Quantum and private capacities of low-noise channels

arXiv:1705.04335

Felix Leditzky

(JILA & CTQM, University of Colorado Boulder)

Joint work with Debbie Leung and Graeme Smith

ITW Kaohsiung, 10 November 2017

Table of Contents

1 Quantum channels and their capacities

2 Main result: capacities of low-noise channels

3 (Approximate) degradability

4 Pauli channels

5 Conclusion

Table of Contents

1 Quantum channels and their capacities

2 Main result: capacities of low-noise channels

3 (Approximate) degradability

4 Pauli channels

5 Conclusion

Quantum channels and their capacities

- Communication (physical evolution) between quantum parties (systems) is modeled with quantum channels.
- A **quantum channel** $\mathcal{N} : A \to B$ is a linear, completely positive, trace-preserving map acting on a quantum system A.
- **Many different capacities** depending on the context.
- **Quantum capacity** $\mathcal{Q}(\mathcal{N})$: maximal rate at which **entanglement** can be generated between A and B through $\mathcal{N}$.
- **Private capacity** $\mathcal{P}(\mathcal{N})$: maximal rate at which **secure key** can be established between A and B through $\mathcal{N}$.

Coding theorem for $\mathcal{Q}$

- **Hashing bound**:

  Coherent information $\mathcal{Q}^{(1)}(\mathcal{N})$ is achievable,

  $$\mathcal{Q}(\mathcal{N}) \geq \mathcal{Q}^{(1)}(\mathcal{N}) := \max_{\rho} [S(\mathcal{N}(\rho)) - S((\mathrm{id} \otimes \mathcal{N})(\psi^{\rho}))],$$

  where $S(\sigma) = -\operatorname{Tr} \sigma \log \sigma$ is the von Neumann entropy, and $|\psi^{\rho}\rangle$ is a purification of ρ. [Lloyd 1997; Shor 2002; Devetak 2005]

- **Quantum capacity theorem**:

  $$\mathcal{Q}(\mathcal{N}) = \lim_{n \to \infty} \frac{1}{n} \mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n})$$

- In general, $\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n}) > n\mathcal{Q}^{(1)}(\mathcal{N})$, and the regularization over n is necessary $\Longrightarrow$ renders $\mathcal{Q}(\mathcal{N})$ intractable to compute!

Complementary channels

- For any quantum channel $\mathcal{N}\colon A \to B$, there is an isometry $V\colon A \to B \otimes E$ such that $\mathcal{N} = \mathrm{Tr}_E(V \cdot V^\dagger)$. [Stinespring 1955]
- Any isometry $V\colon A \to B \otimes E$ gives rise to a **complementary channel** $\mathcal{N}^c\colon A \to E$ to the **environment**,

$$\mathcal{N}^c(\rho) \coloneqq \mathrm{Tr}_B(V\rho V^\dagger).$$

- $\mathcal{N}^c$ models the loss or *leakage* of information to the environment.
- This leakage is “responsible” for super-additivity of $\mathcal{Q}^{(1)}$, and makes regularization of $\mathcal{Q}$ necessary.

Coding theorems for $\mathcal{P}$

- Let $V \colon A \to B \otimes E$ be an isometry for $\mathcal{N} \colon A \to B$, and for an ensemble of states $\{p_x, \rho_x\}$ define the classical-quantum state

$$\rho_{XBE} = \sum_x p_x |x\rangle\langle x|_X \otimes V\rho_x V^\dagger.$$

- Define the **private information**

$$\mathcal{P}^{(1)}(\mathcal{N}) := \max_{\{p_x, \rho_x\}} [I(X;B) - I(X;E)],$$

where $I(X;B) = S(X) + S(B) - S(XB)$ is the mutual information.

- **Private capacity theorem**: [Cai et al. 2004; Devetak 2005]

$$\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \mathcal{P}^{(1)}(\mathcal{N}^{\otimes n})$$

- In general, $\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n}) > n\mathcal{P}^{(1)}(\mathcal{N})$.

