Discriminatory Lossy Source Coding: Side Information Privacy

Ravi Tandon, Lalitha Sankar, H. Vincent Poor
Dept. of Electrical Engineering,
Princeton University, Princeton, NJ 08544.
{rtandon,lalitha,poor}@princeton.edu

***Abstract*—The Heegard-Berger problem models a situation in which encoding at a source has to account for two decoders, one with and one without correlated side information when the same information is not available at the encoder. The Heegard-Berger encoding scheme is proved to be rate-optimal even when an additional constraint on the privacy of side information is imposed at the uninformed decoder. The results are illustrated for a binary source with erasure side information and Hamming distortion, a result that is also of independent interest.**

I. Introduction

Information sources often need to be made accessible to multiple legitimate users simultaneously, some of whom can have correlated side information obtained from other sources or from prior interactions. A natural question that arises in this context is the following: can the source publish (encode) its data in a discriminatory manner such that the uninformed user does not infer the side information, i.e., it is kept private, while providing utility (fidelity) to both users?

This question was addressed from strictly a fidelity viewpoint by C. Heegard and T. Berger in [1], henceforth referred to as the Heegard-Berger (HB) problem, in which they determined the minimal rate at which an information source (encoder), assumed to be discrete and memoryless, can be revealed to two users (decoders) with, in general, different fidelity (distortion) requirements when only one of the decoders has access to correlated side information whose statistics are assumed to be known at all terminals. Using equivocation as the privacy metric, we address the question posed above using the source network model as in [1] with an additional constraint on the side information privacy at the uninformed decoder, i.e., decoder 1 (see Fig. 1).

We prove here that the encoding for the HB problem achieves the minimal rate while guaranteeing the maximal equivocation for any feasible distortion pair at the two decoders. The HB coding scheme involves a combination of a rate-distortion codeword and a conditional Wyner-Ziv code which is revealed to both the decoders. Our proof exploits the fact that conditioned on what is decodable by decoder 1, i.e., the rate-distortion code, the additional information intended for decoder 2, i.e. the conditional Wyner-Ziv bin index, is asymptotically independent of its side information, Y (see Fig. 1). Observing that the generation of the conditional Wyner-Ziv bin index is analogous to the Slepian-Wolf (SW) binning scheme, we first prove this independence property for SW encoding (in Lemma 1). Next, we prove a similar independence property for the HB coding scheme, which in turn allows us to demonstrate the optimality of this scheme. We illustrate our results for the case in which X is a binary symmetric source and the side information Y is an erased version of X with erasure probability p. For this source pair, we explicitly characterize the rate-distortion-equivocation tradeoff and show that maximal equivocation is independent of the fidelity requirement D_2 at decoder 2.

The research was supported in part by the Air Force Office of Scientific Research MURI Grant FA-9550-09-1-0643, and by the National Science Foundation Grants CNS-09-05398 and CCF-10-16671.

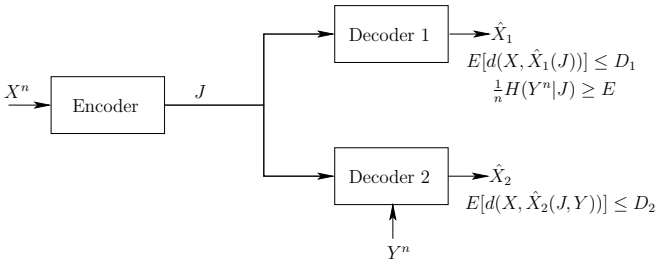

Fig. 1. Source network model.

The problem of source coding with equivocation constraints has gained attention recently [2]–[8]. In contrast to these papers in which the focus is on an external eavesdropper, we address the problem of privacy leakage to a legitimate user, i.e., we seek to understand whether the encoding at the source can discriminate between legitimate users with and without access to correlated side information. The paper is organized as follows. Following a description of the system model in Section II, we present our main results in Section III. In Section IV, we characterize the achievable rate-distortion-equivocation tradeoff for a specific source distribution and conclude in Section V.

