The Likelihood Encoder with Applications to Lossy Compression and Secrecy

Eva C. Song, Paul Cuff, H. Vincent Poor
{ CSONG, CUFF, POOR }@PRINCETON.EDU

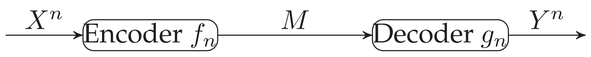
PRINCETON UNIVERSITY

Problem

A likelihood encoder is studied in the context of lossy source compression. The use of a likelihood encoder recovers the point-to-point rate-distortion function, the rate-distortion function with side information at the decoder, and several other important inner bounds for multi-user lossy compression.This tool is particularly handy for analyzing rate-distortion based secrecy systems.

The likelihood encoder

- a stochastic source encoder: $f_n : \mathcal{X}^n \mapsto \mathcal{M}$



Given

- a codebook $\{y^n(m)\}_m$, $m \in [1 : 2^{nR}]$
- a joint distribution P_{XY}

the likelihood function for each codeword:

$$\mathcal{L}(m|x^n) \triangleq \prod_{t=1}^{n} P_{X|Y}(x_t|y_t(m))$$

the likelihood encoder determines the message index according to:

$$P_{M|X^n}(m|x^n) = \frac{\mathcal{L}(m|x^n)}{\sum_{m' \in [1:2^{nR}]} \mathcal{L}(m'|x^n)} \propto \mathcal{L}(m|x^n)$$

Applications

- Lossy Compression
  - Point-to-point rate-distortion theory
  - Wyner-Ziv
  - Berger-Tung inner bound
- Rate-Distortion Based Secrecy
  - Source coding (noisless wiretap channel)
  - Source-channel coding (noisy wiretap channel)

Prerequisite

Total variation distance

$$\|P - Q\|_{TV} \triangleq \sup_{A \in \mathcal{F}} |P(A) - Q(A)|.$$

Soft-Covering Lemma

- Given
  1) P_{XY}
  2) random $\mathcal{C}^{(n)}$ of sequences $Y^n(m) \sim \prod_{t=1}^{n} P_Y(y_t)$, $m \in [1 : 2^{nR}]$,
- $\mathbf{P}_{X^n}$: the output distribution induced by
  1) $M \sim Unif[1 : 2^{nR}]$
  2) $M \to Y^n(M) \to \prod P_{X|Y}$

Then if $R > I(X;Y)$,

$$\mathbb{E}_{\mathcal{C}^n} \left\| \mathbf{P}_{X^n} - \prod_{t=1}^{n} P_X \right\|_{TV} \to_n 0.$$

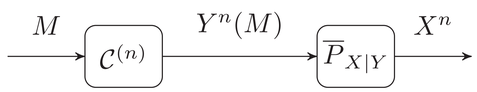
Achieving $R(D)$

$$R(D) = \min_{\overline{P}_{Y|X} : \mathbb{E}[d(X,Y)] \le D} I(X;Y)$$

System induced distribution

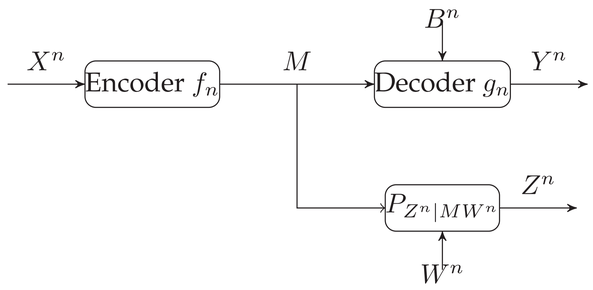
$$\mathbf{P}_{X^n M Y^n}(x^n, m, y^n) = P_{X^n}(x^n)\mathbf{P}_{LE}(m|x^n)\mathbf{P}_D(y^n|m)$$

