Strong converse theorems using Rényi entropies

Felix Leditzky

joint work with Mark M. Wilde and Nilanjana Datta

arXiv:1506.02635

UNIVERSITY OF CAMBRIDGE

5 January 2016

Table of Contents

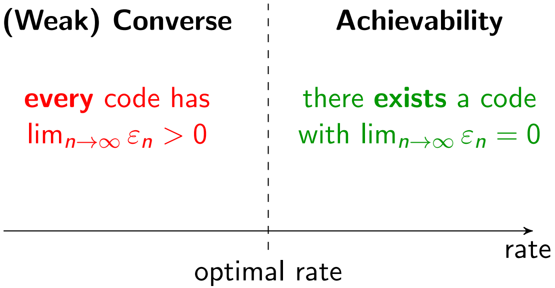
1. Weak vs. strong converse
2. Rényi entropies
3. State redistribution: definition and strong converse
4. Further results and outlook

Table of Contents

1. Weak vs. strong converse
2. Rényi entropies
3. State redistribution: definition and strong converse
4. Further results and outlook

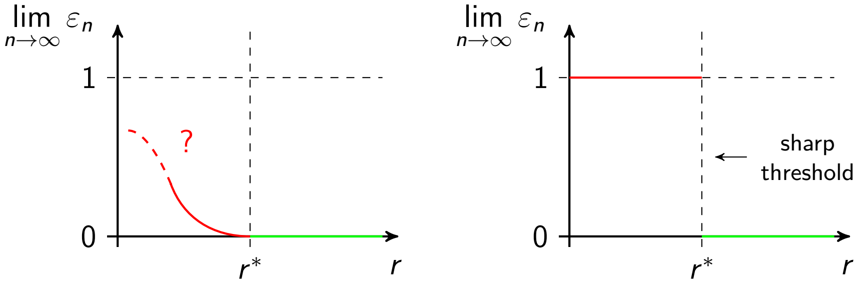
Optimal rates of information-theoretic tasks

- Information-theoretic tasks: source coding, channel coding, ...
- Operational definition of a rate of the code: compression rate, capacity, ...
- Coding theorem establishes entropic quantity as **optimal rate**:



Strong converse property

- Weak converse: trade-off between error ε_n and rate r below optimal rate r^*?
- Strong converse theorem: No!
  Every code at rate below the optimal rate **fails with certainty**!
- Optimal rate satisfies *strong converse property*.



Strong converse property

Example: Quantum data compression

- Optimal compression rate [Schumacher 1995]:
  $r^* = S(\rho) = -\operatorname{Tr}(\rho \log \rho)$
- Strong converse for data compression [Winter 1999]:
  For every code with rate $r < S(\rho)$, we have

$$\varepsilon_n \geq 1 - \exp(-Kn)$$

  for some $K > 0$, and hence $\lim_{n\to\infty} \varepsilon_n = 1$ (since $\varepsilon_n \in [0,1]$).
- Exponential convergence of error
  $\longrightarrow$ strong converse in the *Wolfowitz sense* [Wolfowitz 1961].

How can we prove strong converse theorems?

- Winter: method of types
- Here: Rényi entropy approach [Arimoto 1973; Ogawa and Nagaoka 1999]
- Derive lower bound on error in terms of a **Rényi entropic quantity**

Table of Contents

1 Weak vs. strong converse

2 Rényi entropies

3 State redistribution: definition and strong converse

4 Further results and outlook

Rényi entropies

Definition (Sandwiched Rényi divergence of order α)

Let $\alpha \in (0, \infty) \setminus \{1\}$ and ρ, σ be quantum states with $\operatorname{supp}\rho \subseteq \operatorname{supp}\sigma$:

$$\widetilde{D}_\alpha(\rho\|\sigma) := \frac{1}{\alpha - 1} \log \operatorname{Tr}\left(\sigma^{(1-\alpha)/2\alpha}\rho\sigma^{(1-\alpha)/2\alpha}\right)^\alpha .$$

