Gaussian Multiple Descriptions with Common and Constrained Reconstruction Constraints

Ravi Tandon¹, Behzad Ahmadi², Osvaldo Simeone², and H. Vincent Poor¹

¹Department of Electrical Engineering, Princeton University, Princeton, NJ
²CWCSPR, New Jersey Institute of Technology, Newark, NJ

Abstract—The problem of multiple descriptions for a Gaussian source is considered, in which all the decoders have access to correlated Gaussian side-information. Two variations of this problem are studied. First, the rate-distortion tradeoff is characterized under the assumption of a common reconstruction constraint, in which the estimate produced at each of the decoders is also exactly recoverable at the encoder. Secondly, a generalization of this setup is studied in which possibly different distortions are tolerable between the estimates at the encoder and the respective estimates at each of the decoders.

I. INTRODUCTION

The rate distortion function for lossy transmission of a memoryless source $X$ to a decoder that has access to correlated side information $Y$ was characterized by Wyner and Ziv in [1]. There are two ways in which the side-information is useful in the Wyner-Ziv problem. First, since the side information $Y$ is correlated with the source $X$, the encoder can reduce the communication rate via binning; and secondly, the reconstruction $\hat{X}$ at the decoder depends on both the digital information received from the encoder and the side-information $Y$. The second property, i.e., the dependence of the decoder’s estimate $\hat{X}$ on the side-information $Y$ (which is unavailable at the encoder) may be undesirable for certain applications. As an example, consider the transmission of sensitive medical records, for which it is of utmost importance that the decoder and the encoder agree upon the estimates of the records.

To take such scenarios into account, the problem of common reconstruction (CR) was proposed by Steinberg in [2], in which the rate-distortion function is characterized for a point-to-point system under a common reconstruction constraint. Formally, a common reconstruction constraint refers to a restriction that the encoder should also be able to reconstruct the estimate at the decoder. The common reconstruction constraint can be perhaps too restrictive since it precludes the decoder to use its side-information to create the estimate. A relaxed version of the common reconstruction constraint in which some distortion is tolerable between the estimate at the encoder and the estimate at the decoder was studied in [3]. The corresponding rate-distortion function was characterized in [3] (henceforth referred to as the rate-distortion function under constrained reconstruction (ConR)).

Some generalizations and extensions of [2] to multi-user settings have been studied recently. In particular, the rate-distortion function for the Heegard-Berger problem with CR constraints has been recently obtained in [4]. Furthermore, the rate-distortion tradeoff for a class of cascade source coding problems under the CR constraint has also been obtained in [4]. It is noted that in the latter case, the problem of determining the rate-distortion tradeoff is open when one does not impose the CR constraint. This demonstrates that the CR constraint may simplify the design problem by limiting the space of possible strategies, as already discussed in [2] and [5]. A source coding problem with complementary side information under a CR constraint has been studied in [6]. Joint source-channel coding for a Gaussian source over a slow fading Gaussian broadcast channel is studied in [5], where it is shown that the natural broadcast strategy coupled with successive refinement source coding is in fact optimal under the CR constraint (also see [2, Sec. IV]).

In this paper, we generalize the point-to-point common-reconstruction problem of [2], and the point-to-point constrained reconstruction problem of [3] to the problem of multiple descriptions (MD) with decoder side information. We focus on the MD problem with three decoders, in which all the decoders have access to the same correlated side-information $Y$ (see Figure 1). We focus on Gaussian source and side information. Specifically, an encoder wishes to convey a memoryless Gaussian scalar source $X$ to three decoders via two rate-limited orthogonal links. The distortion constraints at all the decoders are assumed to be measured by the mean-squared error (MSE). The correlated side information $Y$, which is assumed to be jointly Gaussian with $X$ is available at all the three decoders. In the absence of side-information, this problem was solved by Ozarow [7]. Instead, the more general case in which correlated Gaussian side-information is available at all decoders was solved by Diggavi and Vaishampayan [8].

In this paper, we impose an additional CR constraint. We
first characterize the set of achievable rates and distortion tuples for the Gaussian MD problem under the CR constraint. We next consider the ConR generalization of this setup, in which some pre-specified MSE distortions are tolerable between the estimates at the encoder and the corresponding estimates at the decoders. It is shown that the optimal strategy is based on separation, in the sense that a combination of coding for the MD problem, followed by binning with respect to side-information $Y$, is optimal.

