Privacy amplification, lossy compression, and their duality to channel coding

Joseph M. Renes
ETH Zürich

arXiv:1708.05685

Overview

I. Information theory

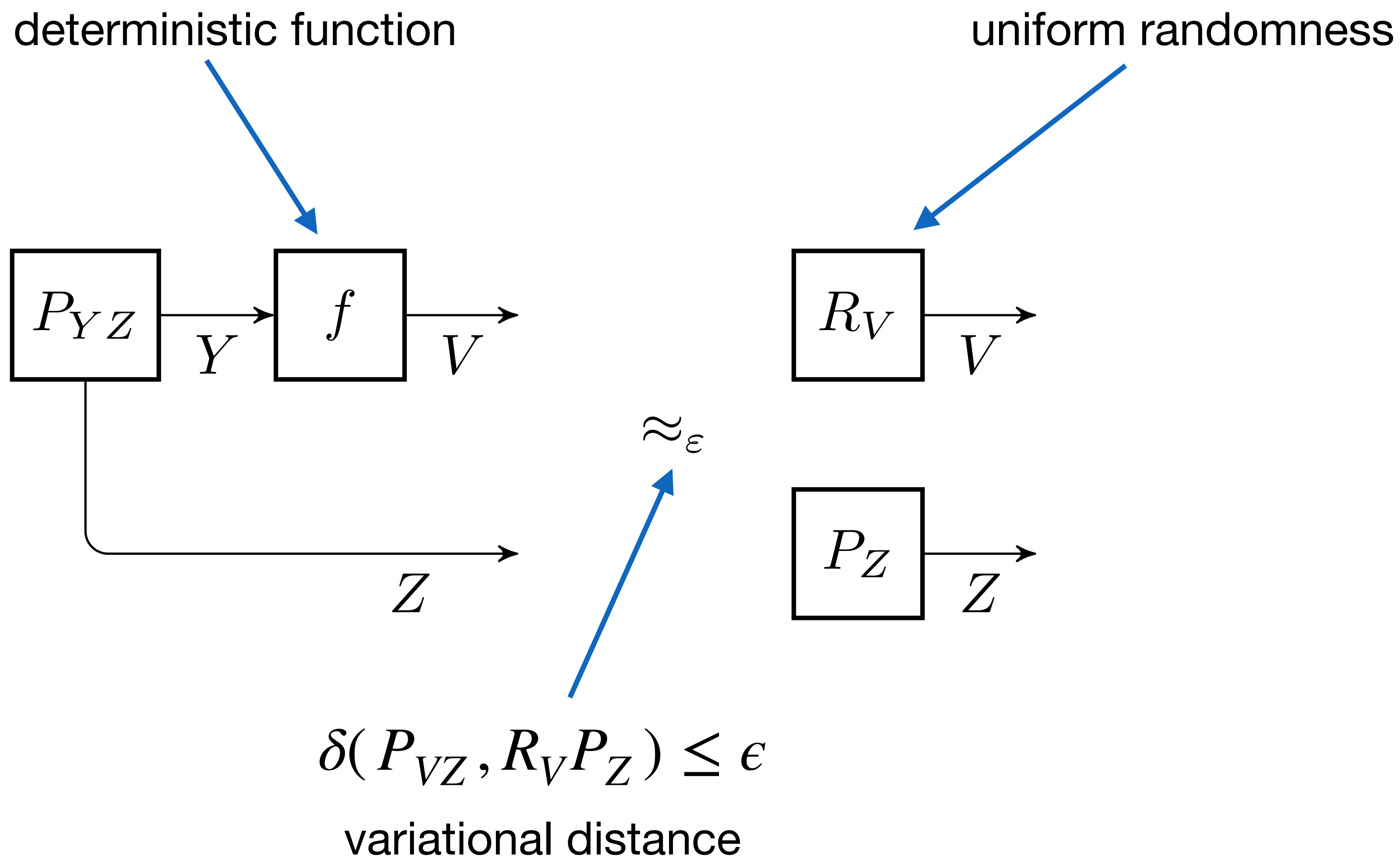
- hypothesis testing converse for privacy amplification against classical side information

