

Constrained Wyner-Ziv Coding

Amos Lapidoth
ETH Zurich
lapidoth@isi.ee.ethz.ch

Andreas Malär
ETH Zurich
amalaer@ee.ethz.ch

Michèle Wigger
Telecom ParisTech
michele.wigger@telecom-paristech.fr

Abstract—We consider a variation on the Wyner-Ziv source coding problem with side-information at the decoder where the encoder is required to be able to compute the decoder's reconstruction sequence with some fidelity. This requirement limits the extent to which the reconstruction sequence can depend on the side-information, which is not available to the encoder.

For finite-alphabet memoryless sources and single-letter distortion measures we compute the minimal description rate as a function of the joint law of the source and side-information and of the allowed distortions at the encoder and decoder. We also treat memoryless Gaussian sources with mean squared-error distortion measures.

I. PROBLEM STATEMENT

Inspired by Steinberg [1], we study a variation on the Wyner-Ziv source coding problem [2]. What makes our problem different from the Wyner-Ziv problem is that we impose the additional requirement that the encoder reproduce the decoder's reconstruction with some prespecified precision. This additional requirement limits the extent to which the decoder's reconstruction can depend on the side-information, which is not available to the encoder.

Our setting is specified by a tuple

$$(\mathcal{X}, \mathcal{Y}, \hat{\mathcal{X}}, P_{XY}, d_d, d_e, D_d, D_e),$$

which we explain next. The set \mathcal{X} is the source alphabet, the set \mathcal{Y} is the side-information alphabet, and the set $\hat{\mathcal{X}}$ is the reconstruction alphabet. All are assumed to be finite except in our treatment of Gaussian sources where they are all equal to the set of real numbers \mathbb{R} . The source and side-information sequence $\{(X_i, Y_i)\}_{i=1}^n$ is assumed to be drawn IID according to the joint law P_{XY} on $\mathcal{X} \times \mathcal{Y}$. The source sequence $X^n = (X_1, \dots, X_n)$ is observed only at the encoder, and the side-information $Y^n = (Y_1, \dots, Y_n)$ only at the decoder. We also specify two single-letter distortion functions $d_d: \mathcal{X} \times \hat{\mathcal{X}} \rightarrow \mathbb{R}^+$ and $d_e: \hat{\mathcal{X}} \times \hat{\mathcal{X}} \rightarrow \mathbb{R}^+$. The former is used to measure the fidelity of the reconstruction at the decoder, and the latter to measure the fidelity with which the encoder estimates the decoder's reconstruction sequence. The allowed distortions are $D_d \geq 0$ and $D_e \geq 0$.

To describe the source sequence X^n , the encoder produces the index

$$M = f^{(n)}(X^n) \quad (1)$$

where $f^{(n)}: \mathcal{X}^n \rightarrow \mathcal{M}$ is the encoding function and $\mathcal{M} \triangleq \{1, \dots, M\}$. The index M is conveyed to the decoder who

uses it and the side-information Y^n to form the decoder's reconstruction sequence

$$\hat{X}_d^n = \phi^{(n)}(M, Y^n) \quad (2)$$

where $\phi^{(n)}: \mathcal{M} \times \mathcal{Y}^n \rightarrow \hat{\mathcal{X}}^n$ is the decoder's reconstruction function. The encoder's estimate of the decoder's reconstruction sequence is

$$\hat{X}_e^n = \psi^{(n)}(X^n) \quad (3)$$

for some $\psi^{(n)}: \mathcal{X}^n \rightarrow \hat{\mathcal{X}}^n$.

We call a triple of functions $(f^{(n)}, \phi^{(n)}, \psi^{(n)})$ as above an (n, R, D_d, D_e) -code if $M \leq 2^{nR}$ and the produced sequences $\hat{X}_d^n = (\hat{X}_{d,1}, \dots, \hat{X}_{d,n})$ and $\hat{X}_e^n = (\hat{X}_{e,1}, \dots, \hat{X}_{e,n})$ satisfy:

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E}[d_d(X_i, \hat{X}_{d,i})] \leq D_d \quad (4)$$

$$\frac{1}{n} \sum_{i=1}^n \mathbb{E}[d_e(\hat{X}_{d,i}, \hat{X}_{e,i})] \leq D_e. \quad (5)$$

The nonnegative triple (R, D_d, D_e) is *achievable* if for every $\epsilon > 0$ and sufficiently large n there exists an $(n, R + \epsilon, D_d + \epsilon, D_e + \epsilon)$ -code. The set of achievable (R, D_d, D_e) triples is denoted by \mathcal{R} , and the *rate-distortions function* by

$$R(D_d, D_e) \triangleq \min_{(R, D_d, D_e) \in \mathcal{R}} R. \quad (6)$$

The region $\mathcal{R} \subseteq \mathbb{R}^3$ is closed, and thus the indicated minimum exists. Fig. 1 shows a model of our problem.