Coding theorems for $\mathcal{Q}$ and $\mathcal{P}$

- All inequalities are strict in general:

$$\begin{array}{ccccc} \mathcal{Q}^{(1)}(\mathcal{N}) & \leq & \mathcal{Q}(\mathcal{N}) & = & \lim_{n\to\infty} \frac{1}{n}\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n}) \\ \rotatebox{90}{$\geq$} & & \rotatebox{90}{$\geq$} & & \\ \mathcal{P}^{(1)}(\mathcal{N}) & \leq & \mathcal{P}(\mathcal{N}) & = & \lim_{n\to\infty} \frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n}) \end{array}$$

- Trivial situation: identity channel $id\colon A \to A$.

$$\mathcal{Q}(\mathrm{id}) = \mathcal{Q}^{(1)}(\mathrm{id}) = \mathcal{P}^{(1)}(\mathrm{id}) = \mathcal{P}(\mathrm{id}) \quad (= \log |A|) \qquad (*)$$

- We call a channel $\mathcal{N}$ **low-noise**, if $\|\mathcal{N} - \mathrm{id}\,\|_\diamond \leq \varepsilon$.

  $\|\cdot\|_\diamond$ ... diamond norm distance on set of quantum channels.

- Is $(*)$ approximately true for low-noise channels? **Yes!**

Table of Contents

1 Quantum channels and their capacities

2 Main result: capacities of low-noise channels

3 (Approximate) degradability

4 Pauli channels

5 Conclusion

Main result

Quantum and private capacities of low-noise channels

For **low-noise channels** $\mathcal{N}$ with $\|\mathrm{id} - \mathcal{N}\|_\diamond \leq \varepsilon$,

$$\mathcal{Q}(\mathcal{N}) = \mathcal{Q}^{(1)}(\mathcal{N}) + O(\varepsilon^{3/2} \log \varepsilon)$$

$$\mathcal{P}(\mathcal{N}) = \mathcal{Q}^{(1)}(\mathcal{N}) + O(\varepsilon^{3/2} \log \varepsilon).$$

For **Pauli channels**, the error term can be improved to $O(\varepsilon^2 \log \varepsilon)$.

- **Main proof tool:** (Approximate) degradability.

Table of Contents

1 Quantum channels and their capacities

2 Main result: capacities of low-noise channels

3 (Approximate) degradability

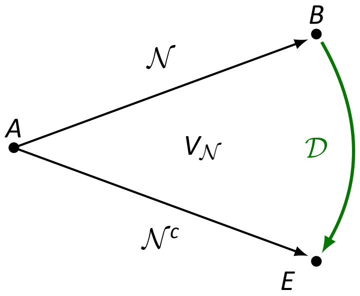
4 Pauli channels

5 Conclusion

Degradable channels

- A channel is called **degradable**, if there is another channel $\mathcal{D}\colon B \to E$ such that $\mathcal{N}^c = \mathcal{D} \circ \mathcal{N}$. [Devetak and Shor 2005]
- For a degradable channel, the receiver B can locally simulate $\mathcal{N}^c$, i.e., the loss to the environment.
- Degradable channels: [Devetak and Shor 2005; Smith 2008]

$$\mathcal{Q}(\mathcal{N}) = \mathcal{Q}^{(1)}(\mathcal{N}) = \mathcal{P}^{(1)}(\mathcal{N}) = \mathcal{P}(\mathcal{N}).$$



degradable:
$\exists \mathcal{D}\colon B \to E$ s.t.
$\mathcal{N}^c = \mathcal{D} \circ \mathcal{N}$