- **Additivity:** $\widetilde{D}_\alpha(\rho_1 \otimes \rho_2\|\sigma_1 \otimes \sigma_2) = \widetilde{D}_\alpha(\rho_1\|\sigma_1) + \widetilde{D}_\alpha(\rho_2\|\sigma_2)$
- **Data processing inequality:** [Beigi 2013; Frank and Lieb 2013]
  For a quantum channel Λ and $\alpha \geq 1/2$,
  $$\widetilde{D}_\alpha(\rho\|\sigma) \geq \widetilde{D}_\alpha(\Lambda(\rho)\|\Lambda(\sigma)).$$
- **Limit property:**
  $$\widetilde{D}_\alpha(\rho\|\sigma) \xrightarrow{\alpha\to 1} D(\rho\|\sigma) = \operatorname{Tr}[\rho(\log\rho - \log\sigma)]$$

Rényi entropic quantities

The sandwiched Rényi divergence (α-SRD) serves as a parent for the following quantities:

Definition (Entropic quantities derived from α-SRD)

Let $\alpha > 0$ and ρ_{AB} be a bipartite quantum state with marginal ρ_A.

- **Rényi entropy**

$$S_\alpha(A)_\rho := -\widetilde{D}_\alpha(\rho_A \| \mathbb{1}_A)$$

- **Rényi conditional entropy** (RCE)

$$\widetilde{S}_\alpha(A|B)_\rho := -\min_{\sigma_B} \widetilde{D}_\alpha(\rho_{AB} \| \mathbb{1}_A \otimes \sigma_B)$$

- **Rényi mutual information** (RMI)

$$\tilde{I}_\alpha(A;B)_\rho := \min_{\sigma_B} \widetilde{D}_\alpha(\rho_{AB} \| \rho_A \otimes \sigma_B)$$

Rényi entropic quantities

These quantities inherit some of the properties of the α-SRD:

- **Additivity** [Hayashi and Tomamichel 2014]
  Let $\rho_{A_1B_1}$ and $\sigma_{A_2B_2}$ be quantum states, then
  $$\widetilde{S}_\alpha(A_1A_2|B_1B_2)_{\rho\otimes\sigma} = \widetilde{S}_\alpha(A_1|B_1)_\rho + \widetilde{S}_\alpha(A_2|B_2)_\sigma$$
  $$\tilde{I}_\alpha(A_1A_2;B_1B_2)_{\rho\otimes\sigma} = \tilde{I}_\alpha(A_1;B_1)_\rho + \tilde{I}_\alpha(A_2;B_2)_\sigma.$$
- **Data processing inequality**
  Let $\Lambda\colon B \to C$ be a quantum channel, and $\omega_{AC} = (\mathrm{id}_A \otimes \Lambda)(\rho_{AB})$, then for $\alpha \geq 1/2$ we have
  $$\widetilde{S}_\alpha(A|B)_\rho \leq \widetilde{S}_\alpha(A|C)_\omega \qquad \tilde{I}_\alpha(A;B)_\rho \geq \tilde{I}_\alpha(A;C)_\omega.$$
- **Limit property**
  $$S_\alpha(A)_\rho \xrightarrow{\alpha\to 1} S(A)_\rho$$
  $$\widetilde{S}_\alpha(A|B)_\rho \xrightarrow{\alpha\to 1} S(A|B)_\rho = S(AB)_\rho - S(B)_\rho$$
  $$\tilde{I}_\alpha(A;B)_\rho \xrightarrow{\alpha\to 1} I(A;B)_\rho = S(A)_\rho - S(A|B)_\rho$$

Extending the Rényi entropy calculus

We prove the following new properties for these quantities:

Theorem (Dimension bounds)

