On converse bounds for classical communication over quantum channels

Xin Wang

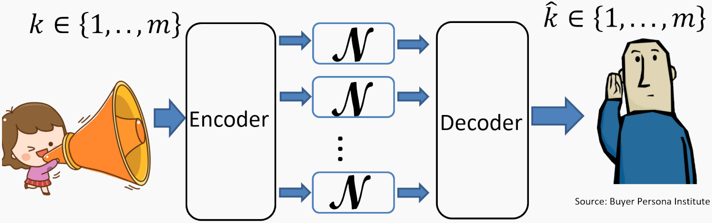
UTS: Centre for Quantum Software and Information

Joint work with Kun Fang, Marco Tomamichel (arXiv:1709.05258)

QIP 2018, QuTech, Delft

Classical communication over quantum channels

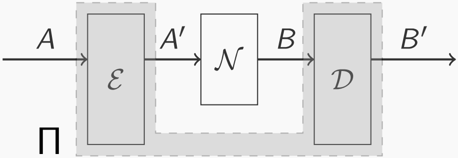
- [Shannon'48] Communication is that of reproducing at one point, either exactly or approximately, a message selected at another point.



Source: Buyer Persona Institute

- Quantum Shannon Theory
  - Ultimate limits of communication with quantum systems.
  - Various kinds of capacities (classical, quantum, private, alphabit), different kinds of assistance.

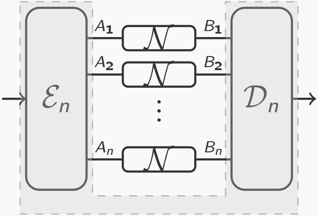
Communication with general codes



- An unassisted code reduces to the product of encoder and decoder, i.e., $\Pi = \mathcal{D}_{B\to B'}\mathcal{E}_{A\to A'}$;
- An entanglement-assisted code (EA) corresponds to a bipartite operation of the form $\Pi = \mathcal{D}_{B\widehat{B}\to B'}\mathcal{E}_{A\widehat{A}\to A'}\Psi_{\widehat{A}\widehat{B}}$
- A no-signalling-assisted code (NS) corresponds to a bipartite operation which is no-signalling from Alice to Bob and vice-versa [Leung, Matthews'16; Duan, Winter'16].
- We use Ω to denote the general code.

How well can we transmit classical information over $\mathcal{N}$?

- Finite blocklength (non-asymptotic) regime studies the practical senario of optimizing the trade-off between:



- r: bits sent per channel use.
- n: number of channel uses.
- ε: error tolerance.

- Capacity is the maximum rate for asymptotically error-free data transmission using the channel many times.
- Considering that the resource is finite, we also want a finite blocklength analysis.
- One-shot analysis yields results in the asymptotic limit.

Communication capability

- Given $\mathcal{N}$ and Ω-assisted code Π with size m, the optimal coding success probability is

$$p_{succ,\Omega}(\mathcal{N}, m) := \frac{1}{m} \sup \sum_{k=1}^{m} \operatorname{Tr} \mathcal{M}(|k\rangle\langle k|)|k\rangle\langle k|,$$

s.t. $\mathcal{M} = \Pi \circ \mathcal{N}$ is the effective channel.

- One-shot ε-error capacity:

$$C_\Omega^{(1)}(\mathcal{N}, \varepsilon) := \sup\{\log m : p_{succ,\Omega}(\mathcal{N}, m) \geq 1 - \varepsilon\}.$$

- The Ω-assisted capacity:

$$C_\Omega(\mathcal{N}) = \lim_{\varepsilon \to 0} \lim_{n \to \infty} \frac{1}{n} C_\Omega^{(1)}(\mathcal{N}^{\otimes n}, \varepsilon).$$

HSW theorem

- [Holevo'73, 98; Schumacher & Westmoreland'97]: the classical capacity of a quantum channel $\mathcal{N}$ is given by

$$C(\mathcal{N}) = \sup_{k\to\infty} \frac{1}{k}\chi(\mathcal{N}^{\otimes k}),$$

with $\chi(\mathcal{N}) = \max_{\{(p_i,\rho_i)\}} H\left(\sum_i p_i \mathcal{N}(\rho_i)\right) - \sum_i p_i H(\mathcal{N}(\rho_i))$.