II. System Model

We consider the following source network. An encoder observes and communicates a part X^n of a discrete, memoryless bivariate source, (X^n, Y^n) to decoders 1 and 2 at distortions D_1 and D_2, respectively, in which decoder 2 has access to

Y^n and an equivocation E about Y^n is required at decoder 1. The problem without the equivocation constraint at decoder 1 is the HB problem for which the set of feasible (R, D_1, D_2) tuples are characterized in [1]. We seek to characterize the set of all achievable (R, D_1, D_2, E) tuples.

Formally, let $(\mathcal{X}, \mathcal{Y}, p(x,y))$ denote the bivariate source with random variables $X \in \mathcal{X}$ and $Y \in \mathcal{Y}$. Furthermore, let $\hat{X}_k$, $k = 1, 2$, be a reconstruction alphabet and d_k:$\mathcal{X} \times \hat{\mathcal{X}} \to [0, \infty)$, $k = 1, 2$, be a distortion measure. An (n, M, D_1, D_2, E) code for this network consists of an encoding function $f : \mathcal{X}^n \to \mathcal{J} = \{1, \ldots, M\}$ and two decoding functions g_1:$\{1, \ldots, M\} \to \hat{\mathcal{X}}_1^n$ and g_2:$\{1, \ldots, M\} \times \mathcal{Y}^n \to \hat{\mathcal{X}}_2^n$. The expected distortion $D = (D_1, D_2)$ for the code is given by

$$D_k = \mathbb{E}\frac{1}{n}\sum_{i=1}^{n} d_k\left(X_i, \hat{X}_i\right), \ k = 1, 2, \tag{1}$$

where $\hat{X}_1 = g_1(f(X^n))$, $\hat{X}_2 = g_2(f(X^n), Y^n)$, and the equivocation rate E is given by

$$E = \frac{1}{n} H(Y^n|J), \ J \in \mathcal{J}. \tag{2}$$

Definition 1: The rate-distortion-equivocation tuple (R, D, E) is achievable for the above source network if there exists an $(n, M, D_1 + \epsilon, D_2 + \epsilon, E - \epsilon)$ code with $M \leq 2^{n(R+\epsilon)}$ for n sufficiently large. Let $\mathcal{R}^*$ denote the set of all achievable (R, D_1, D_2, E) such that the achievable distortion-equivocation region $\mathcal{R}^*_{D-E}$, the rate-distortion-equivocation function $R^*(D, E)$, and the equivocation-distortion function $\Gamma^*(D)$ are defined as

$$\mathcal{R}^*_{D-E} \equiv \{(D, E) : (R, D, E) \in \mathcal{R}^*_{RDE} \text{ for some } R \geq 0\}, \tag{3}$$

$$R^*(D, E) \equiv \min_{(R,D,E)\in\mathcal{R}^*_{RDE}} R, \ \Gamma^*(D) \equiv \max_{(D,E)\in\mathcal{R}^*_{D-E}} E. \tag{4}$$

III. Main Results

A. SW Coding: Independence of Bin Index and Side Information

In [9], a problem of losslessly communicating a sequence X^n of a bivariate source (X, Y) to a single decoder which has access to the Y^n sequences is studied. In the following lemma we address this SW problem and prove that the optimal encoding is such that the encoding index is asymptotically independent of the side information Y^n at the decoder.

Lemma 1: For a bivariate source (X, Y) where X^n is encoded via the encoding function f_{SW}:$\mathcal{X}^n \to J \in \{1, \ldots, M_J\}$ while Y^n is available at the decoder, $\lim_{n\to\infty} H(Y^n|J)/n = H(Y)$, i.e., $\lim_{n\to\infty} I(Y^n; J)/n \to 0$.

Proof: Let $T_A(n, \epsilon)$ denote the set of strongly typical A sequences of length n. We define a binary random variable μ as follows:

$$\mu(x^n, y^n) = \begin{cases} 0, & (x^n, y^n) \notin T_{XY}(n, \epsilon); \\ 1, & \text{otherwise.} \end{cases} \tag{5}$$

From the SW encoding, since a typical sequence x^n is assigned a bin (index) j at random, we have that

$$\Pr(J = j | X^n = x^n \in \mathcal{T}_X(n, \epsilon)) = 1/M_J \tag{6}$$

and

$$\Pr(J = j|\mu = 1) = \sum_{x^n} \Pr(x^n, J = j|\mu = 1) \in ((1-\epsilon)/M_j, 1/M_J) \tag{7}$$

where we have used the fact that for a typical set $\Pr(\mathcal{T}_{XY}(n, \epsilon)) \geq (1 - \epsilon)$ [10, chap. 2].

