Second-Order Coding Rates for Entanglement-Assisted Communication

Nilanjana Datta[1], Marco Tomamichel[2], and Mark M. Wilde[3]

[1]Statistical Laboratory, Centre for Mathematical Sciences, University of Cambridge
[2]School of Physics, The University of Sydney
[3]Center for Computation and Technology, Dept. of Physics & Astronomy, Louisiana State University

THE UNIVERSITY OF SYDNEY

ISIT 2015, Hong Kong

$$C(W) := \max_{P_X} I(X:Y)_T, \quad \text{where} \quad T_{XY} = P_X W_{Y|X}$$

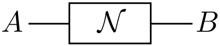
- Shannon's capacity formula is surprisingly robust if we give sender and receiver additional free resources.
  - shared randomness
  - entanglement
  - back-communication
  - non-signaling correlations
- For quantum channels some of these capacities are different.
  - Unassisted capacity: no single-letter formula known.
  - **Entanglement-assisted (EA) capacity**: natural generalization of Shannon's formula (Bennett *et al.*'02).

$$C_{\text{ea}}(\mathcal{N}) = \max_{\rho_A} I(A:B)_\tau, \quad \text{where} \quad \tau_{AB} = \mathcal{N}_{A' \to B}\big(|\psi^\rho\rangle\langle\psi^\rho|_{AA'}\big)$$

- We study non-asymptotic fundamental limits for EA communication over quantum channels.

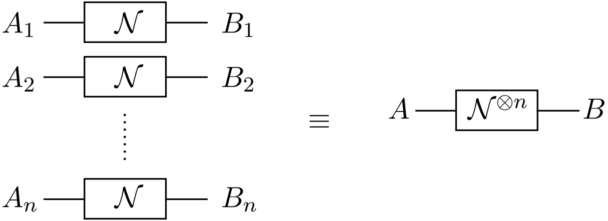
Ingredients: Channel

- **Quantum channel**: completely positive trace-preserving map $\mathcal{N} \equiv \mathcal{N}_{A \to B}$ from (linear operators on) A to B.



  We assume A and B are finite-dimensional Hilbert spaces.

- The channel is memoryless:



Ingredients: Code

- **Entanglement-Assisted Code:** quadruple

$$\mathcal{C}_n = \Big\{ \mathcal{M},\, |\varphi\rangle_{A'B'},\, \{\mathcal{E}^m_{A'\to A}\}_{m\in\mathcal{M}},\, \{\Lambda^m_{BB'}\}_{m\in\mathcal{M}} \Big\}.$$

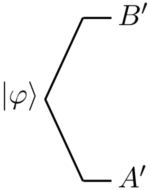
1. Set of messages: $\mathcal{M}$.
2. Resource state: $|\varphi\rangle_{A'B'}$.
3. encoder $\mathcal{E}$: a quantum channel $\mathcal{E}^m_{A'\to A}$ for each message m.
4. decoder $\mathcal{D}$: a positive operator valued measure where $\Lambda^m_{BB'}$ indicates that we decode to m.

Ingredients: Code

- **Entanglement-Assisted Code:** quadruple

$$\mathcal{C}_n = \Big\{ \mathcal{M},\, |\varphi\rangle_{A'B'},\, \{\mathcal{E}^m_{A'\to A}\}_{m\in\mathcal{M}},\, \{\Lambda^m_{BB'}\}_{m\in\mathcal{M}} \Big\}.$$

1. Set of messages: $\mathcal{M}$.
2. Resource state: $|\varphi\rangle_{A'B'}$.
3. encoder $\mathcal{E}$: a quantum channel $\mathcal{E}^m_{A'\to A}$ for each message m.
4. decoder $\mathcal{D}$: a positive operator valued measure where $\Lambda^m_{BB'}$ indicates that we decode to m.

