Communication with Unreliable Entanglement Assistance

Uzi Pereg

Technical University of Munich

Munich Center for Quantum Science and Technology (MCQST)

Joint Work with Christian Deppe and Holger Boche

Motivation

Quantum information technology will potentially boost future 6G systems from both communication and computing perspectives.

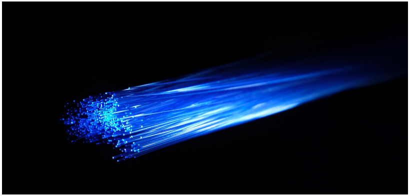
Progress in practice:

Motivation

Quantum information technology will potentially boost future 6G systems from both communication and computing perspectives.

Progress in practice:

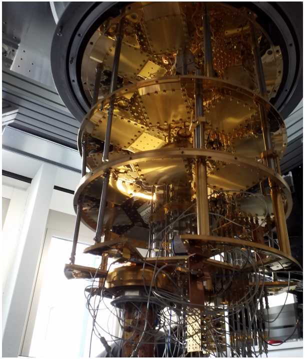
- Quantum key distribution for secure communication (511 km in optical fibers, 1200 km through space)
  - commercially available: MagiQ, IDQuantique (82k$)
  - development: Toshiba, Airbus EuroQCI



unsplash.com

Motivation (Cont.)

- Quantum computation
  - Google Sycamore 53 qubits (2019): Supremacy experiment
  - IBM Eagle 127 qubits (2021)
  - Computer cluster (Aliro) $\rightarrow$ requires quantum communication

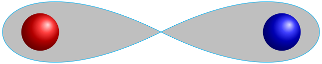


Walther Meißner Institute 6 qubits

Motivation: Entanglement

Entanglement resources are instrumental in a wide variety of quantum network frameworks:

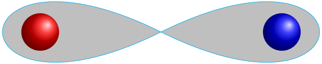
- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]



Motivation: Entanglement

Entanglement resources are instrumental in a wide variety of quantum network frameworks:

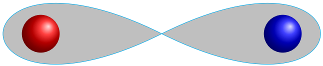
- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]
- Sensor networks [Xia et al. 2021]



Motivation: Entanglement

Entanglement resources are instrumental in a wide variety of quantum network frameworks:

- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]
- Sensor networks [Xia et al. 2021]
- **Communication rate** [Bennett et al. 1999] [Hao et al. 2021]
- ...

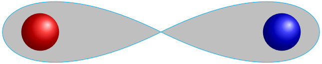


Motivation: Entanglement

Entanglement resources are instrumental in a wide variety of quantum network frameworks:

- Physical-layer security (device-independent QKD, quantum repeaters) [Vazirani and Vidick 2014] [Yin et al. 2020][Pompili et al. 2021]
- Sensor networks [Xia et al. 2021]
- Communication rate [Bennett et al. 1999] [Hao et al. 2021]
- ...

Unfortunately, entanglement is a fragile resource that is quickly degraded by decoherence effects.



Motivation: Entanglement (Cont.)

- In order to generate entanglement in an optical communication system, the transmitter may prepare an entangled pair of photons locally, and then send one of them to the receiver.

Motivation: Entanglement (Cont.)

- In order to generate entanglement in an optical communication system, the transmitter may prepare an entangled pair of photons locally, and then send one of them to the receiver.
- Such generation protocols are not always successful, as photons are easily absorbed before reaching the destination.

Motivation: Entanglement (Cont.)

- Therefore, practical systems require a back channel. In the case of failure, the protocol is to be repeated. The backward transmission may result in a delay, which in turn leads to a further degradation of the entanglement resources.

Motivation: Entanglement (Cont.)

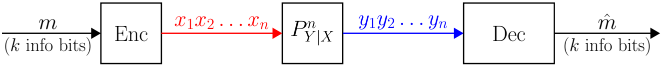
- Therefore, practical systems require a back channel. In the case of failure, the protocol is to be repeated. The backward transmission may result in a delay, which in turn leads to a further degradation of the entanglement resources.
- We propose a new principle of operation: The communication system operates on a rate that is adapted to the status of entanglement assistance. Hence, feedback and repetition are not required.

Classical Channel Capacity

Classical communication

Modern communication relies on error correction codes

- reduce probability of decoding error
- coding rate $R = \frac{k}{n} \frac{\text{information bits}}{\text{transmission}}$ (memory: $\frac{\text{logical bits}}{\text{physical bit registers}}$)



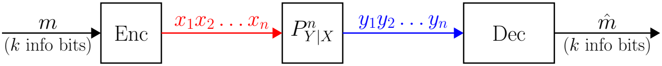
- Channel capacity (Shannon limit)
  - highest communication rate with Pr(error) $\to 0$ for $n \to \infty$
  - simple 'single-letter' formula

Classical Channel Capacity

Classical communication

Modern communication relies on error correction codes

- reduce probability of decoding error
- coding rate $R = \frac{k}{n} \frac{\text{information bits}}{\text{transmission}}$ (memory: $\frac{\text{logical bits}}{\text{physical bit registers}}$)



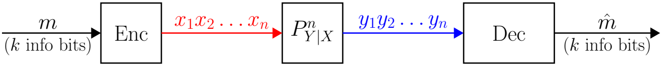
- Channel capacity (Shannon limit)
  - highest communication rate with Pr(error) $\to 0$ for $n \to \infty$
  - simple 'single-letter' formula

Classical Channel Capacity

Classical communication

Modern communication relies on error correction codes

- reduce probability of decoding error
- coding rate $R = \frac{k}{n} \frac{\text{information bits}}{\text{transmission}}$ (memory: $\frac{\text{logical bits}}{\text{physical bit registers}}$)



- Channel capacity (Shannon limit)
  - highest communication rate with Pr(error) $\to 0$ for $n \to \infty$
  - simple 'single-letter' formula

Classical Channel Capacity (Cont.)

Reliability (very partial list):

- Unreliable channel
  - outage capacity [Ozarow, Shamai, and Wyner 1994]
  - automatic repeat request (ARQ) [Caire and Tuninetti 2001] [Steiner and Shamai 2008]
  - cognitive radio [Goldsmith et al. 2008]
  - connectivity [Simeone et al. 2012] [Karasik, Simeone, and Shamai 2013]

Classical Channel Capacity (Cont.)

Reliability (very partial list):

- Unreliable channel
  - outage capacity [Ozarow, Shamai, and Wyner 1994]
  - automatic repeat request (ARQ) [Caire and Tuninetti 2001] [Steiner and Shamai 2008]
  - cognitive radio [Goldsmith et al. 2008]
  - connectivity [Simeone et al. 2012] [Karasik, Simeone, and Shamai 2013]
- Unreliable cooperation [Steinberg 2014]
  - cribbing encoders [Huleihel and Steinberg 2016]
  - conferencing decoders [Huleihel and Steinberg 2017] [Itzhak and Steinberg 2017] [P. and Steinberg 2020]

Quantum Channel Capacities

Different categories for capacity of quantum channels:

Quantum Channel Capacities

Different categories for capacity of quantum channels:

- Classical capacity [Holevo 1998, Schumacher and Westmoreland 1997]
  - transmission of classical bits using a quantum channel

Quantum Channel Capacities

Different categories for capacity of quantum channels:

- Classical capacity [Holevo 1998, Schumacher and Westmoreland 1997]
  - transmission of classical bits using a quantum channel
- Quantum capacity [Lloyd 1998, Shor 2002, Devetak 2005]
  - transmission of qubits (= quantum bits)

Quantum Channel Capacities

Different categories for capacity of quantum channels:

- Classical capacity [Holevo 1998, Schumacher and Westmoreland 1997]
  - transmission of classical bits using a quantum channel
  - multi-letter formula ☹
- Quantum capacity [Lloyd 1998, Shor 2002, Devetak 2005]
  - transmission of qubits (= quantum bits)
  - multi-letter formula ☹

Quantum Channel Capacities (Cont.)

- Entanglement-assisted capacities [Bennett et al. 1999]
  - Alice and Bob share entanglement resources
  - strictly higher capacities
  - single-letter formula ☺

Quantum Channel Capacities (Cont.)

- Classical channel
  - Single user: entanglement resources do not help [Bennett et al. 1999]

Quantum Channel Capacities (Cont.)

- Classical channel
  - Single user: entanglement resources do not help [Bennett et al. 1999]
  - MAC: entanglement resources between two transmitters can increase achievable rates! [Leditzky et al. 2020]

Quantum Channel Capacities (Cont.)