The conditional equivocation $H(Y^n|J)$ can be lower bounded as

$$\begin{aligned} H(Y^n|J) &\geq H(Y^n|J, \mu) && (8)\\ &= \Pr(\mu = 0) H(Y^n|J, \mu = 0) + \Pr(\mu = 1) H(Y^n|J, \mu = 1) \\ &\geq \Pr(\mu = 1) H(Y^n|J, \mu = 1) && (9)\\ &= \Pr(\mu = 1) \textstyle\sum_j \Pr(j|\mu = 1) H(Y^n|j, \mu = 1) && (10) \end{aligned}$$

where (8) follows from the fact that conditioning does not increase entropy, and (9) from the fact that the entropy is non-negative. The probability $\Pr(y^n|j, \mu = 1)$ can be written as

$$\begin{aligned} &\Pr(y^n|j, \mu = 1) \\ &= \sum_{x^n} \Pr(x^n|j, \mu = 1) \Pr(y^n|x^n, j, \mu = 1) && (11a)\\ &= \sum_{x^n} \frac{\Pr(x^n, j|\mu = 1)}{\Pr(j|\mu = 1)} \Pr(y^n|x^n, \mu = 1) && (11b)\\ &\leq 2^{n\epsilon'} \sum_{x^n} \frac{\Pr(x^n|\mu = 1)/M_J}{M_J} \Pr(y^n|x^n, \mu = 1) && (11c)\\ &= 2^{n\epsilon'} \Pr(y^n|\mu = 1) && (11d)\\ &\leq 2^{-n\left(H(Y) - \epsilon''\right)} && (11e) \end{aligned}$$

where (11a) follows from (6) and the fact that $Y^n - X^n - J$ forms a Markov chain (by construction), and (11c) follows from (7). Expanding $H(Y^n|j, \mu = 1)$, we have

$$\begin{aligned} H(Y^n|j, \mu = 1) &= \sum_{y^n} p(y^n|j, \mu = 1) \log \frac{1}{\Pr(y^n|j, \mu = 1)} && (12)\\ &\geq \sum_{y^n} p(y^n|j, \mu = 1) \log 2^{n\left(H(Y) - \epsilon''\right)} && (13)\\ &= n\left(H(Y) - \epsilon''\right) \sum_{y^n} p(y^n|j, \mu = 1) && (14)\\ &\geq n(1 - \epsilon)\left(H(Y) - \epsilon''\right) && (15) \end{aligned}$$

where (13) results from the upper bound on $\Pr(y^n|j, \mu = 1)$ in (11e) and (15) from the fact that for a typical set $\Pr(\mathcal{T}_{XY}(n, \epsilon)) \geq (1 - \epsilon)$ [10, chap. 2]. Thus, the equivocation $H(Y^n|J)$ can be lower bounded as

$$\begin{aligned} H(Y^n|J) &\geq \Pr(\mu = 1) \textstyle\sum_j \Pr(j|\mu = 1)(1 - \epsilon) n\left(H(Y) - \epsilon''\right) && (16)\\ &\geq n(1 - \epsilon)^3 \left(H(Y) - \epsilon''\right) && (17) \end{aligned}$$

where we have used (7) and the fact that for a typical set $\Pr(\mathcal{T}_{XY}(n,\epsilon)) \geq (1-\epsilon)$ [10, chap. 2]. The proof concludes by observing that $H(Y^n) \geq H(Y^n|J)$ and that $\epsilon \to 0$ and $\epsilon'' \to 0$ as $n \to \infty$. ∎

Remark 1: Lemma 1 captures the intuition that it suffices to encode only that part of X^n that is independent of the decoder side-information Y^n.

We now use Lemma 1 to demonstrate the optimality of the HB encoding for the source model studied here. Before doing so, we first present the rate-distortion-equivocation region for this model.