For $\alpha \geq 1/2$ and a tripartite state ρ_{ABC} with C quantum,

$$\widetilde{S}_\alpha(A|BC)_\rho + 2\log|C| \geq \widetilde{S}_\alpha(A|B)_\rho$$
$$\tilde{I}_\alpha(A;B)_\rho + 2\log|C| \geq \tilde{I}_\alpha(A;BC)_\rho$$

whereas for ρ_{ABX} with X classical,

$$\widetilde{S}_\alpha(A|BX)_\rho + \log|X| \geq \widetilde{S}_\alpha(A|B)_\rho$$
$$\tilde{I}_\alpha(A;B)_\rho + \log|X| \geq \tilde{I}_\alpha(A;BX)_\rho.$$

Extending the Rényi entropy calculus

We prove the following new properties for these quantities:

Theorem (Fidelity bounds)

For $\alpha \in (1/2, 1)$, $\beta = \alpha/(2\alpha - 1)$, and bipartite states ρ_{AB} and σ_{AB},

$$S_\alpha(A)_\rho - S_\beta(A)_\sigma \geq \frac{2\alpha}{1-\alpha} \log F(\rho_A, \sigma_A) \qquad (*)$$

$$\widetilde{S}_\alpha(A|B)_\rho - \widetilde{S}_\beta(A|B)_\sigma \geq \frac{2\alpha}{1-\alpha} \log F(\rho_{AB}, \sigma_{AB})$$

$$\tilde{I}_\beta(A;B)_\rho - \tilde{I}_\alpha(A;B)_\sigma \geq \frac{2\alpha}{1-\alpha} \log F(\rho_{AB}, \sigma_{AB})$$

where $F(\omega, \tau) := \|\sqrt{\omega}\sqrt{\tau}\|_1$ is the fidelity.

Eq. $(*)$ first appeared in [van Dam and Hayden 2002], and we generalize this result to the Rényi conditional entropy and mutual information.

Table of Contents

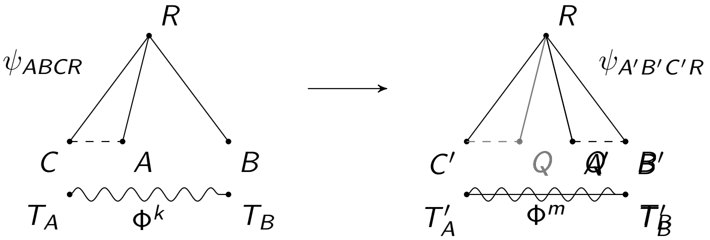
1 Weak vs. strong converse

2 Rényi entropies

3 State redistribution: definition and strong converse

4 Further results and outlook

State redistribution: protocol



- target state: $\psi_{A'B'C'R} \otimes \Phi^m_{T'_A T'_B}$ $(A'B'C' \cong ABC)$
- figure of merit: $F\left(\psi \otimes \Phi^m, (\mathcal{D} \circ \mathcal{E})(\psi \otimes \Phi^k)\right)$
- # of qubits sent from Alice to Bob: $\log |Q|$
- # of ebits consumed: $\log |T_A| - \log |T'_A| = \log k - \log m$
(if $\log k < \log m$, then ebits are gained)

State redistribution: protocol

n copies of ρ_{ABC}:

- **Initial state:** $\psi_{ABCR}^{\otimes n} \otimes \Phi_{T_A T_B}^{k_n}$
- **Overall map:** Encoding $\mathcal{E}_n$, quantum communication Q, and decoding $\mathcal{D}_n$.
- **Target state:** $\psi_{A'B'C'R}^{\otimes n} \otimes \Phi_{T_A' T_B'}^{m_n}$
- **Figure of merit:** $F_n := F\left(\psi^{\otimes n} \otimes \Phi^{m_n}, (\mathcal{D}_n \circ \mathcal{E}_n)(\psi^{\otimes n} \otimes \Phi^{k_n})\right)$
- **Quantum communication cost:** $q_n := \frac{1}{n} \log |Q^n|$
- **Entanglement cost:** $e_n := \frac{1}{n}(\log k_n - \log m_n)$

