Quantum and private capacities of low-noise channels

Contact: felix.leditzky@jila.colorado.edu

arXiv:1705.04335

Felix Leditzky
(JILA, CTQM)

Debbie Leung
(IQC, Univ. Waterloo)

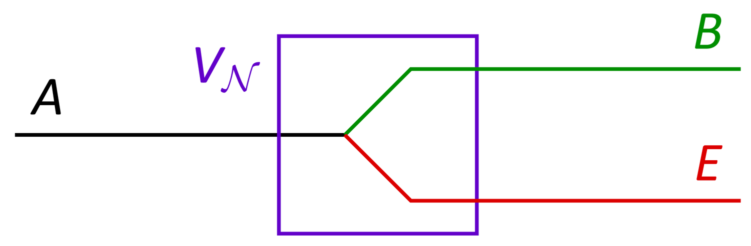
Graeme Smith
(JILA, CTQM, CU Boulder)

A long-standing open problem:
What is the quantum capacity of the qubit depolarizing channel?

Quantum channels

Quantum channel $\mathcal{N}: A \to B$

$\mathcal{N} = \mathrm{Tr}_E(V_\mathcal{N} \cdot V_\mathcal{N}^\dagger)$



Isometric extension $V_\mathcal{N}: A \to B \otimes E$

Complementary channel $\mathcal{N}^c: A \to E$

$\mathcal{N}^c = \mathrm{Tr}_B(V_\mathcal{N} \cdot V_\mathcal{N}^\dagger)$

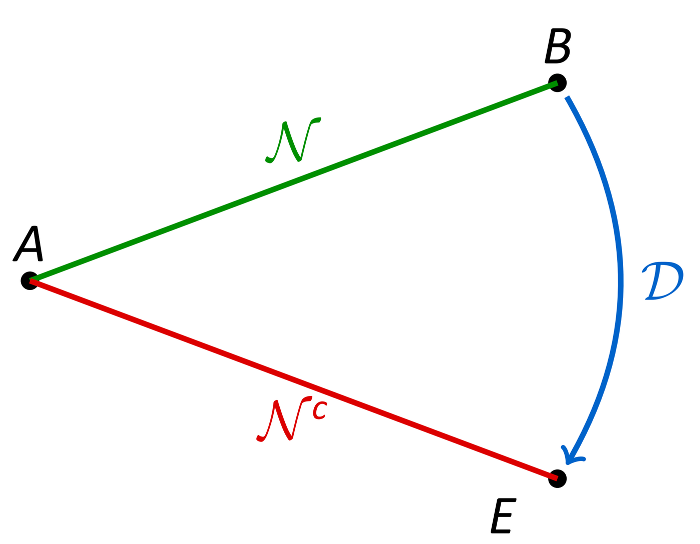
Quantum and private capacities

- Quantum capacity $Q(\mathcal{N})$: highest possible rate of *reliable quantum information transmission* through $\mathcal{N}$.
- Coherent information $I_c(\mathcal{N}) := \max_\rho \{S(\mathcal{N}(\rho)) - S(\mathcal{N}^c(\rho))\}$.
- LSD-theorem: $Q(\mathcal{N}) = \sup_n \frac{1}{n} I_c(\mathcal{N}^{\otimes n})$.
  [Lloyd 97], [Shor 02], [Devetak 05]
- Private capacity $P(\mathcal{N})$: highest possible rate of *classical information transmission unknown to the environment* through $\mathcal{N}$.