B. Rate-Distortion-Equivocation Region

Definition 2: For the two-source HB problem with additional equivocation constraints at the decoder, the functions $\Gamma(D)$ and $R(D,E)$ and the regions $\mathcal{R}_{D-E}$ and $\mathcal{R}$ are defined as

$$\Gamma(D) \equiv \sup H(Y|W_1) \tag{18}$$

$$R(D,E) \equiv \inf I(X;W_1) + I(X;W_2|W_1Y) \tag{19}$$

$$\mathcal{R}_{D-E} \equiv \{(D,E) : D_l \geq 0, l = 1,2, 0 \leq E \leq \Gamma(D)\} \tag{20}$$

$$\mathcal{R}_{RDE} \equiv \{(R,D,E) : (D,E) \in \mathcal{R}_{D-E}, R \geq R(D,E)\} \tag{21}$$

where the supremum and infimum are over sets $\mathcal{P}(D)$ and $\mathcal{P}(D,E)$, respectively such that $\mathcal{P}(D,E)$ is the set of all $p(x,y)p(w_1,w_2|x)$ such that (1) and (2) are satisfied, where W_1 and W_2 are auxiliary random variables, while $\mathcal{P}(D)$ is defined as $\mathcal{P}(D) \equiv \bigcup_{H(Y|W_1) \leq E \leq H(Y)} \mathcal{P}(D,E)$.

Lemma 2: $\Gamma(D)$ is a non-decreasing, concave function of $D \geq 0$ (i.e., $D_l \geq 0,\ l = 1,2$).

Theorem 1: For a bivariate source (X,Y) where X^n is available at the source, and Y^n is available at decoder 2 but not at decoder 1, we have

$$\mathcal{R}^*_{RDE} = \mathcal{R}_{RDE}, \quad \Gamma^*(D) = \Gamma(D), \tag{22}$$

$$\mathcal{R}^*_{D-E} = \mathcal{R}_{D-E}, \text{ and } \quad R^*(D,E) = R(D,E). \tag{23}$$

Remark 2: From (19), we have $R(D,E) = R_{HB}(D)$, i.e., the HB encoding scheme achieves the maximal privacy for a given distortion pair.

Proof: Converse: The lower bound on $R(D,E)$ follow directly from the converse for $R(D)$ in the HB problem and is omitted here in the interest of space. We now upper bound the maximum achievable equivocation as

$$\frac{1}{n}H(Y^n|J) = \sum_{i=1}^{n} \frac{1}{n} H\left(Y_i|Y^{i-1}J\right) \tag{24}$$

$$= \sum_{i=1}^{n} \frac{1}{n} H(Y_i|U_i) \tag{25}$$

$$\leq \Gamma(D) \tag{26}$$

where (25) follows from defining $W_{1,i} \equiv \left(J, Y^{i-1}\right)$ (see [1, sec. IV]) and (26) follows from the definition of $\Gamma(D)$ in (18) and its concavity property in Lemma 2.

Achievability: We briefly summarize the HB coding scheme [1]. Fix $p(w_1,w_2|x)$. First generate $M_1 = 2^{n(I(W_1;X)+\epsilon)}$, $W_1^n(j_1)$ sequences, $j_1 = 1,2,\ldots,M_1$, independently and identically distributed (i.i.d.) according to $p(w_1)$. For every $W_1^n(j_1)$ sequence, generate $M_2 = 2^{n(I(W_2;X|W_1)+\epsilon)}$ $W_2^n(j_2|j_1)$ sequences i.i.d. according to $p(w_2|w_1(j_1))$. Bin the resulting W_2^n sequences into S bins (analogously to the Wyner-Ziv binning), chosen at random where $S = 2^{n(I(X;W_2|W_1)-I(Y;W_2|W_1)+\epsilon)}$, and index these bins as $b(j_2)$. Upon observing a source sequence x^n, the encoder searches for a $W_1^n(j_1)$ sequence such that $(x^n, w_1^n(j_1)) \in \mathcal{T}_{XW_1}(n,\epsilon)$ (the choice of M_1 ensures that there exists at least one such j_1). Next, the encoder searches for a $w_2^n(j_2|j_1)$ such that $(x^n, w_1^n(j_1), w_2^n(j_2|j_1)) \in \mathcal{T}_{XW_1W_2}(n,\epsilon)$ (the choice of M_2 ensures that there exists at least one such j_2). The encoder sends $(j_1, b(j_2))$ where $b(j_2)$ is the bin index of the $w_2^n(j_2|j_1)$ sequence. Thus, we have that $(XW_1) - W_2 - B$ forms a Markov chain and

$$\Pr(B = b(j_2) \,|\, (x^n, w_1^n(j_1), w_2^n(j_2|j_1)) \in \mathcal{T}_{XW_1W_2}(n,\epsilon))$$
$$= \Pr(B = b(j_2) \,|\, w_2^n(j_2|j_1) \in \mathcal{T}_{W_2}(n,\epsilon)) = 1/S. \tag{27}$$

