathbf{U}^n(s^n, m_2)$ , where  $m_2 \in \{1, 2, \dots, 2^{nR_2}\}$ . For each pair  $(s^n, \mathbf{U}^n)$ , generate  $2^{nR_1}$   $\mathbf{X}_1^n$  sequences drawn according to  $\prod_{j=1}^n p(x_j | \mathbf{u}_j, s_j)$ . Call these sequences  $\mathbf{X}^n(s^n, m_1, m_2)$  where  $m_1 \in \{1, 2, \dots, 2^{nR_1}\}$ . In this way, the codebook is generated at the encoder and revealed to both the decoders.
- **Encoding:** Encoder, upon observing  $s^n$  at the output of host source, sends messages  $W_1 \in \{1, 2, \dots, 2^{nR_1}\}$  and  $W_2 \in \{1, 2, \dots, 2^{nR_2}\}$  by transmitting the codeword  $\mathbf{X}^n(s^n, W_1, W_2)$ . In this way, the codeword  $\mathbf{X}^n$  is chosen and transmitted from the encoder for a given host sequence  $S^n$ , and a given message pair  $(W_1, W_2)$ .
- **Decoder 1:** Decoder 1, up on receiving the channel output  $\mathbf{Y}^n$ , looks for  $\mathbf{U}^n(s^n, m_2)$  such that  $(\mathbf{U}^n(s^n, m_2), \mathbf{Y}^n) \in T_\epsilon^n[\mathbf{U}, \mathbf{Y} | s^n]$  for all  $s^n \in T_{\epsilon_1}^n[\mathbf{S}]$ . If a unique codeword  $\mathbf{U}^n(s^n, m_2)$  exists, Decoder 1 again looks for  $\mathbf{X}^n(s^n, m_1, m_2)$  such that  $(\mathbf{X}^n(s^n, m_1, m_2), \mathbf{Y}^n) \in T_\epsilon^n[\mathbf{X}, \mathbf{Y} | s^n, \mathbf{U}^n(s^n, m_2)]$ . If a unique codeword  $\mathbf{X}^n(s^n, m_1, m_2)$  exists, Decoder 1 declares that  $(\hat{W}_1, \hat{S}_2^n) = (m_1, s^n)$ . In this way, the message intended for Decoder 1 and the host sequences are decoded at Decoder 1.
- **Decoder 2:** Decoder 2, up on receiving the channel output  $\mathbf{Z}^n$ , looks for  $\mathbf{U}^n(s^n, m_2)$  such that  $(\mathbf{U}^n(s^n, m_2), \mathbf{Z}^n) \in T_\epsilon^n[\mathbf{U}, \mathbf{Z} | s^n]$  for all  $s^n \in T_{\epsilon_1}^n[\mathbf{S}]$ . If a unique codeword  $\mathbf{U}^n(s^n, m_2)$  codeword exists, Decoder 2 declares that  $(\hat{W}_2, \hat{S}_1^n) = (m_2, s^n)$ . Otherwise, Decoder 2 declares an error. In this way, the message intended for Decoder 2 and the host sequences are decoded at Decoder 2.

- **Probability of error:** The average probability of error is given by the following

$$\begin{aligned}
P_e^n &= \sum_{(s^n) \in \mathcal{S}^n} p(s^n) \Pr[\text{error}|s^n] \\
&\leq \sum_{s^n \notin T_{\epsilon_1}^n[\mathcal{S}]} p(s^n) + \sum_{s^n \in T_{\epsilon_1}^n[\mathcal{S}]} p(s^n) \Pr[\text{error}|s^n], \\
&= \sum_{s^n \notin T_{\epsilon_1}^n[\mathcal{S}]} p(s^n) + \sum_{s^n \in T_{\epsilon_1}^n[\mathcal{S}]} p(s^n) \Pr[E(1) \cup E((2)|s^n)], \tag{35}
\end{aligned}$$

where  $E(i)$  is the event that the error is made at Decoder  $i$ , for  $i = 1, 2$ . The first term,  $\Pr[s^n \notin T_{\epsilon_1}^n[\mathcal{S}]]$ , in the right hand side expression of (35) goes to zero as  $n \rightarrow \infty$  by Lemma 2.