II. PROBLEM STATEMENT

The encoder observes a memoryless source $X_n$ and produces two indices

$$J_1 = f_1^{(n)}(X^n) \quad \text{and} \quad J_2 = f_2^{(n)}(X^n),$$

where $\{f_j^{(n)} : X^n \rightarrow J_j\}_{j=1,2}$ are the encoding functions. The index $J_1$ (resp. $J_2$) is received at decoder 1 (resp. decoder 2). Both the indices $(J_1, J_2)$ are received at decoder 0. The decoders form their estimates as follows:

$$\hat{X}_j^n = g_j^{(n)}(J, Y^n), \quad j = 1, 2, \quad \text{and} \quad \hat{X}_0^n = g_0^{(n)}(J_1, J_2, Y^n),$$

where $g_j^{(n)}$ is the reconstruction function at decoder $j$, for $j = 0, 1, 2$. We denote the estimates at the encoder as follows:

$$\hat{X}_{e,1} = \psi_1(X^n), \quad \hat{X}_{e,2} = \psi_2(X^n) \quad \text{and} \quad \hat{X}_{e,0} = \psi_0(X^n).$$

A. Common Reconstruction (CR)

We call the set of $\{(f_j^{(n)})_{j=1,2}, \{g_j^{(n)}\}_{j=0,1,2}, \{\psi_j^{(n)}\}_{j=0,1,2}\}$ functions an $(n, R_1, R_2, D_0, D_1, D_2)$-code if $|J_1| \leq 2^nR_1$, $|J_2| \leq 2^nR_2$, and the reconstruction sequences satisfy

$$\frac{1}{n} \sum_{i=1}^{n} E[d_d(X_i, \hat{X}_{j,i})] \leq D_j, \quad j = 0, 1, 2,$$

and

$$\Pr(\psi_1(X^n) \neq g_1(J_1, Y^n)) \leq \epsilon \quad \quad \text{(1)}$$

$$\Pr(\psi_2(X^n) \neq g_2(J_1, Y^n)) \leq \epsilon \quad \quad \text{(2)}$$

The non-negative tuple $(R_1, R_2, D_0, D_1, D_2)$ is achievable if for every $\epsilon > 0$ and sufficiently large $n$, there exists an $(n, R_1 + \epsilon, R_2 + \epsilon, D_0 + \epsilon, D_1 + \epsilon, D_2 + \epsilon)$-code. We denote $\mathcal{RD}_{\text{CR}}$ as the closure of the set of all achievable $(R_1, R_2, D_0, D_1, D_2)$ tuples.

B. Constrained Reconstruction (ConR)

We next extend the CR constraint to the ConR constraint. In this setting, some distortion is permissible between the estimate at the decoder(s) and the respective estimate(s) at the encoder. We call the set of $\{(f_j^{(n)})_{j=1,2}, \{g_j^{(n)}\}_{j=0,1,2}, \{\psi_j^{(n)}\}_{j=0,1,2}\}$ functions an $(n, R_1, R_2, D_0, D_1, D_2, D_{e,0}, D_{e,1}, D_{e,2})$-code if $|J_1| \leq 2^nR_1$, $|J_2| \leq 2^nR_2$, and the reconstruction sequences satisfy

$$\frac{1}{n} \sum_{i=1}^{n} E[d_e(\hat{X}_{j,i}, \hat{X}_{e,j,i})] \leq D_{e,j}, \quad j = 0, 1, 2, \quad \text{(5)}$$

The non-negative tuple $(R_1, R_2, D_0, D_1, D_2, D_{e,0}, D_{e,1}, D_{e,2})$ is achievable if for every $\epsilon > 0$ and sufficiently large $n$, there exists an $(n, R_1 + \epsilon, R_2 + \epsilon, D_0 + \epsilon, D_1 + \epsilon, D_2 + \epsilon, D_{e,0} + \epsilon, D_{e,1} + \epsilon, D_{e,2} + \epsilon)$-code. We denote $\mathcal{RD}_{\text{ConR}}$ as the closure of the set of all achievable $(R_1, R_2, D_0, D_1, D_2, D_{e,0}, D_{e,1}, D_{e,2})$ tuples.