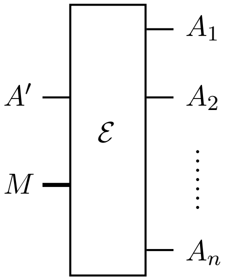


Ingredients: Code

- **Entanglement-Assisted Code:** quadruple

$$\mathcal{C}_n = \left\{ \mathcal{M},\, |\varphi\rangle_{A'B'},\, \{\mathcal{E}^m_{A'\to A}\}_{m\in\mathcal{M}},\, \{\Lambda^m_{BB'}\}_{m\in\mathcal{M}} \right\}.$$

1. Set of messages: $\mathcal{M}$.
2. Resource state: $|\varphi\rangle_{A'B'}$.
3. encoder $\mathcal{E}$: a quantum channel $\mathcal{E}^m_{A'\to A}$ for each message m.
4. decoder $\mathcal{D}$: a positive operator valued measure where $\Lambda^m_{BB'}$ indicates that we decode to m.

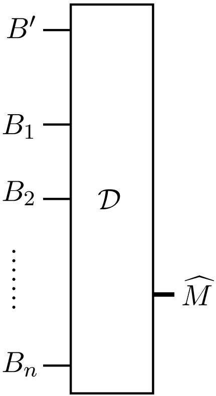


Ingredients: Code

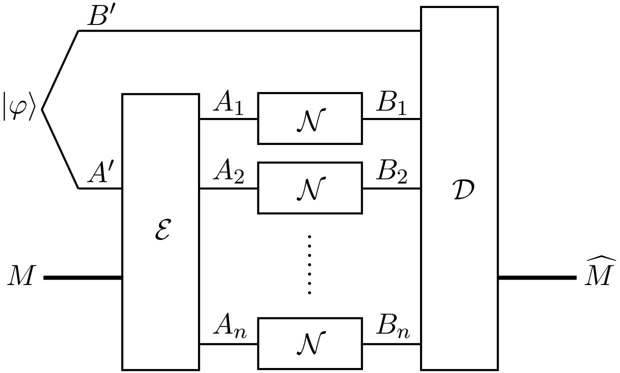
- **Entanglement-Assisted Code:** quadruple

$$\mathcal{C}_n = \left\{ \mathcal{M},\ |\varphi\rangle_{A'B'},\ \{\mathcal{E}^m_{A'\to A}\}_{m\in\mathcal{M}},\ \{\Lambda^m_{BB'}\}_{m\in\mathcal{M}} \right\}.$$

1. Set of messages: $\mathcal{M}$.
2. Resource state: $|\varphi\rangle_{A'B'}$.
3. encoder $\mathcal{E}$: a quantum channel $\mathcal{E}^m_{A'\to A}$ for each message m.
4. decoder $\mathcal{D}$: a positive operator valued measure where $\Lambda^m_{BB'}$ indicates that we decode to m.



Ingredients: Error Probability



- **Average Probability of Error**: M uniformly random in $\mathcal{M}$,

$$p_{\text{err}}(\mathcal{C}_n, \mathcal{N}^{\otimes n}) := \Pr\left[M \neq \hat{M}\right].$$

Ingredients: Non-Asymptotic Achievable Region

- **Non-Asymptotic Achievable Region**: A triple $\{R, n, \varepsilon\}$ is achievable if there exists a code $\mathcal{C}_n$ for $\mathcal{N}^{\otimes n}$ with

$$\frac{1}{n} \log |\mathcal{M}| \geq R, \quad \text{and} \quad p_{\text{err}}(\mathcal{C}_n, \mathcal{N}^{\otimes n}) \leq \varepsilon$$

- **Tolerated Error**: Fixed $\varepsilon \in (0, 1)$.
- **Boundary of Achievable Region:** $R^*_{\mathcal{N}}(n; \varepsilon)$ is the maximum rate R such that $\{R, n, \varepsilon\}$ is achievable.