Without loss of generality, it can be assumed that the output of the host source is  $\tilde{s}^n$ , and  $(W_1, W_2) = (1, 1)$  is being transmitted from the encoder. Hence, the codeword  $X^n(\tilde{s}^n, 1, 1)$  is transmitted from the encoder. Let  $F_1$  be the event that  $\tilde{s}^n \in T_{\epsilon_1}^n[\mathcal{S}]$  is output of the host source.

The following error events are considered to compute  $\Pr[E(2)|F]$  and can be made to approach zero as  $n \rightarrow \infty$ .

- 1)  $E_1: (\mathcal{U}^n(\tilde{s}^n, 1), X^n(\tilde{s}^n, 1, 1), Y^n, Z^n) \notin T_\epsilon^n[\mathcal{S}, \mathcal{U}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}|\tilde{s}^n]$  under the event  $F$ . By using Lemma 2, we can show that  $\Pr[E_1|F] \rightarrow 0$  as  $n \rightarrow \infty$ .
- 2)  $E_2: (\mathcal{U}^n(\tilde{s}^n, m_2), Y^n) \in T_\epsilon^n[\mathcal{S}, \mathcal{U}, \mathcal{Z}|\tilde{s}^n]$  under the event  $F \cap E_1^c$  for all  $m_2 \neq 1$ . It can be shown that  $\Pr(E_2|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_2 < \mathbb{I}(\mathcal{U}; \mathcal{Z}|\mathcal{S})$ .
- 3)  $E_3: (\mathcal{U}^n(s^n, m_2), Y^n) \in T_\epsilon^n[\mathcal{S}, \mathcal{U}, \mathcal{Z}|s^n]$  under the event  $F \cap E_1^c$  for all  $m_1$  and  $s^n \neq \tilde{s}^n$ . It can be shown that  $\Pr(E_3|F) \rightarrow 0$  as  $n \rightarrow \infty$  by using Lemma 2 and Lemma 3 if  $0 \leq R_2 < \mathbb{I}(\mathcal{U}, \mathcal{S}; \mathcal{Z}) - \mathbb{H}(\mathcal{S})$ .

From the all above error events, it can be concluded that  $\Pr[E(1)|F] \rightarrow 0$  as  $n \rightarrow \infty$  if  $0 \leq R_2 < \mathbb{I}(\mathcal{U}, \mathcal{S}; \mathcal{Z}) - \mathbb{H}(\mathcal{S})$ . The following error events are considered to compute  $\Pr[E(1)|F]$  and can be made to approach zero as  $n \rightarrow \infty$ .

- 1)  $E_4: (\mathcal{U}^n(s^n, m_2), Y^n) \in T_\epsilon^n[\mathcal{S}, \mathcal{U}, \mathcal{Y}|s^n]$  for  $m_1 \neq 1$  or  $s^n \neq \tilde{s}^n$ . By considering the error events similar to  $E_2$  and  $E_3$ , it can be shown that  $\Pr(E_4|F, E_1^c) \rightarrow 0$  as  $n \rightarrow \infty$  if  $0 \leq R_2 < \mathbb{I}(\mathcal{U}, \mathcal{S}; \mathcal{Y}) - \mathbb{H}(\mathcal{S})$ .

2)  $E_5: (X^n(\tilde{s}^n, m_1, 1), Y^n) \in T_\epsilon^n[\mathcal{S}, \mathcal{U}, \mathcal{X}, \mathcal{Y} | \tilde{s}^n, \mathcal{U}^n(\tilde{s}^n, 1)]$  for  $m_1 \neq 1$ . It can be shown that  $\Pr(E_5 | F, E_1^c, E_4^c) \rightarrow 0$  as  $n \rightarrow \infty$  if  $0 \leq R_1 < \mathbb{I}(\mathcal{X}; \mathcal{Y} | \mathcal{S}, \mathcal{U})$ .

