The Tight Exponent Analysis for Quantum Privacy Amplification

Yongsheng Yao[1]

[arxiv : 2111.01075]

[1] Harbin Institute of Technology
Institute for Advanced Study in Mathmatics
School of Mathmatics

Outline

- Preliminaries
- Introduction of the reliability function
- Reliability function in smoothing the max-relative entropy
- Reliability function for privacy amplification
- Summary and open questions

Preliminaries

a physics system A ⟷ a finite dimension Hilbert space $\mathcal{H}_A$

composite system AB ⟷ $\mathcal{H}_A \otimes \mathcal{H}_B$

states of the system A ⟷ positive semi-definite operator on $\mathcal{H}_A$ with trace 1

the classical-quantum state of system XA ⟷ $\rho_{XA} = \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x| \otimes \rho_A^x$

quantum measurement ⟷ $\{\Lambda_i\}_{i \in \mathcal{I}}, \quad \Lambda_i \geq 0, \quad \sum_{i=1}^{|\mathcal{I}|} \Lambda_i = \mathbb{1}$

$\rho \xrightarrow{\{\Lambda_i\}_{i \in \mathcal{I}}}$ The probability of obtaining i is $\operatorname{Tr} \rho \Lambda_i$

Preliminaries

quantum channel $\mathcal{N}_{A\to B}$ $\Longleftrightarrow$ completely positive and trace-preserving linear map from $\mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$

common quantum channel

measure-prepare channel

$$\Phi(\rho) = \sum_{i=1}^{|\mathcal{I}|} (\operatorname{Tr} \rho\Lambda_i)|i\rangle\langle i|, \text{ where } \{\Lambda_i\}_{i\in\mathcal{I}} \text{ is a measurement.}$$

pinching channel

$$\Psi(\rho) = \sum_{k=1}^{n} \Pi_i\rho\Pi_i, \text{ where } \Pi_i \text{ is projection and } \sum_{i=1}^{n} \Pi_i = \mathbb{1}.$$

Measure on the set of states :

For two states ρ, σ :

- trace norm distance: $\frac{\|\rho-\sigma\|_1}{2}$, where $\|A\|_1 = \mathrm{Tr}\sqrt{A^*A}$
- purified distance: $P(\rho,\sigma) = \sqrt{1-\|\sqrt{\rho}\sqrt{\sigma}\|_1^2}$ (fedelity: $F(\rho,\sigma) = \|\sqrt{\rho}\sqrt{\sigma}\|_1$)
- Umegaki relative entropy: $D(\rho,\sigma) = \mathrm{Tr}(\rho\log\rho - \rho\log\sigma)$
- Rényi relative entropy

  Petz: $\tilde{D}_\alpha(\rho\|\sigma) = \frac{\log \mathrm{Tr}\,\rho^\alpha\sigma^{1-\alpha}}{\alpha-1}$

  Sandwiched: $D_\alpha(\rho\|\sigma) = \frac{\log \mathrm{Tr}(\sigma^{\frac{1-\alpha}{2\alpha}}\rho\sigma^{\frac{1-\alpha}{2\alpha}})^\alpha}{\alpha-1}$

Sandwiched Rényi relative entropy

Properties:

- Monotonicity: $D_\alpha(\rho\|\sigma) \leq D_{\alpha'}(\rho\|\sigma), \text{ when } \alpha' \geq \alpha.$
- Limits: $\lim_{\alpha\to 1} D_\alpha(\rho\|\sigma) = D(\rho\|\sigma)$

  $\lim_{\alpha\to\infty} D_\alpha(\rho\|\sigma) = D_{\max}(\rho\|\sigma) = \inf\{\lambda : \rho \leq 2^\lambda \sigma\}$

Muller-Lennert et al, JMP, 2013;
Wilde, Winter, Yang, CMP, 2014.