With μ as defined in (5) for the typical set $\mathcal{T}_{XYW_1W_2}$, and $J \equiv (J_1, B(J_2))$, the achievable equivocation can be lower bounded as

$$\frac{1}{n}H(Y^n|J_1, B(J_2))$$

$$\geq \frac{1}{n}H(Y^n|J_1, B(J_2), \mu) \tag{28a}$$

$$= \frac{1}{n}H(Y^n|W_1^n(J_1), B(J_2), \mu) \tag{28b}$$

$$\geq \Pr(\mu = 1)\frac{1}{n}H(Y^n|W_1^n(J_1), B(J_2), \mu = 1). \tag{28c}$$

The probability $\Pr(y^n|w_1^n(j_1), b(j_2), \mu = 1)$ for all j_1, j_2, and y^n can be written as

$$\sum_{(x^n,j_2)} \Pr(y^n, j_2, x^n|w_1^n(j_1), b(j_2), \mu = 1)$$

$$= \sum_{(x^n,j_2)} \Pr(x^n, j_2|w_1^n(j_1), b(j_2), \mu = 1)\Pr(y^n|x^n, \mu = 1) \tag{29a}$$

$$= \sum_{(x^n,j_2)} \frac{\Pr(x^n, j_2, w_1^n(j_1)|\mu = 1)/S}{\Pr(w_1^n(j_1)|\mu = 1)/S}\Pr(y^n|x^n, \mu = 1) \tag{29b}$$

$$\leq 2^{n\epsilon'} \sum_{(x^n,j_2)} \Pr(x^n, j_2|w_1^n(j_1), \mu = 1)\Pr(y^n|x^n, \mu = 1) \tag{29c}$$

$$= 2^{n\epsilon'}\Pr(y^n|w_1^n(j_1), \mu = 1) \tag{29d}$$

where (29a) follows from the fact that $Y - X - (W_1, W_2)$ forms a Markov chain and (29c) is obtained by expanding $\Pr(w_1^n(j_1), b(j_2)|\mu = 1)$ as follows:

$$\Pr(w_1^n(j_1), b(j_2)|\mu = 1)$$

$$= \Pr(w_1^n(j_1)|\mu = 1)\sum_{w_2^n}\Pr(w_2^n(j_1)|w_1^n(j_1), \mu = 1)\frac{1}{S} \tag{30a}$$

$$\geq \Pr(w_1^n(j_1)|\mu = 1)\frac{2^{-n\epsilon'}}{S} \tag{30b}$$

where (30a) follows from the fact that $W_1 - W_2 - B$ forms a Markov chain and (27), while (30b) follows the fact that for a typical set $\Pr\left(\mathcal{T}_{W_1W_2}\left(n,\epsilon\right)\right) \geq (1-\epsilon)$ [10, chap. 2]. Thus, from (29) we have that

$$\Pr\left(y^n|w_1^n\left(j_1\right),b\left(j_2\right),\mu=1\right) \leq 2^{n\epsilon'}\Pr\left(y^n|w_1^n\left(j_1\right),\mu=1\right) \tag{31}$$

$$\leq 2^{-n\left(H(Y|W_1)-\epsilon''\right)}. \tag{32}$$

From (28c) and (32), we then have

$$H\left(Y^n|w_1^n\left(j_1\right),b\left(j_2\right),\mu=1\right) \tag{33}$$

$$\geq \sum_{y^n}\Pr\left(y^n|w_1^n\left(j_1\right),\mu=1\right)n\left(H\left(Y|W_1\right)-\epsilon''\right) \tag{34}$$

$$\geq n\left(1-\epsilon\right)\left(H\left(Y|W_1\right)-\epsilon''\right) \tag{35}$$