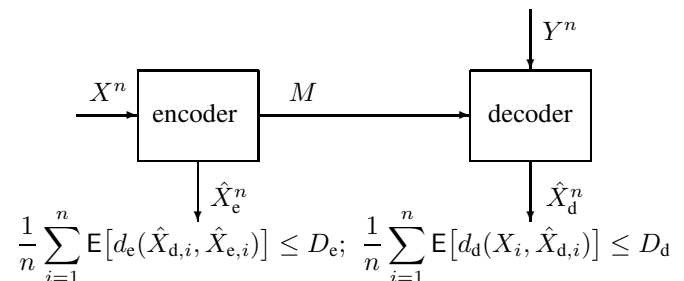


Fig. 1. Constrained Wyner-Ziv coding.

Remark 1: Our setup differs from the Wyner-Ziv setup [2] only in the additional constraint (5). When d_e is the Hamming distance and $D_e = 0$ our setup is nearly identical to that of Steinberg's [1].

II. RESULTS

In our first result the sets $\mathcal{X}, \mathcal{Y}, \hat{\mathcal{X}}$ are assumed to be finite.
Theorem 1: For finite sets $\mathcal{X}, \mathcal{Y}, \hat{\mathcal{X}}$:

$$R(D_d, D_e) = \min_{Z, \phi, \psi} (I(X; Z) - I(Y; Z)) \quad (7)$$

where $(X, Y) \sim P_{XY}$, and where the minimization is over a discrete random variable Z taking value in an auxiliary alphabet \mathcal{Z} of size at most $|\mathcal{X}| + 3$ and forming the Markov chain

$$Z \text{---} \circ \text{---} X \text{---} \circ \text{---} Y \quad (8)$$

and over the functions $\phi: \mathcal{Y} \times \mathcal{Z} \rightarrow \hat{\mathcal{X}}$ and $\psi: \mathcal{X} \times \mathcal{Z} \rightarrow \hat{\mathcal{X}}$ satisfying

$$\mathbb{E}[d_d(X, \phi(Y, Z))] \leq D_d \quad (9)$$

$$\mathbb{E}[d_e(\phi(Y, Z), \psi(X, Z))] \leq D_e. \quad (10)$$

Proof: See Section III. ■

Remark 2: If $d_e(\cdot, \cdot)$ is the Hamming distance, then for all $D_d \geq 0$, $R(D_d, 0)$ coincides with Steinberg's common-reconstruction rate-distortion function $R_{\text{cr}}(D_d)$ [1].

Proof: Omitted. ■

In our second result we consider the Gaussian case with quadratic distortion measures. We assume that $\mathcal{X}, \mathcal{Y}, \hat{\mathcal{X}}$ are the reals; d_d and d_e are quadratic distortions

$$d_d(x, \hat{x}_d) = (x - \hat{x}_d)^2, \quad (11)$$

$$d_e(\hat{x}_d, \hat{x}_e) = (\hat{x}_d - \hat{x}_e)^2; \quad (12)$$

and P_{XY} is the law of a centered bivariate Gaussian (X, Y) , where X is of variance σ_X^2 and $Y = X + U$ for U independent of X and of variance σ_U^2 .

Theorem 2: For the Gaussian setup with quadratic distortion measures:

- If $\sqrt{D_e \sigma_U^2} \geq \min \left\{ D_d, \frac{\sigma_X^2 \sigma_U^2}{\sigma_X^2 + \sigma_U^2} \right\}$, then

$$R(D_d, D_e) = \max \left\{ 0, \frac{1}{2} \log \left(\frac{\sigma_X^2 \sigma_U^2}{(\sigma_X^2 + \sigma_U^2) D_d} \right) \right\}.$$

- If $\sqrt{D_e \sigma_U^2} < \min \left\{ D_d, \frac{\sigma_X^2 \sigma_U^2}{\sigma_X^2 + \sigma_U^2} \right\}$, then

$$R(D_d, D_e) = \max \left\{ 0, \frac{1}{2} \log \left(\frac{\sigma_X^2 \sigma_U^2 + D_d - 2\sqrt{\sigma_U^2 D_e}}{D_d - D_e} \right) \right\}.$$