Superadditivity

- *Problem:* $\exists \mathcal{N}$ and $n \in \mathbb{N}$ s.t. $I_c(\mathcal{N}^{\otimes n}) > n I_c(\mathcal{N})$.
- Renders both capacities *intractable to compute* in most cases.
- Example: Qubit depolarizing channel $\mathcal{D}_p(\rho) := (1 - \frac{4p}{3})\rho + \frac{4p}{3}\pi_2$.
- $I_c(\mathcal{D}_p) = 0$ for $p \geq 0.1894$, but $I_c(\mathcal{D}_p^{\otimes 5}) > 0$ for $p \leq 0.1904$.
  [DiVincenzo, Shor, Smolin 97]

(Approximate) degradability



- Degradable channel: $\exists \mathcal{D}: B \to E$ s.t. $\mathcal{N}^c = \mathcal{D} \circ \mathcal{N}$.
- For degradable channels, $I_c(\mathcal{N}^{\otimes n}) = n I_c(\mathcal{N})$ for all n, $Q(\mathcal{N}) = P(\mathcal{N}) = I_c(\mathcal{N})$.
  [Devetak, Shor 05], [Smith 08]
- Diamond norm: $\|\Phi\|_\diamond := \sup\{\|(\mathrm{Id}_n \otimes \Phi)(X)\|_1 : \|X\|_1 \leq 1, n\}$ (can be efficiently computed using SDP).
- Channel $\mathcal{N}$ is called *ε-approximate degradable*, if $\exists \mathcal{D}$ s.t. $\|\mathcal{N}^c - \mathcal{D} \circ \mathcal{N}\|_\diamond \leq \varepsilon$. [Sutter, Scholz, Winter, Renner 17]
- *Degradability parameter* $\mathrm{dg}(\mathcal{N})$: smallest such ε.
- Capacity bounds: For $\varepsilon = \mathrm{dg}(\mathcal{N})$ and $F \in \{Q, P\}$ we have $|F(\mathcal{N}) - I_c(\mathcal{N})| \leq f(\varepsilon)$, where $f(\varepsilon) \in O(\varepsilon \log \varepsilon)$.
  [Sutter, Scholz, Winter, Renner 17], based on [Leung, Smith 09]

Low-noise channels

- The identity channel id is trivially degraded by its own complementary channel, $\mathrm{id}^c = \mathrm{id}^c \circ \mathrm{id}$.
- Hence, for a channel $\mathcal{N} \approx \mathrm{id}$ the complementary channel $\mathcal{N}^c$ should then also be a good degrading map, $\mathcal{N}^c \approx \mathcal{N}^c \circ \mathcal{N}$.
- We call $\mathcal{N}$ a *low-noise channel*, if $\|\mathcal{N} - \mathrm{id}\|_\diamond \leq \varepsilon$.

Main result: Capacities of low-noise channels

- A low-noise channel $\mathcal{N}$ with $\|\mathcal{N} - \mathrm{id}\|_\diamond \leq \varepsilon$ is $2\varepsilon^{1.5}$-approximate degradable: $\|\mathcal{N}^c - \mathcal{N}^c \circ \mathcal{N}\|_\diamond \leq 2\varepsilon^{1.5}$.
- Hence, $|F(\mathcal{N}) - I_c(\mathcal{N})| \leq O(\varepsilon^{1.5} \log \varepsilon)$ for $F \in \{Q, P\}$.