such that

$$\frac{1}{n}H\left(Y^n|J\right) \geq \left(1-\epsilon\right)^3\left(H\left(Y|W_1\right)-\epsilon''\right) \tag{36}$$

where we have used the fact that for a typical set $\Pr\left(\mathcal{T}_{YW_1W_2}\left(n,\epsilon\right)\right) \geq (1-\epsilon)$ [10, chap. 2]. The proof concludes by observing that $H\left(Y^n\right) \geq H\left(Y^n|J\right)$ and $\epsilon \to 0$, $\epsilon'' \to 0$ as $n \to \infty$. ∎

Remark 3: An intuitive way to interpret the equivocation is as follows:

$$\frac{1}{n}H(Y^n|J_1B\left(J_1,J_2\right)) = \frac{1}{n}H(Y^n|W_1^n\left(J_1\right)) - \frac{1}{n}I\left(Y^n;B\left(J_1,J_2\right)|W_1^n\left(J_1\right)\right). \tag{37a}$$

The first term in (37) is approximately equal to $H\left(Y|W_1\right)$ while the second term, which in the limit goes to 0, follows from a conditional version of Lemma 1.

IV. Illustration of Results

We consider the following pair of correlated sources. X is binary and uniform, and

$$Y = \begin{cases} X, & \text{w.p. } (1-p); \\ E, & \text{w.p. } p. \end{cases}$$

We are interested in the rate-distortion-equivocation tradeoff, given as

$$R(D_1,D_2) \geq I(X;W_1) + I(X;W_2|Y,W_1) \tag{38}$$

$$\Gamma(D_1,D_2) \leq H(Y|W_1) \tag{39}$$

where the tradeoff is over all random variables (W_1,W_2) which satisfy the Markov chain $(W_1,W_2) \to X \to Y$ and for which there exist functions $f_1(\cdot)$ and $f_2(\cdot,\cdot,\cdot)$ satisfying,

$$E[d(X,f_1(W_1))] \leq D_1 \tag{40a}$$

$$E[d(X,f_2(W_1,W_2,Y))] \leq D_2. \tag{40b}$$

Consider the Hamming distortion metric, i.e., $d(x,\hat{x}) = x \oplus \hat{x}$. Let $h\left(a\right)$ denote the binary entropy function defined for $a \in [0,1]$. The rate-distortion-equivocation tradeoff is given as follows:

$$R(D_1,D_2) = \begin{cases} 0; & \text{if } D_1 \geq 1/2, D_2 \geq p/2, \\ 1-h(D_1); & \text{if } D_1 \leq D_2/p, \\ p(1-h(D_2/p)); & \text{if } D_2 \leq p/2, D_1 \geq 1/2, \\ p(1-h(D_2/p)+(1-p)(1-h(D_1)); & \text{o.w.} \end{cases}$$

and

$$\Gamma(D_1,D_2) = \begin{cases} h(p)+(1-p)h(D_1); & \text{if } D_1 \leq 1/2, \\ h(p)+(1-p); & \text{otherwise.} \end{cases}$$

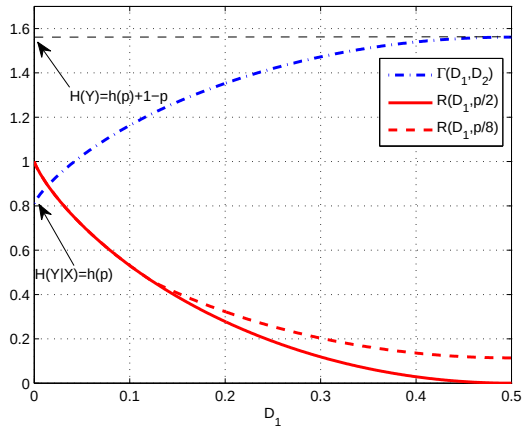

Fig. 2. Illustration of rate-equivocation tradeoff for $p = 0.25$.

In Figure 2, we have plotted $R(D_1,D_2)$ and $\Gamma(D_1,D_2)$ for the cases in which $D_2 = p/2$ and $D_2 = p/8$, and $D_1 \in [0,1/2]$.