This paper considers the case in which the source $X$ is Gaussian with variance $\sigma_X^2$ and the side information $Y$ is jointly Gaussian with $X$. Under this model, we can write

$$Y = X + Z,$$

where $Z$ is a zero-mean, Gaussian random variable with variance $\sigma_Z^2$, and independent of $X$. The distortion measures are quadratic and are defined as follows:

$$d_d(a, b) \triangleq (a - b)^2 \quad \text{and} \quad d_e(a, b) \triangleq (a - b)^2.$$

Before presenting our results, we recall the rate-distortion region without side-information [7]:

$$D_{1, e}^{\text{No-SI}} \geq \exp(-2R_1) \quad \quad \text{(8)}$$

$$D_{2, e}^{\text{No-SI}} \geq \exp(-2R_2) \quad \quad \text{(9)}$$

$$D_{0, e}^{\text{No-SI}} \geq \exp(-2(R_1 + R_2)) \frac{1}{1 - (\sqrt{\Pi^{\text{No-SI}}} - \sqrt{\Delta^{\text{No-SI}}})^2}, \quad \text{(10)}$$

The rate-distortion region with side-information (without any constraints) [8] is given as

$$D_j^{\text{SI}} \geq \exp(-2R_j) \quad \quad \text{(14)}$$

$$D_{0, e}^{\text{SI}} \geq \exp(-2(R_1 + R_2)) \frac{1}{1 - (\sqrt{\Pi^{\text{SI}}} - \Delta^{\text{SI}})^2}, \quad \text{(16)}$$

with $D_j^{\text{SI}}$ being defined as

$$D_j^{\text{SI}} \triangleq D_j \cdot \left(\frac{\sigma_X^2 + \sigma_Z^2}{\sigma_X^2 \sigma_Z^2}\right) = \frac{D_j}{V_{X|Y}}, \quad j = 0, 1, 2, \quad \text{(17)}$$

where the quantities $(\Pi^{\text{SI}}, \Delta^{\text{SI}})$ are defined as in (12) and (13) with $(D_1^{\text{No-SI}}, D_2^{\text{No-SI}})$, replaced by $(D_1^{\text{SI}}, D_2^{\text{SI}})$ and $V_{X|Y} = \text{Var}(X|Y) = \frac{\sigma_X^2 \sigma_Z^2}{\sigma_X^2 + \sigma_Z^2}$ denotes the variance of $X$ given $Y$.

III. MAIN RESULTS

Theorem 1: The set $\mathcal{RD}_{\text{CR}}$ of all achievable $(R_1, R_2, D_0, D_1, D_2)$-tuples for the Gaussian MD problem with decoder side-information and CR constraints is given as
follows:

\begin{align}
D_{10}^{CR} & \geq \exp(-2R_1) \\
D_{20}^{CR} & \geq \exp(-2R_2) \\
D_0^{CR} & \geq \exp(-2(R_1 + R_2)) - \frac{1}{1 - (\sqrt{\Pi^{CR}} - \sqrt{\Delta^{CR}})^2},
\end{align}

where we have defined

\begin{align}
D_j^{CR} & \triangleq \left( \frac{\sigma_0^2 + \sigma_j^2}{\sigma_0^2 + \frac{1}{D_j} \sigma_j^2} \right) D_j, \quad j = 0, 1, 2. \\
\Pi^{CR} & \triangleq (1 - D_1^{CR})(1 - D_2^{CR}) \\
\Delta^{CR} & \triangleq D_1^{CR} D_2^{CR} - \exp(-2(R_1 + R_2)).
\end{align}

The proof of Theorem 1 is given in the appendix.