- Classical channel
  - Single user: entanglement resources do not help [Bennett et al. 1999]
  - MAC: entanglement resources between two transmitters can increase achievable rates! [Leditzky et al. 2020]
  - Broadcast: entanglement resources between two receivers cannot increase achievable rates [P. et al. 2021]

Quantum Channel Capacities (Cont.)

Unique features and challenges:

- Information measures
    - super additivity
    - negative conditional entropy
- Super-activation of *operational* capacity

Quantum Channel Capacities (Cont.)

- Correlations
  - entanglement increases performance
  - no-cloning theorem
  - entanglement monogamy
- Proof techniques
  - operator inequalities
  - gentle measurement
  - decoupling approach

Other Settings: Privacy, Security, and Estimation

Quantum channel state masking

- Alice has access to a quantum state that should be hidden from Bob

U. Pereg, C. Deppe and H. Boche, "Quantum Channel State Masking," *IEEE Transactions on Information Theory*, vol. 67, no. 4, pp. 2245-2268, April 2021; presented in *ITW'20*, *QIP'21*.

U. Pereg, C. Deppe and H. Boche, "Classical state masking over a quantum channel," *submitted to Physical Review A*, October 2021; accepted to *IZS'22*.

Layered secrecy, key assistance, and key agreement for bosonic broadcast networks

U. Pereg, R. Ferrara and M. R. Bloch, *ITW'21*.

Parameter estimation

- Watermarking with a quantum embedding

U. Pereg, *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 359-383, January 2022.

MCQST

Other Settings: Cooperation and Reliability

Quantum repeaters

U. Pereg, C. Deppe and H. Boche, "Quantum Broadcast Channels with Cooperating Decoders: An Information-Theoretic Perspective on Quantum Repeaters,"

Journal of Mathematical Physics, 62, 062204, June 2021.

Cribbing measurement

U. Pereg, C. Deppe and H. Boche, "The Quantum Multiple-Access Channels with Cribbing Encoders," submitted to *IEEE Transactions on Information Theory*, November 2021,

arXiv:2111.15589 [quant-ph]

Unreliable entanglement

U. Pereg, C. Deppe and H. Boche, "Communication Communication with Unreliable Entanglement Assistance," submitted to *Nature Communications*, December 2021.

arXiv:2112.09227 [quant-ph]

Outline

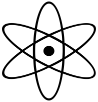
- Background: Quantum Information Theory
- The Fundamental Problem
- Coding
- Main Results

Quantum Theory

Quantum mechanics is arguably the most successful theory in physics.

Postulates

1. a physical system is associated with a Hilbert space
   - the physical state is **completely** specified by a wavefunction
2. unitary evolution (Schrödinger equation)
3. composite system
4. measurement

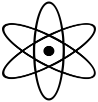


Quantum Theory

Quantum mechanics is arguably the most successful theory in physics.

Postulates

1. a physical system is associated with a Hilbert space
   - the physical state is **completely** specified by a wavefunction
2. unitary evolution (Schrödinger equation)
3. composite system
4. measurement



Pure States

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

Qubit

For a quantum bit (qubit),

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

Pure States

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

Qubit

For a quantum bit (qubit),

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

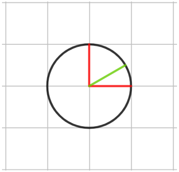
$$|\psi\rangle = \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \alpha|0\rangle + \beta|1\rangle$$

Pure States (Cont.)

Qubit (Cont.)

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

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

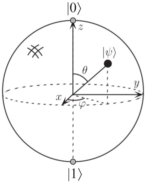


Pure States (Cont.)

Qubit (Cont.)

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

For $\alpha, \beta \in \mathbb{C}$: Bloch sphere



from the book “Quantum Computation and Quantum Information",
M. A. Nielsen and I. L. Chuang (2000).

Pure States (Cont.)

A pure bi-partite state $|\psi_{AB}\rangle$ is a normalized vector in the product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

Two qubits

For two qubits, $|\psi_{AB}\rangle = |i\rangle \otimes |j\rangle$, or

$$|\psi_{AB}\rangle = \sum_{i,j=0,1} \alpha_{ij} |i\rangle \otimes |j\rangle \ , \ \text{with} \sum |\alpha_{ij}|^2 = 1$$

Pure States (Cont.)

A pure bi-partite state $|\psi_{AB}\rangle$ is a normalized vector in the product Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$.

Two qubits

For two qubits, $|\psi_{AB}\rangle = |i\rangle \otimes |j\rangle$, or

$$|\psi_{AB}\rangle = \sum_{i,j=0,1} \alpha_{ij} |i\rangle \otimes |j\rangle \;, \text{ with } \sum |\alpha_{ij}|^2 = 1$$

Entanglement

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

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

Elementary Operations

Qubit Gate	Circuit	Matrix
Pauli X (Bit flip, NOT)	$-\boxed{\Sigma_X}-$	$\Sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ $\|a\rangle \rightarrow \|a \oplus 1\rangle$
Pauli Y (Bit&Phase flip)	$-\boxed{\Sigma_Y}-$	$\Sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix} = i\Sigma_X \Sigma_Z$ $\|a\rangle \rightarrow i(-1)^a \|a \oplus 1\rangle$
Pauli Z (Phase flip)	$-\boxed{\Sigma_Z}-$	$\Sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ $\|a\rangle \rightarrow (-1)^a \|a\rangle$

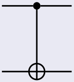
Elementary Operations (Cont.)

Hadamard

$$H = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$|a\rangle \to \frac{1}{\sqrt{2}}(|0\rangle + (-1)^a |1\rangle)$$

CNOT
(Controlled X)



$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

$$|a\rangle \otimes |b\rangle \to |a\rangle \otimes |a \oplus b\rangle$$

Quantum States, Measurement

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

Quantum States, Measurement

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

Spectral Decomposition

There exists a random variable $X \sim p_X$ such that

$$\rho_A = \sum_{x \in \mathcal{X}} p_X(x) |\psi_x\rangle\langle\psi_x|$$

where $|\psi_x\rangle$ form an orthonormal basis, $\langle\psi_x| = (|\psi_x\rangle)^\dagger$.

Quantum States, Measurement

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

Spectral Decomposition

There exists a random variable $X \sim p_X$ such that

$$\rho_A = \sum_{x \in \mathcal{X}} p_X(x) |\psi_x\rangle\langle\psi_x|$$

where $|\psi_x\rangle$ form an orthonormal basis, $\langle\psi_x| = (|\psi_x\rangle)^\dagger$.

Measurement

A POVM (= positive-operator valued measure) is a set of positive semi-definite operators $\{D_x\}$ such that $\sum_x D_x = \mathbb{1}$. Born rule: the probability of the measurement outcome x is $\Pr\{\text{outcome} = x\} = \mathrm{Tr}(D_x \rho_A)$.

Quantum Entropy and Mutual Information

Entropy

Given ρ_A, define

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

Quantum Entropy and Mutual Information

Entropy

Given ρ_A, define

$$H(A)_\rho \equiv -\mathrm{Tr}(\rho_A \log \rho_A) = -\sum_{x \in \mathcal{X}} p_X(x) \log p_X(x)$$

Quantum Entropy and Mutual Information

Entropy

Given ρ_{AB}, define

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

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

Maximally Entangled Qubits

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

MCQST

Maximally Entangled Qubits

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \qquad H(AB)_\Phi = 0$$

$$\rho_{AB} = |\Phi_{AB}\rangle\langle\Phi_{AB}|$$

Maximally Entangled Qubits

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \qquad H(AB)_\Phi = 0$$
$$\rho_{AB} = |\Phi_{AB}\rangle\langle\Phi_{AB}|$$

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \frac{1}{2}\mathbb{1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$

MCQST

Maximally Entangled Qubits

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \qquad H(AB)_\Phi = 0$$

$$\rho_{AB} = |\Phi_{AB}\rangle\langle\Phi_{AB}|$$

$$\rho_A = \mathrm{Tr}_B(\rho_{AB}) = \frac{1}{2}\mathbb{1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \qquad H(A)_\Phi = H(B)_\Phi = 1$$

Maximally Entangled Qubits

$$|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle) \qquad H(AB)_\Phi = 0$$
$$\rho_{AB} = |\Phi_{AB}\rangle\langle\Phi_{AB}|$$

$$\rho_A = \text{Tr}_B(\rho_{AB}) = \frac{1}{2}\mathbb{1} = \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix} \qquad H(A)_\Phi = H(B)_\Phi = 1$$

Thus,

$$H(A|B)_\Phi = -1$$

Quantum Entropy and Mutual Information (Cont.)