Then by using the union bound,  $\Pr[E(1) \cup E(2) | F]$  goes to zero as  $n \rightarrow \infty$  if rate pair  $(R_1, R_2)$  satisfies (12). It can be concluded that  $P_e^n \rightarrow 0$  as  $n \rightarrow \infty$  if rate pair  $(R_1, R_2)$  satisfies (12).

- **Average distortions:** Since  $(X^n, \tilde{s}^n)$  is jointly strongly typical with high probability and the distribution belongs to  $\mathcal{P}(\Delta)$ , it can be shown that the average distortion  $D^{(n)}$  associated with the generated code satisfies the distortion constraint  $\Delta$  as  $n \rightarrow \infty$  as in the Proof of Theorem 1.

2) *Converse:* We show that any sequence of  $(\lceil 2^{nR_1} \rceil, \lceil 2^{nR_2} \rceil, D^{(n)}, n)$  codes, i.e.,  $X^n = f(W_1, W_2, S^n)$ ,  $g_{1,C'}^n(Y^n) = (\hat{W}_1, \hat{W}_2, \hat{S}^n)$ , and  $g_{2,C'}^n(Z^n) = (\hat{W}_2, \hat{S}^n)$ , with  $\lim_{n \rightarrow \infty} P_e^n = 0$  and  $\lim_{n \rightarrow \infty} D^{(n)} \leq \Delta$ , the rate pair  $(R_1, R_2)$  must satisfy (12) for some  $(\mathcal{U}, \mathcal{S}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}) \in \mathcal{P}(\Delta)$ . Consider a given code of block length  $n$ . The joint distribution on  $\mathcal{W}_1 \times \mathcal{W}_2 \times \mathcal{S}^n \times \mathcal{X}^n \times \mathcal{Y}^n \times \mathcal{Z}^n$  induced by the code is given by

$$\begin{aligned} p(w_1, w_2, s^n, x^n, y^n, z^n) &= \\ &= \frac{1}{\lceil 2^{nR_1} \rceil \lceil 2^{nR_2} \rceil} p(s^n) p(x^n | w_1, w_2, s^n) \\ &\quad \times \prod_{j=1}^n p(y_j | x_j, s_j) p(z_j | y_j), \end{aligned}$$

where,  $p(x^n | w_1, w_2, s^n)$  is 1 if  $x^n = f^n(w_1, w_2, s^n)$  and 0 otherwise.

We can bound the rate  $R_1$  as follows:

$$\begin{aligned} nR_1 &\leq \mathbb{H}(W_1) \\ &\stackrel{(a)}{=} \mathbb{H}(W_1 | W_2, S^n) \\ &= \mathbb{H}(W_1 | W_2, S^n) - \mathbb{H}(W_1 | W_2, S^n, Y^n) + \mathbb{H}(W_1 | W_2, S^n, Y^n) \\ &\stackrel{(b)}{\leq} \mathbb{I}(W_1; Y^n | W_2, S^n) + n\epsilon_n \\ &= \sum_{j=1}^n \mathbb{I}(W_1; Y_j | W_2, S^n, Y^{j-1}) + n\epsilon_n \\ &= \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, S^n, Y^{j-1}) - \mathbb{H}(Y_j | W_1, W_2, S^n, Y^{j-1})] + n\epsilon_n \end{aligned}$$

$$\begin{aligned}
&\stackrel{(c)}{=} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, S^n, Y^{j-1}, Z^{j-1}) - \mathbb{H}(Y_j | W_1, W_2, S^n, Y^{j-1}, Z^{j-1})] + n\epsilon_n \\
&\stackrel{(d)}{\leq} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, S^n, Z^{j-1}) - \mathbb{H}(Y_j | W_1, W_2, S^n, Y^{j-1}, Z^{j-1}, X^n)] + n\epsilon_n \\
&\stackrel{(e)}{=} \sum_{j=1}^n [\mathbb{H}(Y_j | W_2, S^n, Z^{j-1}) - \mathbb{H}(Y_j | X_j, S_j)] + n\epsilon_n \\
&\stackrel{(f)}{=} \sum_{j=1}^n [\mathbb{H}(Y_j | S_j, \tilde{U}_j) - \mathbb{H}(Y_j | X_j, S_j)] + n\epsilon_n \\
&= \sum_{j=1}^n \mathbb{I}(X_j; Y_j | S_j, \tilde{U}_j) + n\epsilon_n, \tag{36}
\end{aligned}$$