- Data processing inequality: $D_\alpha(\Phi(\rho)\|\Phi(\sigma)) \leq D_\alpha(\rho\|\sigma)$ for any $\alpha \geq \frac{1}{2}$ and quantum channel Φ

Operational meanings for Sandwiched Rényi relative entropy:

Prior work: strong converse exponents

- Mosonyi, Ogawa, CMP, 2015. (Quantum hypothesis testing)
- Mosonyi, Ogawa, CMP, 2017. (The capacity of the classical-quantum channel)
- Cheng, Hanson, Datta, Hsieh, IEEE Trans. Inf. Theory, 2020. (Data compression)

Introduction of the reliability function

Classical communication protocol:

classical channel $W:\mathcal{X}\to\mathcal{Y}$: a stochastic matrix

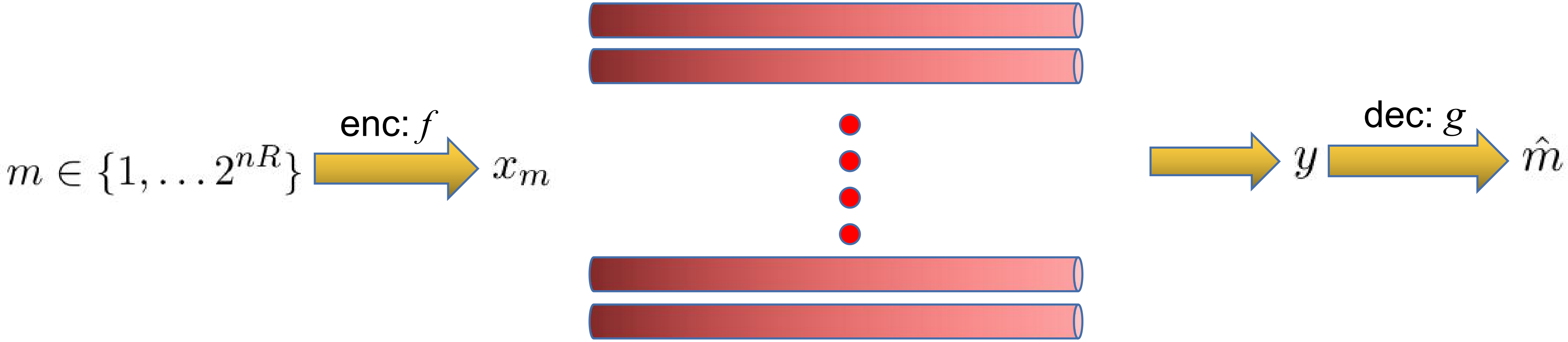
$$\sum_{y\in\mathcal{Y}} W(y|x) = 1,\ W(y|x)\geq 0, \quad \forall x\in\mathcal{X}, y\in\mathcal{Y}$$

$$m\in\mathcal{M}=\{1,\ldots,M\} \xrightarrow{\text{enc: } f} x_m \longrightarrow \boxed{W} \longrightarrow y \xrightarrow{\text{dec: } g} \hat{m}$$

The error for sending m: $\displaystyle\sum_{y\notin g^{-1}(m)} W(y|x_m)$

The average error: $\displaystyle P_e = \sum_{m\in\mathcal{M}} \frac{\sum_{y\notin g^{-1}(m)} W(y|x_m)}{M}$

Shannons second theorem:



$$R < C(W) = \max_{P_X} I(X:Y)_P, \quad P(x,y) = P(x)W(x|y)$$

$$R > C(W)$$

Reliability function for a classical channel

Definition 1 *Let* $W : \mathcal{X} \to \mathcal{Y}$ *be a classical channel. For a transmission rate* $0 < R < C(W)$*, the reliability function* $E(R)$ *of* W *is defined as*

$$E(R) := -\lim_{n\to\infty} \frac{1}{n} \log \min_{\mathcal{C}_n} \bar{P}_e(\mathcal{C}_n),$$

where $\mathcal{C}_n$ *runs over all protocol with* $|\mathcal{C}_n| = 2^{nR}$.