Theorem 2: The set \( \mathcal{R}_D^{ConR} \) of all achievable \((R_1, R_2, D_0, D_1, D_2, D_{e,0}, D_{e,1}, D_{e,2})\)-tuples for the Gaussian MD problem with decoder side-information and ConR constraints is given as follows:

\begin{align}
D_1^{ConR} & \geq \exp(-2R_1) \\
D_2^{ConR} & \geq \exp(-2R_2) \\
D_0^{ConR} & \geq \exp(-2(R_1 + R_2)) - \frac{1}{1 - (\sqrt{\Pi^{ConR}} - \sqrt{\Delta^{ConR}})^2},
\end{align}

where for \( j = 0, 1, 2 \), we have defined

\begin{align}
D_j^{ConR} & \triangleq \begin{cases} 
\left( \frac{\sigma_0^2 + \sigma_j^2}{\sigma_0^2 + \frac{1}{D_j} \sigma_j^2} \right) D_j, \quad \sqrt{\sigma_j^2 D_{e,j}} \geq \min \left\{ D_j, \frac{\sigma_0^2 \sigma_j^2}{\sigma_0^2 + \sigma_j^2} \right\}; \\
\left( \frac{\sigma_0^2 + \sigma_j^2}{\sigma_0^2 + \frac{1}{D_j} \sigma_j^2} \right) \left( \frac{\sigma_0^2 (D_j - D_{e,j})}{\sigma_0^2 + D_j - 2\sigma_j^2 D_{e,j}} \right), & \text{otherwise,}
\end{cases}
\end{align}

and

\begin{align}
\Pi^{ConR} & \triangleq (1 - D_1^{ConR})(1 - D_2^{ConR}) \\
\Delta^{ConR} & \triangleq D_1^{ConR} D_2^{ConR} - \exp(-2(R_1 + R_2)).
\end{align}

The proof of Theorem 2 is omitted due to space limitations and can be found in [9].

Remark 1: The optimal coding schemes achieving the tradeoffs in Theorems 1 and 2 are based on a separation based strategy, i.e., a combination of coding for the MD problem, followed by binning with respect to side-information \( Y \). This is evident by comparing the expressions in Theorems 1 and 2 to the corresponding tradeoff regions in (8)-(10) and (14)-(16). It is interesting to note that all four regions are described by a similar set of constraints, except that the definition of the effective distortions \( D^{No-SI}, D^{SI}, D^{CR} \) and \( D^{ConR} \) differ depending on the problem under consideration. We also note that as \( D_{e,j} \to 0 \), for \( j = 0, 1, 2 \), we have \( D_j^{ConR} \to D_j^{CR} \), and the region in Theorem 2 collapses to the one in Theorem 1.

We illustrate these tradeoffs in Figure 2 for the symmetric case in which \( D_1 = D_2 = D_0 = D_{sym} \), and \( R_1 = R_2 = R_{sym} \), \( D_{e,0} = D_{e,2} = D_{e,0} = D_{e,sym} = 0.05 \), with \( \sigma_X^2 = 4 \) and \( \sigma_Y^2 = 1 \). From Figure 2, it is worth noting that for values of \( D_{sym} \) below a certain threshold, the ConR constraints are automatically satisfied, and hence the minimal rate under ConR coincides with the minimal rate without any constraints.

IV. CONCLUSIONS

This paper has focused on the generalization of the Gaussian multiple-description problem with side-information at the decoders by imposing a common reconstruction constraint as in [2] and also constrained reconstruction constraints as in [3]. These additional distortion constraints effectively control the amount of side-information to be used in creating the source estimate at each decoder. The complete rate-distortion tradeoff has been characterized for the case of common-reconstruction constraints. This result is then generalized to the constrained-reconstruction setting with MSE distortion measures at each of the decoders. These tradeoffs reflect the penalty in terms of additional communication rates of the encoder, if it seeks to agree with the estimates at the decoders.

V. ACKNOWLEDGEMENT

The work of H. V. Poor and R. Tandon was supported in part by the Air Force Office of Scientific Research MURI Grant FA-9550-09-1-0643 and in part by the National Science Foundation Grant CNS-09-05398. The work of O. Simeone was supported by the U.S. National Science Foundation under Grant CCF-0914899.

VI. APPENDIX

A. Proof of Theorem 1

1) Coding Scheme with CR: The following region is achievable for the MD problem with a CR constraint:

\begin{align}
R_1 & \geq I(X; U_1 | Y) \\
R_2 & \geq I(X; U_2 | Y) \\
R_1 + R_2 & \geq I(X; U_1, U_2 | Y) + I(U_1; U_2 | Y)
\end{align}

where the random variables \((U_1, U_2, X, Y)\) satisfy the Markov condition \((U_1, U_2) \rightarrow X \rightarrow Y\), and there exist functions...
where we have used (32).

