Quantum Channel State Masking

Uzi Pereg
Christian Deppe
Holger Boche

Technical University of Munich

Motivation

Quantum Communication and Information Theory

- Natural extension of the classical theory to quantum systems

Motivation

Quantum Communication and Information Theory

- Natural extension of the classical theory to quantum systems
- reveals "strange" phenomena: negative conditional entropy, super-activation, etc.

Motivation

Quantum Communication and Information Theory

- Natural extension of the classical theory to quantum systems
- reveals "strange" phenomena: negative conditional entropy, super-activation, etc.
- Progress in practice
  - Quantum key distribution for secure communication (307 km in optical fibers, 1200 km through space)

Motivation

Quantum Communication and Information Theory

- Natural extension of the classical theory to quantum systems
- reveals "strange" phenomena: negative conditional entropy, super-activation, etc.
- Progress in practice
  - Quantum key distribution for secure communication (307 km in optical fibers, 1200 km through space)
  - Computation power: Google's supremacy experiment

Motivation (Cont.)

State-dependent channels

- Channel state information (CSI)
  - classical applications: cognitive radio in wireless systems, memory storage, digital watermarking, etc.
- State masking: the state sequence represents information that should remain hidden from the receiver [Merhav and Shamai, 2007]

Background: State-Dependent Channels

Classical results with channel state information (CSI) at the encoder:

- Causal CSI [Shannon 1958]
- Strictly-causal CSI [Csiszár and Körner 1981]
- Non-causal CSI [Gel'fand and Pinsker 1980]

Classical state masking [Merhav and Shamai, 2007]

- Empirical coordination [Le Treust and Bloch 2016]
- Broadcast channel [Koyluoglu et al. 2016] [Dikshtein et al. 2019]
- Source coding [Courtade 2012]
- Non-causal CSI [Gel'fand and Pinsker 1980]

Background: State-Dependent Channels (Cont.)

Quantum channels with side information

- Without entanglement assistance: classical-quantum channels with causal or non-causal CSI [Boche, Cai, and Nötzel 2016]
- Entanglement assistance with non-causal CSI [Dupuis 2008]
- Entanglement assistance with causal CSI [P. 2020]
- Rate & State channel (parameter estimation) [P. 2020]

Main Contributions

- Rate-limited entanglement assistance
  - Achievable rate-leakage region: tradeoff between communication, leakage, and entanglement resources.

Main Contributions

- Rate-limited entanglement assistance
  - Achievable rate-leakage region: tradeoff between communication, leakage, and entanglement resources.
- Quantum capacity-leakage region
  - unlimited entanglement assistance
  - without assistance

Main Contributions

- Rate-limited entanglement assistance
  - Achievable rate-leakage region: tradeoff between communication, leakage, and entanglement resources.
- Quantum capacity-leakage region
  - unlimited entanglement assistance
  - without assistance
- Proof:
  - Achievability is based on the decoupling approach
  - Converse proof: classical arguments do not work

Outline

- Definitions
- Main Results

Quantum States

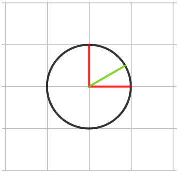
A pure quantum state $|\psi\rangle$ is a vector in the Hilbert space $\mathcal{H}_A$.

Qubit

For a qubit, $|\psi\rangle = |0\rangle$, $|1\rangle$, or

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \ , \ \text{with } |\alpha|^2 + |\beta^2| = 1$$

For $\alpha, \beta \in \mathbb{R}$:



Quantum States

A pure quantum state $|\psi\rangle$ is a vector in the Hilbert space $\mathcal{H}_A$.

Qubit

For a qubit, $|\psi\rangle = |0\rangle$, $|1\rangle$, or

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \;, \;\; \text{with } |\alpha|^2 + |\beta^2| = 1$$

Entanglement

Systems A and B are entangled if $|\psi_{AB}\rangle \neq |\psi_A\rangle \otimes |\psi_B\rangle$

For example, $|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$.
Entanglement can generate shared randomness, but it is a much more powerful resource.

Quantum States (Cont.)

The state ρ_A of a quantum system A is an Hermitian, positive semidefinite, unit-trace density matrix over $\mathcal{H}_A$.