Proof: See Section IV. ■

Remark 3: If

$$\sqrt{D_e \sigma_U^2} \geq \min \left\{ D_d, \frac{\sigma_X^2 \sigma_U^2}{\sigma_X^2 + \sigma_U^2} \right\} \quad (13)$$

or

$$\left(1 - \sqrt{\frac{D_e}{\sigma_U^2}} \right)^2 \sigma_X^2 \leq D_d - D_e \quad (14)$$

then our result coincides with Wyner and Ziv's [2]: in this case removing Constraint (5) or revealing the side-information also to the encoder do not decrease the rate-distortion function.

Our results can be extended to a scenario where the encoder observes not only the source sequence $\{X_i\}$ but also some

sequence $\{W_i\}$ which is correlated with the decoder's side-information sequence $\{Y_i\}$. This additional sequence $\{W_i\}$ makes it easier for the encoder to estimate the decoder's reconstruction sequence and thus allows the decoder to rely more heavily on its side information $\{Y_i\}$. To see how this seemingly more general scenario reduces to our scenario assume that $\{(X_i, W_i, Y_i)\}_{i=1}^n$ are IID random triples of law P_{XWY} and that W_i takes value in the finite set \mathcal{W} . Consider now a new IID source $\{\tilde{X}_i\}$ taking value in the set $\tilde{\mathcal{X}} = \mathcal{X} \times \mathcal{W}$ according to the law P_{XW} with $\tilde{X}_i = (X_i, W_i)$. The encoder now observes the source sequence $\{\tilde{X}_i\}$ only and no additional sequences. The decoder side information is still $\{Y_i\}$, and the joint law of \tilde{X}_i, Y_i is P_{XWY} . Finally define the new decoder distortion function $\tilde{d}_d: \tilde{\mathcal{X}} \times \hat{\mathcal{X}} \rightarrow \mathbb{R}^+$ as

$$\tilde{d}_d((X_i, W_i), \hat{X}_i) = d_d(X_i, \hat{X}_i).$$

Solving the original scenario for this new source and new decoder distortion function is equivalent to solving the seemingly more general problem we described.

III. PROOF OF THEOREM 1

The proof of the achievability part of Theorem 1 is based on random coding and binning [3], [4, Chapter 12.3] and is omitted.

We next sketch the converse. To this end, we define the *information rate-distortions function* $R^*(D_d, D_e)$ as the right-hand side of (7). It satisfies the following lemma.

Lemma 1 (Monotonicity and Convexity of $R^(D_d, D_e)$):*

The function $R^*(D_d, D_e)$ is nondecreasing in both distortions, i.e.,

$$R^*(D'_d, D'_e) \leq R^*(D_d, D_e), \quad (D'_d \geq D_d \geq 0, \quad D'_e \geq D_e \geq 0). \quad (15)$$

It is also convex, i.e., for nonnegative distortion pairs $(D_d^{(1)}, D_e^{(1)})$ and $(D_d^{(2)}, D_e^{(2)})$ and any $\lambda \in [0, 1]$

$$R^*(\lambda D_d^{(1)} + (1 - \lambda) D_d^{(2)}, \lambda D_e^{(1)} + (1 - \lambda) D_e^{(2)}) \leq \lambda R^*(D_d^{(1)}, D_e^{(1)}) + (1 - \lambda) R^*(D_d^{(2)}, D_e^{(2)}). \quad (16)$$

Proof: Omitted. ■

To prove the converse, it suffices that we show that if a triple (R, D_d, D_e) is achievable, then for every $\epsilon > 0$

$$R + \epsilon \geq R^*(D_d + \epsilon, D_e + \epsilon). \quad (17)$$

Indeed, by letting ϵ tend to zero and using the continuity of $R^*(D_d, D_e)$, this implies that $R \geq R^*(D_d, D_e)$ whenever (R, D_d, D_e) is achievable, and consequently that $R(D_d, D_e) \geq R^*(D_d, D_e)$.