State redistribution: optimal rates

Definition (Achievable rates)

(e, q) is achievable: For $\rho \equiv \rho_{ABC}$ there is a protocol $\{(\rho^{\otimes n}, \mathcal{E}_n, \mathcal{D}_n)\}_{n\in\mathbb{N}}$ with $\lim_{n\to\infty} F_n = 1$ and

$$\limsup_{n\to\infty} e_n = e, \qquad \limsup_{n\to\infty} q_n = q.$$

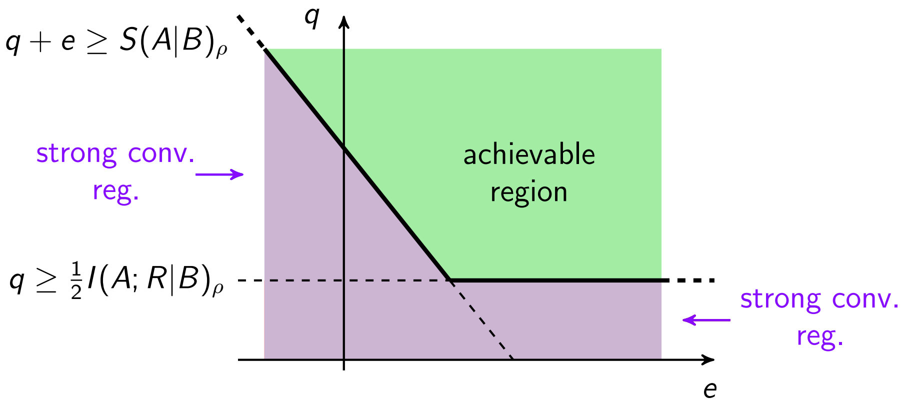
Theorem (Luo and Devetak 2009; Yard and Devetak 2009)

The pair (e, q) is achievable if and only if

$$q \geq \frac{1}{2} I(A; R|B)_\rho \qquad q + e \geq S(A|B)_\rho.$$

Conditional mutual information (CMI): $I(A; R|B)_\rho = S(A|B)_\rho - S(A|RB)_\rho$

Main result: strong converse region



State redistribution: Strong converse theorem

Main result:

Theorem

For every state redistribution protocol with initial state ρ_{ABC}, we have the following bounds on F_n for all $n \in \mathbb{N}$ and $\alpha \in (1/2, 1)$, setting $\beta = \alpha/(2\alpha - 1)$ and $\kappa(\alpha) = (1-\alpha)/(2\alpha) > 0$:

$$F_n \leq \exp\left\{-n\kappa(\alpha)\left[S_\beta(AB)_\rho - S_\alpha(B)_\rho - (q_n + e_n)\right]\right\}$$

$$F_n \leq \exp\left\{-n\kappa(\alpha)\left[\widetilde{S}_\beta(R|B)_\rho - \widetilde{S}_\alpha(R|AB)_\rho - 2q_n\right]\right\}$$

As an alternative to the second bound, we also have

$$F_n \leq \exp\left\{-n\kappa(\alpha)\left[\tilde{I}_\alpha(R;AB)_\rho - \tilde{I}_\beta(R;B)_\rho - 2q_n\right]\right\}$$

State redistribution: Strong converse theorem

Bounds on fidelity ($\beta \equiv \beta(\alpha) = \alpha/(2\alpha - 1)$)

$$F_n \leq \exp\{-n\kappa(\alpha)[S_\beta(AB)_\rho - S_\alpha(B)_\rho - (q_n + e_n)]\}$$

$$F_n \leq \exp\left\{-n\kappa(\alpha)\left[\widetilde{S}_\beta(R|B)_\rho - \widetilde{S}_\alpha(R|AB)_\rho - 2q_n\right]\right\}$$