Introduction of the reliability function

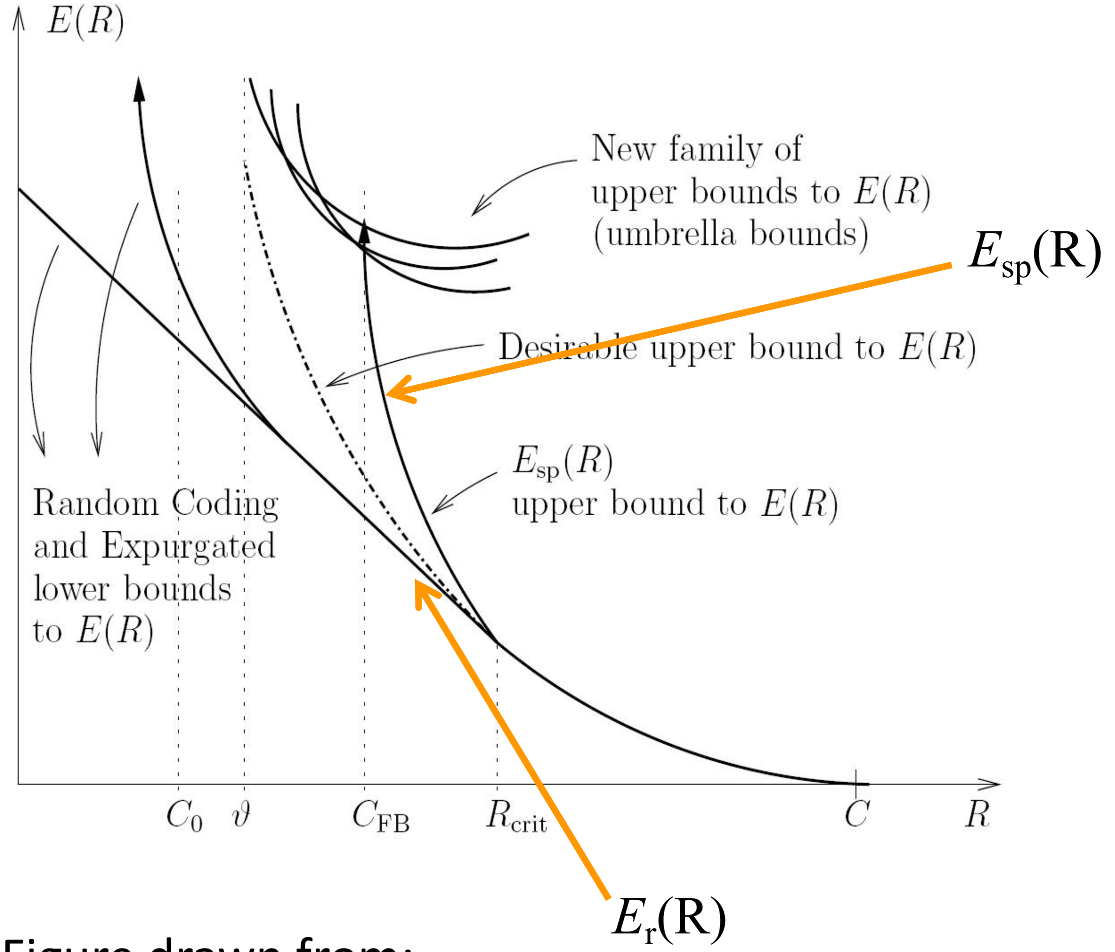


Figure drawn from:

Marco Dalai, IEEE Trans. Inf. Theory, 2013.

Random coding lower bound [Fano'61, Gallager'65]:

$$E_r(R) = \max_{0\leq\rho\leq 1} [E_0(\rho) - \rho R]$$

Sphere packing upper bound [Shannon-Gallager-Berlekamp'67]:

$$E_{sp}(R) = \sup_{\rho\geq 0} [E_0(\rho) - \rho R]$$

Where

$$E_0(\rho) = \max_P \; -\log \sum_y \left(\sum_x P(x) W_x(y)^{1/(1+\rho)} \right)^{1+\rho}$$

Reliability function in smoothing the max-relative entropy

Renner, Ph. D thesis, 2005.
Datta, IEEE Trans. Inf. Theory, 2009.