The first part of our proof follows the steps in [4]. For a

given $(n, R + \epsilon, D_d + \epsilon, D_e + \epsilon)$ -code, we have

$$\begin{aligned} n(R + \epsilon) & \stackrel{(a)}{\geq} H(M) \end{aligned} \quad (18)$$

$$\stackrel{(b)}{\geq} I(X^n; M|Y^n) \quad (19)$$

$$\stackrel{(c)}{=} \sum_{i=1}^n I(X_i; M|Y^n, X^{i-1}) \quad (20)$$

$$= \sum_{i=1}^n H(X_i|Y^n, X^{i-1}) - H(X_i|M, Y^n, X^{i-1}) \quad (21)$$

$$\stackrel{(d)}{=} \sum_{i=1}^n H(X_i|Y_i) - H(X_i|M, Y^n, X^{i-1}) \quad (22)$$

$$\stackrel{(e)}{\geq} \sum_{i=1}^n H(X_i|Y_i) - H(X_i|M, Y^n) \quad (23)$$

$$\stackrel{(f)}{=} \sum_{i=1}^n H(X_i|Y_i) - H(X_i|Z_i, Y_i) \quad (24)$$

$$= \sum_{i=1}^n I(X_i; Z_i|Y_i) \quad (25)$$

$$\stackrel{(g)}{=} \sum_{i=1}^n H(Z_i|Y_i) - H(Z_i|X_i) \quad (26)$$

$$= \sum_{i=1}^n I(X_i; Z_i) - I(Y_i; Z_i), \quad (27)$$

where (a) follows because $M \leq 2^{n(R+\epsilon)}$; (b) follows because conditioning cannot increase entropy and because $H(M|Y^n, X^n) \geq 0$; (c) follows from the chain rule for mutual information; (d) follows because X_i is independent of the past and future Y 's and X 's given Y_i ; (e) follows from the fact that conditioning cannot increase entropy; (f) follows by defining

$$Z_i \triangleq (M, Y^{i-1}, Y_{i+1}^n); \quad (28)$$

and (g) follows because

$$Z_i \text{---} X_i \text{---} Y_i \quad (29)$$

forms a Markov chain.

We define $\phi_i^{(n)}$ to be the function that maps (M, Y^n) to the i -th symbol of $\phi^{(n)}(M, Y^n)$ and $\psi_i^{(n)}$ to be the function that maps X^n to the i -th symbol of $\psi^{(n)}(X^n)$. We then notice that by the definition of Z_i :

$$\phi_i(Y_i, Z_i) \triangleq \phi_i^{(n)}(M, Y^n), \quad (30)$$

for some function ϕ_i with arguments in the respective domains. We now define

$$D_{d,i} \triangleq \mathbb{E}[d_d(X_i, \phi_i^{(n)}(M, Y^n))], \quad (31)$$

where $\mathbb{E}[\cdot]$ is with respect to P_{X^n, Y^n} . By definitions (30) and (31), we have

$$\mathbb{E}[d_d(X_i, \phi_i(Y_i, Z_i))] = D_{d,i}, \quad (32)$$

where $\mathbb{E}[\cdot]$ is with respect to $P_{X_i, Y_i} P_{Z_i|X_i}$.

For the encoder-side distortion, we next argue that there exists a deterministic function $\psi_i: \mathcal{X} \times \mathcal{Z} \rightarrow \hat{\mathcal{X}}$ that achieves a distortion no larger than $\psi_i^{(n)}(X^n)$. To this end we define

$$D_{e,i} \triangleq \mathbb{E}[d_e(\phi_i^{(n)}(M, Y^n), \psi_i^{(n)}(X^n))], \quad (33)$$

where the expectation is with respect to P_{X^n, Y^n} . We then express $D_{e,i}$ as

$$\begin{aligned} D_{e,i} & = \mathbb{E}_{X^n, Y_i, Z_i} [d_e(\phi_i(Y_i, Z_i), \psi_i^{(n)}(X^n))] \end{aligned} \quad (34)$$

$$= \mathbb{E}_{X^n, Z_i} \mathbb{E}_{Y_i|X^n, Z_i} [d_e(\phi_i(Y_i, Z_i), \psi_i^{(n)}(X^n))] \quad (35)$$

$$= \mathbb{E}_{X^n, Z_i} \mathbb{E}_{Y_i|X_i, X_{\setminus i}, Z_i} [d_e(\phi_i(Y_i, Z_i), \psi_i^{(n)}(X_i, X_{\setminus i}))], \quad (36)$$

where $X_{\setminus i} \triangleq (X^{i-1}, X_{i+1}^n)$. For every $(x_i, z_i) \in \mathcal{X} \times \mathcal{Z}$, we define $x_{\setminus i}^*(x_i, z_i)$ (or for short $x_{\setminus i}^*$) as:¹

