The Duality Between Information Embedding and Source Coding with Side Information and Some Applications

Richard J. Barron, Brian Chen, and Gregory W. Wornell: {rjb,bchen,gww}@allegro.mit.edu
Dept. EECS, MIT, Cambridge, MA, 02139

Abstract — **A formal duality between the information embedding (data hiding) problem and the Wyner-Ziv problem of source coding with decoder side information is developed, including results for the quadratic Gaussian and binary-symmetric-Hamming cases, with implications for a number of important applications.**

I. Introduction

This paper develops and exploits the theoretical duality between *information embedding*, the robust communication of information embedded into a host signal, and *source coding with side information*; the case where the side information is known only at the decoder is the well-known "Wyner-Ziv problem". A detailed exposition of our results is found in [1].

The information embedding encoder observes an n-dimensional host $\mathbf{x}$ and an information signal m from which it creates a *composite signal* $\mathbf{w}$, which is assumed to closely approximate $\mathbf{x}$. All signals in this paper are assumed to be from finite alphabets, unless otherwise indicated. The composite signal is passed through a memoryless channel, the output which, $\mathbf{y}$, is decoded to retrieve an estimate $\hat{m} \approx m$ of the information signal. The decoder may be supplied with an observation of $\mathbf{x}$ (*private* information embedding) or it may not (*public* information embedding), which is the case that is the focus of this paper.

In source coding with side information, the n-dimensional vector $\mathbf{y}$ is a source, drawn iid from $p_y(y)$, that is sent uncoded through a memoryless channel, the output of which is $\mathbf{x}$, which may or may not be fed back to the encoder. The source is coded by the encoder, creating an information signal m, which is sent to the decoder. From the signals $\mathbf{x}$ and m, the decoder outputs a signal $\mathbf{w}$, which is intended to be a close approximation of the source $\mathbf{y}$.

We show in the sequel that an information embedding encoder serves as a Wyner-Ziv decoder and vice versa. We have defined variables in the associated problems so as to indicate their dual correspondences.

II. Information embedding capacity

Public and private information embedding capacities are denoted $C^{\text{IE}}(d)$ and $C^{\text{IE}}_{\text{priv}}(d)$, respectively. Under their respective constraints, the capacities are defined as the maximum achievable rate for communicating a message m such that $P(\hat{m} \neq m)$ is arbitrarily small and $E[\frac{1}{n}\sum_{k=1}^{n} D(x_k, w_k)]$ is arbitrarily close to d for large enough n. As an extension of the results in [2], we have shown that the capacity expressions are given by $C^{\text{IE}}(d) = \sup I(y;u) - I(x;u)$, where the supremum is taken over all distributions $p_{u|x}(u|x)$ and functions $f : \mathcal{U} \times \mathcal{X} \to \mathcal{W}$ satisfying $E[D(x,w)] \leq d$, where $w = f(u,x)$, and $C^{\text{IE}}_{\text{priv}}(d) = \sup I(y;w|x)$, where the supremum is taken over all distributions $p_{w|x}(w|x)$ satisfying $E[D(x,w)] \leq d$.

[1]This work has been supported in part by the U.S. Air Force Office of Scientific Research under Grant AFOSR-F49620-96-1-0072, and in part through collaborative participation in the Advanced Sensors Consortium sponsored by the U.S. Army Research Laboratory under Cooperative Agreement DAAL01-96-2-0001, and in part by the National Science Foundation under Grant No. CCR-0073520.

The equations for capacity provide a generalization of previous results [2, 3] that encompass only difference distortion measures. The optimized quantities on the right hand sides of the capacity equations are identical to the corresponding rate-distortion limit expressions. The rate-distortion limits are, in a dual manner to information embedding capacities, the infima over these quantities.

III. Important Special Cases

Quadratic Gaussian case: For the information embedding scenario, consider an iid Gaussian host $\mathbf{x} \sim \mathcal{N}(0, \sigma_x^2 I)$ and a channel comprised of additive white Gaussian noise $\mathbf{v} \sim \mathcal{N}(0, \sigma_v^2 I)$ independent from $\mathbf{x}$. The distortion metric is squared error. We construct a capacity-achieving system based on two nested lattices $\mathcal{L}_1$ and $\mathcal{L}_2 \subset \mathcal{L}_1$, appropriately parameterized [1]. The lattice decoding functions for each lattice are nearest neighbor quantizing functions. The information embedding encoder simply uses the information m to specify a coset of $\mathcal{L}_2$, and quantizes the host with the coset lattice. The composite signal is formed as a linear combination of the host and the quantized host, the so-called distortion-compensated composite signal [3]. The decoder simply quantizes the channel output with $\mathcal{L}_1$ and reads off the coset shift with respect to $\mathcal{L}_2$.

Binary-symmetric-Hamming case: In [1] we derive $C^{\text{IE}}(d)$ for the case of binary symmetric host and channel (with crossover probability p) and Hamming distortion metric to be the upper concave envelope of the function $h(d) - h(p)$ and the point $(R,d) = (0,0)$. We construct a capacity-achieving system based on nested linear codes $\mathcal{C}_1$ and $\mathcal{C}_2 \subset \mathcal{C}_1$, which are uniquely specified by their parity check matrices $\mathbf{H}_1$ and $\mathbf{H}_2 = [\mathbf{H}_1^T \mathbf{H}_a^T]^T$, respectively. Using the syndrome former associated with $\mathbf{H}_2$ [1], the encoder finds the composite signal $\mathbf{w} \in \mathcal{C}_1$ that is closest in Hamming distance to the host $\mathbf{x}$, such that $\mathbf{H}_a\mathbf{w} = \text{Bin}(m)$, where $\text{Bin}(m)$ is the length n binary expansion of m. The decoder decodes $\mathbf{y}$ with $\mathcal{C}_1$ to form $\hat{\mathbf{w}}$, and calculates the information by $\mathbf{H}_a\hat{\mathbf{w}}$. In both special cases, exchanging the roles of encoder and decoder yields coding systems (previously discovered in [4]) that achieve the Wyner-Ziv rate-distortion limit.

We have also discovered that Slepian-Wolf coding ($d = 0$) is the dual of noise-free embedding ($\sigma_v^2 = 0$ or $p = 0$). And we have developed a natural hybrid analog-digital source representation inspired by our framework.

References

[1] R.J. Barron, "Systematic Hybrid Analog/Digital Signal Coding," MIT Ph.D. Thesis, Cambridge, MA, June 2000.

[2] S.I. Gel'fand, M.S. Pinsker, "Coding for Channel with Random Parameters," *Problems of Control and Information Theory*, vol.9, no. 1, pp. 19-31, 1980.

[3] B. Chen and G.W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding," accepted to *IEEE Trans. Inform. Theory.*

[4] R. Zamir and S. Shamai, "Nested Linear/Lattice Codes for Wyner-Ziv Encoding," *1998 Information Theory Workshop, Kilarney, Ireland*, pp 92-93, June 1998.

0-7803-7123-2/01/$10.00 ©2001 IEEE