Given ρ_{AB}, define

$$H(A)_\rho \equiv -\mathrm{Tr}(\rho_A \log \rho_A)$$

$$H(A|B)_\rho \equiv H(AB)_\rho - H(B)_\rho$$

For $|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$,

$$H(AB)_\Phi = 0\,,\ H(A)_\Phi = H(B)_\Phi = 1 \ \Rightarrow\ H(A|B)_\Phi = -1$$

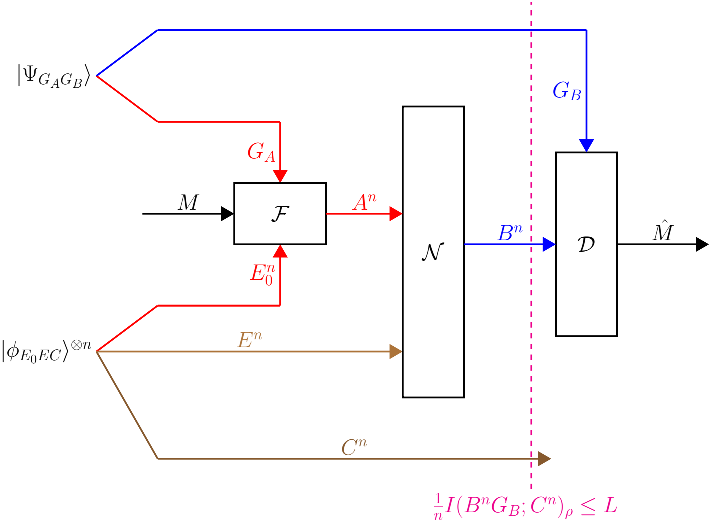
Quantum States (Cont.)

- Mutual information $I(A;B)_\rho = H(A)_\rho + H(B)_\rho - H(AB)_\rho$
- Coherent information $I(A\rangle B)_\rho = -H(A|B)_\rho$.

Channel Model

Quantum state-dependent channel

- A given CPTP linear map $\mathcal{N}_{EA \to B}$
- A pure state $|\phi_{EE_0C}\rangle^{\otimes n}$ (memoryless)
- Channel state information (CSI): Alice has E_0^n
- Entanglement resources: Alice and Bob share $\Psi_{G_A G_B}$


$|\Psi_{G_A G_B}\rangle$
G_B
G_A
M
$\mathcal{F}$
A^n
$\mathcal{N}$
B^n
$\mathcal{D}$
$\hat{M}$
E_0^n
$|\phi_{E_0 EC}\rangle^{\otimes n}$
E^n
C^n
$\frac{1}{n} I(B^n G_B; C^n)_\rho \leq L$

Channel Model (Cont.)

Leakage

- In the classical case, the leakage requirement need not include shared randomness (cannot help the decoder).
- Our leakage requirement includes the entanglement resource system because Bob could use it to extract information on the channel state, using teleportation for instance.

Outline

- Definitions
- Main Results

Main Results: Rate-Limited Assistance

Theorem

A quantum communication rate Q is achievable with leakage rate L and entanglement-assitance rate R_e if

$$\begin{aligned} Q + R_e &\leq H(A|EC)_\rho \\ Q - R_e &\leq -H(A|B)_\rho \\ L &\geq I(C;AB)_\rho \end{aligned}$$

for some $\rho_{AA'EC}$ with $\rho_{EC} = \phi_{EC}$, where $\rho_{ABC} = \mathcal{N}_{EA' \to B}(\rho_{AEA'C})$.

- demonstrates tradeoff between communication, leakage, and entanglement rates.
- Proof is based on the decoupling approach.

Proof

Main Results: Unassisted Region

Define

$$\underline{\mathcal{Q}}(\mathcal{N}) \equiv \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\phi_{EC}} \left\{ \begin{array}{rl} (Q,L)\ :\ 0 \leq Q \leq & \min\{-H(A|B)_\rho\,,\ H(A|EC)_\rho\} \\ L \geq & I(C;AB)_\rho \end{array} \right\}$$

and

$$\overline{\mathcal{Q}}(\mathcal{U}^{\mathsf{H}}) \equiv \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\phi_{EC}} \left\{ \begin{array}{rl} (Q,L)\ :\ 0 \leq Q \leq & H(A|CK)_\rho \\ L \geq & I(C;AB)_\rho \end{array} \right\}$$

with $\rho_{ABC} = \mathcal{N}_{EA'\to B}(\rho_{AEA'C})$ and $\rho_{ABKC} = \mathcal{U}^{\mathsf{H}}_{EA'\to BK}(\rho_{AEA'C})$.

Main Results: Unassisted Region (Cont.)

Theorem

1. *the quantum masking region without assistance is given by*

$$\mathcal{R}_Q = \bigcup_{k=1}^{\infty} \frac{1}{k} \underline{\mathcal{Q}}(\mathcal{N}^{\otimes k})\,.$$

2. *For a Hadamard channel,*

$$\underline{\mathcal{Q}}(\mathcal{N}^{H}) \subseteq \mathcal{R}_Q \subseteq \overline{\mathcal{Q}}(\mathcal{U}^{H})$$

- arguments of Merhav and Shamai (2007) do **not** work in the quantum setting because $H(M|B^nC^n)_\rho < 0$.