where,

- (a) follows from the fact that  $W_1$ ,  $W_2$  and  $S^n$  are mutually independent,
- (b) follows from Fano's inequality and  $\epsilon_n \rightarrow 0$  as  $n \rightarrow \infty$ ,
- (c) follows from  $Y_j \leftrightarrow (W_2, S^n, Y^{j-1}) \leftrightarrow Z^{j-1}$  and  $Y_j \leftrightarrow (W_1, W_2, S^n, Y^{j-1}) \leftrightarrow Z^{j-1}$ ,
- (d) follows from  $\mathbb{H}(Y_j | W_2, S^n, Y^{j-1}, Z^{j-1}) \leq \mathbb{H}(Y_j | W_2, S^n, Z^{j-1})$ , and  $X^n$  is a deterministic function of  $(W_1, W_2, S^n)$ ,
- (e) follows from memoryless properties of the broadcast channel, and
- (f) follows from  $\tilde{U}_j := \{W_2, S_1^{j-1}, S_{j+1}^n\}$ .

We can also bound the rate  $R_2$  as follows:

$$\begin{aligned}
nR_2 &\leq \mathbb{H}(W_2) \\
&\stackrel{(a)}{\leq} \mathbb{H}(W_2, S^n) - \mathbb{H}(S^n) \\
&\stackrel{(b)}{\leq} \mathbb{I}(W_2, S^n; Z^n) - \mathbb{H}(S^n) + n\epsilon_n \\
&= \sum_{j=1}^n [\mathbb{I}(W_2, S^n; Z_j | Z^{j-1}) - \mathbb{H}(S_j | S^{j-1})] + n\epsilon_n \\
&\stackrel{(c)}{=} \sum_{j=1}^n [\mathbb{H}(Z_j | Z^{j-1}) - \mathbb{H}(Z_j | W_2, S^n, Z^{j-1}) - \mathbb{H}(S_j)] + n\epsilon_n \\
&\stackrel{(d)}{\leq} \sum_{j=1}^n [\mathbb{H}(Z_j) - \mathbb{H}(Z_j | \tilde{U}_j, S_j) - \mathbb{H}(S_j)] + n\epsilon_n \\
&= \sum_{j=1}^n [\mathbb{I}(\tilde{U}_j, S_j; Z_j) - \mathbb{H}(S_j)] + n\epsilon_n
\end{aligned}$$

where,

(a) follows from the fact that  $W_1$ ,  $W_2$  and  $S^n$  are mutually independent,

(b) follows from Fano's inequality and  $\epsilon_n \rightarrow 0$  as  $n \rightarrow \infty$ ,

(c) follows from the fact that  $S^n$  is an i.i.d. random vector,

(d) follows from  $\mathbb{H}(Z_j|Z^{j-1}) \leq \mathbb{H}(Z_j)$ , and  $\tilde{\mathbf{U}}_j := \{W_2, S_1^{j-1}, S_{j+1}^n\}$ .

We can then write (36) and (37a) as

$$R_1 \leq \mathbb{I}(X; Y|Q, S, \tilde{\mathbf{U}}) + \epsilon_n, \quad (37a)$$

$$R_2 \leq \mathbb{I}(\tilde{\mathbf{U}}, S; Z|Q) - \mathbb{H}(S) + \epsilon_n, \quad (37b)$$

where  $Q$  takes values in the set  $\mathcal{Q} \in \{1, 2, \dots, n\}$  with equal probability and the joint probability distribution on  $(S, Q, \tilde{\mathbf{U}}, X, Y, Z)$  is  $p(S = s, Q = q, \tilde{\mathbf{U}} = \tilde{\mathbf{u}}, X = x)p(y|x, s)p(z|y)$ , with

$$\begin{aligned} p(S = s, Q = q, \tilde{\mathbf{U}} = \tilde{\mathbf{u}}, X = x) &= \\ p(s)p(q)p(\mathbf{U}_q = \tilde{\mathbf{u}}|s, q)p(X_q = x|s, q, \tilde{\mathbf{u}}). \end{aligned}$$