Information Measures

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

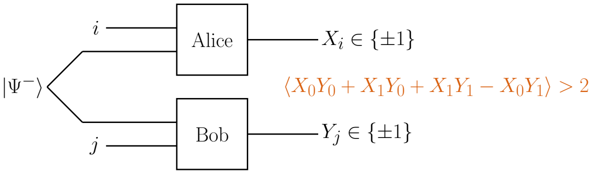
For example, for $|\Phi_{AB}\rangle = \frac{1}{\sqrt{2}}(|0\rangle \otimes |0\rangle + |1\rangle \otimes |1\rangle)$,

$$I(A;B)_\Phi = 2$$
$$I(A\rangle B)_\Phi = 1$$

Quantum Entropy and Mutual Information (Cont.)

Quantum correlations

- Bell experiment: Entanglement leads to correlations that exceed classical predictions
  - EPR's hidden-variable model (1935) is incompatible with measurements [Aspect et al. 1982]



Quantum Entropy and Mutual Information (Cont.)

Quantum correlations

- Bell experiment: Entanglement leads to correlations that exceed classical predictions
  - EPR's hidden-variable model (1935) is incompatible with measurements [Aspect et al. 1982]

- Information measures:

  - for classical bits, $H(X), H(X|Y), I(X;Y) \in [0,1]$

  - for quantum bits, $I(A;B)_\rho \in [0,2]$

Quantum Measurement

Remark: State Collapse

In general, measurements change the state. For example,

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad \begin{array}{ll} \nearrow & |0\rangle \qquad \Pr(0) = |\alpha|^2 \\ \searrow & |1\rangle \qquad \Pr(1) = |\beta|^2 \end{array}$$

Zero entropy — Positive entropy

Quantum Channel

Unitary vs. Noisy Evolution

- Unitary evolution

$$|\psi\rangle \xrightarrow{U} U|\psi\rangle \qquad\qquad U^\dagger U = UU^\dagger = \mathbb{1}$$

Quantum Channel

Unitary vs. Noisy Evolution

- Unitary evolution

$$|\psi\rangle \xrightarrow{U} U|\psi\rangle \qquad U^\dagger U = UU^\dagger = \mathbb{1}$$

- Noisy channel $\mathcal{N}_{A\to B}$

$$\rho_A \xrightarrow{\mathcal{N}} \rho_B \equiv \mathrm{Tr}_E(U\rho_A U^\dagger) \qquad U \equiv U^{\mathcal{N}}_{A\to BE}$$

$$U^\dagger U = \mathbb{1}_A$$

Quantum Channel (Cont.)

A quantum channel $\mathscr{N}_{A\to B}$ is a completely-positive trace-preserving map

$$\rho_A \xrightarrow{\mathscr{N}} \rho_B$$

Outline

- Background: Quantum Information Theory
- The Fundamental Problem
- Coding
- Main Results

Fundamental Problem: Noiseless Channel

Classical Bit-Pipe

The capacity of a classical noiseless bit channel is

$$1 \ \frac{\text{classical bit}}{\text{transmission}}$$

Holevo Bound

The classical capacity of a noiseless qubit channel is

$$1 \ \frac{\text{classical bit}}{\text{transmission}}$$

Fundamental Problem: Noiseless Channel + Assistance

Theorem

The classical *common-randomness* (CR) capacity of a noiseless bit-pipe is

$$1 \ \frac{\text{classical bit}}{\text{transmission}}$$

Holevo Bound

The classical capacity of a noiseless qubit channel is

$$1 \ \frac{\text{classical bit}}{\text{transmission}}$$

MCQST

Fundamental Problem: Noiseless Channel + Assistance

Theorem

The classical *common-randomness* (CR) capacity of a noiseless bit-pipe is

$$1 \ \frac{\text{classical bit}}{\text{transmission}}$$

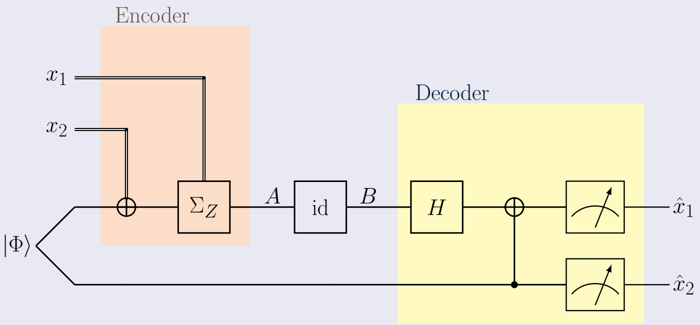
Theorem

The classical *entanglement-assisted* (EA) capacity of a noiseless qubit channel is

$$2 \ \frac{\text{classical bits}}{\textit{transmission}}$$

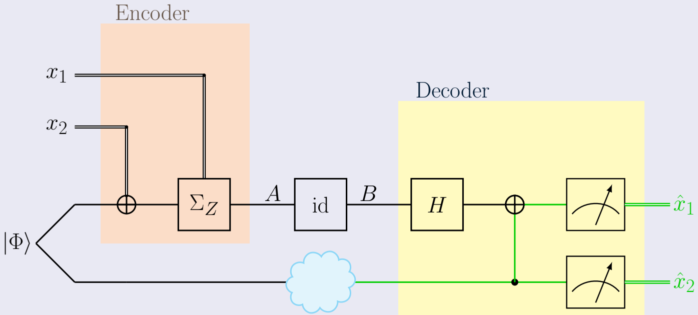
Fundamental Problem: Noiseless Channel + EA

Superdense Coding



Fundamental Problem: Noiseless Channel + EA (Cont.)

Superdense Coding



Fundamental Problem: Noiseless Channel + EA (Cont.)

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1. Uncoded communication

Fundamental Problem: Noiseless Channel + EA (Cont.)

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1. Uncoded communication
   - Guaranteed rate: $R = 1$
   - Excess rate: $R' = 0$

Fundamental Problem: Noiseless Channel + EA (Cont.)

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1. Uncoded communication
   - Guaranteed rate: $R = 1$
   - Excess rate: $R' = 0$

2. Alice: Employ superdense encoder.

   Bob: If EA is **present**, employ superdense decoder.

Fundamental Problem: Noiseless Channel + EA (Cont.)

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1. Uncoded communication
   - Guaranteed rate: $R = 1$
   - Excess rate: $R' = 0$

2. Alice: Employ superdense encoder.

   Bob: If EA is present, employ superdense decoder.
   If EA is **absent**, abort.

Fundamental Problem: Noiseless Channel + EA (Cont.)

We consider transmission with unreliable EA:
The entangled resource may fail to reach Bob.

Extreme Strategies

1. Uncoded communication
   - Guaranteed rate: $R = 1$
   - Excess rate: $R' = 0$

2. Alice: Employ superdense encoder.

   Bob: If EA is present, employ superdense decoder.
   If EA is absent, abort.

   - Guaranteed rate: $R = 0$
   - Excess rate: $R' = 2$

Fundamental Problem: Noiseless Channel + EA (Cont.)

Time Division

1st sub-block:

- Alice sends $(1-\lambda)n$ uncoded bits.
- Bob measures $(1-\lambda)n$ qubits without assistance.

2nd sub-block:

- Alice employs superdense encoding λn times.
- If EA is present, Bob decodes $2 \cdot \lambda n$ bits by superdense decoding.
- If EA is absent, Bob ignores λn qubits.

Fundamental Problem: Noiseless Channel + EA (Cont.)

Rates

- Guaranteed rate: $R = 1 - \lambda$
- Excess rate: $R' = 2\lambda$

⋆ Can we do better?

Main Contributions

- New principle of operation: communication over quantum channels with unreliable entanglement assistance.

- Classical information:
  Alice sends classical messages to Bob

Main Contributions

- New principle of operation: communication over quantum channels with unreliable entanglement assistance.
- Classical information:
  Alice sends classical messages to Bob
- Quantum information:
  Alice teleports a quantum state to Bob

Main Contributions

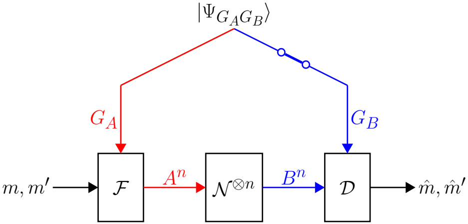
- New principle of operation: communication over quantum channels with unreliable entanglement assistance.
- Classical information:
  Alice sends classical messages to Bob
- Quantum information:
  Alice teleports a quantum state to Bob
- Time division, between entanglement-assisted and unassisted coding schemes, is optimal for a noiseless channel, but strictly sub-optimal for the depolarizing channel.