Smoothed max-relative entropy:

$$D_{\max}^{\epsilon}(\rho\|\sigma) := \inf_{\tilde{\rho}\in S_{\leq}(\mathcal{H}):P(\rho,\tilde{\rho})\leq\epsilon} D_{\max}(\tilde{\rho}\|\sigma).$$

Its inverse function (smoothing quantity):

$$\epsilon(\rho\|\sigma, r) := \inf\{\epsilon : D_{\max}^{\epsilon}(\rho\|\sigma) \leq r\} = \inf\{P(\rho,\tilde{\rho}) : \tilde{\rho} \leq 2^r\sigma \text{ and } \tilde{\rho} \in \mathrm{S}_{\leq}(\mathcal{H})\}$$

The meanings of the smoothed max-relative entropy :

- A basic tool in one-shot information theory (information spectrum relative entropy, hypothesis testing relative entropy, smoothed max-relative entropy).

- The ϵ-approximate distinguishability cost [Wang, Wilde, Physics Review Reasearch, 2019, Wilde, arxiv:2202.12433].

Reliability function in smoothing the max-relative entropy

The derivation for the upper bound of $\epsilon(\rho\|\sigma, r)$

Construct a subnormalized state $\tilde{\rho} := Q\rho Q,\quad \text{where } Q := \{\mathcal{E}_\sigma(\rho) \leq \frac{1}{v(\sigma)} 2^r \sigma\}$

$v(\sigma)$ denotes the number of different eigenvalues of σ

$\mathcal{E}_\sigma(\rho) = \sum_{i=1}^{v(\sigma)} \Pi_i \rho \Pi_i$, where Π_i is the projection onto the eignsubspace

by pinching inequality

$$\rho \leq v(\sigma)\mathcal{E}_\sigma(\rho)$$

$$\tilde{\rho} \leq v(\sigma) Q \mathcal{E}_\sigma(\rho) Q \leq 2^r \sigma$$

$$\epsilon(\rho\|\sigma, r) \leq P(\rho, \tilde{\rho}) \leq \sqrt{2 \operatorname{Tr} \rho(\mathbb{1} - Q)}$$

Reliability function in smoothing the max-relative entropy

Let $p = \operatorname{Tr} \rho(\mathbb{1} - Q)$ and $q = \operatorname{Tr} \sigma(\mathbb{1} - Q)$, then for any $s \geq 0$, we have

$$
\begin{aligned}
P(\rho, \tilde{\rho}) &\leq \sqrt{2 p^{1+s} p^{-s}} \leq \sqrt{2 \left(p^{1+s} \big(\frac{1}{v(\sigma)} 2^{\lambda} q\big)^{-s} \right)} \\
&\leq \sqrt{2 \left(p^{1+s} \big(\frac{1}{v(\sigma)} 2^{\lambda} q\big)^{-s} + (1-p)^{1+s} \big(\frac{1}{v(\sigma)} 2^{\lambda} (\operatorname{Tr} \sigma - q)\big)^{-s} \right)} \\
&= \sqrt{2 v(\sigma)^{s}\, 2^{s \left(D_{1+s}((p, 1-p) \| (q, \operatorname{Tr} \sigma - q)) - \lambda \right)}} \\
&\leq \sqrt{2 v(\sigma)^{s}\, 2^{s \left(D_{1+s}(\rho \| \sigma) - \lambda \right)}},
\end{aligned}
$$