- For certain classes of channels, $C(\mathcal{N}) = \chi(\mathcal{N})$, e.g.,
  - Classical-quantum channel, $\mathcal{N}: |j\rangle\langle j| \to \rho_j$.
  - Quantum erasure channel [Bennett, DiVincenzo, Smolin'97].
  - Depolarizing channel [King'03].
- However, $\chi(\mathcal{N})$ is not additive for general $\mathcal{N}$ [Hastings'09].

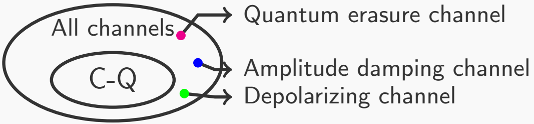
Challenges

Asymptotic regime

- The capacity $C(\mathcal{N})$ is extremely difficult to compute.
- Few known efficiently computable bounds:
  - Entanglement-assisted capacity [Bennett et al.'99],
  - Upper bound from entanglement measure [Brandao et al.'11,]
  - SDP converse bound [XW, Xie, Duan.'17],
  - Bounds via approximate additivity [Leditzky et al.'17].
- Even for the amplitude damping channel, we do not know.

Finite blocklength regime

- We know a lot about classical-quantum channel coding, e.g., second-order asymptotics [Tan, Tomamichel'15].
- But we know little beyond classical-quantum channels.



Outline of this talk

- Activated no-signalling-assisted codes.
- New meta-converse for unassisted codes via constant-bounded subchannels.
- Converse on asymptotic capacity.

Activated no-signalling-assisted codes

Hypothesis testing converse and NS-assisted capacity

- Classical channels
  - Polyanskiy-Poor-Verdu hypothesis testing converse.
  - Achieving PPV converse via NS codes [Matthews'12]
- Quantum channels
  - PPV converse for unassisted capacity [Wang, Renner'12]
  - PPV converse for EA capacity: [Matthews, Wehner'14],

$$R_{MW}(\mathcal{N},\varepsilon) = \max_{\rho_{A'}} \min_{\sigma_B} D_H^{\varepsilon}(\mathcal{N}_{A\to B}(\phi_{A'A}) \| \rho_{A'} \otimes \sigma_B).$$

    where D_H^{ε} is the hypothesis testing relative entropy and $\phi_{A'A}$ is the purification of ρ_A.
  - One-shot NS-assisted capacity [Wang, Xie, Duan'17]:

$$C_{\text{NS}}^{(1)}(\mathcal{N},\varepsilon) \le R_{MW}(\mathcal{N},\varepsilon).$$

  - However, the inequality can be strict for quantum channels!
- Q: Why the gap appears or how to fix the gap?

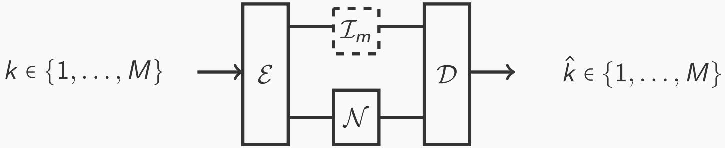
Activated capacity

- Potential capacity [Winter, Yang'16]

$$C_p(\mathcal{N}) = \sup_{\mathcal{M}} \big(C(\mathcal{N} \otimes \mathcal{M}) - C(\mathcal{M}) \big).$$

- Activated NS-assisted capacity
  - Restrict the catalytic channel to noiseless channel;
  - One-shot ε-error activated NS-assisted capacity

$$C^{(1)}_{\mathrm{NS,a}}(\mathcal{N}, \varepsilon) := \sup_{m \geq 1} \left[C^{(1)}_{\mathrm{NS}}(\mathcal{N} \otimes \mathcal{I}_m, \varepsilon) - \log m \right], \qquad (1)$$



  - Zero-error inforation theory [Acín, Duan, Roberson, Sainz, Winter'17; Duan, Wang'15].

Result 1: Achieving MW converse via activated NS codes

Theorem

For any quantum channel $\mathcal{N}_{A\to B}$, we have

$$C^{(1)}_{\mathrm{NS,a}}(\mathcal{N},\varepsilon) = \max_{\rho_{A'}} \min_{\sigma_B} D_H^{\varepsilon}(\mathcal{N}_{A\to B}(\phi_{A'A}) \| \rho_{A'} \otimes \sigma_B).$$

- It generalizes the case of classical channels [Matthews'12].
- For quantum channels, the NS codes require a classical noiseless channel as a catalyst to achieve the hypothesis testing converse.
- Ituition of achievability: the catalytic noiseless channel provides a larger solution space to activate the capacity.
- Converse part: duality theory of SDP.