\( \hat{X}_1 = g_1(U_1), \quad \hat{X}_2 = g_2(U_2), \quad \hat{X}_0 = g_0(U_1, U_2), \)
satisfying \( \mathbb{E}[d(X, \hat{X}_j)] \leq D_j \) for \( j = 0, 1, 2. \)

2) **Gaussian MD with CR constraints:** For the case in which \((X, Y)\) are jointly Gaussian, we select

\[
U_1 = X + N_1, \quad U_2 = X + N_2,
\]
where \((N_1, N_2)\) are jointly Gaussian, independent of \(X\), with a covariance matrix as follows:

\[
K_{N_1, N_2} = \begin{bmatrix}
\sigma_1^2 & \rho \sigma_1 \sigma_2 \\
\rho \sigma_1 \sigma_2 & \sigma_2^2
\end{bmatrix}.
\]

The estimates \( \hat{X}_i \) are selected as the minimum MSE (MMSE) estimators of \(X\) given \(U_1, U_2\) and \((U_1, U_2)\) for decoders 1, 2 and decoder 0, respectively. Note that such a selection automatically satisfies the common reconstruction constraints for all the three decoders. The achievable distortions are hence given as

\[
D_1 = \frac{\sigma_2^2}{\sigma_X^2} \hat{X}, \quad D_2 = \frac{\sigma_2^2}{\sigma_X^2} \hat{X}
\]

and

\[
D_0 = \frac{\sigma_2^2 \sigma_X^2}{\sigma_X^2 (1 - \rho^2)} = \frac{\sigma_2^2 \sigma_X^2}{\sigma_X^2 (1 - \rho^2)}.
\]

We select \( \sigma_1^2 \) and \( \sigma_2^2 \) such that the distortion constraints in (32) are met with equality, i.e., we select

\[
\sigma_j^2 = \frac{D_j \sigma_X^2}{\sigma_X^2 - D_j}, \quad j = 1, 2.
\]

Also, note that we have for \( j = 1, 2 \)

\[
D_j^{\text{CR}} \triangleq \left( \frac{\sigma_2^2}{\sigma_X^2 + \sigma_2^2} \right) \left( \frac{D_j \sigma_2^2}{\sigma_2^2 + \sigma_2^2} \right)
\]

\[
= \frac{\sigma_2^2 (\sigma_X^2 + \sigma_2^2)}{\sigma_X^2 \sigma_2^2 + \sigma_2^2 \sigma_2^2}.
\]

where we have used (32).

The individual rate constraints for \( j = 1, 2 \) are given as

\[
R_j \geq I(X; U_j|Y) = \frac{1}{2} \log \left( \frac{D_j^{\text{CR}}}{} \right).
\]

The sum-rate constraint is given as

\[
R_1 + R_2 \geq I(X; U_1, U_2|Y) + I(U_1; U_2|Y)
\]

\[
= h(U_1|Y) + h(U_2|Y) - h(U_1, U_2|Y)
\]

\[
= \frac{1}{2} \log \left( \frac{(V_X|Y + \sigma_2^2)(V_X|Y + \sigma_2^2)}{\sigma_2^2 \sigma_2^2 (1 - \rho^2)} \right)
\]

\[
= \frac{1}{2} \log \left( \frac{1}{D_j^{\text{CR}} D_j^{\text{CR}} (1 - \rho^2)} \right).
\]

Hence, \( \rho \) can be chosen arbitrarily as long as it satisfies

\[
\rho^2 \leq \frac{D_1^{\text{CR}} D_2^{\text{CR}}}{D_1^{\text{CR}} D_2^{\text{CR}}}.
\]

We select \( \rho \) as follows:

\[
\rho = -\frac{\sqrt{D_1^{\text{CR}} D_2^{\text{CR}}} - \exp(-2(R_1 + R_2))}{\sqrt{D_1^{\text{CR}} D_2^{\text{CR}}} - \exp(-2(R_1 + R_2))}.
\]

Substituting this value of \( \rho \) in the expression for \( D_0 \) in (33) and using (32), we arrive at

\[
D_1^{\text{CR}} \geq \exp(-2R_1)
\]

\[
D_2^{\text{CR}} \geq \exp(-2R_2)
\]

\[
D_0^{\text{CR}} \geq \exp(-2(R_1 + R_2)) \frac{1}{1 - (\sqrt{\Pi^{\text{CR}}} - \Delta^{\text{CR}})^2},
\]

with \( \Pi^{\text{CR}} \) and \( \Delta^{\text{CR}} \) as defined in Theorem 1.