Outline

- Background: Quantum Information Theory
- The Fundamental Problem
- Coding
- Main Results

Communication Scheme (1)

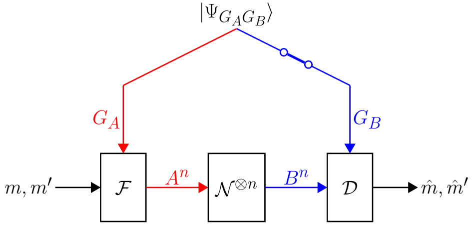
Alice chooses two messages, m and m'.



Classical Coding

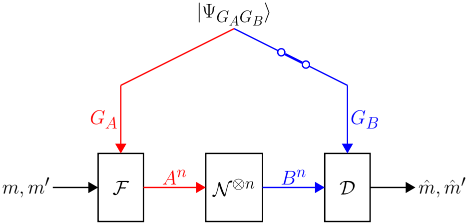
Communication Scheme (2)

Input: Alice prepares $\rho_{A^n}^{m,m'} = \mathcal{F}^{m,m'}(\Psi_{G_A})$, and transmits A^n.
Output: Bob receives B^n.



Decoding with Entanglement Assistance

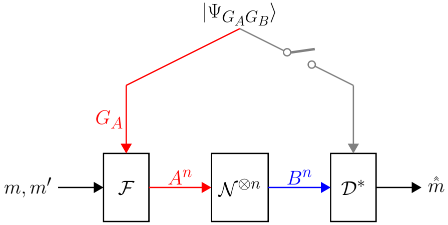
If EA is *present*, Bob performs a measurement $\mathcal{D}$ to estimate m, m'.



Classical Coding

Decoding without Assistance

If EA is absent, Bob performs a measurement $\mathcal{D}^*$ to estimate m alone.



Classical Coding (Cont.)

Error Probabilities

$$P^{(n)}_{e|m,m'} = 1 - \mathrm{Tr}\left[D_{m,m'}(\mathcal{N}^{\otimes n}_{A\to B} \otimes \mathsf{id})(\mathcal{F}^{m,m'} \otimes \mathsf{id})(\Psi_{G_A,G_B})\right]$$

$$P^{*(n)}_{e|m,m'} = 1 - \mathrm{Tr}\left[D^{*}_{m}\mathcal{N}^{\otimes n}_{A\to B}\,\mathcal{F}^{m,m'}(\Psi_{G_A})\right].$$

Classical Coding (Cont.)

Error Probabilities

$$P^{(n)}_{e|m,m'} = 1 - \mathrm{Tr}\left[D_{m,m'}(\mathcal{N}^{\otimes n}_{A\to B} \otimes \mathrm{id})(\mathcal{F}^{m,m'} \otimes \mathrm{id})(\Psi_{G_A,G_B})\right]$$

$$P^{*(n)}_{e|m,m'} = 1 - \mathrm{Tr}\left[D^{*}_{m}\, \mathcal{N}^{\otimes n}_{A\to B}\, \mathcal{F}^{m,m'}(\Psi_{G_A})\right].$$

Capacity Region

- (R, R') is achievable with unreliable entanglement assistance if there exists a sequence of $(2^{nR}, 2^{nR'}, n)$ codes such that $P^{(n)}_{e|m,m'}$, $P^{*(n)}_{e|m,m'} \to 0$ as $n \to \infty$.

Classical Coding (Cont.)

Error Probabilities

$$P^{(n)}_{e|m,m'} = 1 - \mathrm{Tr}\left[D_{m,m'}(\mathcal{N}^{\otimes n}_{A\to B} \otimes \mathrm{id})(\mathcal{F}^{m,m'} \otimes \mathrm{id})(\Psi_{G_A,G_B})\right]$$

$$P^{*(n)}_{e|m,m'} = 1 - \mathrm{Tr}\left[D^{*}_{m}\mathcal{N}^{\otimes n}_{A\to B}\,\mathcal{F}^{m,m'}(\Psi_{G_A})\right].$$

Capacity Region

- (R, R') is achievable with unreliable entanglement assistance if there exists a sequence of $(2^{nR}, 2^{nR'}, n)$ codes such that $P^{(n)}_{e|m,m'}$, $P^{*(n)}_{e|m,m'} \to 0$ as $n \to \infty$.
- The classical capacity region $\mathcal{C}_{\mathsf{EA}*}(\mathcal{N})$ is the set of achievable rate pairs.

MCQST

Quantum Coding

Quantum Coding

- Alice has a product state $\theta_M \otimes \xi_{\bar{M}}$ over Hilbert spaces of dimension $|\mathcal{H}_M| = 2^{nQ}$ and $|\mathcal{H}_{\bar{M}}| = 2^{n(Q+Q')}$
- She encodes by applying $\mathcal{F}_{G_A M \bar{M} \to A^n}$ to $\Psi_{G_A} \otimes \theta_M \otimes \xi_{\bar{M}}$, and transmits A^n.
- Bob receives ρ_{B^n}
- If EA is present, he applies $\mathcal{D}_{B^n G_B \to \tilde{M}}$.
  If EA is absent, he applies $\mathcal{D}^*_{B^n \to \hat{M}}$.

Quantum Coding

Quantum Coding

- Alice has a product state $\theta_M \otimes \xi_{\bar{M}}$ over Hilbert spaces of dimension $|\mathcal{H}_M| = 2^{nQ}$ and $|\mathcal{H}_{\bar{M}}| = 2^{n(Q+Q')}$
- She encodes by applying $\mathcal{F}_{G_A M\bar{M}\to A^n}$ to $\Psi_{G_A} \otimes \theta_M \otimes \xi_{\bar{M}}$, and transmits A^n.
- Bob receives ρ_{B^n}
- If EA is present, he applies $\mathcal{D}_{B^n G_B\to\tilde{M}}$.
  If EA is absent, he applies $\mathcal{D}^*_{B^n\to\hat{M}}$.

(Q, Q') is an achievable rate pair if there exists a sequence of $(2^{nQ}, 2^{nQ'}, n)$ codes such that

$$\|\xi_{\bar{M}} - \mathcal{D}(\rho_{B^n G_B})\|_1 \to 0 \quad \text{and} \quad \|\theta_M - \mathcal{D}^*(\rho_{B^n})\|_1 \to 0$$

as $n \to \infty$.

Related Work: Without Assistance

Let $\mathscr{N}_{A\to B}$ be quantum channel. Define the Holevo information

$$\chi(\mathscr{N}) = \max_{p_X(x),|\phi_A^x\rangle} I(X;B)_\rho$$

with $|\mathcal{X}| \leq |\mathcal{H}_A|^2$ and $\rho_{XB} \equiv \sum_{x\in\mathcal{X}} p_X(x)|x\rangle\langle x| \otimes \mathscr{N}_{A\to B}(\phi_A^x)$.

MCQST

Related Work: Without Assistance (Cont.)

HSW Theorem
(Holevo 1998, Schumacher and Westmoreland 1997)

The classical capacity of a quantum channel $\mathscr{N}_{A\to B}$ without assistance satisfies

$$C_0(\mathscr{N}) = \lim_{k\to\infty} \frac{1}{k}\chi\left(\mathscr{N}^{\otimes k}\right)$$

Related Work: Without Assistance (Cont.)

HSW Theorem
(Holevo 1998, Schumacher and Westmoreland 1997, Shor 2002)

The classical capacity of a quantum channel $\mathscr{N}_{A\to B}$ without assistance satisfies

$$C_0(\mathscr{N}) = \lim_{k\to\infty} \frac{1}{k}\chi\left(\mathscr{N}^{\otimes k}\right)$$

If $\mathscr{N}_{A\to B}$ is entanglement-breaking, then $C_{Cl}(\mathscr{N}) = \chi(\mathscr{N})$.

MCQST

Related Work: Without Assistance (Cont.)

HSW Theorem
(Holevo 1998, Schumacher and Westmoreland 1997, Shor 2002)

The classical capacity of a quantum channel $\mathscr{N}_{A\to B}$ without assistance satisfies

$$C_0(\mathscr{N}) = \lim_{k\to\infty} \frac{1}{k}\chi\left(\mathscr{N}^{\otimes k}\right)$$

If $\mathscr{N}_{A\to B}$ is entanglement-breaking, then $C_{Cl}(\mathscr{N}) = \chi(\mathscr{N})$.

Fundamental question

$$\frac{1}{k}\chi\left(\mathscr{N}^{\otimes k}\right) = \chi(\mathscr{N})\ ?$$

Related Work: Without Assistance (Cont.)