- We investigate $n \mapsto R^*_{\mathcal{N}}(n; \varepsilon)$ for large n and fixed ε.
- The $O(\cdot)$ and $o(\cdot)$ describe the asymptotics for $n \to \infty$. The implied constants may depend on $\mathcal{N}$ and ε.
- Φ is the cumulative (normal) Gaussian distribution function.

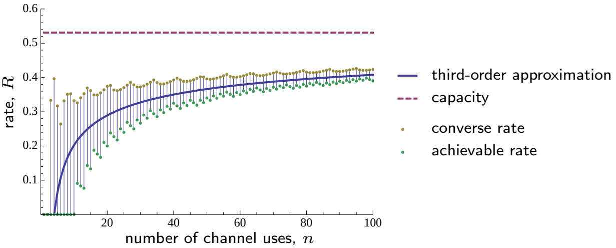
Known Results: Classical

- Shannon'48 and Wolfowitz'60 established that

$$R_W^*(n;\varepsilon) = C(W) + o(1) \qquad (\text{as } n \to \infty)\,.$$

- Refined by Strassen'62, Hayashi'09, and Polyanskiy *et al.*'10.
- Under some regularity conditions (Polyanskiy'10, T & Tan'13):

$$R_W^*(n;\varepsilon) = C(W) + \sqrt{\frac{V(W)}{n}}\,\Phi^{-1}(\varepsilon) + \frac{\log n}{2n} + O\Big(\frac{1}{n}\Big)\,.$$



Known Results: Quantum

- Bennett *et al.*'99–02 established

$$\lim_{\varepsilon \to 0} \lim_{n \to \infty} R^*_{\mathcal{N}}(n;\varepsilon) = C_{\mathrm{ea}}(\mathcal{N}) .$$

- The strong converse follows from the quantum reverse Shannon theorem (Bennett *et al.*'14, Berta *et al.*'11):

$$R^*_{\mathcal{N}}(n;\varepsilon) = C_{\mathrm{ea}}(\mathcal{N}) + o(1)$$

- Gupta and Wilde'15 proved

$$R^*_{\mathcal{N}}(n;\varepsilon) = C_{\mathrm{ea}}(\mathcal{N}) + O\Big(\frac{1}{\sqrt{n}}\Big)$$

- Our main result reveals the second-order term scaling as $1/\sqrt{n}$ in the above for covariant channels.

Main Result: Covariant Channels

- Covariant channels: $\mathcal{N}_{A\to B} \circ \mathcal{U}_A(g) = \mathcal{U}_B(g) \circ \mathcal{N}_{A\to B}$ for all $g \in G$ for some group G, with $\mathcal{U}_A(g)$ irreducible.
- They include qubit Pauli and depolarizing channels.

Result

For any covariant quantum channel $\mathcal{N}$ and $\varepsilon \in (0,1)$, we have

$$R^*_{\mathcal{N}}(n,\varepsilon) = C_{\mathrm{ea}}(\mathcal{N}) + \sqrt{\frac{V_{ea}(\mathcal{N})}{n}}\,\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right).$$

Main Result: Covariant Channels

Result

For any covariant quantum channel $\mathcal{N}$ *and* $\varepsilon \in (0,1)$, *we have*

$$R^*_{\mathcal{N}}(n,\varepsilon) = C_{\mathrm{ea}}(\mathcal{N}) + \sqrt{\frac{V_{ea}(\mathcal{N})}{n}}\,\Phi^{-1}(\varepsilon) + O\Big(\frac{\log n}{n}\Big).$$

- Let $\psi_{AA'}$ be the maximally entangled state. Then, entanglement-assisted **channel capacity** and **dispersion** are

$$C_{\mathrm{ea}}(\mathcal{N}) = D\Big(\mathcal{N}_{A\to B}(\psi_{AA'})\Big\|\psi_{A'} \otimes \mathcal{N}_{A\to B}(\psi_A)\Big),$$
$$V_{\mathrm{ea}}(\mathcal{N}) = V\Big(\mathcal{N}_{A\to B}(\psi_{AA'})\Big\|\psi_{A'} \otimes \mathcal{N}_{A\to B}(\psi_A)\Big).$$

- relative entropy: $D(\rho\|\tau) := \mathrm{tr}\,\big(\rho(\log\rho - \log\tau)\big)$.
- its variance: $V(\rho\|\tau) := \mathrm{tr}\,\big(\rho(\log\rho - \log\tau - D(\rho\|\tau))^2\big)$.