II. Coding theory

- how to use channel codes for lossy compression

Information theory

Privacy amplification



$K_\epsilon(Y|Z)_P := \max |V|$ such that ε-good *f* exists

Guessing probability converse

Watanabe/Hayashi ISIT 2013

$$\frac{1}{K_\epsilon(Y|Z)_P} \geq P^\epsilon_{\text{guess}}(Y|Z)_P$$

Consider worst case (for Alice) guessing probability (for Eve)

$$P_{\text{guess}}(Y|Z)_P := \max_{y,z} P_{Y|Z=z}(y) \qquad P^\epsilon_{\text{guess}}(Y|Z)_P := \min_{Q\approx_\epsilon P} \max_{y,z} \frac{Q_{YZ}(y,z)}{P_Z(z)}$$

$$P^\epsilon_{\text{guess}}(f(Y)|Z) \geq P^\epsilon_{\text{guess}}(Y|Z)$$

Difficult to compute for finite-blocklength due to Q minimization; relax to information spectrum quantity

Guessing probability LP formulation

$$
\begin{aligned}
P^{\epsilon}_{\text{guess}}(Y|Z)_P \quad = \quad & \underset{\lambda,Q,T}{\text{minimum}} \quad \lambda \\
& \text{such that} \quad \lambda \mathbb{1}_Y P_Z \geq Q_{YZ} \\
& \qquad T_{YZ} \geq P_{YZ} - Q_{YZ} \\
& \qquad \mathrm{Tr}[T_{YZ}] \leq \epsilon \\
& \qquad \mathrm{Tr}[Q_{YZ}] = 1 \\
& \qquad \lambda, T_{YZ}, Q_{YZ} \geq 0
\end{aligned}
$$

Note: by normalization of Q, we have $\lambda |Y| \geq 1$

Guessing bound is never looser than the trivial bound $K_\epsilon(Y|Z)_P \leq |Y|$