HSW Theorem
(Holevo 1998, Schumacher and Westmoreland 1997, Shor 2002)

The classical capacity of a quantum channel $\mathscr{N}_{A\to B}$ without assistance satisfies

$$C_0(\mathscr{N}) = \lim_{k\to\infty} \frac{1}{k}\chi\left(\mathscr{N}^{\otimes k}\right)$$

If $\mathscr{N}_{A\to B}$ is entanglement-breaking, then $C_{Cl}(\mathscr{N}) = \chi(\mathscr{N})$.

Fundamental question

$$\frac{1}{k}\chi\left(\mathscr{N}^{\otimes k}\right) = \chi(\mathscr{N}) \text{ ?}$$

Simplified question (Fukuda and Wolf, 2007)

$$\chi(\mathscr{N} \otimes \mathcal{L}) = \chi(\mathscr{N}) + \chi(\mathcal{L}) \text{ ?}$$

MCQST

Related Work: Additivity

Super-Additivity Property (Hastings 2009)

There exist quantum channels $\mathscr{N}_{A_1 \to B_1}$ and $\mathcal{L}_{A_2 \to B_2}$ such that

$$\chi(\mathscr{N} \otimes \mathcal{L}) > \chi(\mathscr{N}) + \chi(\mathcal{L})$$

and thus, the regularization in the HSW theorem is necessary.

- $\mathscr{N}$ is constructed as a random mixture of unitary transformations and $\mathcal{L}$ is the complex conjugate. Hastings (2009) observed that the minimum-output entropy is sub-additive.

MCQST

Related Work: Additivity (Cont.)

Preskill (2018) referred to the current phase of quantum computation as the Noisy Intermediate-Scale Quantum (NISQ) era. In this spirit, we consider an encoding constraint.

Corollary (P., 2022)

The classical capacity of a quantum channel $\mathscr{N}_{A\to B}$ without assistance, under the encoding constraint that the input state is a product of d-fold states, is given by

$$C_0(\mathscr{N}, d) = \frac{1}{d}\chi\left(\mathscr{N}^{\otimes d}\right)$$

U. Pereg, *IEEE Transactions on Information Theory*, vol. 68, no. 1, pp. 359-383, January 2022.

MCQST

Related Work: Without Assistance (Cont.)

Let $\mathscr{N}_{A\to B}$ be quantum channel. Define

$$I_c(\mathscr{N}) = \max_{|\phi_{A_1 A}\rangle} I(A_1\rangle B)_\rho$$

with $\rho_{A_1 B} \equiv (\text{id} \otimes \mathscr{N}_{A\to B})(\phi_{A_1 A})$ and $|\mathcal{H}_{A_1}| = |\mathcal{H}_A|$.

Related Work: Without Assistance (Cont.)

Let $\mathscr{N}_{A\to B}$ be quantum channel. Define

$$I_c(\mathscr{N}) = \max_{|\phi_{A_1 A}\rangle} \left(-H(A_1|B)_\rho\right)$$

with $\rho_{A_1 B} \equiv (\text{id} \otimes \mathscr{N}_{A\to B})(\phi_{A_1 A})$ and $|\mathcal{H}_{A_1}| = |\mathcal{H}_A|$.

Related Work: Without Assistance (Cont.)

Let $\mathscr{N}_{A\to B}$ be quantum channel. Define

$$I_c(\mathscr{N}) = \max_{|\phi_{A_1 A}\rangle} \left(-H(A_1|B)_\rho\right)$$

with $\rho_{A_1 B} \equiv (\text{id} \otimes \mathscr{N}_{A\to B})(\phi_{A_1 A})$ and $|\mathcal{H}_{A_1}| = |\mathcal{H}_A|$.

LSD Theorem (Lloyd (1997), Shor (2002), and Devetak (2005))

The quantum capacity of a quantum channel $\mathscr{N}_{A\to B}$ is given by

$$Q_0(\mathscr{N}) = \lim_{k\to\infty} \frac{1}{k} I_c\left(\mathscr{N}^{\otimes k}\right)$$

If there is a degraded $U_{A\to BE}$, then $Q_0(\mathscr{N}) = I_c(\mathscr{N})$.

MCQST

Related Work: Without Assistance (Cont.)

Super-Activation (Smith and Yard, 2008)

There exist quantum channels $\mathscr{N}_{A_1 \to B_1}$ and $\mathcal{L}_{A_2 \to B_2}$ such that

$$Q_0(\mathscr{N}) = Q_0(\mathcal{L}) = 0 \quad \text{but} \quad Q_0(\mathscr{N} \otimes \mathcal{L}) > 0$$

- $\mathscr{N}$ is as an erasure channel $\varepsilon = \frac{1}{2}$ and $\mathcal{L}$ is an entanglement-binding channel, *i.e.* $(\mathcal{L} \otimes \text{id})\Phi_{AB}$ cannot be distilled [Horodecki et al. 1999].

Related Work: Entanglement Assistance

Theorem (Bennett, Shor, Smolin, and Thapliyal 1999)

The entanglement-assisted classical capacity of a quantum channel $\mathscr{N}_{A\to B}$ is given by

$$C_{EA}(\mathscr{N}) = \max_{|\phi_{A_1 A}\rangle} I(A_1; B)_\rho$$

with $\rho_{A_1 B} \equiv (id \otimes \mathscr{N})(\phi_{A_1 A})$.

Related Work: Entanglement Assistance

Theorem (Bennett, Shor, Smolin, and Thapliyal 1999)

The entanglement-assisted classical capacity of a quantum channel $\mathscr{N}_{A\to B}$ is given by

$$C_{EA}(\mathscr{N}) = \max_{|\phi_{A_1 A}\rangle} I(A_1;B)_\rho$$

and the entanglement-assisted quantum capacity is given by

$$Q_{EA}(\mathscr{N}) = \max_{|\phi_{A_1 A}\rangle} \frac{1}{2} I(A_1;B)_\rho$$

with $\rho_{A_1 B} \equiv (id \otimes \mathscr{N})(\phi_{A_1 A})$.

- With entanglement assistance, a qubit is exchangable with two classical bits (teleportation + superdense-coding protocols).

Outline

- Background: Quantum Information Theory
- The Fundamental Problem
- Coding
- Main Results

Main Results: Classical Capacity

Let $\mathscr{N}_{A\to B}$ be a quantum channel. Define

$$\mathcal{R}_{\mathrm{EA}*}(\mathscr{N}) = \bigcup_{p_X\,,\,|\phi_{A_0A_1}\rangle\,,\,\mathcal{F}^{(x)}} \left\{ \begin{array}{rl} (R,R') : R \leq & I(X;B)_\rho \\ R' \leq & I(A_1;B|X)_\rho \end{array} \right\}$$

where the union is over the distributions p_X such that $|\mathcal{X}| \leq |\mathcal{H}_A|^2 + 1$, the pure states $|\phi_{A_0A_1}\rangle$, and the quantum channels $\mathcal{F}^{(x)}_{A_0\to A}$, with

$$\rho_{XA_1A} = \sum_{x\in\mathcal{X}} p_X(x)|x\rangle\langle x| \otimes (\mathrm{id}\otimes\mathcal{F}^{(x)}_{A_0\to A})(|\phi_{A_1A_0}\rangle\langle\phi_{A_1A_0}|)\,,$$
$$\rho_{XA_1B} = (\mathrm{id}\otimes\mathscr{N}_{A\to B})(\rho_{XA_1A})\,.$$

Main Results: Classical Capacity (Cont.)

Theorem

The classical capacity region of a quantum channel $\mathscr{N}_{A\to B}$ with unreliable entanglement assistance satisfies

$$\mathcal{C}_{\mathsf{EA}*}(\mathscr{N}) = \bigcup_{k=1}^{\infty} \frac{1}{k}\mathcal{R}_{\mathsf{EA}*}(\mathscr{N}^{\otimes k}) \,.$$

Main Results: Classical Capacity (Cont.)

Classical "Superposition Coding"

- An auxiliary variable U is associated with the message m.

Main Results: Classical Capacity (Cont.)

Classical "Superposition Coding"

- An auxiliary variable U is associated with the message m.
- Alice encodes the second message m' by a random codeword $\sim p_{X|U}$.

Main Results: Classical Capacity (Cont.)

Classical “Superposition Coding"

- An auxiliary variable U is associated with the message m.
- Alice encodes the second message m' by a random codeword $\sim p_{X|U}$.