Main Result: Achievable Rate

Result

For any quantum channel $\mathcal{N}$ and $\varepsilon \in (0,1)$, we have

$$R^*_{\mathcal{N}}(n,\varepsilon) \geq C_{\mathrm{ea}}(\mathcal{N}) + \sqrt{\frac{V^{\varepsilon}_{\mathrm{ea}}(\mathcal{N})}{n}}\,\Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right).$$

- Entanglement-Assisted Capacity:

$$C_{\mathrm{ea}}(\mathcal{N}) := \max_{\rho_A} D\left(\mathcal{N}_{A\to B}(\rho_{AA'}) \middle\| \rho_{A'} \otimes \mathcal{N}_{A\to B}(\rho_A)\right).$$

- Capacity achieving input states:

$$\Pi_A := \arg\max_{\rho_A} D\left(\mathcal{N}_{A\to B}(\rho_{AA'}) \middle\| \rho_{A'} \otimes \mathcal{N}_{A\to B}(\rho_A)\right).$$

- Entanglement-Assisted Channel Dispersion:

$$V_{\mathrm{ea}}(\mathcal{N}) := \begin{cases} \min_{\rho_A \in \Pi_A} V(\mathcal{N}_{A\to B}(\rho_{AA'}) \| \rho_{A'} \otimes \mathcal{N}_{A\to B}(\rho_A)) & \text{if } \varepsilon < \frac{1}{2} \\ \max_{\rho_A \in \Pi_A} V(\mathcal{N}_{A\to B}(\rho_{AA'}) \| \rho_{A'} \otimes \mathcal{N}_{A\to B}(\rho_A)) & \text{if } \varepsilon \geq \frac{1}{2} \end{cases}.$$

Binary Hypothesis Testing

- The ε-hypothesis testing relative entropy:

$$D_h^\varepsilon(\rho\|\sigma) := -\log \beta_\varepsilon(\rho\|\sigma)\,,$$
$$\beta_\varepsilon(\rho\|\sigma) := \min\left\{ \operatorname{tr}(Q\sigma) : 0 \leq Q \leq I,\ \operatorname{tr}(Q\rho) \geq 1-\varepsilon \right\}.$$

- Its asymptotics for i.i.d. states $\rho^{\otimes n}$ and $\sigma^{\otimes n}$ for large n are the main ingredient.
- Second-order expansion (T & Hayashi'13 and Li'14):

$$D_h^\varepsilon\left(\rho^{\otimes n}\middle\|\sigma^{\otimes n}\right) = nD(\rho\|\sigma) + \sqrt{nV(\rho\|\sigma)}\,\Phi^{-1}(\varepsilon) + O(\log n)\,.$$

Achievability: Code (1)

- Key Idea: random superdense coding on type subspaces.
- **Resource state:** Use $\mathcal{H}_{A'} \equiv \mathcal{H}_{B'} \equiv \mathcal{H}_A$ and decompose

$$\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B^{\otimes n} = \bigoplus_{\lambda} \mathcal{H}_{A^n}^{\lambda} \otimes \mathcal{H}_{B^n}^{\lambda}$$

where $\mathcal{H}^{\lambda}$ is the subspace spanned by vectors of type λ.