Proof

Main Results: Entanglement-Assisted Region

Theorem

Given entanglement assistance, the quantum capacity-leakage region is

$$\mathcal{R}_Q^{ea} = \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\varphi_{EC}} \left\{ \begin{array}{rl} (Q,L)\ :\ 0 \leq Q \leq & \frac{1}{2}[I(A;B)_\rho - I(A;EC)_\rho] \\ L \geq & I(C;AB)_\rho \end{array} \right\}$$

and the classical capacity-leakage region is

$$\mathcal{R}_{Cl}^{ea} = \bigcup_{\rho_{EA'AC}\,:\,\rho_{EC}=\varphi_{EC}} \left\{ \begin{array}{rl} (R,L)\ :\ 0 \leq R \leq & I(A;B)_\rho - I(A;EC)_\rho \\ L \geq & I(C;AB)_\rho \end{array} \right\}$$

assuming ***maximally correlated*** *channel state systems:*

$$\varphi_{EE_0C} = \sum_{s\in\mathcal{S}} q(s)|s\rangle\langle s|_E \otimes |s\rangle\langle s|_{E_0} \otimes |s\rangle\langle s|_C$$

Example

Conclusion

Our results demonstrate the following common phenomena in quantum information theory:

- Entanglement-assisted protocols can accomplish a performance increase compared to unassisted protocols.
- Introducing entanglement resources transforms the capacity formula from multi-letter to single-letter form
- Dimension bound is an open problem — also for quantum wiretap channel, quantum broadcast channel, squashed entanglement, etc.

Thank you

Example: Dephasing Channel

State-dependent dephasing channel

Given a classical channel state $S \sim \text{Bernoulli}(q)$,

$$\mathcal{N}_{EA\to B}(\rho_{EA}) =(1-q)\mathcal{P}^{(0)}_{A\to B}(\sigma_0) + q\mathcal{P}^{(1)}_{A\to B}(\sigma_1)$$

$$\mathcal{P}^{(s)}_{A\to B}(\sigma) =(1-\varepsilon_s)\sigma + \varepsilon_s Z\sigma Z \ , \quad s=0,1,$$

for $\rho_{EA} = (1-q)|0\rangle\langle 0|_E \otimes \sigma_0 + q|1\rangle\langle 1|_E \otimes \sigma_1$.

Example: Dephasing Channel

State-dependent dephasing channel

Given a classical channel state $S \sim \text{Bernoulli}(q)$,

$$\mathcal{N}_{EA\to B}(\rho_{EA}) = (1-q)\mathcal{P}^{(0)}_{A\to B}(\sigma_0) + q\mathcal{P}^{(1)}_{A\to B}(\sigma_1)$$

$$\mathcal{P}^{(s)}_{A\to B}(\sigma) = (1-\varepsilon_s)\sigma + \varepsilon_s Z\sigma Z \ , \quad s = 0, 1,$$

for $\rho_{EA} = (1-q)|0\rangle\langle 0|_E \otimes \sigma_0 + q|1\rangle\langle 1|_E \otimes \sigma_1$.

If Alice applies Z gate controlled by $S \oplus Y$, $Y \sim \text{Bernoulli}(\lambda)$, this achieves

$$\mathcal{R}^{\text{ea}}_{\text{Cl}} \supseteq \bigcup_{0\leq\lambda\leq\frac{1}{2}} \left\{ \begin{array}{l} (R, L) \ : \ 0 \leq R \leq 2 - h_2(\lambda * \hat{\varepsilon}) \\ L \geq h_2(\lambda * \hat{\varepsilon}) - (1-q)h_2(\lambda * \varepsilon_0) - qh_2(\lambda * \varepsilon_1) \end{array} \right\}$$

where $a * b = (1-a)b + a(1-b)$ and $\hat{\varepsilon} = (1-q)\varepsilon_0 + q(1-\varepsilon_1)$.