Finally, we can write (37) as

$$R_1 \leq \mathbb{I}(X; Y|\mathbf{U}, S) + n\epsilon_n,$$

$$R_2 \leq \mathbb{I}(\mathbf{U}, S; Z) - \mathbb{H}(S) + n\epsilon_n,$$

where  $\mathbf{U} := (Q, \tilde{\mathbf{U}})$ , since  $\mathbb{I}(\tilde{\mathbf{U}}, S; Z|Q) \leq \mathbb{I}(Q, \tilde{\mathbf{U}}, S; Z)$ .

Given any  $\delta > 0$ , the associated distortion  $D^{(n)}$ , for sufficiently large  $n$ , satisfies

$$\begin{aligned} \Delta + \delta &\geq D^{(n)} \\ &= \mathbb{E}d(\mathbf{X}^n, S^n) \\ &= \frac{1}{n} \sum_{j=1}^n \sum_{\mathbf{x}, \mathbf{s}} p(X_j = x, S_j = s)d(\mathbf{x}, \mathbf{s}) \\ &= \sum_{\mathbf{x}, \mathbf{s}} p(X = \mathbf{x}, S = \mathbf{s})d(\mathbf{x}, \mathbf{s}) \\ &= \mathbb{E}d(\mathbf{X}, S). \end{aligned}$$

As  $n \rightarrow \infty$  and  $\delta \rightarrow 0$ ,  $(\mathbf{U}, S, X, Y, Z) \in \mathcal{P}(\Delta)$  and  $(R_1, R_2) \in \mathcal{C}_{C'}$ .

## REFERENCES

- [1] B. Chen, “Design and Analysis of Digital Watermarking, Information Embedding, and Data Hiding Systems,” Ph.D. dissertation, Massachusetts Institute of Technology, Cambridge, MA, 2000.
- [2] B. Chen and G. W. Wornell, “Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding,” *IEEE Trans. Inform. Theory*, vol. 47, no. 4, pp. 1423–1443, May 2001.
- [3] R. J. Anderson and F. A. P. Petitcolas, “On the Limits of Steganography,” *IEEE Journal of Selected Areas in Communications*, vol. 16, no. 4, pp. 474–484, May 1998.
- [4] M. D. Swanson, M. Kobayashi, and A. H. Tewfik, “Multimedia Data-Embedding and Watermarking Technologies,” in *Proc. IEEE Int. Conf. Communications (ICC)*, vol. 2, 1998, pp. 823–827.
- [5] S. I. Gel’fand and M. S. Pinsker, “Coding for Channel with Random Parameters,” *Probl. Contr. and Information Theory*, vol. 9, no. 1, pp. pp.19–31, 1980.
- [6] M. H. M. Costa, “Writing on Dirty Paper,” *IEEE Trans. Inform. Theory*, vol. vol.IT-29, pp. 439–441, May 1983.
- [7] P. Moulin and J. O’Sullivan, “Information-theoretic Analysis of Information Hiding,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 563–593, 2003.
- [8] A. S. Cohen, “The Gaussian Watermarking Game,” *IEEE Trans. Inform. Theory*, vol. vol.48, pp. 1639–1669, June 2002.
- [9] T. Kalker and F. Willems, “Capacity Bounds and Constructions for Reversible Data-hiding,” in *Proc. Int. Conf. Digital Signal Processing*, 2002, pp. 71–76.
- [10] —, “Capacity Bounds and Constructions for Reversible Data-hiding,” in *Proc. SPIE Int. Conf. Security and Watermarking of Multimedia Contents*, vol. 5020, 2003, pp. 604–611.
- [11] A. Somekh-Baruch and N. Merhav, “On the error exponent and capacity games of private watermarking systems,” *IEEE Trans. Inform. Theory*, vol. 49, no. 3, pp. 537–562, Mar. 2003.
- [12] —, “On the capacity game of public watermarking system,” *IEEE Trans. Inform. Theory*, vol. 50, no. 3, pp. 511–524, Mar. 2004.
- [13] —, “On the capacity game of private fingerprinting systems under collusion attacks,” *IEEE Trans. Inform. Theory*, vol. 51, no. 3, pp. 884–899, Mar. 2005.
- [14] A. Maor and N. Merhav, “On Joint Information Embedding and Lossy Compression,” *IEEE Trans. Inform. Theory*, vol. 51, no. 8, pp. 2998–3008, Aug. 2005.
- [15] —, “On Joint Information Embedding and Lossy Compression in the Presence of a Memoryless Attack,” *IEEE Trans. Inform. Theory*, vol. 51, no. 9, pp. 3166–3175, 2005.
- [16] N. Merhav, “On Joint Coding for Watermarking and Encryption,” *IEEE Trans. Inform. Theory*, vol. 52, no. 1, pp. 190–205, Jan. 2006.
- [17] S. I. Gel’fand and M. S. Pinsker, “On Gaussian Channels with Random Parameters,” in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, 1983.
- [18] Y. H. Kim, A. Sutivong, and S. Sigurjónsson, “Multiple User Writing on Dirty Paper,” in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, June 27 - July 2 2004.
- [19] A. Khisti, U. Erez, and G. W. Wornell, “Writing on Many Pieces of Dirty Paper at Once: The Binary Case,” in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, June 27 – July 2 2004.
- [20] S. Kotagiri and J. N. Laneman, “Achievable Rates for Multiple Access Channels with State Information Known at One Encoder,” in *Proc. Allerton Conf. Communications, Control, and Computing*, 2004.