Quantum Counterpart

- An auxiliary variable X is associated with the classical message m, which Bob decodes whether there is entanglement assistance or not.

MCQST

Main Results: Classical Capacity (Cont.)

Classical "Superposition Coding"

- An auxiliary variable U is associated with the message m.
- Alice encodes the second message m' by a random codeword $\sim p_{X|U}$.

Quantum Counterpart

- An auxiliary variable X is associated with the classical message m, which Bob decodes whether there is entanglement assistance or not.
- The entangled state $\phi_{A_0 A_1}$ is non-correlated with the messages, since the resources are pre-shared before communication takes place.

Main Results: Classical Capacity (Cont.)

Classical "Superposition Coding"

- An auxiliary variable U is associated with the message m.
- Alice encodes the second message m' by a random codeword $\sim p_{X|U}$.

Quantum Counterpart

- An auxiliary variable X is associated with the classical message m, which Bob decodes whether there is entanglement assistance or not.
- The entangled state $\phi_{A_0 A_1}$ is non-correlated with the messages, since the resources are pre-shared before communication takes place.
- Alice encodes the message m' using the encoding channel $\mathcal{F}^{(x)}_{A_0 \to A}$

Main Results: Classical Capacity (Cont.)

Corollary

For a noiseless qubit channel,

$$\mathcal{C}_{\mathsf{EA}*}(\mathscr{N}) = \bigcup_{0\leq\lambda\leq 1} \left\{ \begin{array}{rl} (R,R') : \; R \leq & 1-\lambda \\ R' \leq & 2\lambda \end{array} \right\}$$

Main Results: Classical Capacity (Cont.)

Corollary

For a noiseless qubit channel,

$$\mathcal{C}_{\text{EA}*}(\mathscr{N}) = \bigcup_{0\leq\lambda\leq 1} \left\{ \begin{array}{rl} (R,R') \,:\, R \leq & 1-\lambda \\ R' \leq & 2\lambda \end{array} \right\}$$

Proof: Achievability follows by time division. As for the converse part,

$$R \leq \frac{1}{n} I(X;B^n)_\omega \leq 1 - \frac{1}{n} H(B^n|X)_\omega$$

Main Results: Classical Capacity (Cont.)

Corollary

For a noiseless qubit channel,

$$\mathcal{C}_{\mathsf{EA}*}(\mathscr{N}) = \bigcup_{0\leq\lambda\leq 1} \left\{ \begin{array}{rl} (R,R') \,:\, R \leq & 1-\lambda \\ R' \leq & 2\lambda \end{array} \right\}$$

Proof: Achievability follows by time division. As for the converse part,

$$R \leq \frac{1}{n} I(X;B^n)_\omega \leq 1 - \frac{1}{n} H(B^n|X)_\omega$$

Since $I(A;B)_\rho \leq 2H(B)_\rho$ in general, we have

$$R' \leq \frac{1}{n} I(A_1;B^n|X)_\omega \leq \frac{1}{n} \cdot 2H(B^n|X)_\omega$$

Set $\lambda \equiv \frac{1}{n} H(B^n|X)_\omega$. $\square$

Main Results: Classical Capacity (Cont.)

Remark

The following tradeoff is observed:

- To maximize the unassisted rate, set an encoding channel $\mathcal{F}^{(x)}_{A_0 \to A}$ that outputs the pure state $|\psi^x_A\rangle$ that is optimal for the Holevo information, *i.e.*

$$\mathcal{F}^{(x)}(\varphi_{A_1 A_0}) = \varphi_{A_1} \otimes \psi^x_A$$
$$\Rightarrow (R, R') = (\chi(\mathcal{N}), 0)$$

  ▸ $\chi(\mathcal{N})$ **is achieved for an entanglement-breaking encoder**.

- For R' to achieve the entanglement-assisted capacity, set $\varphi_{A_0 A_1}$ as the entangled state that maximizes $I(A_1; B)_\rho$. Take $\mathcal{F}^{(x)} = \text{id}_{A_0 \to A}$.
$\Rightarrow (R, R') = (0, C_{\text{EA}}(\mathcal{N}))$

  ▸ $C_{\text{EA}}(\mathcal{N})$ **is achieved for an entanglement-preserving encoder**.

Main Results: Classical Capacity (Cont.)

Remark

The following tradeoff is observed:

- To maximize the unassisted rate, set an encoding channel $\mathcal{F}^{(x)}_{A_0 \to A}$ that outputs the pure state $|\psi^x_A\rangle$ that is optimal for the Holevo information, *i.e.*

$$\mathcal{F}^{(x)}(\varphi_{A_1 A_0}) = \varphi_{A_1} \otimes \psi^x_A$$
$$\Rightarrow (R, R') = (\chi(\mathcal{N}), 0)$$

  - **$\chi(\mathcal{N})$ is achieved for an entanglement-breaking encoder.**

- For R' to achieve the entanglement-assisted capacity, set $\varphi_{A_0 A_1}$ as the entangled state that maximizes $I(A_1; B)_\rho$. Take $\mathcal{F}^{(x)} = \mathrm{id}_{A_0 \to A}$.
$\Rightarrow$ $(R, R') = (0, C_{\mathrm{EA}}(\mathcal{N}))$

  - **$C_{\mathrm{EA}}(\mathcal{N})$ is achieved for an entanglement-preserving encoder.**

Main Results: Classical Capacity (Cont.)

Remark

The following tradeoff is observed:

- To maximize the unassisted rate, set an encoding channel $\mathcal{F}^{(x)}_{A_0\to A}$ that outputs the pure state $|\psi^x_A\rangle$ that is optimal for the Holevo information, *i.e.*

$$\mathcal{F}^{(x)}(\varphi_{A_1A_0}) = \varphi_{A_1} \otimes \psi^x_A$$
$$\Rightarrow (R, R') = (\chi(\mathscr{N}), 0)$$

  - $\chi(\mathscr{N})$ **is achieved for an entanglement-breaking encoder**.

- For R' to achieve the entanglement-assisted capacity, set $\varphi_{A_0A_1}$ as the entangled state that maximizes $I(A_1;B)_\rho$. Take $\mathcal{F}^{(x)} = \mathrm{id}_{A_0\to A}$.
$\Rightarrow (R, R') = (0, C_{\mathrm{EA}}(\mathscr{N}))$

  - $C_{\mathrm{EA}}(\mathscr{N})$ **is achieved for an entanglement-preserving encoder**.

Example: Depolarizing Channel

Qubit depolarizing channel

$$\mathscr{N}(\rho) = (1-\varepsilon)\rho + \varepsilon\frac{\mathbb{1}}{2} \quad , \quad 0 \le \varepsilon \le 1$$

Example: Depolarizing Channel

Qubit depolarizing channel

$$
\begin{aligned}
\mathscr{N}(\rho) &= (1-\varepsilon)\rho + \varepsilon\frac{\mathbb{1}}{2} \\
&= \left(1 - \frac{3\varepsilon}{4}\right)\rho + \frac{\varepsilon}{4}\left(\Sigma_X\rho\Sigma_X + \Sigma_Y\rho\Sigma_Y + \Sigma_Z\rho\Sigma_Z\right)
\end{aligned}
$$

Example: Depolarizing Channel (Cont.)

Corner Points

- $\left[C(\mathscr{N}) = 1 - H_2\left(\frac{\varepsilon}{2}\right)\ ,\ 0\right]$ is achieved with $\left\{p_X = \left(\frac{1}{2}, \frac{1}{2}\right)\ ,\ \{|0\rangle, |1\rangle\}\right\}$
- $\left[0\ ,\ C_{\text{EA}}(\mathscr{N}) = 1 - H\left(1 - \frac{3\varepsilon}{4}, \frac{\varepsilon}{4}, \frac{\varepsilon}{4}, \frac{\varepsilon}{4}\right)\right]$ is achieved with $|\Phi_{A_0 A_1}\rangle$ and $\mathcal{F}^{(x)} = \text{id}_{A_0 \to A}$.

Classical Mixture

Let $Z \sim \text{Bernoulli}(\lambda)$. Define $\mathcal{F}^{(x,z)}$ by $\mathcal{F}^{(x,0)}(\rho_A) = |x\rangle\langle x|$ and $\mathcal{F}^{(x,1)} = \text{id}$. Plugging $\tilde{X} \equiv (X, Z)$, we obtain the time-division achievable region,

$$\mathcal{R}_{\text{EA}*}(\mathscr{N}) \supseteq \bigcup_{0 \le \lambda \le 1} \left\{ \begin{array}{rl} (R, R') : \ R \le & (1-\lambda)\, C(\mathscr{N}) \\ R' \le & \lambda C_{\text{EA}}(\mathscr{N}) \end{array} \right\}$$

Example: Depolarizing Channel (Cont.)