IID Decoupling

Theorem

Let $|\omega_{ABK}\rangle$, $|\sigma_{SRG_1G_2}\rangle = |\Psi_{SR}\rangle \otimes |\Phi_{G_1G_2}\rangle$ *in* $\mathcal{H}_S^{\otimes 2} \otimes \mathcal{H}_G^{\otimes 2}$. *Let* $W_{SG_1 \to A^n}$ *be a full-rank partial isometry, and denote* $|\sigma_{A^nRG_2}\rangle = W_{SG_1\to A^n}|\sigma_{SRG_1G_2}\rangle$ .. *Define*

$$\mathcal{T}_{A\to K}(\rho_A) = |\mathcal{H}_A| \mathrm{Tr}_B \left[op_{A\to BK}(|\omega_{ABK}\rangle)(\rho_A) \right]$$

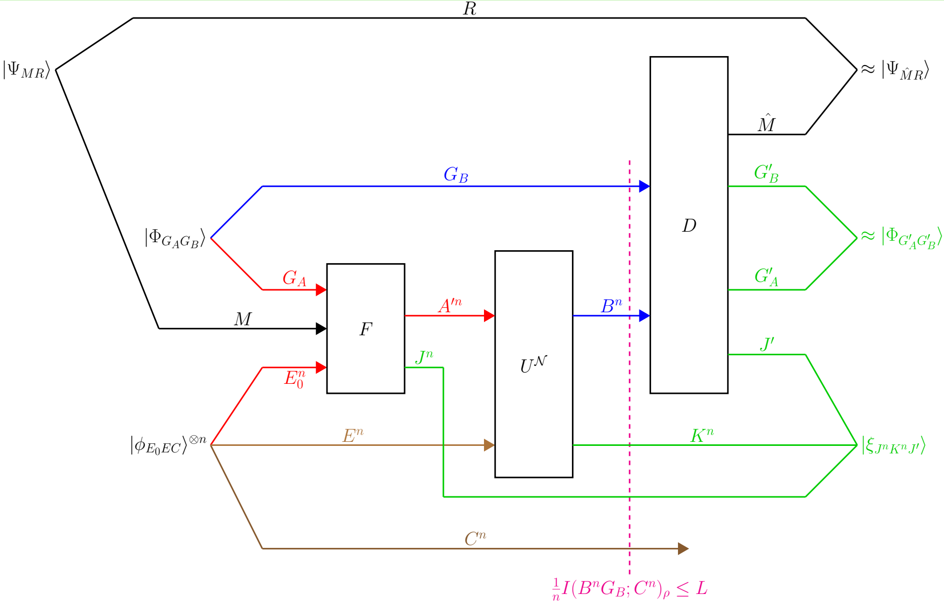
where $op_{A\to B}(|i_A\rangle \otimes |j_B\rangle) \equiv |j_B\rangle\langle i_A|$. *Then,*

$$\int_{\mathbb{U}_{A^n}} dU_{A^n} \left\| \mathcal{T}_{A\to K}^{\otimes n}(U_{A^n}\sigma_{A^nR}) - \omega_K \otimes \sigma_R \right\|_1 \leq \sqrt{\frac{|\mathcal{H}_S|}{|\mathcal{H}_G|} 2^{-nH(A|K)_\omega + n\varepsilon_n}}$$

$$\int_{\mathbb{U}_{A^n}} dU_{A^n} \left\| \mathcal{T}_{A\to K}^{\otimes n}(U_{A^n}\sigma_{A^nRG_2}) - \omega_K \otimes \sigma_{RG_2} \right\|_1 \leq \sqrt{|\mathcal{H}_S||\mathcal{H}_G| 2^{-nH(A|K)_\omega + n\varepsilon_n}}$$

where the integral is over the Haar measure on all unitaries U_{A^n}.

Achievability Scheme



Converse Proof (Unassisted)

The leakage is bounded by

$$\begin{aligned} n(L+\beta_n) &\geq I(C^n;B^n)_\rho \\ &= I(C^n;MB^n)_\rho - I(C^n;M|B^n)_\rho \\ &= I(C^n;MB^n)_\rho - H(M|B^n)_\rho + H(M|B^nC^n)_\rho \end{aligned}$$

$\hookleftarrow$

Converse Proof (Unassisted)

The leakage is bounded by

$$
\begin{aligned}
n(L+\beta_n) &\geq I(C^n;B^n)_\rho \\
&= I(C^n;MB^n)_\rho - I(C^n;M|B^n)_\rho \\
&= I(C^n;MB^n)_\rho - H(M|B^n)_\rho + H(M|B^nC^n)_\rho \\
&= I(C^n;MB^n)_\rho + I(M\rangle B^n)_\rho + H(M|B^nC^n)_\rho \\
&\geq I(C^n;MB^n)_\rho + n(Q-\varepsilon_n) + H(M|B^nC^n)_\rho
\end{aligned}
$$

Since $H(M|B^nC^n)_\rho \geq -\log|\mathcal{H}_M| = -nQ$,

$$
L+\beta_n+\varepsilon_n \geq \frac{1}{n} I(C^n;MB^n)_\rho
$$

$\hookleftarrow$