Optimal rates: $q + e \geq S(A|B)_\rho$, $q \geq \frac{1}{2}I(A;R|B)_\rho$

- Rényi generalization of conditional entropy: $S_{\beta(\alpha)}(AB)_\rho - S_\alpha(B)_\rho \xrightarrow{\alpha\to 1} S(AB)_\rho - S(B)_\rho = S(A|B)_\rho$
- Converse region: $q_n + e_n < S(A|B)_\rho$
- There is $\alpha_0 \in (1/2, 1)$ such that $C := \kappa(\alpha_0)[S_{\beta(\alpha_0)}(AB)_\rho - S_{\alpha_0}(B)_\rho - (q_n + e_n)] > 0.$
- **Strong converse:** $F_n \leq \exp\{-nC\} \xrightarrow{n\to\infty} 0$

State redistribution: Strong converse theorem

Bounds on fidelity ($\beta \equiv \beta(\alpha) = \alpha/(2\alpha - 1)$)

$$F_n \leq \exp\{-n\kappa(\alpha)[S_\beta(AB)_\rho - S_\alpha(B)_\rho - (q_n + e_n)]\}$$

$$F_n \leq \exp\left\{-n\kappa(\alpha)\left[\widetilde{S}_\beta(R|B)_\rho - \widetilde{S}_\alpha(R|AB)_\rho - 2q_n\right]\right\}$$

Optimal rates: $q + e \geq S(A|B)_\rho$, $q \geq \frac{1}{2}I(A;R|B)_\rho$

- Rényi generalization of conditional mutual information: $\widetilde{S}_{\beta(\alpha)}(R|B)_\rho - \widetilde{S}_\alpha(R|AB)_\rho \xrightarrow{\alpha\to 1} S(R|B)_\rho - S(R|AB)_\rho = I(A;R|B)_\rho$
- Converse region: $2q_n < I(A;R|B)_\rho$
- As before, this yields a **strong converse:** $F_n \leq \exp\{-nC\} \xrightarrow{n\to\infty} 0$ for some $C > 0$.

Proof sketch

Strong converse property for $q_n + e_n$

- Strategy: Prove for $n = 1$ and then use additivity of Rényi quantities.
- Define post-encoding state

$$|\omega_{C'QBRT'_A T_B E}\rangle := U_{\mathcal{E}}\left(|\psi_{ABCR}\rangle \otimes |\Phi^k_{T_A T_B}\rangle\right)$$

  where $U_{\mathcal{E}}$ is a Stinespring isometry of Alice's encoding map $\mathcal{E}\colon ACT_A \to QC'T'_A$ with environment E.
- **"Subadditivity" property for Rényi entropies:**
  [van Dam and Hayden 2002] For $\alpha > 0$ and a bipartite state ρ_{AB},

$$S_\alpha(A)_\rho - \log|B| \leq S_\alpha(AB)_\rho \leq S_\alpha(A)_\rho + \log|B|$$

- For the marginal ω_{QBT_B}, this yields

$$S_\alpha(QBT_B)_\omega \leq \log|Q| + \log|T_A| + S_\alpha(B)_\rho.$$

Proof idea

- Define final state

$$|\sigma_{A'B'C'RT'_AT'_BED}\rangle := U_{\mathcal{D}}|\omega_{C'QBRT'_AT_BE}\rangle$$

  where $U_{\mathcal{D}}$ is a Stinespring isometry of Bob's decoding map $\mathcal{D}\colon QBT_B \to A'B'T'_B$ with environment D.
- Isometric invariance: $S_\alpha(QBT_B)_\omega = S_\alpha(A'B'T'_BD)_\sigma$.
- Uhlmann:

$$F = F(\psi \otimes \Phi^m, (\mathcal{D} \circ \mathcal{E})(\psi \otimes \Phi^k)) \leq F(\sigma_{A'B'T'_BD}, \pi^m_{T'_A} \otimes \rho_{A'B'} \otimes \chi_D)$$