Remark 4: This example shows that the equivocation does not depend on the distortion achieved by decoder 2 that has access to side-information Y and it depends only on the distortion achieved by the uninformed decoder 1. In contrast to this example, more generally, the equivocation will depend explicitly on both D_1 and D_2.

A. Upper Bound on $\Gamma(D_1,D_2)$

For any $D_1 \geq 1/2$, we use the trivial upper bound

$$\Gamma(D_1,D_2) \leq H(Y|W_1) \leq H(Y) \tag{41}$$

$$= h(p)+1-p. \tag{42}$$

For any $D_1 \leq 1/2$, we use the following:

$$\Gamma(D_1,D_2) \leq H(Y|W_1) \tag{43a}$$

$$= H(Y,X|W_1) - H(X|Y,W_1) \tag{43b}$$

$$= H(X|W_1) + H(Y|X) - H(X|Y,W_1) \tag{43c}$$

$$= H(X|W_1) + H(Y|X) - pH(X|W_1) \tag{43d}$$

$$= H(Y|X) + (1-p)H(X|W_1,\hat{X}_1) \tag{43e}$$

$$\leq H(Y|X) + (1-p)H(X|\hat{X}_1) \tag{43f}$$

$$\leq H(Y|X) + (1-p)H(X \oplus \hat{X}_1) \tag{43g}$$

such that

$$\Gamma(D_1, D_2) \leq H(Y|X) + (1-p)h(P(X \neq \hat{X}_1)) \quad (44)$$
$$\leq h(p) + (1-p)h(D_1) \quad (45)$$

where (43d) follows from a direct verification that $H(X|Y, W_1) = pH(X|W_1)$ if X is uniform and Y is an erased version of X and $W_1 - X - Y$ forms a Markov chain.

B. Lower Bound on $R(D_1, D_2)$

- If $D_1 \geq 1/2, D_2 \geq p/2$, we use the lower bound $R(D_1, D_2) \geq 0$.
- If $D_1 \leq D_2/p$, we use the lower bound $R(D_1, D_2) \geq 1 - h(D_1)$.
- If $D_2 \leq p/2, D_1 \geq 1/2$, we use the lower bound $R(D_1, D_2) \geq R_{WZ}^{(Y)}(D_2)$ [11].
- For any other pair (D_1, D_2), we show that

$$R(D_1, D_2) \geq p(1 - h(D_2/p) + (1-p)(1 - h(D_1)).$$

Consider an arbitrary (W_1, W_2) such that $(W_1, W_2) \to X \to Y$ is a Markov chain and there exist functions f_1 and f_2 satisfying (40). We now have

$$\begin{aligned} &I(X; W_1) + I(X; W_2|Y, W_1) \\ &= H(X) - H(X|W_1) + H(X|Y, W_1) - H(X|Y, W_1, W_2) \\ &= H(X) + H(Y|X) - H(Y|W_1) - H(X|Y, W_1, W_2). \end{aligned} \quad (46)$$

Consider the following term appearing in (46):

$$H(Y|W_1) = H(Y, X|W_1) - H(X|Y, W_1) \quad (47a)$$
$$= H(Y|X) + H(X|W_1) - H(X|Y, W_1) \quad (47b)$$
$$= H(Y|X) + (1-p)H(X|W_1) \quad (47c)$$
$$\leq H(Y|X) + (1-p)h(D_1) \quad (47d)$$

where (47d) follows from (43d)-(45). We also have

$$D_2 \geq \Pr(X \neq \hat{X}_2) \quad (48a)$$
$$\geq \Pr(Y = E) \Pr(X \neq \hat{X}_2|Y = E) \quad (48b)$$
$$= p \Pr(X \neq \hat{X}_2|Y = E) \quad (48c)$$

which implies that

$$\Pr(X \neq \hat{X}_2|Y = E) \leq \frac{D_2}{p} \leq \frac{1}{2}. \quad (49)$$

Now consider the following sequence of inequalities for the last term in (46):

$$H(X|Y, W_1, W_2) = H(X|Y, W_1, W_2, \hat{X}_2) \quad (50a)$$
$$\leq H(X|Y, \hat{X}_2) \quad (50b)$$
$$= pH(X|Y = E, \hat{X}_2) \quad (50c)$$
$$\leq pH(X \oplus \hat{X}_2|Y = E) \quad (50d)$$
$$= ph(P(X \neq \hat{X}_2|Y = E)) \quad (50e)$$
$$\leq ph(D_2/p) \quad (50f)$$