Quantum Superposition State

Define

$$|u_\beta\rangle \equiv \sqrt{1-\beta}\,|0\rangle \otimes |0\rangle + \sqrt{\beta}\,|\Phi\rangle \ .$$

Example: Depolarizing Channel (Cont.)

Quantum Superposition State

Define

$$|u_\beta\rangle \equiv \sqrt{1-\beta}\,|0\rangle \otimes |0\rangle + \sqrt{\beta}\,|\Phi\rangle \ .$$

Set

$$|\phi_{A_0 A_1}\rangle \equiv \frac{1}{\||u_\beta\|\|}|u_\beta\rangle \quad , \quad p_X = \left(\frac{1}{2}, \frac{1}{2}\right) \quad , \quad \mathcal{F}^{(x)}(\rho) \equiv \Sigma_X^x \rho \Sigma_X^x$$

- For $\beta = 0$, the input state is $\mathcal{F}^{(x)}(|0\rangle\langle 0|) = |x\rangle\langle x|$, which achieves $C(\mathscr{N})$
- For $\beta = 1$, the parameter x chooses one of two bell states, achieving $C_{\text{EA}}(\mathscr{N})$

MCQST

Example: Depolarizing Channel (Cont.)

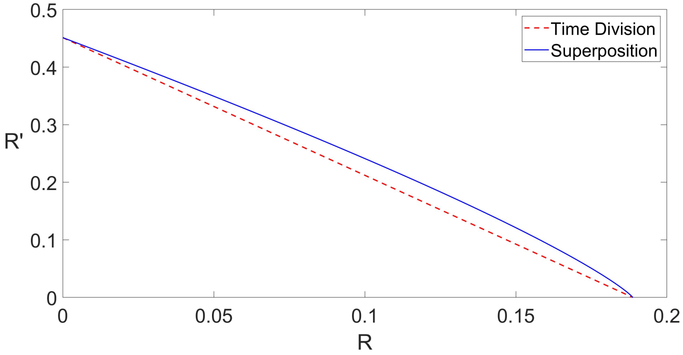


Figure: Achievable rate regions for the depolarizing channel with $\varepsilon = \frac{1}{2}$.

Main Results: Quantum Capacity

Let $\mathscr{N}_{A\to B}$ be a quantum channel. Define

$$\mathscr{L}_{\text{EA*}}(\mathscr{N}) = \bigcup_{\varphi_{A_1 A_2 A}} \left\{ \begin{array}{l} (Q, Q') \ : \\ Q \leq \min\{I(A_1\rangle B)_\rho \, , \ H(A_1|A_2)_\rho\} \, , \\ Q + Q' \leq \frac{1}{2} I(A_2; B)_\rho \end{array} \right\}$$

where the union is over the states $\varphi_{AA_1A_2}$, with $\rho_{A_1A_2B} = (\text{id} \otimes \mathscr{N}_{A\to B})(\varphi_{A_1A_2A})$

MCQST

Main Results: Quantum Capacity (Cont.)

Theorem

The quantum capacity region of a quantum channel $\mathscr{N}_{A\to B}$ with unreliable entanglement assistance satisfies

$$\mathcal{Q}_{\mathsf{EA}*}(\mathscr{N}) = \bigcup_{k=1}^{\infty} \frac{1}{k} \mathscr{L}_{\mathsf{EA}*}(\mathscr{N}^{\otimes k}) \,.$$

- The proof is based on the decoupling approach: By Uhlmann's theorem, if we can encode such that Alice and Bob's environments are in a product state, then there exists a decoding map such that $\mathcal{D} \circ \mathscr{N} \circ \mathcal{E} \approx \text{id}$.

Information-Theoretic Tools, Decoupling.

MCQST

Summary and Concluding Remarks

- We considered communication over a quantum channel $\mathscr{N}_{A\to B}$, where Alice and Bob are provided with *unreliable* entanglement resources.

Summary and Concluding Remarks

- We considered communication over a quantum channel $\mathscr{N}_{A\to B}$, where Alice and Bob are provided with *unreliable* entanglement resources.
- Inspired by Steinberg's classical cooperation model, we developed a theory for **reliability by design** for entanglement-assisted point-to-point quantum communication systems.

Summary and Concluding Remarks

- We considered communication over a quantum channel $\mathscr{N}_{A\to B}$, where Alice and Bob are provided with *unreliable* entanglement resources.

- Inspired by Steinberg's classical cooperation model, we developed a theory for **reliability by design** for entanglement-assisted point-to-point quantum communication systems.

- The quantum capacity formula has the following interpretation: Without assistance, A_2 behaves as a channel state system. The classical capacity formula resembles the superposition bound. A straightforward extension of our methods yields the capacity region of the broadcast channel with degraded message sets and one-sided entanglement assistance.

Summary and Concluding Remarks

- We considered communication over a quantum channel $\mathscr{N}_{A\to B}$, where Alice and Bob are provided with *unreliable* entanglement resources.

- Inspired by Steinberg's classical cooperation model, we developed a theory for **reliability by design** for entanglement-assisted point-to-point quantum communication systems.

- The quantum capacity formula has the following interpretation: Without assistance, A_2 behaves as a channel state system. The classical capacity formula resembles the superposition bound. A straightforward extension of our methods yields the capacity region of the broadcast channel with degraded message sets and one-sided entanglement assistance.

- In the future, it would be interesting to apply this methodology to other quantum information areas that rely on entanglement resources.

Thank you

Subspace Transmission Vs. Remote Preparation

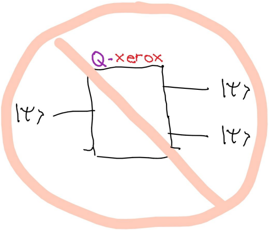
Remark

- In many communication models in the literature, it does not matter whether the messages are chosen by the sender Alice, or given to her by an external source.
- However, for a quantum message state, there is a fundamental distinction.

Subspace Transmission Vs. Remote Preparation

- In remote state preparation, Alice knows the message state. In this case, our model includes the case that M is a sub-system of $\bar{M}$.

- In subspace transmission, Alice can perform any operation on the system, she does not necessarily know its state. By the no-cloning theorem, she cannot duplicate the state. Hence, the problem where M is a sub-system of $\bar{M}$ remains open.



Method of Types

δ-Typical Set

$$\mathcal{A}^{\delta}(p_X) \equiv \left\{ x^n \in \mathcal{X}^n \,:\, \left| \frac{N(a|x^n)}{n} - p_X(a) \right| \leq \delta \cdot p_X(a) \right\}$$

Method of Types

δ-Typical Set

$$\mathcal{A}^{\delta}(p_X) \equiv \left\{ x^n \in \mathcal{X}^n \, : \, \left| \frac{N(a|x^n)}{n} - p_X(a) \right| \leq \delta \cdot p_X(a) \right\}$$

$$\left| \mathcal{A}^{\delta}(p_X) \right| \approx 2^{nH(X)}$$

$$\Pr\left(X^n \in \mathcal{A}^{\delta}(p_X) \right) \approx 1 \quad \text{for} \quad X^n \sim \prod_{i=1}^{n} p_X(x_i)$$

$$p_{X^n}(x^n) \approx 2^{-nH(X)} \quad \text{for} \quad x^n \in \mathcal{A}^{\delta}(p_X)$$

Method of Types (Cont.)