Approximate degradability

- **Idea**: What if degradability is only approximately satisfied?
  Do we have $\mathcal{Q}(\mathcal{N}) \approx \mathcal{Q}^{(1)}(\mathcal{N})$?
- **Goal:** Find map $\mathcal{D}$ that brings $\mathcal{N}$ as close as possible to $\mathcal{N}^c$.
- Measured by **degradability parameter** [Sutter et al. 2015]

$$\mathrm{dg}(\mathcal{N}) := \min_{\mathcal{D}\colon B\to E} \|\mathcal{N}^c - \mathcal{D}\circ\mathcal{N}\|_\diamond.$$

- For $\mathcal{N}$ with $\mathrm{dg}(\mathcal{N}) = \varepsilon$,

$$|\mathcal{Q}(\mathcal{N}) - \mathcal{Q}^{(1)}(\mathcal{N})| \leq f_1(\varepsilon)$$

$$|\mathcal{P}(\mathcal{N}) - \mathcal{P}^{(1)}(\mathcal{N})| \leq f_2(\varepsilon),$$

  where $f_i(\varepsilon) \in O(\varepsilon \log \varepsilon)$ and $f_i(\varepsilon) \xrightarrow{\varepsilon\to 0} 0$. [Sutter et al. 2015]
- $\mathrm{dg}(\mathcal{N})$ can be computed using **semidefinite programming**.

Approximately degrading a low-noise channel

- Complementary channel id^c of identity channel: completely depolarizing map $\mathrm{id}^c = \mathrm{Tr}(\cdot)|0\rangle\langle 0|$, and

$$\mathrm{id}^c = \mathrm{id}^c \circ \mathrm{id}\,.$$

- We prove: For a low-noise channel $\mathcal{N}$ with $\|\mathcal{N} - \mathrm{id}\,\|_\diamond \leq \varepsilon$,

$$\|\mathcal{N}^c - \mathcal{N}^c \circ \mathcal{N}\|_\diamond \leq 2\varepsilon^{3/2}. \qquad (*)$$

- **Intuition:** $\mathcal{N}^c$ is *very* noisy and almost useless, so you might as well use it as the degrading map!

- $(*)$ implies $\mathrm{dg}(\mathcal{N}) \leq 2\varepsilon^{3/2}$ and our main result.

Table of Contents

1 Quantum channels and their capacities

2 Main result: capacities of low-noise channels

3 (Approximate) degradability

4 Pauli channels

5 Conclusion

Pauli channels

- Consider a Pauli channel

$$\mathcal{N}_{\vec{q}}(\rho) = q_0\,\rho + q_1\,X\rho X + q_2\,Y\rho Y + q_3\,Z\rho Z,$$

  where X, Y, Z are the usual Pauli matrices and $\vec{q}$ is a probability distribution.

- $\mathcal{N}_{\vec{q}}$ is a **low-noise channel**, since $\|\mathcal{N}_{\vec{q}} - \mathrm{id}\,\|_\diamond = 2(q_1 + q_2 + q_3)$.

- Hence, with our results from before,

$$\mathcal{Q}(\mathcal{N}_{\vec{q}}) = \mathcal{Q}^{(1)}(\mathcal{N}_{\vec{q}}) + O(\varepsilon^{3/2}\log\varepsilon)$$

  for $\varepsilon = 2(q_1 + q_2 + q_3)$, and same for $\mathcal{P}(\mathcal{N}_{\vec{q}})$.

- We can improve this to $O(\varepsilon^2\log\varepsilon)$!

Pauli channels

- Assume for simplicity that $q_i = q_i(p)$ for some underlying **single noise parameter** $p \in [0, 1]$.

- Example: **Depolarizing channel** $\mathcal{D}_p$

  $$\mathcal{D}_p \colon \rho \longmapsto (1-p)\rho + \frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

- Example: **XZ-channel** $\mathcal{C}_p$ (a.k.a. BB84-channel)

  $$\mathcal{C}_p \colon \rho \longmapsto (1-p)^2\rho + (p-p^2)\, X\rho X + p^2\, Y\rho Y + (p-p^2)\, Z\rho Z$$

- In both cases, numerics suggest that

  $$\mathrm{dg}(\mathcal{D}_p) = O(p^2) \qquad \text{and} \qquad \mathrm{dg}(\mathcal{C}_p) = O(p^2).$$

- **Strategy:** Prove this by guessing good degrading map!