Reliability function in smoothing the max-relative entropy

The derivation for the lower bound of $\epsilon(\rho\|\sigma, r)$

Let ρ_n be any subnormalized state with $\rho_n \leq 2^{nr}\sigma^{\otimes n}$, $Q_n := \{\rho^{\otimes n} > 9.2^{nr}\sigma^{\otimes n}\}$ and $p_n = \operatorname{Tr}\rho^{\otimes n}Q_n$, $q_n = \operatorname{Tr}\rho_n Q_n$

$$\boxed{\begin{aligned} Q_n\rho^{\otimes n}Q_n &\geq 9 \cdot 2^{nr} Q_n \sigma^{\otimes n} Q_n \\ &\geq 9 Q_n \rho_n Q_n, \end{aligned}}$$

$$p_n \geq 9 q_n$$

by the monotonicity of the fidelity under quantum channels

$$\begin{aligned} F(\rho^{\otimes n}, \rho_n) &\leq F\big((p_n, 1-p_n), (q_n, \operatorname{Tr}\rho_n - q_n)\big) \\ &\leq \sqrt{p_n}\sqrt{q_n} + \sqrt{1-p_n} \\ &\leq \frac{p_n}{3} + \sqrt{1-p_n}, \end{aligned}$$

Reliability function in smoothing the max-relative entropy

$$
\begin{aligned}
F(\rho^{\otimes n}, \rho_n) &\leq F\big((p_n, 1-p_n), (q_n, \operatorname{Tr}\rho_n - q_n)\big) \\
&\leq \sqrt{p_n}\sqrt{q_n} + \sqrt{1-p_n} \\
&\leq \frac{p_n}{3} + \sqrt{1-p_n},
\end{aligned}
$$

$$
\begin{aligned}
P(\rho^{\otimes n}, \rho_n) &= \sqrt{1 - F^2(\rho^{\otimes n}, \rho_n)} \\
&\geq \sqrt{1 - \left(\frac{p_n}{3} + \sqrt{1-p_n}\right)^2} \\
&= \sqrt{-\frac{p_n^2}{9} + p_n - \frac{2p_n}{3}\sqrt{1-p_n}} \\
&\geq \sqrt{p_n}\sqrt{-\frac{p_n}{9} + 1 - \frac{2}{3}} \\
&= \sqrt{p_n}\sqrt{\frac{1}{3} - \frac{p_n}{9}}.
\end{aligned}
$$

$$
\epsilon(\rho^{\otimes n} \| \sigma^{\otimes n}, nr) \geq \sqrt{p_n}\sqrt{\frac{1}{3} - \frac{p_n}{9}}.
$$

Reliability function in smoothing the max-relative entropy

For any $s \geq 0$, we have

$$\sqrt{p_n}\sqrt{\frac{1}{3}-\frac{p_n}{9}} \leq \epsilon(\rho^{\otimes n}\|\sigma^{\otimes n}, nr) \leq \sqrt{2v(\sigma^{\otimes n})^s 2^{ns(D_{1+s}(\rho\|\sigma)-r)}}$$

Main result 1:

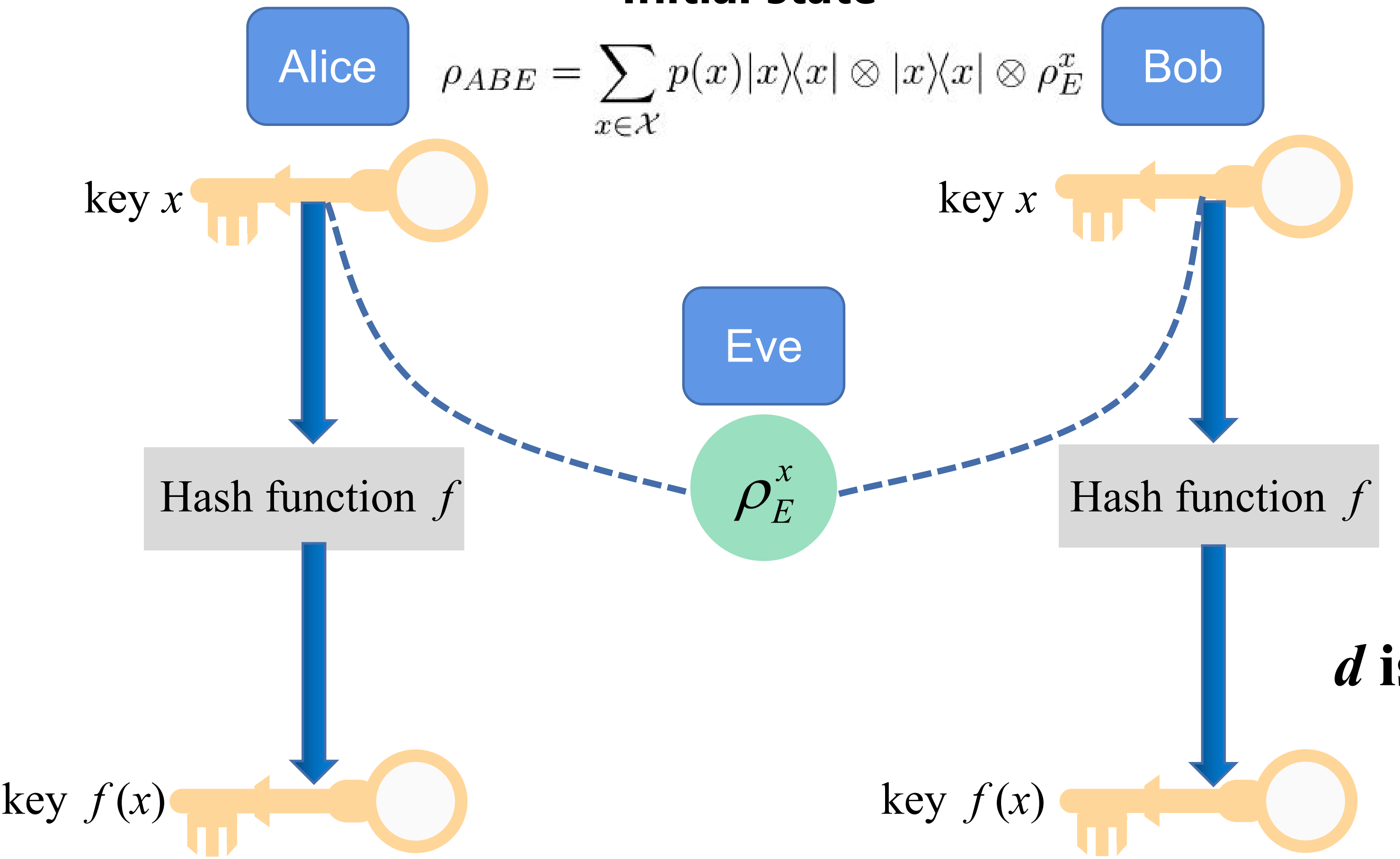
Theorem 1 *For quantum states ρ, σ and $r \in \mathbb{R}$, we have*

$$\lim_{n\to+\infty} \frac{-1}{n}\epsilon(\rho^{\otimes n}\|\sigma^{\otimes n}, nr) = \frac{1}{2}\sup_{s\geq 0}\left\{s\big(r - D_{1+s}(\rho\|\sigma)\big)\right\}.$$

Reliability function for privacy amplification

Initial state

$$\rho_{ABE} = \sum_{x \in \mathcal{X}} p(x) |x\rangle\langle x| \otimes |x\rangle\langle x| \otimes \rho_E^x$$



Final state

$$\rho^f_{ZZ'E} = \sum_{z \in \mathcal{Z}} |z\rangle\langle z| \otimes |z\rangle\langle z| \otimes \Big(\sum_{x \in f^{-1}(z)} p(x) \rho_E^x \Big)$$

Devetak, Winter, P. Roy. Soc. A, 2005

The performance of the scheme

$$\boxed{d\left(\rho^f_{ZE}, \frac{\mathbb{1}_Z}{|\mathcal{Z}|} \otimes \rho_E\right)}$$

d **is a security measure on the set of states**

d
- trace norm distance
- purified distance
- Umegaki relative entropy
- ⋮

Reliability function for privacy amplification

Definition 2 *For a classical-quantum state ρ_{XE} and a key rate $0 < R < H(X|E)_\rho$, the reliability function $E(R)$ under distance d is defined as*

$$E(R) := -\lim_{n\to\infty} \frac{1}{n} \log \min_{f_n} d(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}),$$

where f_n runs over all hash function from $\mathcal{X}^{\times n} :\to \mathcal{Z}_n = \{1, \ldots, 2^{nR}\}$.