Hypothesis-testing converse

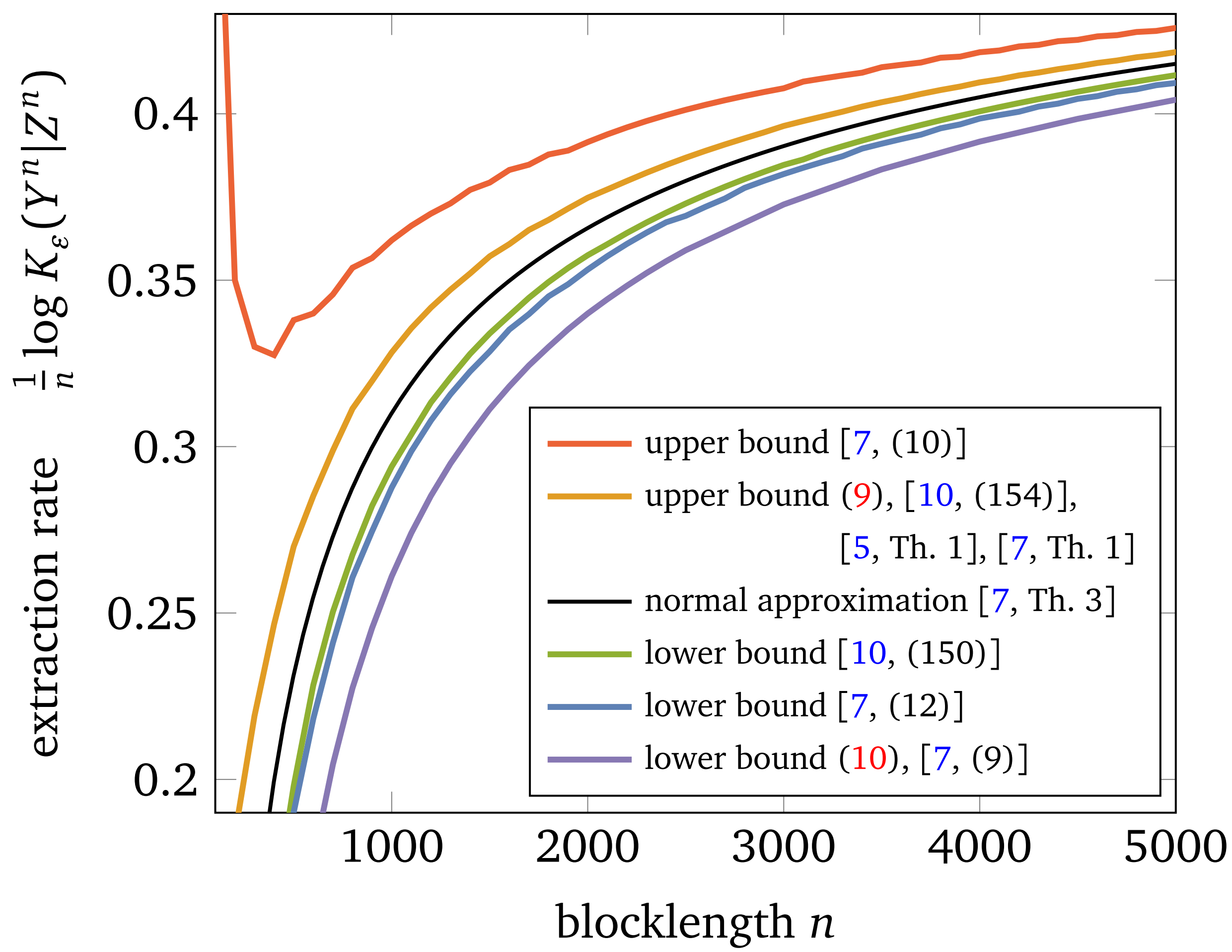
R, arXiv:1708.05685

$$K_\epsilon(Y|Z)_P \leq \min_{\eta \in [0,1-\epsilon]} \frac{1}{\eta} \beta_{\epsilon+\eta}(P_{YZ}, 1_Y P_Z)$$

- $\beta_\alpha(P,Q) := \min\{\mathrm{Tr}[\Lambda Q] : \mathrm{Tr}[\Lambda P] \geq \alpha, 0 \leq \Lambda \leq 1\}$
- $\alpha - \delta(P,Q) \leq \beta_\alpha(P,Q)$
- $\beta_\alpha(P_{f(Y)Z}, 1_{f(Y)} P_Z) \leq \beta_\alpha(P_{YZ}, 1_Y P_Z)$

bound does not hold for quantum Z

Finite blocklength example



$\epsilon = 1/10^{10}$ $\quad Z = Y + X \quad$ $X = \mathrm{Ber}(0.11)$

311 ± 17 at blocklength 1000

Relation to guessing bound

$$K_\epsilon(Y|Z)_P \leq \min_{\eta\in[0,1-\epsilon]} \frac{1}{\eta}\beta_{\epsilon+\eta}(P_{YZ}, 1_Y P_Z) \quad \Longleftrightarrow \quad \epsilon \geq E_{Y/K_\epsilon}(P_{YZ}, R_Y P_Z)$$

Yang, Schaefer, Poor
IEEE TIT 2019

$$E_\gamma(P, Q) := \max\{\mathrm{Tr}[\Lambda P] - \gamma \mathrm{Tr}[\Lambda Q] : 0 \leq \Lambda \leq 1\}$$

Using properties of E_γ divergence from Liu, Cuff, Verdú (IEEE TIT 2017), we obtain

$$\frac{1}{K_\epsilon(Y|Z)_P} \geq \hat{P}^\epsilon_{\mathrm{guess}}(Y|Z)_P$$

$$\begin{aligned}
\hat{P}^\epsilon_{\mathrm{guess}}(Y|Z)_P \; = \; & \underset{\lambda,Q,T}{\text{minimum}} && \lambda \\
& \text{such that} && \lambda \mathbb{1}_Y P_Z \geq Q_{YZ} \\
&&& T_{YZ} \geq P_{YZ} - Q_{YZ} \\
&&& \mathrm{Tr}[T_{YZ}] \leq \epsilon \\
&&& \cancel{\mathrm{Tr}[Q_{YZ}] = 1} \\
&&& \lambda, T_{YZ}, Q_{YZ} \geq 0
\end{aligned}$$

Hence the HT bound is a relaxation
of the guessing bound

Equivalence!