$$\begin{aligned} x_{\setminus i}^*(x_i, z_i) & \triangleq \arg \min_{x_{\setminus i} \in \mathcal{X}^{n-1}} \\ & \mathbb{E}_{Y_i|X_i=x_i, X_{\setminus i}=x_{\setminus i}, Z_i=z_i} [d_e(\phi_i(Y_i, z_i), \psi_i^{(n)}(x_i, x_{\setminus i}))] \end{aligned} \quad (37)$$

or in any other way that guarantees

$$\begin{aligned} & \mathbb{E}_{X_{\setminus i}|X_i=x_i, Z_i=z_i} \mathbb{E}_{Y_i|X_i=x_i, X_{\setminus i}, Z_i=z_i} \\ & [d_e(\phi_i(Y_i, z_i), \psi_i^{(n)}(x_i, X_{\setminus i}))] \\ & \geq \mathbb{E}_{Y_i|X_i=x_i, X_{\setminus i}=x_{\setminus i}^*, Z_i=z_i} [d_e(\phi_i(Y_i, z_i), \psi_i^{(n)}(x_i, x_{\setminus i}^*))] \end{aligned} \quad (38)$$

We can now define the function ψ_i as

$$\psi_i: \mathcal{X} \times \mathcal{Z} \rightarrow \hat{\mathcal{X}} \quad (39a)$$

$$(x_i, z_i) \mapsto \psi_i^{(n)}(x_i, x_{\setminus i}^*(x_i, z_i)). \quad (39b)$$

For every $(x_i, x_{\setminus i}, z_i) \in \mathcal{X}^n \times \mathcal{Z}$, we have

$$\begin{aligned} & \mathbb{E}_{Y_i|X_i=x_i, X_{\setminus i}=x_{\setminus i}, Z_i=z_i} [d_e(\phi_i(Y_i, z_i), \psi_i^{(n)}(x_i, x_{\setminus i}))] \\ & \stackrel{(a)}{\geq} \mathbb{E}_{Y_i|X_i=x_i, X_{\setminus i}=x_{\setminus i}^*, Z_i=z_i} [d_e(\phi_i(Y_i, z_i), \psi_i^{(n)}(x_i, x_{\setminus i}^*))] \end{aligned} \quad (40)$$

$$\stackrel{(b)}{=} \mathbb{E}_{Y_i|X_i=x_i, Z_i=z_i} [d_e(\phi_i(Y_i, z_i), \psi_i^{(n)}(x_i, x_{\setminus i}^*))] \quad (41)$$

$$\stackrel{(c)}{=} \mathbb{E}_{Y_i|X_i=x_i, Z_i=z_i} [d_e(\phi_i(Y_i, z_i), \psi_i(x_i, z_i))], \quad (42)$$

where: (a) follows from the definition of $x_{\setminus i}^*$; (b) follows from the fact that

$$X_{\setminus i} \text{---} (X_i, Z_i) \text{---} Y_i \quad (43)$$

forms a Markov chain; and (c) follows from the definition of ψ_i .

It now follows from (36) and (42) that

$$\mathbb{E}_{X_i, Y_i, Z_i} [d_e(\phi_i(Y_i, Z_i), \psi_i(X_i, Z_i))] \leq D_{e,i}. \quad (44)$$

¹If $\arg \min$ is not unique, $x_{\setminus i}^*(x_i, z_i)$ is defined as the first in lexicological order.

We can now continue from (27):

$$\sum_{i=1}^n I(X_i; Z_i) - I(Y_i; Z_i) \stackrel{(a)}{\geq} \sum_{i=1}^n R^*(D_{d,i}, D_{e,i}) \quad (45)$$

$$\stackrel{(b)}{=} n \frac{1}{n} \sum_{i=1}^n R^*(D_{d,i}, D_{e,i}) \quad (46)$$

$$\stackrel{(c)}{\geq} n R^*\left(\frac{1}{n} \sum_{i=1}^n D_{d,i}, \frac{1}{n} \sum_{i=1}^n D_{e,i}\right) \quad (47)$$

$$\stackrel{(d)}{\geq} n R^*(D_d + \epsilon, D_e + \epsilon) \quad (48)$$

where: (a) follows from the definition of $R^*(D_d, D_e)$ and from (29), (32), and (44); (b) follows by multiplying by 1; (c) follows from Lemma 1 and Jensen's inequality; and (d) follows from the monotonicity of $R^*(D_d, D_e)$ (Lemma 1) and the fact that for a $(n, R+\epsilon, D_d+\epsilon, D_e+\epsilon)$ -code $D_d+\epsilon \geq \frac{1}{n} \sum_{i=1}^n D_{d,i}$ and $D_e+\epsilon \geq \frac{1}{n} \sum_{i=1}^n D_{e,i}$. Inequality (48) combines with (27) to establish (17).