Reliability function for privacy amplification

The derivation for the upper bound of the reliability function

For any hash function $f : \mathcal{X} \to \mathcal{Z}$, we have

$$H^{\epsilon}_{\min}(X|E)_{\rho} \geq H^{\epsilon}_{\min}(Z|E)_{\rho^f},$$

where $H^{\epsilon}_{\min}(X|E)_{\rho} = -D^{\epsilon}_{\max}(\rho_{XE} \| \mathbb{1}_X \otimes \rho_E)$.

For any hash function $f : \mathcal{X} \to \mathcal{Z}$ and $\lambda \in \mathbb{R}$, we have

$$\epsilon(\rho^f_{ZE} \| \mathbb{1}_Z \otimes \rho_E, \lambda) \geq \epsilon(\rho_{XE} \| \mathbb{1}_X \otimes \rho_E, \lambda).$$

Reliability function for privacy amplification

$$P\left(\rho^f_{ZE}, \frac{\mathbb{1}_Z}{|\mathcal{Z}|} \otimes \rho_E\right) \geq \epsilon\left(\rho^f_{ZE} \| \mathbb{1}_Z \otimes \rho_E, -\log|\mathcal{Z}|\right) \geq \epsilon\left(\rho_{XE} \| \mathbb{1}_X \otimes \rho_E, -\log|\mathcal{Z}|\right)$$

$$\min_{f_n} P\left(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\right) \geq \epsilon\left(\rho_{XE}^{\otimes n} \| \mathbb{1}_X^{\otimes n} \otimes \rho_E^{\otimes n}, -nR\right)$$

Main result 2

Theorem 2 *Let ρ_{XE} be a classical-quantum state, $0 < R < H(X|E)_\rho$. We have*

$$\lim_{n\to+\infty} \frac{-1}{n} \log \min_{f_n} P\left(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\right) \leq \frac{1}{2} \max_{t\geq 0} t\left(H_{1+t}(X|E)_\rho - R\right).$$

Error exponent for randomness extraction against quantum side information

Our upper bound:

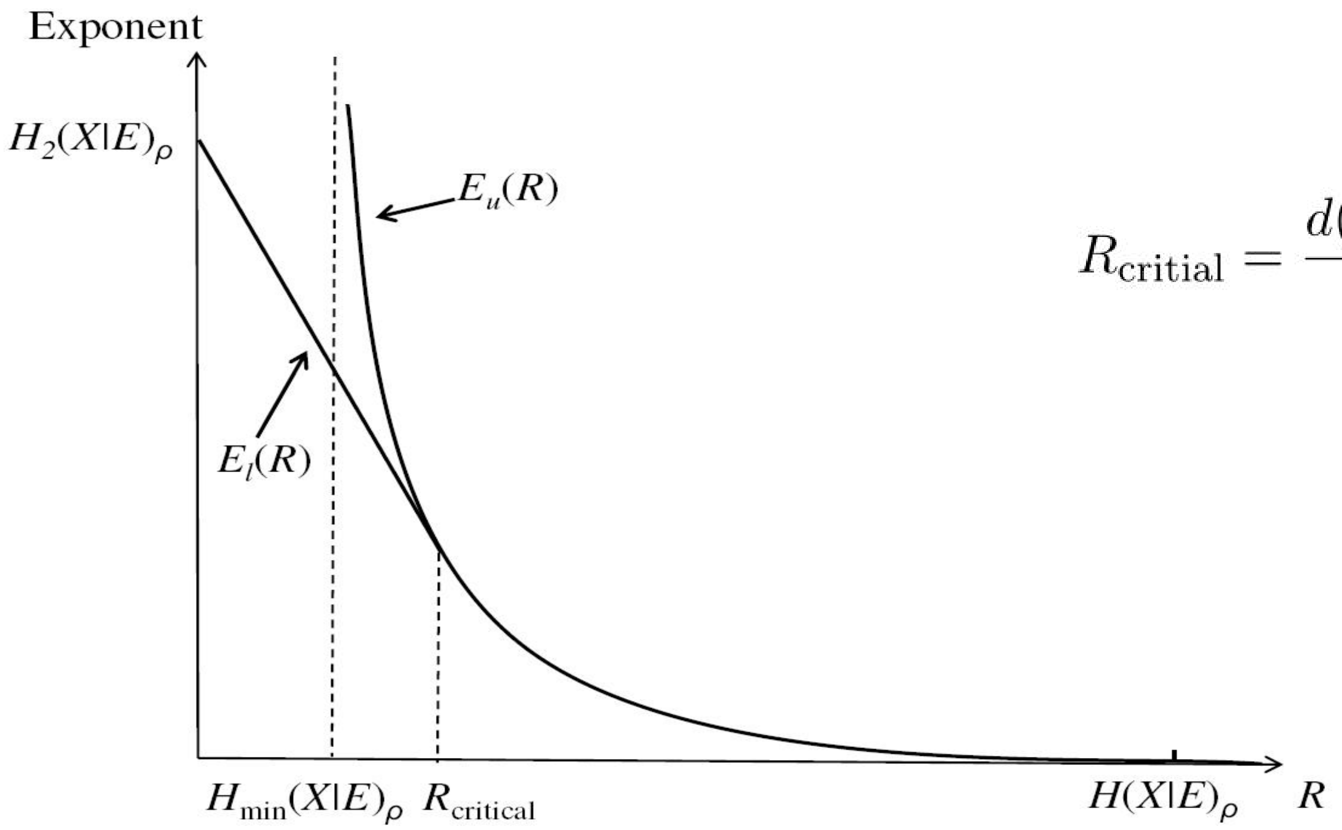
Theorem 2 *Let ρ_{XE} be a classical-quantum state, $0 < R < H(X|E)_\rho$. We have*

$$\lim_{n\to+\infty} \frac{-1}{n} \log \min_{f_n} P\left(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\right) \leq \frac{1}{2} \max_{t\geq 0} t\left(H_{1+t}(X|E)_\rho - R\right).$$

Corresponding lower bound derived from [Hayashi, CMP, 2015]: $P(\rho,\sigma) \leq \sqrt{(\ln 2) D(\rho||\sigma)}$

$$\lim_{n\to+\infty} \frac{-1}{n} \log \min_{f_n} P\left(\rho^{f_n}_{Z_n E^n}, \frac{\mathbb{1}_{Z_n}}{|\mathcal{Z}_n|} \otimes \rho_E^{\otimes n}\right) \geq \frac{1}{2} \max_{0\leq t\leq 1} t\left(H_{1+t}(X|E)_\rho - R\right).$$

Error exponent for randomness extraction against quantum side information



$$R_{\text{critial}} = \frac{d(sH_{1+s}(X|E)_\rho)}{ds}\Big|_{s=1}$$

$$E_u(R) := \frac{1}{2}\max_{t\geq 0}\left\{t\big(H_{1+t}(X|E)_\rho - R\big)\right\}$$ (Our upper bound)

$$E_l(R) := \frac{1}{2}\max_{0\leq t\leq 1}\left\{t\big(H_{1+t}(X|E)_\rho - R\big)\right\}$$ (lower bound derived from [Hayashi, CMP, 2015])

Summary and open questions

- We derive the reliability function in smoothing the max-relative entropy and of privacy amplification.
- We provide new type of operational meanings for the sandwiched Rényi divergence, in characterizing how fast the performance of quantum tasks approach the perfect.
- The reliability function in smoothing the max-relative entropy has applications in quantum information decoupling and quantum channel simulation [K. Li, Y. Yao, arxiv: 2111.06343, 2112.04475].
- Question 1: reliability function for privacy amplification below the critical rate?
- Question 2: reliability function for more quantum information tasks? (might discover new quantum Rényi relative entropy.)

Thank you !