It can happen that $\hat{P}^{\epsilon}_{\text{guess}}(Y|Z)_P < \dfrac{1}{|Y|}$

meaning the HT bound can be looser than the trivial bound (!)

$$\begin{aligned}
\hat{P}^{\epsilon}_{\text{guess}}(Y|Z)_P \quad = \quad & \underset{\lambda,Q,T}{\text{minimum}} \quad \lambda \\
& \text{such that} \quad \lambda \mathbb{1}_Y P_Z \geq Q_{YZ} \\
& \qquad\qquad\quad Q_{YZ} \geq P_{YZ} - T_{YZ} \\
& \qquad\qquad\quad \mathrm{Tr}[T_{YZ}] \leq \epsilon \\
& \qquad\qquad\quad \lambda, T_{YZ}, Q_{YZ} \geq 0
\end{aligned}$$

$$\left.\begin{matrix} \lambda \mathbb{1}_Y P_Z \geq Q_{YZ} \\ Q_{YZ} \geq P_{YZ} - T_{YZ} \\ \mathrm{Tr}[T_{YZ}] \leq \epsilon \end{matrix}\right\} \Rightarrow 1 - \epsilon \leq \mathrm{Tr}[\mathrm{Q_{YZ}}] \leq \lambda |\mathrm{Y}|$$

Therefore, whenever HT is nontrivial

the HT and guessing bounds are equivalent!

More equivalence: Achievability

Recent approach from quantum information: partial smoothing

$$
\begin{aligned}
P^{\epsilon}_{\text{guess}}(Y|\dot{Z})_P \quad = \quad & \underset{\lambda,Q,T}{\text{minimum}} \quad \lambda \\
& \text{such that} \quad \lambda \mathbb{1}_Y P_Z \geq Q_{YZ} \\
& \qquad T_{YZ} \geq P_{YZ} - Q_{YZ} \\
& \qquad \mathrm{Tr}[T_{YZ}] \leq \epsilon \\
& \qquad \cancel{\mathrm{Tr}[Q_{YZ}] = 1} \\
& \qquad Q_Z \leq P_Z \\
& \qquad \lambda, T_{YZ}, Q_{YZ} \geq 0
\end{aligned}
$$

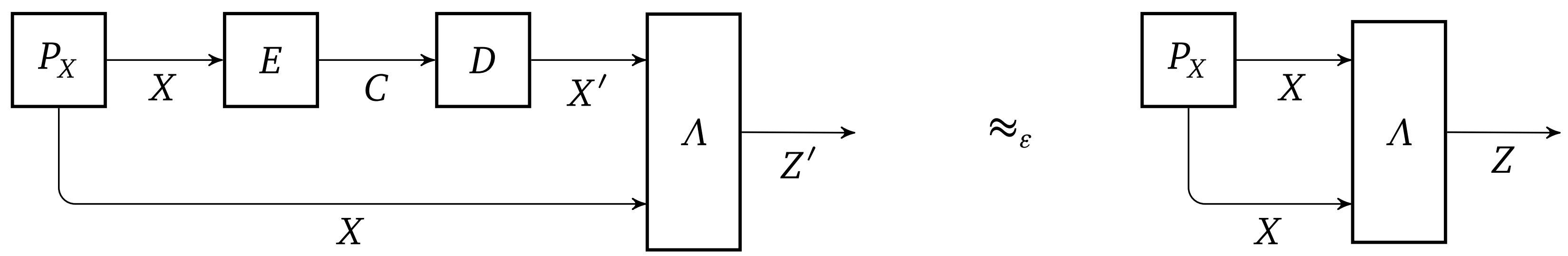
Anshu, Berta,
Jain, and Tomamichel
arXiv:1807.05630