where (50f) follows from (49). Using (47d) and (50f), we can lower bound (46), to arrive at

$$R(D_1, D_2) \geq p(1 - h(D_2/p) + (1-p)(1 - h(D_1)).$$

C. Coding Scheme

Due to space limitations, we outline the coding scheme only for the non-trivial regime, i.e., when $D_2/p \leq D_1 \leq 1/2$. For this case, we select $W_2 = X \oplus N_2$, and $W_1 = W_2 \oplus N_1$, where $N_2 \sim Ber(D_2/p)$, and $N_1 \sim Ber(\alpha)$, where $\alpha = (D_1 - D_2/p)/(1 - 2D_2/p)$, and the random variables N_1 and N_2 are independent of each other and are also independent of X. At the uninformed decoder, the estimate is created as $\hat{X}_1 = W_1$, so that the desired distortion D_1 is achieved. At the decoder with side-information Y, the estimate $\hat{X}_2$ is created as follows:

$$\hat{X}_2 = \begin{cases} Y; & \text{if } Y \neq E; \\ W_2; & \text{if } Y = E. \end{cases}$$

Therefore the achievable distortion at this decoder is $(1-p)0 + p(D_2/p) = D_2$. It is straightforward to check that the rate required by this scheme matches the stated lower bound on $R(D_1, D_2)$, and $\Gamma(D_1, D_2) = H(Y|W_1) = h(p) + (1-p)h(D_1)$. This completes the proof of the achievable part.

V. Concluding Remarks

We have determined the rate-distortion-equivocation region for the two-decoder HB problem with an additional constraint on the side information privacy at the uninformed decoder. We have illustrated our results for a binary source with erasure side information and Hamming distortion, a result that is also of independent interest. Extensions of these results to the case of an informed encoder are developed in [12].

References

[1] C. Heegard and T. Berger, "Rate distortion when side information may be absent," *IEEE Trans. Inform. Theory*, vol. 31, pp. 727–733, Nov. 1985.

[2] D. Gündüz, E. Erkip, and H. V. Poor, "Lossless compression with security constraints," in *Proc. IEEE Intl. Symp. Inform. Theory*, Toronto, ON, Canada, 2008, pp. 111–115.

[3] L. Grokop, A. Sahai, and M. Gastpar, "Discriminatory source coding for a noiseless broadcast channel," in *Proc. IEEE Intl. Symp. Inform. Theory*, Adelaide, Australia, 2005, p. 77.

[4] J. Villard and P. Piantanida, "Secure lossy source coding with side information at the decoders," in *Proc. 48th Annual Allerton Conf. Commun., Control and Computing*, Monticello, IL, Sept. 2010, pp. 733–739.

[5] R. Tandon, S. Mohajer, and H. V. Poor, "Cascade source coding with erased side information," in *Proc. IEEE Symp. Inform. Theory*, St. Petersburg, Russia, Aug. 2011.

[6] R. Tandon, L. Sankar, and H. V. Poor, "Multi-user privacy: The Gray-Wyner system and generalized common information," in *Proc. IEEE Symp. Inform. Theory*, St. Petersburg, Russia, Aug. 2011.

[7] R. Tandon and S. Ulukus, "Secure source coding with a helper," Oct. 2009, submitted to the *IEEE Trans. Inform. Theory*.

[8] L. Sankar, S. R. Rajagopalan, and H. V. Poor, "A theory of privacy and utility in databases," Feb. 2011, submitted to the *IEEE Trans. Inform. Theory*.

[9] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inform. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[10] T. M. Cover and J. A. Thomas, *Elements of Information Theory*. New York: Wiley, 1991.

[11] T. Weissman and S. Verdú, "The information lost in erasures," *IEEE Trans. Inform. Theory*, vol. 54, no. 11, pp. 5030–5058, Nov. 2008.

[12] R. Tandon, L. Sankar, and H. V. Poor, "Discriminatory lossy source coding: Side information privacy," May 2011, submitted to the *IEEE Trans. Inform. Theory*; [arXiv:1106.2057].