3) **Converse Proof under the CR Constraint:** We note that \( R_1 \) and \( R_2 \) must always satisfy the following bounds:

\[
R_j \geq R_{\text{CR}}(D_j), \quad j = 1, 2.
\]

From [2, Eq. (25)], \( R_{\text{CR}}(D) \) is given as

\[
R_{\text{CR}}(D) = \frac{1}{2} \log \left( \frac{\sigma_2^2 + \sigma_2^2}{\sigma_2^2 + \sigma_2^2} D \right)
\]

\[
\geq \frac{1}{2} \log \left( \frac{1}{D_{\text{CR}}} \right).
\]

where \( D_{\text{CR}} \) is as defined in (21). Hence, from (47) and (49), we have the following bounds:

\[
D_j^{\text{CR}} \geq \exp(-2R_j), \quad j = 1, 2.
\]

We now obtain a lower bound on the sum rate \( R_1 + R_2 \) as follows:

\[
n(R_1 + R_2) = H(J_1) + H(J_2)
\]

\[
\geq H(J_1|Y^n) + H(J_2|Y^n)
\]

\[
= H(J_1, J_2|Y^n) + H(J_1|Y^n) + H(J_2|Y^n) - H(J_1, J_2|Y^n)
\]

\[
= H(J_1, J_2|Y^n) + I(J_1; J_2|Y^n)
\]

\[
= I(X^n; J_1, J_2|Y^n) + I(J_1; J_2|Y^n)
\]

\[
\geq n R_{\text{CR}}(D_0) + I(J_1; J_2|Y^n).
\]

As in [7], we define

\[
T \triangleq \exp \left( \frac{2}{n} I(J_1; J_2|Y^n) \right).
\]

Using (56), we have the following inequalities:

\[
D_1^{\text{CR}} \geq \exp(-2R_1)
\]

\[
D_2^{\text{CR}} \geq \exp(-2R_2)
\]

\[
D_0^{\text{CR}} \geq \exp(-2(R_1 + R_2)) T.
\]

We now obtain a lower bound on \( T \) by using Ozarow's technique of inducing conditional independence [7]. For this purpose, we define an artificial Gaussian random variable as follows:

\[
S_i = X_i + W_i, \quad i = 1, \ldots, n,
\]
where the sequence of random variables \( \{W_i\}_{i=1}^n \) is independent and identically distributed with each element being a zero-mean, Gaussian random variable with variance \( \eta \), and \( W^n \) is assumed to be independent of \((X^n, Y^n)\). To lower bound \( T \), we have the following sequence of inequalities:

\[
I(J_1; J_2 | Y^n) \\
\geq I(J_1; J_2 | Y^n) - I(J_1; J_2 | Y^n, S^n) \\
= I(J_1; S^n | Y^n) - I(J_1; S^n | Y^n, J_2) \\
= h(S^n | Y^n) + h(S^n | J_1, J_2, Y^n) \\
\quad - h(S^n | J_1, Y^n) - h(S^n | J_2, Y^n) \\
= h(S^n | Y^n) + h(S^n | J_1, J_2, Y^n) \\
\quad - h(S^n | Y^n, X^n) - h(S^n | J_1, J_2, Y^n) \\
\geq h(S^n | Y^n) + h(S^n | J_1, J_2, Y^n) \\
\quad - \frac{n}{2} \log(2\pi e (D_1^2 + \eta)) - \frac{n}{2} \log(2\pi e (D_2^2 + \eta)) \\
= \frac{n}{2} \log \left( \frac{1}{V_{X|Y}} \right) + h(S^n | J_1, J_2, Y^n) \\
\quad - \frac{n}{2} \log(2\pi e (D_1^2 + \eta)) - \frac{n}{2} \log(2\pi e (D_2^2 + \eta)),
\]