The proof of the cardinality bound for the auxiliary alphabet and the justification of the *minimum* (as opposed to an *infimum*) are omitted. They are similar to the proofs in [2].

IV. PROOF OF THEOREM 2

Recall that in this section we assume that d_d and d_e are the quadratic distortion measures (11) and (12), and we assume that $Y = X + U$, where X and U are independent zero-mean Gaussians of variances σ_X^2 and σ_U^2 .

The achievability part of Theorem 2 can be proved using geometric arguments related to random coding over n -spheres. The details are omitted.

We focus on the converse. For $\sqrt{D_e \sigma_U^2} \geq \min\left\{D_d, \frac{\sigma_X^2 \sigma_U^2}{\sigma_X^2 + \sigma_U^2}\right\}$, the converse follows directly from Remark 1 and the Wyner-Ziv result [2], because adding Constraint (5) cannot decrease the rate-distortion function.

We also note that by definition $R(D_d, D_e)$ is nonnegative for all $D_d, D_e \geq 0$. Thus, to establish the converse for the case

$$\sqrt{D_e \sigma_U^2} < \min\left\{D_d, \frac{\sigma_X^2 \sigma_U^2}{\sigma_X^2 + \sigma_U^2}\right\} \quad (49)$$

it suffices to prove that in this case

$$R(D_d, D_e) \geq \frac{1}{2} \log \left(\frac{\sigma_X^2}{\sigma_X^2 + \sigma_U^2} \frac{\sigma_U^2 + D_d - 2\sqrt{\sigma_U^2 D_e}}{D_d - D_e} \right). \quad (50)$$

To this end, we define the *continuous information rate-distortions function* $R_{\text{cnt}}^*(D_d, D_e)$ like $R^*(D_d, D_e)$, except that the minimum is replaced by an infimum and the size of the auxiliary alphabet \mathcal{Z} can be unbounded. Thus, if we introduce $\hat{X}_d \triangleq \phi(Y, Z)$ and $\hat{X}_e \triangleq \psi(X, Z)$, then

$$R_{\text{cnt}}^*(D_d, D_e) \triangleq \inf_{Z, \hat{X}_d, \hat{X}_e} I(X; Z|Y) \quad (51)$$

where the infimum is over all choices of the random variables Z, \hat{X}_d, \hat{X}_e satisfying

$$E[(X - \hat{X}_d)^2] \leq D_d, \quad (52a)$$

$$E[(\hat{X}_d - \hat{X}_e)^2] \leq D_e, \quad (52b)$$

$$Z \text{---} X \text{---} Y, \quad (52c)$$

$$\hat{X}_d = \phi(Y, Z), \quad (52d)$$

$$\hat{X}_e = \psi(X, Z). \quad (52e)$$

Following the proof of the converse in Theorem 1, it is not difficult to show that no rate below $R_{\text{cnt}}^*(D_d, D_e)$ is achievable. This is the content of the following lemma whose proof is omitted

Lemma 2: For every $D_d, D_e \geq 0$

$$R(D_d, D_e) \geq R_{\text{cnt}}^*(D_d, D_e). \quad (53)$$

It remains to show that if (49) holds then $R_{\text{cnt}}^*(D_d, D_e)$ cannot be smaller than the right hand side of (50). This is the content of the following lemma.

Lemma 3: For all $D_d, D_e \geq 0$ satisfying (49)

$$R_{\text{cnt}}^*(D_d, D_e) \geq \frac{1}{2} \log \left(\frac{\sigma_X^2}{\sigma_X^2 + \sigma_U^2} \frac{\sigma_U^2 + D_d - 2\sqrt{\sigma_U^2 D_e}}{D_d - D_e} \right). \quad (54)$$

Proof: We first notice that

$$\begin{aligned} I(X; Z|Y) &= h(X|Y) - h(X|Y, Z) \\ &= \frac{1}{2} \log \left(2\pi e \frac{\sigma_X^2 \sigma_U^2}{\sigma_X^2 + \sigma_U^2} \right) - h(X|Y, Z). \end{aligned} \quad (55)$$

Showing (54) is thus equivalent to showing

$$\Omega \leq \frac{1}{2} \log \left(2\pi e \sigma_U^2 \frac{D_d - D_e}{\sigma_U^2 + D_d - 2\sqrt{\sigma_U^2 D_e}} \right), \quad (56)$$

where

$$\Omega \triangleq \sup_{Z, \hat{X}_d, \hat{X}_e} h(X|Y, Z) \quad (57)$$

and where the supremum is over all choices of Z, \hat{X}_d, \hat{X}_e satisfying (52).