Pauli channels

- **Ansatz:** Again the complementary channel, but make it slightly noisier, $\mathcal{D}_s^c$ with $s = p + ap^2$.

- We prove: For $a = \frac{8}{3}$,

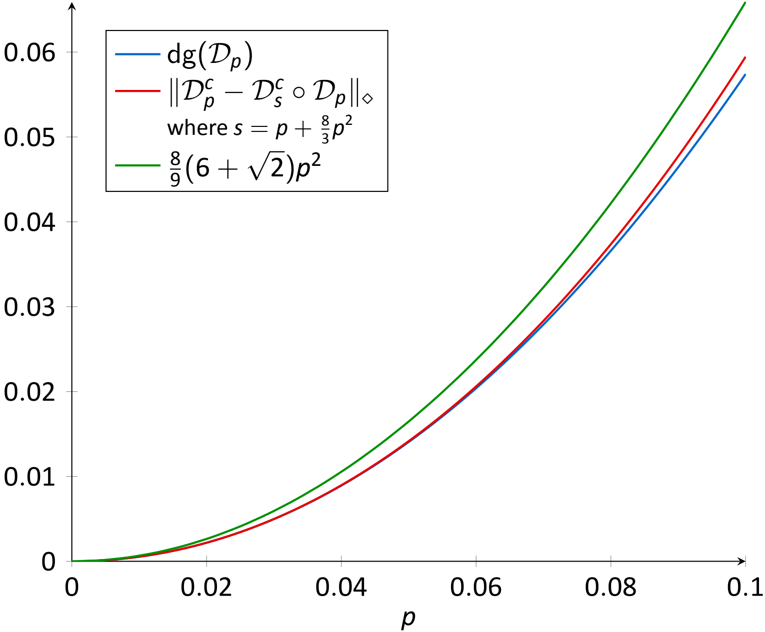
$$\mathrm{dg}(\mathcal{D}_p) \leq \|\mathcal{D}_p^c - \mathcal{D}_{p+ap^2}^c \circ \mathcal{D}_p\|_\diamond \leq \tfrac{8}{9}(6 + \sqrt{2})p^2 + O(p^3)$$

- Similarly, for $a = 4$,

$$\mathrm{dg}(\mathcal{C}_p) \leq \|\mathcal{C}_p^c - \mathcal{C}_{p+ap^2}^c \circ \mathcal{C}_p\|_\diamond \leq 16p^2 + 32p^{5/2} + O(p^3)$$

- These are remarkably accurate approximations to the true degradability parameters $\mathrm{dg}(\mathcal{D}_p)$ and $\mathrm{dg}(\mathcal{C}_p)$!

$$\mathcal{D}_p(\rho) = (1-p)\rho + \tfrac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)$$



$$\mathcal{C}_p(\rho) = (1-p)^2\rho + (p-p^2)\,X\rho X + p^2\,Y\rho Y + (p-p^2)\,Z\rho Z$$