(65)

where we have defined

\[
V_{X|Y} = \frac{\sigma_X^2 \sigma_Y^2}{\sigma_X^2 + \sigma_Y^2}, \quad D_1 \triangleq \frac{D_1 \sigma_Y^2}{D_1 + \sigma_Y^2} \quad \text{and} \quad D_2 \triangleq \frac{D_2 \sigma_Y^2}{D_2 + \sigma_Y^2}.
\]

The bounding step (66) follows from the following sequence of inequalities:

\[
\begin{align*}
& h(X^n + W^n | J_1, Y^n) \\
& \leq h(X^n + W^n | X^n_1, Y^n) \\
& = h(S^n | X^n_1, Y^n) \\
& = h(S^n | \psi_1(X^n), \tilde{X}^n_1, Y^n) + I(\psi_1(X^n); S^n | \tilde{X}^n_1, Y^n) \\
& \leq h(S^n | \psi_1(X^n), \tilde{X}^n_1, Y^n) + n\epsilon \\
& \leq h(S^n | \psi_1(X^n), Y^n) + n\epsilon \\
& = h(X^n + W^n | \psi_1(X^n), Y^n) + n\epsilon \\
& \leq \frac{n}{2} \log (D_1^2 + \eta) + n\epsilon,
\end{align*}
\]

(69)

and

\[
\begin{align*}
& \exp \left( \frac{2}{n} h(X^n + W^n | J_1, J_2, Y^n) \right) \\
& \geq \exp \left( \frac{2}{n} h(X^n | J_1, J_2, Y^n) \right) + \exp \left( \frac{2}{n} h(W^n | J_1, J_2, Y^n) \right) \\
& = \exp \left( \frac{2}{n} h(X^n | J_1, J_2, Y^n) \right) + (2\pi e)(\eta),
\end{align*}
\]

(76)

where in (76), we have used the fact that \( W^n \) is independent of \((X^n, Y^n, J_1, J_2)\) and the conditional version of the entropy power inequality (EPI).

We now note the following sequence of inequalities:

\[
\begin{align*}
h(X^n | J_1, J_2, Y^n) \\
& = h(X^n | Y^n) - I(X^n; J_1, J_2 | Y^n) \\
& = h(X^n | Y^n) - H(J_1, J_2 | Y^n) \\
& = h(X^n | Y^n) - H(J_1 | Y^n) - H(J_2 | Y^n) + I(J_1; J_2 | Y^n),
\end{align*}
\]

(78)

(79)

(80)

\[
\begin{align*}
& \geq h(X^n | Y^n) - H(J_1) - H(J_2) + I(J_1; J_2 | Y^n), \\
& \geq h(X^n | Y^n) - nR_1 - nR_2 + I(J_1; J_2 | Y^n),
\end{align*}
\]

(81)

(82)

which implies that

\[
\exp \left( \frac{2}{n} h(X^n | J_1, J_2, Y^n) \right) \geq \exp \left( \frac{2}{n} h(X^n | Y^n) \right) \exp(-2(R_1 + R_2))T \\
= (2\pi e V_{X|Y} \exp(-2(R_1 + R_2))T
\]

(83)

(84)

Hence, from (77) and (84), and using (67), we obtain the following lower bound on \( T \):

\[
T \geq \frac{\eta^* (\eta^* + 1)}{(D_1^{CR} + \eta^*) (D_2^{CR} + \eta^*) - (\eta^* + 1) \exp(-2(R_1 + R_2))},
\]

where \( \eta^* \triangleq \frac{n}{\log(2\pi e V_{X|Y})} \) and \( D_j^{CR} = D_j^{CR}(\eta^*) \) for \( j = 1, 2 \). The following choice of \( \eta^* \) maximizes the right hand side above:

\[
\eta^* = \frac{\sqrt{\Delta^{CR}}}{\sqrt{\Pi^{CR}} - \sqrt{\Delta^{CR}}},
\]

(85)

which upon substitution, yields the following lower bound on \( T \):

\[
T \geq \frac{1}{1 - (\sqrt{\Pi^{CR}} - \sqrt{\Delta^{CR}})^2}.
\]

(86)

Hence, (58)-(60) and (86) complete the proof of Theorem 1.

REFERENCES