Define a second optimization problem:

$$\Gamma \triangleq \sup h(X - \hat{X}_d | X - \hat{X}_d + U) \quad (58)$$

where the supremum is over all choices of \hat{X}_d satisfying

$$\text{Var}(X - \hat{X}_d) \leq D_d, \quad (59a)$$

$$\left(\text{Cov}(X - \hat{X}_d, U) \right)^2 \leq D_e \sigma_U^2. \quad (59b)$$

In the following we will show that

$$\Omega \leq \Gamma \quad (60)$$

and that for all $D_d, D_e \geq 0$ satisfying (49)

$$\Gamma = \frac{1}{2} \log \left(2\pi e \sigma_U^2 \frac{D_d - D_e}{\sigma_U^2 + D_d - 2\sqrt{\sigma_U^2 D_e}} \right). \quad (61)$$

This will establish (56) and conclude the proof of the lemma.

Inequality (60) is established by showing that for every choice of Z, \hat{X}_d, \hat{X}_e satisfying (52) the following two statements hold.

- 1) the objective function of the optimization problem in (57) defining Ω is upper bounded by the objective function of the optimization problem in (61) defining Γ :

$$h(X|Y, Z) \leq h(X - \hat{X}_d|X - \hat{X}_d + U). \quad (62)$$

- 2) Constraints (52) imply Constraints (59).

To prove the first statement we note that for all Z, \hat{X}_d, \hat{X}_e satisfying (52c)–(52e), Inequality (62) holds because:

$$h(X|Y, Z) = h(X - \hat{X}_d|Y, Z) \quad (63)$$

$$= h(X - \hat{X}_d|Y, Z, \hat{X}_d) \quad (64)$$

$$= h(X - \hat{X}_d|X + U, Z, \hat{X}_d) \quad (65)$$

$$= h(X - \hat{X}_d|X - \hat{X}_d + U, Z, \hat{X}_d) \quad (66)$$

$$\leq h(X - \hat{X}_d|X - \hat{X}_d + U). \quad (67)$$

We next prove the second statement. Constraint (59a) follows from (52a), and Constraint (59b) is proved as follows. We notice that by the Markov chain (52c), by the fact that $Y = X + U$, and by the fact that U is independent of X , it follows that the pair (X, Z) is independent of U . By (52e), this implies that also \hat{X}_e is independent of U and therefore

$$\text{Cov}(\hat{X}_d - \hat{X}_e, U) = -\text{Cov}(X - \hat{X}_d, U). \quad (68)$$

Since the magnitude of the correlation coefficient cannot exceed 1, it follows from (52b) that

$$|\text{Cov}(\hat{X}_d - \hat{X}_e, U)|^2 \leq D_e \sigma_U^2, \quad (69)$$

which combined with (68) implies the desired constraint (59b).

Having established the two statements and hence (60), we next prove (61) under the assumption that $D_d, D_e \geq 0$ satisfy (49). Notice that (49) implies:

$$D_e < \min\{\sigma_U^2, D_d\}. \quad (70)$$

From the conditional max-entropy theorem [5] it follows that when solving the optimization problem in (58) we can restrict attention to $X - \hat{X}_d$ jointly Gaussian with U . To simplify notation we introduce $A \triangleq X - \hat{X}_d$, and we denote its variance by $\sigma_A^2 \triangleq \text{Var}(A)$ and its covariance with U by $\kappa_{AU} \triangleq \text{Cov}(A, U)$. We notice that $A = -U$ is not a valid choice in our optimization problem, because this choice would imply $|\kappa_{AU}|^2 = \sigma_U^4$, which, by (70), violates (59b). For all other choices of A (jointly Gaussian with U), the conditional differential entropy $h(A|A + U)$ can be written as

$$h(A|A + U) = \frac{1}{2} \log \left(2\pi e \frac{\sigma_A^2 \sigma_U^2 - \kappa_{AU}^2}{\sigma_A^2 + \sigma_U^2 + 2\kappa_{AU}} \right) \quad (71)$$

$$= \frac{1}{2} \log \left(2\pi e \left(\sigma_U^2 - \frac{(\sigma_U^2 + \kappa_{AU})^2}{\sigma_A^2 + \sigma_U^2 + 2\kappa_{AU}} \right) \right) \quad (72)$$

$$= \frac{1}{2} \log \left(2\pi e \frac{\sigma_A^2 \sigma_U^2 - \kappa_{AU}^2}{\sigma_A^2 + \sigma_U^2 + 2\kappa_{AU}} \right). \quad (73)$$