- [21] Y. Steinberg, "Coding for the Degraded Broadcast Channel with Random parameters, with Causal and Noncausal Side Information," *IEEE Trans. Inform. Theory*, vol. vol.51, pp. 2867–2877, August 2005.
- [22] Y. Cemal and Y. Steinberg, "Multiple Access Channel with Partial State Information at the Encoders," *IEEE Trans. Inform. Theory*, vol. vol.IT-51, pp. 3992–4003, November 2005.
- [23] S. A. Jafar, "Capacity with Causal and Non-Causal Side Information - A Unified View," *IEEE Trans. Inform. Theory*, vol. 52, no. 12, pp. 5468–5475, Dec. 2006.
- [24] S. Kotagiri and J. N. Laneman, "Multiple Access Channels with State Information Known at Some Encoders," submitted to *EURASIP J. Wireless Comm. Net.*, September 2007.
- [25] A. Somekh-Baruch, S. Shamai, and S. Verdú, "Cooperative Encoding with Asymmetric State Information at the Transmitters," in *Proc. Allerton Conf. Communications, Control, and Computing*, 2006.
- [26] S. Kotagiri and J. N. Laneman, "Multiaccess Channels with State Known to One Encoder: A Case of Degraded Message Sets," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, June 24 - June 29 2007.
- [27] A. Somekh-Baruch, S. Shamai, and S. Verdú, "Cooperative Multiple Access Encoding with States Available at One Transmitter," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, June 24 - June 29 2007.
- [28] Y. Steinberg, "Reversible Information Embedding with Compressed Hosts at the Decoder," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, July 9 - July 14 2006.
- [29] W. Sun and E. Yang, *Information Hiding*, ser. Lecture Notes in Computer Science. Berlin / Heidelberg: Springer Berlin / Heidelberg, Dec. 2004, ch. On Achievable Regions of Public Multiple-Access Gaussian Watermarking Systems, pp. 38–51.
- [30] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: John Wiley & Sons, Inc., 1991.
- [31] I. Csiszár and J. Körner, Eds., *Information Theory: Coding Theorems for Discrete Memoryless Systems*. New York: Academic Press Inc., 1981.
- [32] S. Tung, "Multiterminal Source Coding," Ph.D. dissertation, Cornell University, Ithaca, New York, May 1978.