Constant-bounded subchannels and a new meta-converse

Brief idea: constant-bounded subchannel

- Rough intuition: The "divergence" between $\mathcal{N}$ and "useless channels" measures the communication capability of $\mathcal{N}$. (E.g., entanglement theory, $E_D(\rho) \leq \min_{\sigma \in \mathrm{SEP}} D(\rho \| \sigma)$.)
- The useless channel for c.c. is the constant channel:

$$\mathcal{N}(\rho) = \sigma_B, \quad \forall \rho \in \mathcal{S}(A)$$

- As a natural extension, we say a CP map $\mathcal{M}$ is constant-bounded if there exists a state σ_B such that

$$\mathcal{M}(\rho) \leq \sigma_B, \quad \forall \rho \in \mathcal{S}(A).$$

Bounded by constant σ_B

- Constant-bounded (CB) CP map = CB subchannel.
- We denote the set of constant-bounded subchannels as $\mathcal{V}$.

Result 2: converse bounds on one-shot capacities

Theorem

For any quantum channel $\mathcal{N}_{A'\to B}$, we have

$$C^{(1)}(\mathcal{N},\varepsilon) \le \max_{\rho_{A'}} \min_{\mathcal{M}\in\mathcal{V}} D_H^{\varepsilon}(\mathcal{N}_{A'\to B}(\phi_{A'A}) \| \mathcal{M}_{A'\to B}(\phi_{A'A}))$$

where $\phi_{A'A}$ is a purification of $\rho_{A'}$.

- Hypothesis test between $\mathcal{N}$ and the useless channel $\mathcal{M}$

$$D_H^{\varepsilon}(\rho_1\|\rho_2) = -\log \boxed{\begin{aligned} \min\ & \operatorname{Tr} M_1\rho_2 \\ \text{s.t. }\ & \operatorname{Tr} M_2\rho_1 \le \varepsilon, \\ & M_1, M_2 \ge 0, \\ & M_1 + M_2 = \mathbb{1}. \end{aligned}}$$

Type-II error

Type-I error

- We have a necessary SDP condition for $\mathcal{M} \in \mathcal{V}$.

Sketch of proof

- Unassisted code with inputs $\{\rho_k\}_{k=1}^m$ POVM $\{M_k\}_{k=1}^m$, average input $\rho_A = \sum_{k=1}^m \rho_k/m$ and error ε.
- **Idea**: construct a hypothesis test via the code above.
- Let us choose the POVM $\{G, \mathbb{1} - G\}$ with

$$0 \le G = (\rho_A^T)^{-1/2}(\sum_{k=1}^m \frac{1}{m}\rho_k^T \otimes M_k)(\rho_A^T)^{-1/2} \le \mathbb{1}.$$

- The coding success probagility satisfies

$$p_{\mathrm{s}}(\mathcal{N}, m) = \operatorname{Tr} \mathcal{N}_{A' \to B}(\phi_{AA'}) G \ge 1 - \varepsilon.$$

- Moreover, for any constant-bounded subchannel $\mathcal{M}$,

$$\operatorname{Tr} \mathcal{M}_{A' \to B}(\phi_{AA'}) G \le \frac{1}{m} \sum_{k=1}^m \operatorname{Tr} \sigma_B M_k = \frac{1}{m}.$$

Sketch of proof (cont.)

- Based on the hypothesis test, we have

$$\log m \leq -\log \operatorname{Tr} \mathcal{M}(\phi_{AA'}) G,$$
$$1 - \operatorname{Tr} \mathcal{N}(\phi_{AA'}) G \leq \varepsilon.$$

- $D_H^\varepsilon(\rho_1 \| \rho_2) := -\log \min\{\operatorname{Tr} G\rho_2 : 1 - \operatorname{Tr} G\rho_1 \leq \varepsilon, 0 \leq G \leq \mathbb{1}\}.$
- Then we can wrap up and obtain

$$C^{(1)}(\mathcal{N}, \rho_A, \varepsilon) \leq \min_{\mathcal{M} \in \mathcal{V}} D_H^\varepsilon(\mathcal{N}(\phi_{AA'}) \| \mathcal{M}(\phi_{AA'}))$$

.