Therefore, we can rewrite the optimization problem in (58) as

$$\Gamma = \sup_{\kappa_{AU}, \sigma_A^2} \frac{1}{2} \log \left(2\pi e \frac{\sigma_A^2 \sigma_U^2 - \kappa_{AU}^2}{\sigma_A^2 + \sigma_U^2 + 2\kappa_{AU}} \right) \quad (74)$$

subject to

$$0 \leq \sigma_A^2 \leq D_d, \quad (75)$$

$$0 \leq |\kappa_{AU}|^2 \leq D_e \sigma_U^2 \quad (76)$$

$$0 \leq |\kappa_{AU}|^2 \leq \sigma_A^2 \sigma_U^2. \quad (77)$$

(We have to add the last constraint because a correlation coefficient has absolute value not exceeding 1.) For fixed κ_{AU} , the objective function in (74) is increasing in σ_A^2 (see Equality (72)), and so is the right-hand side of Constraint (77). Therefore, without loss of optimality we can choose

$$\sigma_A^2 = D_d. \quad (78)$$

We substitute (78) into (74) and (77), and obtain:

$$\Gamma = \sup_{\kappa_{AU}} \frac{1}{2} \log \left(2\pi e \frac{D_d \sigma_U^2 - \kappa_{AU}^2}{D_d + \sigma_U^2 + 2\kappa_{AU}} \right) \quad (79)$$

subject to (76) and

$$0 \leq |\kappa_{AU}|^2 \leq D_d \sigma_U^2. \quad (80)$$

In view of (70) and (76), Constraint (80) is redundant, and hence ignored in the following.

We compute the derivative of the objective function in (79) with respect to κ_{AU} :

$$\begin{aligned} \frac{d}{d\kappa_{AU}} \left(\frac{1}{2} \log \left(2\pi e \frac{D_d \sigma_U^2 - \kappa_{AU}^2}{D_d + \sigma_U^2 + 2\kappa_{AU}} \right) \right) \\ = \frac{-(D_d + \kappa_{AU})(\sigma_U^2 + \kappa_{AU})}{(D_d + \sigma_U^2 + 2\kappa_{AU})(D_d \sigma_U^2 - \kappa_{AU}^2)}. \end{aligned} \quad (81)$$

Inequalities (70) and (76) imply that $|\kappa_{AU}| < \min\{D_d, \sigma_U^2\}$, and therefore, when (70) holds, the derivative in (81) is finite and negative for all κ_{AU} satisfying (76). Hence, the objective function in (79) is decreasing on the interval of interest, and in the optimization problem in (79) subject to (76) it is optimal to choose

$$\kappa_{AU} = -\sqrt{D_e \sigma_U^2}. \quad (82)$$

Plugging (82) into the objective function in (79) results in the right-hand side of (61), which concludes the proof of (61) and of the lemma. ■

REFERENCES

- [1] Y. Steinberg, "Coding and common reconstruction," *IEEE Transactions on Information Theory*, vol. 55, no. 11, pp. 4995–5010, 2009.
- [2] A. Wyner and J. Ziv, "The rate-distortion function for source coding with side information at the decoder," *IEEE Transactions on Information Theory*, vol. 22, no. 1, pp. 1–10, 1976.
- [3] T. Cover, "A proof of the data compression theorem of Slepian and Wolf for ergodic sources (Corresp.)," *IEEE Transactions on Information Theory*, vol. 21, no. 2, pp. 226–228, 1975.
- [4] A. E. Gamal and Y.-H. Kim, "Lecture notes on network information theory," 2009, available online: <http://arxiv.org/abs/1001.3404>.
- [5] J. Thomas, "Feedback can at most double Gaussian multiple access channel capacity (Corresp.)," *IEEE Transactions on Information Theory*, vol. 33, no. 5, pp. 711–716, 1987.