- Random $\mathcal{C}^{(n)}$ on $Y^n(m) \sim \prod_{t=1}^{n} \overline{P}_Y(y_t)$
- $\mathbf{P}_{LE}(m|x^n) \propto \mathcal{L}(m|x^n)$ w.r.t. $\overline{P}_{X|Y}$
- $\mathbf{P}_D(y^n|m) = \mathbb{1}\{y^n = Y^n(m)\}$
- $\mathbf{Q}_{M|X^n}(m|x^n) = \mathbf{P}_{LE}(m|x^n)$
- $\mathbf{Q}_{Y^n|M}(y^n|m) = \mathbf{P}_D(y^n|m)$
- $\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{Q}}[d(X^n, Y^n)]\right] = \mathbb{E}_{\overline{P}}[d(X,Y)]$
- SCL $\Rightarrow \|\mathbf{P} - \mathbf{Q}\|_{TV} \to_n 0$
- Distortion under $\mathbf{P} \to_n$ Distortion under $\mathbf{Q}$



Idealized distribution $\mathbf{Q}$

A source coding secrecy setup



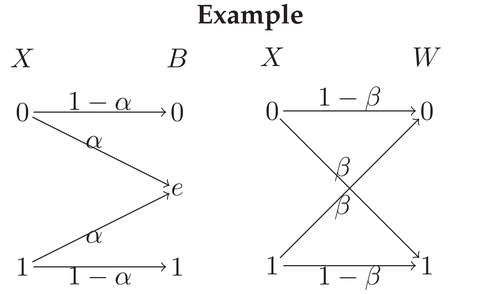
Definition 1. *The rate-distortion triple (R, D_b, D_w) is achievable if there exists a sequence of rate R encoders and decoders (f_n, g_n) such that*

$$\mathbb{E}[d(X^n, Y^n)] \le_n D_b$$

and

$$\min_{P_{Z^n|MW^n}} \mathbb{E}[d(X^n, Z^n)] \ge_n D_w.$$

Example



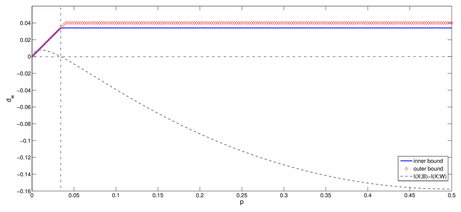
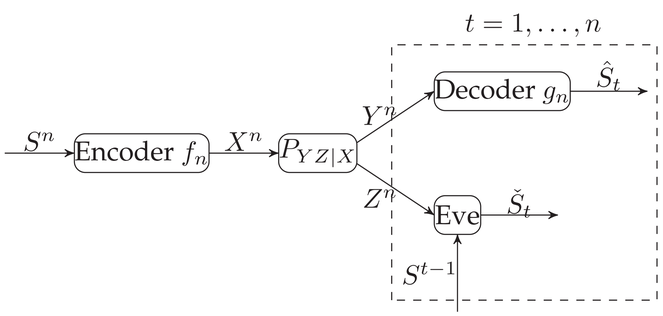


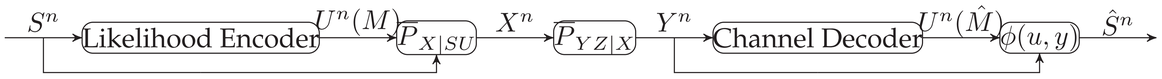
Figure 1: Distortion at the eavesdropper as a function of source distribution p with $\alpha = 0.4$, $\beta = 0.04$

A source-channel coding secrecy setup



Definition 3. *A distortion pair (D_b, D_e) is achievable if there exists a sequence of source-channel encoders and decoders (f_n, g_n) such that*

$$\mathbb{E}[d(S^n, \hat{S}^n)] \le_n D_b$$
and
$$\min_{\{P_{\check{S}_t|Z^n S^{t-1}}\}_{t=1}^n} \mathbb{E}[d(S^n, \check{S}^n)] \ge_n D_e$$



Example

- **Source** i.i.d. $Bern(p)$
- **Channel** BSCs with crossover probabilities
  - $p_1 = 0, p_2 = 0.3$
- Lossless decoding at legitimate receiver
- Hamming distortion
- Scheme O–"Separate" SC coding
- Scheme I–Hybrid coding