- Finally, one can maximize over ρ_A.

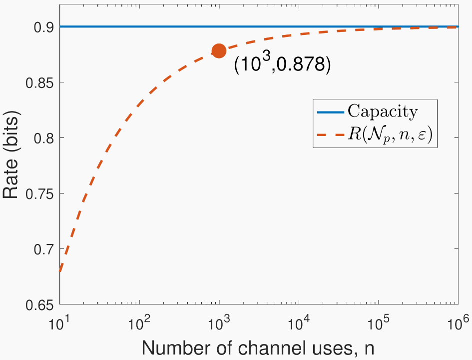
Application: second-order asymptotics of q erasure channel

- Quantum erasure channel [Bennett, DiVincenzo, Smolin'97]:

$$\mathcal{N}_p : \rho \to (1-p)\rho + p|e\rangle\langle e|, \quad C(\mathcal{N}_p) = (1-p)\log d_{in}.$$

- For channel uses n, error tolerance ε, the optimal rate is

$$R(\mathcal{N}_p, n, \varepsilon) = (1-p)\log d + \sqrt{p(1-p)(\log d)^2/n}\ \Phi^{-1}(\varepsilon) + O\left(\frac{\log n}{n}\right).$$



- Let us choose the erasure parameter $p = 0.1$ and error tolerance $\varepsilon = 0.01$.
- Red point: the optimal number of bits that can be sent faithfully ($\varepsilon = 0.01$) via $\mathcal{N}_{0.1}^{\otimes 1000}$ is about 878.
- Φ is the cumulative distribution function of a standard normal R. V..
- Our result also implies the strong converse of $\mathcal{N}_p$ [Wilde, Winter'14].

Application: quantum erasure channel (cont.)

- Achievable part: reduce to classical channel.
- Converse part:
  - Construct a constant-bounded subchannel $\mathcal{M}_p$:

$$\rho \longrightarrow \boxed{\mathcal{M}_p} \longrightarrow \frac{1-p}{d}\rho + p|e\rangle\langle e| \leq \frac{1-p}{d}\mathbb{1}_d + p|e\rangle\langle e|$$

  - Explore properties of D_H^ε.
  - Second-order of D_H^ε (Tomamichel, Hayashi'13, Li'13).
  - Then we have

$$\begin{aligned} C^{(1)}(\mathcal{N}^{\otimes n}, \varepsilon) &\leq D_H^\varepsilon(\mathcal{N}_p^{\otimes n}(\Phi_{A'^n A^n}) \| \mathcal{M}_p^{\otimes n}(\Phi_{A'^n A^n})) \\ &\leq n(1-p)\log d + \sqrt{np(1-p)(\log d)^2}\, \Phi^{-1}(\varepsilon) + \ldots \end{aligned}$$

Asymptotic communication capability

Result 3: New upper bound

- Inspired by our meta-converse, we define the Υ-information

$$\Upsilon(\mathcal{N}) := \max_{\rho_{A'}} \min_{\mathcal{M}\in\mathcal{V}} D(\mathcal{N}_{A'\to B}(\phi_{A'A}) \| \mathcal{M}_{A'\to B}(\phi_{A'A}))$$

New converse for χ and C

For any quantum channel $\mathcal{N}$, we have

$$\chi(\mathcal{N}) \leq \Upsilon(\mathcal{N}),\ C(\mathcal{N}) \leq \Upsilon^{\infty}(\mathcal{N}).$$

- $\Upsilon(I_d) = \log d$, $\Upsilon(\mathcal{N}) > 0$ iff $C(\mathcal{N}) > 0$.
- Sketch of proof:

$$\begin{aligned}
\Upsilon(\mathcal{N}) &= \min_{\mathcal{M}\in\mathcal{V}} \max_{\rho_{A'}} D(\mathcal{N}_{A'\to B}(\phi_{A'A}) \| \mathcal{M}_{A'\to B}(\phi_{A'A})) \longrightarrow \text{Sion's minimax theorem} \\
&\geq \min_{\mathcal{M}\in\mathcal{V}} \max_{\rho_{A'}} D(\mathcal{N}_{A'\to B}(\rho_{A'}) \| \mathcal{M}_{A'\to B}(\rho_{A'})) \longrightarrow \text{Data processing inequality} \\
&\geq \min_{\sigma_{\mathcal{M}}} \max_{\rho_{A'}} D(\mathcal{N}_{A'\to B}(\rho_{A'}) \| \sigma_{\mathcal{M}}) \\
&= \chi(\mathcal{N}).
\end{aligned}$$