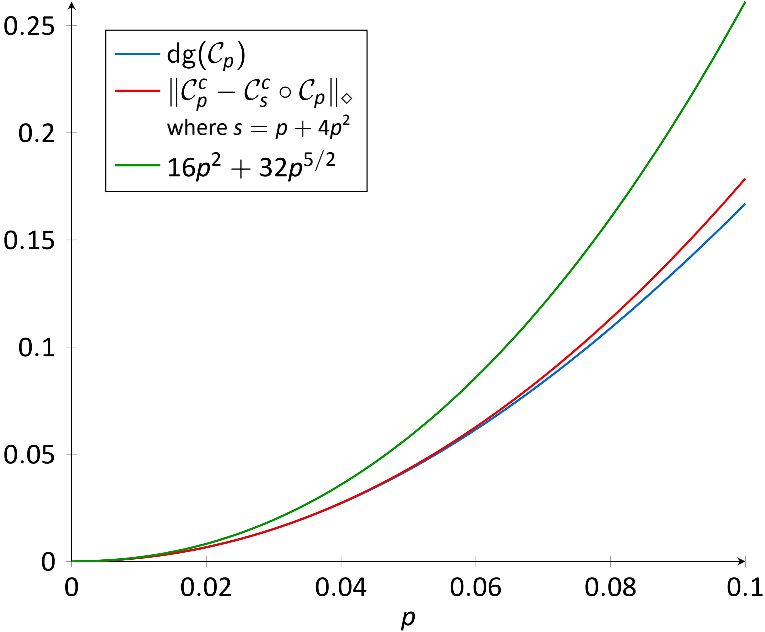


Table of Contents

1 Quantum channels and their capacities

2 Main result: capacities of low-noise channels

3 (Approximate) degradability

4 Pauli channels

5 Conclusion

Summary of results

- Quantum and private capacity: **regularization** of the coherent and private information, notoriously hard to compute, except for (approximately) degradable channels.
- **Low-noise channels** are approximately degraded by their complementary channel.
- Consequence: both capacities of low-noise channels are essentially equal to the **single-letter coherent information**.
- Approximation is even better for the class of Pauli channels (includes depolarizing channel and BB84 channel).

Discussion and open problems

- The regularization for $\mathcal{Q}(\mathcal{N})$ is necessary because we know of instances where $\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n}) > n\mathcal{Q}^{(1)}(\mathcal{N})$.
- This is called **superadditivity** of the coherent information, and is achieved by **degenerate** quantum codes.

  [DiVincenzo et al. 1998; Smith and Smolin 2007]
- For the private information $\mathcal{P}^{(1)}(\mathcal{N})$, super-additivity is achieved by **shielding** private data from corruption.

  [Horodecki et al. 2005; Leung et al. 2014]
- Our results show that for low-noise channels degeneracy and shielding have **no considerable effect**.
- Capacities are still poorly understood in the high-noise regime!

References

Cai, N. et al. (2004). *Problems of Information Transmission* 40.4, pp. 318–336.

Devetak, I. (2005). *IEEE Transactions on Information Theory* 51.1, pp. 44–55. arXiv: quant-ph/0304127.

Devetak, I. and P. W. Shor (2005). *Communications in Mathematical Physics* 256.2, pp. 287–303. arXiv: quant-ph/0311131 [quant-ph].

DiVincenzo, D. et al. (1998). *Physical Review A* 57.2, pp. 830–839. arXiv: quant-ph/9706061.

Horodecki, K. et al. (2005). *Physical Review Letters* 94.16, p. 160502. arXiv: quant-ph/0309110.

Leditzky, F. et al. (2017). *arXiv preprint*. arXiv: 1705.04335 [quant-ph].

Leung, D. et al. (2014). *Physical Review Letters* 113.3, p. 030502. arXiv: 1312.4989 [quant-ph].

Lloyd, S. (1997). *Physical Review A* 55, pp. 1613–1622. arXiv: quant-ph/9604015.

Shor, P. (2002). Lecture notes, MSRI Workshop on Quantum Computation.

Smith, G. (2008). *Physical Review A* 78.2, p. 022306. arXiv: 0705.3838 [quant-ph].

Smith, G. and J. A. Smolin (2007). *Physical Review Letters* 98.3, p. 030501. arXiv: quant-ph/0604107.

Stinespring, W. F. (1955). *Proceedings of the American Mathematical Society* 6.2, pp. 211–216.

Sutter, D. et al. (2015). *arXiv preprint*. arXiv: 1412.0980 [quant-ph].

Thank you very much for your attention!