Can also obtain achievability bounds using the collision entropy

But partial smoothing = global smoothing classically,
therefore Anshu et al.'s bound = Yang et al.'s bound

Coding theory

Lossy compression



- Compress X so that average distortion of the reconstruction X' is small.
- Usual examples:
  - Gaussian source: recover up to small mean-squared error
  - Uniform discrete source: recover up to Hamming distortion
    (fraction of incorrect bits)

Rate-distortion function

$$R(\bar{d}) = \min_{P_{Y|X}:\langle d(X,Y)\rangle \leq \bar{d}} I(X:Y)$$

A “curious duality”

Erasure quantization BEQ(e):

$\mathcal{X}$	0	1	?
P_X	$\frac{1}{2}(1-e)$	$\frac{1}{2}(1-e)$	e

$$R(\bar{d}) = (1-e)(1-h_2(\frac{\bar{d}}{1-e}))$$

Martinian & Yedidia Allerton 2004

$$d(x,x') = \begin{cases} 0 & x =?, x' =?, x = x' \\ 1 & \text{else} \end{cases}$$

Kostina & Verdú IEEE TIT 2012

- Consider zero distortion
- Quantize using linear code: Assign 0/1 to ?’s to get a codeword
- M&Y:

If linear codes C_n achieve the capacity 1-e for BEC(e) under optimal decoding, then their duals C^d_n achieve R(0) for BEQ(1-e) under optimal quantization.

“The statement and proof of the two preceding results contain a curious duality between erased/known symbols in source coding and known/erased symbols in channel coding.”

This curious duality is quantum!

Compression via privacy amplification

1. Pick a channel achieving R. This gives P_{XY}.
2. Find (linear) f for PA of Y relative to X.
3. Extend to reversible $g{:}Y \to (V,T)$. This gives P_{TVX}.
4. Quantizer is channel $P_{T|VX}$.
   Dequantizer is g^{-1}.
5. Both use common randomness V.
   Derandomize if desired.
6. Size of the code is $|T|=|Y|/|V|$

Similar to, but more direct than:
Muramatsu, IEEE TIT 2014,
Yassaee, Aref, Gohari, IEEE TIT 2014

Why does it work?

* Input to quantizer is: $R_V P_X \approx_\epsilon P_{VX}$
* Quantizer produces: $\mathcal{Q}(R_V P_X) \approx_\epsilon P_{TVX}$
* Dequantizer gives: $\mathcal{D} \circ \mathcal{Q}(R_V P_X) \approx_\epsilon P_{YX}$

$f(x^n)$ = syndromes of C,

$g^{-1}(t,v)$ = t-th codeword,
offset to v-th coset

Privacy amplifcation via channel coding

- P_{XY} also defines the channel $P_{X|Y}$.
- Get extractor for $Y \mid X$ from channel code for dual of $P_{X|Y}$

$$(M,\epsilon) \text{ code for } P^{\perp}_{X|Y} \iff (M,\sqrt{2\epsilon}) \text{ extractor for } Y|X$$

R IEEE TIT 2018

$$(M,\epsilon) \text{ code for } P^{\perp}_{X|Y} \implies (|Y|/M,\sqrt{2\epsilon}) \text{ quantizer for } P_{XY}$$

For i.i.d. X^n, achieve a rate of $\frac{1}{n}\log\frac{|Y|}{M} \to 1 - C(P^{\perp}_{X|Y})$

If capacity optimizer is uniform, then $C(P^{\perp}_{X|Y}) = 1 - I(X:Y)$

- Hamming distortion
- BEQ(e)

Therefore, we recover the optimal quantizer rate!
The “curious duality” is a quantum duality.

Dual of uniform bit compression: pure state channel

Outlook

I. Information theory

- Still missing good PA bounds for quantum adversaries… (Could try duality.)

II. Coding theory

- Can we go from lossy compression to channel coding? (Does compression always effectively implement PA?)