$\chi(\mathcal{N})$ as divergence radius [Schumacher, Westmoreland'01]

More: Operator radius and Amplitude damping channel

- [XW, Xie, Duan'17] For amplitude damping channel, $\mathcal{N}_\gamma^{AD}(\rho) = \sum_{i=0}^1 E_i\rho E_i^\dagger$ with $E_0 = |0\rangle\langle 0| + \sqrt{1-\gamma}|1\rangle\langle 1|$, $E_1 = \sqrt{\gamma}|0\rangle\langle 1|$,

$$C(\mathcal{N}_\gamma^{AD}) \leq C_\beta(\mathcal{N}_\gamma^{AD}) = \log(1+\sqrt{1-\gamma}).$$

- In last QIP, people asked about the intuition of this bound.
- Based on the idea of constant-bounded subchannel, we could introduce the operator radius, i.e.,

$$\eta(\mathcal{N}) := \log\{\min \operatorname{Tr} S : \mathcal{N}(\rho) \leq S, \forall \rho \in \mathcal{S}(A)\}.$$

- For AD channel,

$$\boxed{\eta(\mathcal{N}_\gamma^{AD}) = C_\beta(\mathcal{N}_\gamma^{AD}) = \log(1+\sqrt{1-\gamma}).}$$

- $\chi(\mathcal{N}) \leq \eta(\mathcal{N})$, and more.

Summary

- Achieving Matthews-Wehner converse via activated NS-assisted codes.
- By introducing constant-bounded subchannels, we provide a hypothesis testing converse for one-shot ε-error capacity.
- Application: finite resource analysis of Q erasure channel, including the second-order expansion of classical capacity beyond cq channels.
- New converse Υ-information, operator radius.
- An interpratation of the best known bound for AD channel.

Open questions

- Reall $\Upsilon(\mathcal{N}) = \max_{\rho_{A'}} \min_{\mathcal{M}\in\mathcal{V}} D(\mathcal{N}(\phi_{A'A}) \| \mathcal{M}(\phi_{A'A}))$
  Q: Is Υ-information additive?
- Better converse without using CB subchannel?

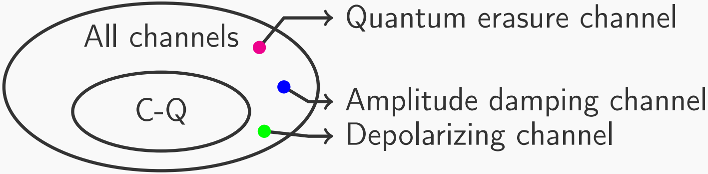
$$\begin{tikzcd}
C_E \arrow[rr, leftrightarrow, "\setminus" description] \arrow[d] \arrow[drr] & & C_\beta \arrow[d] \arrow[dll] \\
\Upsilon^\infty \arrow[d] & & \Upsilon \arrow[ll, "?"'] \arrow[d] \\
C \arrow[rr] & & \chi
\end{tikzcd}$$

An arrow $A \longrightarrow B$ indicates that $A(\mathcal{N}) \geq B(\mathcal{N})$ for any channel $\mathcal{N}$.
$A \longleftrightarrow\!\!\!\!\!\!\!\!\setminus\;\;\;\; B$ indicates that A and B are not comparable.

- C_E: entanglement-assisted classical capacity [Bennett et al.'99].
- C_β: SDP strong converse [XW, Xie, Duan'17].

Outlook

- Our understanding of the classical communication capability of quantum channels is still limited.
- Classical capacity of amplitude damping channel?
- More analysis beyond classical-quantum channels?



- For instance, the second-order asymptotics for depolarizing channels and entanglement-breaking channels?

Thank you for your attention!

See arXiv:1709.05258 for further details.