- Fidelity bound applied to $\sigma_{A'B'T'_BD}$ and $\pi^m_{T'_A} \otimes \rho_{A'B'} \otimes \chi_D$ yields

$$S_\alpha(A'B'T'_BD)_\sigma \geq \log|T'_A| + S_\beta(A'B')_\rho + \frac{2\alpha}{1-\alpha}\log F.$$

Proof idea

- Both bounds together:

$$\frac{2\alpha}{1-\alpha}\log F \leq \log|Q| + \log|T_A| - \log|T'_A| - S_\beta(AB)_\rho + S_\alpha(B)_\rho$$

- $\log|Q| \longleftrightarrow$ quantum communication cost (for $n=1$)
- $\log|T_A| - \log|T'_A| \longleftrightarrow$ entanglement cost (for $n=1$)
- n copies of ρ_{ABC}:

$$\begin{aligned}\frac{2\alpha}{1-\alpha}\log F_n &\leq \log|Q| + \log|T_A| - \log|T'_A| \\ &\quad - S_\beta(A^nB^n)_{\rho^{\otimes n}} + S_\alpha(B^n)_{\rho^{\otimes n}} \\ &= n\left(q_n + e_n - S_\beta(AB)_\rho + S_\alpha(B)_\rho\right)\end{aligned}$$

Table of Contents

1 Weak vs. strong converse

2 Rényi entropies

3 State redistribution: definition and strong converse

4 Further results and outlook

More strong converse theorems

Using the Rényi entropy method, we derive strong converse theorems for the following protocols (details in [arXiv:1506.02635]):

1. State redistribution with feedback (allowing quantum communication from Bob to Alice)
2. Coherent state merging and quantum state splitting (special cases of state redistribution)
3. Measurement compression with quantum side information (QSI)
4. Randomness extraction against QSI
5. Data compression with QSI

Open questions

Applications of the fidelity bound

- Crucial mathematical result in the proofs:

$$\widetilde{S}_\alpha(A|B)_\rho - \widetilde{S}_\beta(A|B)_\sigma \geq \frac{2\alpha}{1-\alpha} \log F(\rho_{AB}, \sigma_{AB})$$

  where $\alpha \in (1/2, 1)$ and $\beta = \alpha/(2\alpha - 1)$.
- Can we use this to derive strong converse theorems for other protocols?
- Example: Strong converse for degradable channels
- In entanglement generation, fidelity bound yields a bound on figure of merit in terms of entanglement generation capacity and a "Rényi coherent information".
- Additivity result or other estimates for this quantity needed to infer strong converse theorem.

References

Arimoto, S. (1973). *IEEE Transactions on Information Theory* 19.3, pp. 357–359.

Beigi, S. (2013). *Journal of Mathematical Physics* 54.12, p. 122202. arXiv: 1306.5920 [quant-ph].

Berta, M. et al. (2014). *arXiv preprint arXiv:1409.4338*.

Frank, R. L. and E. H. Lieb (2013). *Journal of Mathematical Physics* 54.12, p. 122201. arXiv: 1306.5358 [math-ph].

Hayashi, M. and M. Tomamichel (2014). *arXiv preprint*. arXiv: 1408.6894 [quant-ph].

Leditzky, F. et al. (2015). *arXiv preprint arXiv:1506.02635*.

Luo, Z. and I. Devetak (2009). *IEEE Transactions on Information Theory* 55.3, pp. 1331–1342.

Ogawa, T. and H. Nagaoka (1999). *IEEE Transactions on Information Theory* 45, pp. 2486–2489.

Schumacher, B. (1995). *Physical Review A* 51.4, p. 2738.

Winter, A. (1999). *IEEE Transactions on Information Theory* 45.7, pp. 2481–2485.

Wolfowitz, J. (1961). 31. Springer Berlin-Göttingen-Heidelberg.

Yard, J. T. and I. Devetak (2009). *IEEE Transactions on Information Theory* 55.11, pp. 5339–5351.

van Dam, W. and P. Hayden (2002). *arXiv preprint quant-ph/0204093*.

Thank you very much!