Qubit depolarizing channel

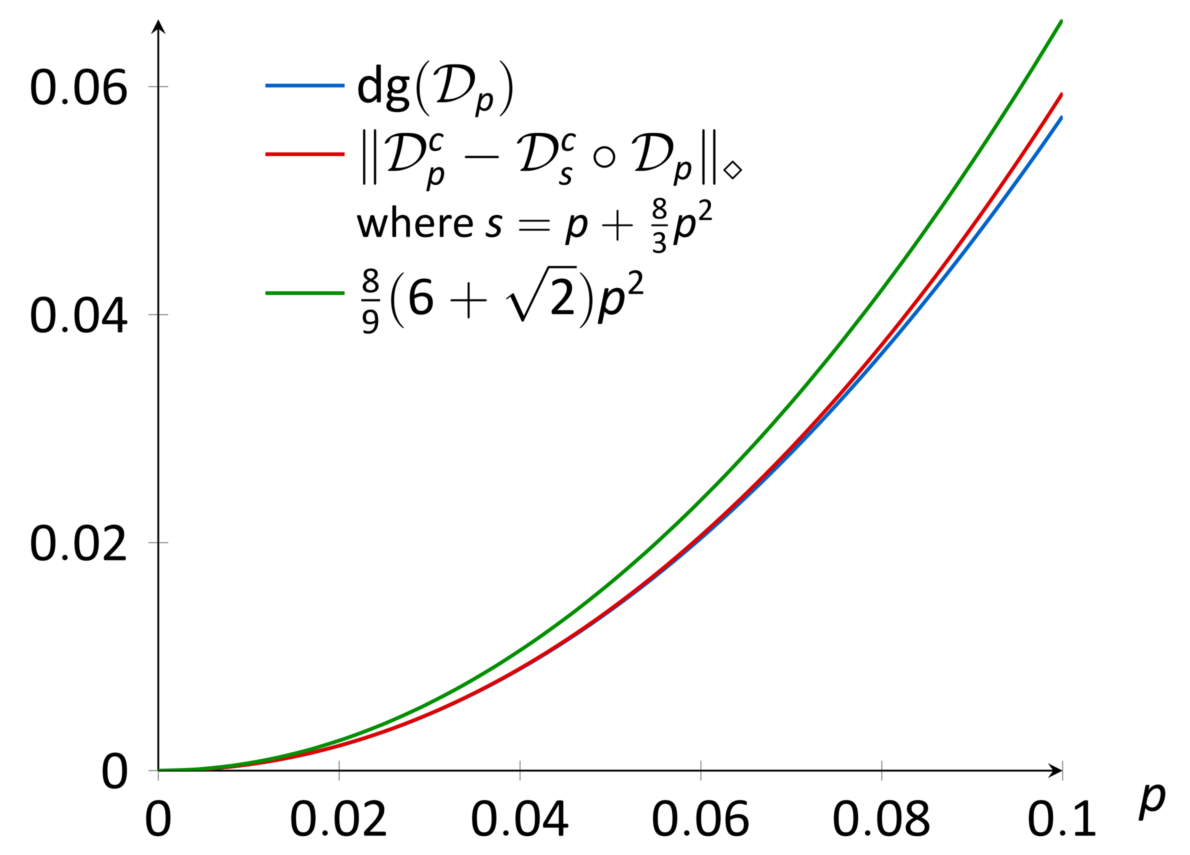
- The qubit depolarizing channel $\mathcal{D}_p(\rho) := (1 - \frac{4p}{3})\rho + \frac{4p}{3}\pi_2$ is a low-noise channel for small p, since $\|\mathcal{D}_p - \mathrm{id}\|_\diamond = 2p$.
- By the above, $\mathrm{dg}(\mathcal{D}_p) = O(p^{1.5})$ when using $\mathcal{D}_p^c$ as degrading map, but we can improve this to $O(p^2)$!
- Idea: Make the *degrading map slightly less noisy*, $\mathcal{D}_{p+ap^2}^c$, so that we "give a little more to E" to compensate for the lossy $\mathcal{D}_p$.

Main result: Qubit depolarizing channel

- For the optimal $a = \frac{8}{3}$, we obtain

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

- Hence, $|F(\mathcal{D}_p) - I_c(\mathcal{D}_p)| \leq O(p^2 \log p)$ for $F \in \{Q, P\}$.



Generalization to all Pauli channels

- An arbitrary Pauli channel $\mathcal{N}_\mathbf{q} = q_0\,\mathrm{id} + q_1 X \cdot X + q_2 Y \cdot Y + q_3 Z \cdot Z$ with $q_i = q_i(p)$ satisfies $\mathrm{dg}(\mathcal{N}_\mathbf{q}) = O(p^2)$.
- Example from QKD: BB84-channel $\mathcal{C}_p(\rho) = (1-p)^2\rho + (p - p^2)X\rho X + p^2 Y\rho Y + (p - p^2)Z\rho Z$.
- We show that $\mathrm{dg}(\mathcal{C}_p) \leq 16p^2 + O(p^{2.5})$.