- We use the state

$$\left|\varphi_{A^n B^n}\right\rangle = \sum_{\lambda} \sqrt{p(\lambda)} \left|\psi_{A^n B^n}^{\lambda}\right\rangle,$$

where $\psi_{A^n B^n}^{\lambda}$ is maximally entangled on $\mathcal{H}_{A^n}^{\lambda} \otimes \mathcal{H}_{B^n}^{\lambda}$.

Achievability: Code (2)

- **Random code:** For each $m \in \mathcal{M}$, randomly chose $s_m = \{b_t, x_t, z_t\}_t$ where $b_t \in \{0,1\}$, and $x_t, z_t \in \{0, 1, \ldots, d_t - 1\}$.
- **Encoder:** Define $\mathcal{E}^m(\,\cdot\,) = U_A(s_m) \cdot U_A^\dagger(s_m)$ where

$$U_A(s) := \bigoplus_t (-1)^{b_t} X(x_t) Z(z_t),$$

  where X and Z are Heisenberg-Weyl operators.
- **Decoder:** “Pretty-good” measurement.

Achievability: One-Shot to Asymptotics

Recall: $\left|\varphi_{A^n B^n}\right\rangle = \sum_{\lambda} \sqrt{p(\lambda)} \left|\psi^{\lambda}_{A^n B^n}\right\rangle,$

Lemma

For any $\delta \in (0, \frac{\varepsilon}{2})$, we have

$$R^*_{\mathcal{N}}(\varepsilon) \geq \frac{1}{n} D_H^{\varepsilon - 2\delta}\left(\mathcal{N}^{\otimes n}_{A \to B'}(\varphi_{A^n B^n}) \,\middle\|\, \sum_{\lambda} p(\lambda)\left(\pi^{\lambda}_{B^n} \otimes \mathcal{N}^{\otimes n}_{A \to B'}(\pi^{\lambda}_{A^n})\right)\right) - \frac{1}{n}\log\frac{1-\varepsilon}{\delta^2},$$

where $\pi^{\lambda}_{A^n}$ is the maximally mixed state on the space $\mathcal{H}^{\lambda}_{A^n}$.

- Every pure state $\rho^{\otimes n}_{AA'}$ can be written in the above form.
- Moreover, we show that

$$\sum_{\lambda} p(\lambda)\left(\pi^{\lambda}_{B^n} \otimes \mathcal{N}^{\otimes n}_{A \to B'}(\pi^{\lambda}_{A^n})\right) \lesssim \mathrm{poly}(n) \cdot \left(\phi_B \otimes \mathcal{N}_{A \to B'}(\phi_A)\right)^{\otimes n}$$

Converse

- We use the one-shot converse by Matthews & Wehner'14:

$$R^*_{\mathcal{N}}(n;\varepsilon) \leq \max_{\rho_{A^n}} \frac{1}{n} D_h^{\varepsilon}\big(\mathcal{N}_{A\to B}^{\otimes n}(\rho_{A^nA'^n}) \big\| \rho_{A'^n} \otimes \mathcal{N}_{A\to B}^{\otimes n}(\rho_{A^n})\big)$$

- The functional is quasi-concave in ρ_{A^n}, allowing to reduce the optimization to states invariant under the channel symmetry.
- Generally these are the permutation invariant states.
- For covariant channels the only invariant state is the fully mixed state ψ_A. Then,

$$R^*_{\mathcal{N}}(n;\varepsilon) \leq \frac{1}{n} D_h^{\varepsilon}\big((\mathcal{N}_{A\to B}(\psi_{AA'}))^{\otimes n} \big\| (\psi_{A'} \otimes \mathcal{N}_{A\to B}(\psi_A)^{\otimes n})\big) .$$

- Second order expansion for hypothesis testing yields result.

Conclusion

- We have established the second-order approximation for the EA capacity of covariant channels.
- We also show a second-order achievability for general channels.
- We conjecture that this is tight also for general channels.
- Establishing a general second-order converse bound requires new techniques, and constitutes an interesting open problem.
  - Reduction from permutation invariant to product states using de Finetti argument is not tight enough.