Conditional δ-Typical Set

$$\mathcal{A}^{\delta}(p_{Y|X}|x^n) \equiv \left\{ y^n \in \mathcal{Y}^n \,:\, (x^n, y^n) \in \mathcal{A}^{\delta}(p_{XY}) \right\}$$

with $p_X(a) \equiv N(a|x^n)/n$.

$$\left| \mathcal{A}^{\delta}(p_{Y|X}|x^n) \right| \approx 2^{nH(Y|X)}$$

$$\Pr\left(Y^n \in \mathcal{A}^{\delta}(p_{Y|X}|x^n) | X^n = x^n \right) \approx 1 \quad \text{for} \quad Y^n|X^n = x^n \sim \prod_{i=1}^{n} p_{Y|X}(y_i|x_i)$$

$$p_{Y^n|X^n}(y^n|x^n) \approx 2^{-nH(Y|X)} \quad \text{for} \quad y^n \in \mathcal{A}^{\delta}(p_{Y|X}|x^n)$$

Quantum Method of Types

Let

$$\rho_A = \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x| \, .$$

Quantum Method of Types

Let

$$\rho_A = \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x| \,.$$

δ-Typical Projector

$$\Pi^\delta(\rho_A) \equiv \sum_{x^n \in \mathcal{A}^\delta(p_X)} |x^n\rangle\langle x^n| \qquad |x^n\rangle \equiv |x_1\rangle \otimes \cdots \otimes |x_n\rangle$$

Quantum Method of Types

Let

$$\rho_A = \sum_{x \in \mathcal{X}} p_X(x) |x\rangle\langle x| \,.$$

δ-Typical Projector

$$\Pi^\delta(\rho_A) \equiv \sum_{x^n \in \mathcal{A}^\delta(p_X)} |x^n\rangle\langle x^n| \qquad |x^n\rangle \equiv |x_1\rangle \otimes \cdots \otimes |x_n\rangle$$

$$\mathrm{Tr}(\Pi^\delta(\rho_A)) \approx 2^{nH(A)_\rho}$$

$$\mathrm{Tr}(\Pi^\delta(\rho_A)\rho_A^{\otimes n}) \approx 1$$

$$\Pi^\delta(\rho_A)\rho_A^{\otimes n}\Pi^\delta(\rho_A) \approx 2^{-nH(A)_\rho}\Pi^\delta(\rho_A)$$

Quantum Method of Types (Cont.)

Let

$$\rho_B = \sum_{x\in\mathcal{X}} p_X(x)\rho_B^x$$

Quantum Method of Types (Cont.)

Let

$$\rho_B = \sum_{x \in \mathcal{X}} p_X(x) \rho_B^x$$

Conditional δ-Typical Projector

$$\Pi^\delta(\rho_B | x^n) \equiv \bigotimes_{a \in \mathcal{X}} \Pi^\delta_{B^{\mathcal{I}(a)}}(\rho_B^a) \qquad \mathcal{I}(a) \equiv \{i : x_i = a\}$$

Quantum Method of Types (Cont.)

Let

$$\rho_B = \sum_{x \in \mathcal{X}} p_X(x) \rho_B^x$$

Conditional δ-Typical Projector

$$\Pi^\delta(\rho_B | x^n) \equiv \bigotimes_{a \in \mathcal{X}} \Pi^\delta_{B^{\mathcal{I}(a)}}(\rho_B^a) \qquad \mathcal{I}(a) \equiv \{i : x_i = a\}$$

$$\mathrm{Tr}(\Pi^\delta(\rho_B|x^n)) \approx 2^{nH(B|X)_\rho}$$

$$\mathrm{Tr}(\Pi^\delta(\rho_B|x^n)\rho_{B^n}^{x^n}) \approx 1$$

$$\Pi^\delta(\rho_B|x^n)\rho_B^{x^n}\Pi^\delta(\rho_B|x^n) \approx 2^{-nH(B|X)_\rho}\Pi^\delta(\rho_B|x^n)$$

Quantum Packing Lemma

Quantum Packing Lemma [Hsieh, Devetak, and Winter 2008]

Let

$$\rho = \sum_{x\in\mathcal{X}} p_X(x)\rho_x$$

Suppose that $\exists$ a code projector Π and codeword projectors Π_{x^n}, $x^n \in \mathcal{A}_\delta(p_X)$, such that

$$\mathrm{Tr}(\Pi\rho_{x^n}) \geq 1-\alpha \qquad \mathrm{Tr}(\Pi_{x^n}) \leq 2^{n\lambda}$$

$$\mathrm{Tr}(\Pi_{x^n}\rho_{x^n}) \geq 1-\alpha \qquad \Pi\rho^{\otimes n}\Pi \preceq 2^{-nL}\Pi$$

Then, there exist codewords $x^n(m)$, $m \in [1:2^{nR}]$, and a POVM $\{D_m\}_{m\in[1:2^{nR}]}$ such that

$$\mathrm{Tr}\left(D_m\rho_{x^n(m)}\right) \geq 1-2^{-n[L-\lambda-R-\varepsilon_n(\alpha)]} \;\forall m$$

Quantum Method of Types (Cont.)

Square-Root Measurement Decoder

Define

$$\Upsilon_m \equiv \Pi \Pi_{x^n(m)} \Pi$$

and

$$D_m = \left(\sum_{\tilde{m}=1}^{2^{nR}} \Upsilon_{\tilde{m}} \right)^{-1/2} \Upsilon_m \left(\sum_{\tilde{m}=1}^{2^{nR}} \Upsilon_{\tilde{m}} \right)^{-1/2}$$

Quantum Method of Types (Cont.)

Square-Root Measurement Decoder

Define

$$\Upsilon_m \equiv \Pi \Pi_{x^n(m)} \Pi$$

and

$$D_m = \left(\sum_{\tilde{m}=1}^{2^{nR}} \Upsilon_{\tilde{m}} \right)^{-1/2} \Upsilon_m \left(\sum_{\tilde{m}=1}^{2^{nR}} \Upsilon_{\tilde{m}} \right)^{-1/2}$$

Hayashi-Nagaoka Inequality (2003)

For every $0 \preceq S, T \preceq \mathbb{1}$,

$$\mathbb{1} - (S+T)^{-1/2} S (S+T)^{-1/2} \preceq 2(\mathbb{1} - S) + 4T$$

Proof

The Decoupling Approach

Consider a quantum channel $\mathscr{N}_{A\to B}$ without entanglement assistance.

- Let $|\theta_{MK}\rangle$ be a purification of the quantum message state.
- Suppose that $|\psi_{KB^nE^nJ_1}\rangle$ is a purification of the channel output.

The Decoupling Approach (Cont.)

- If $\psi_{KE^nJ_1}$ is a product state, i.e. $\psi_{KE^nJ_1} = \theta_K \otimes \omega_{E^nJ_1}$, then it has a purification of the form $|\theta_{MK}\rangle \otimes |\omega_{E^nJ_1J_2}\rangle$.

The Decoupling Approach (Cont.)

- If $\psi_{KE^nJ_1}$ is a product state, i.e. $\psi_{KE^nJ_1} = \theta_K \otimes \omega_{E^nJ_1}$, then it has a purification of the form $|\theta_{MK}\rangle \otimes |\omega_{E^nJ_1J_2}\rangle$.
- Since all purifications are related by isometries, there exists an isometry $D_{B^n \to MJ_2}$ such that $|\theta_{MK}\rangle \otimes |\omega_{E^nJ_1J_2}\rangle = D_{B^n \to MJ_2} |\psi_{RB^nE^nJ_1}\rangle$.

The Decoupling Approach (Cont.)

- If $\psi_{KE^nJ_1}$ is a product state, i.e. $\psi_{KE^nJ_1} = \theta_K \otimes \omega_{E^nJ_1}$, then it has a purification of the form $|\theta_{MK}\rangle \otimes |\omega_{E^nJ_1J_2}\rangle$.
- Since all purifications are related by isometries, there exists an isometry $D_{B^n \to MJ_2}$ such that $|\theta_{MK}\rangle \otimes |\omega_{E^nJ_1J_2}\rangle = D_{B^n \to MJ_2} |\psi_{RB^nE^nJ_1}\rangle$.
- Tracing out K, E^n, J_1, and J_2, it follows that there exists a decoding map $\mathcal{D}_{B^n \to M}$ that recovers the message state, i.e. $\theta_M = \mathcal{D}_{B^n \to M}(\psi_{B^n})$.

The Decoupling Approach (Cont.)

Conclusion

In order to show that there exists a reliable coding scheme, it is sufficient to encode in such a manner that approximately decouples between Alice's reference system and Bob's environment, i.e., such that $\psi_{KE^nJ_1} \approx \theta_K \otimes \omega_{E^nJ_1}$.

The Decoupling Approach (Cont.)

Min-Entropy

- Conditional min-entropy:

$$H_{\min}(\rho_{AB}|\sigma_B) = -\log\inf\left\{\lambda\in\mathbb{R}\,:\,\,\rho_{AB}\preceq\lambda\cdot(\mathbb{1}_A\otimes\sigma_B)\right\}$$
$$H_{\min}(A|B)_\rho = \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B)\,,$$

In general,

$$-\log|\mathcal{H}_B| \leq H_{\min}(A|B)_\rho \leq \log|\mathcal{H}_A|$$

The Decoupling Approach (Cont.)

Min-Entropy

- Conditional min-entropy:

$$H_{\min}(\rho_{AB}|\sigma_B) = -\log \inf\{\lambda \in \mathbb{R} \,:\, \rho_{AB} \preceq \lambda \cdot (\mathbb{1}_A \otimes \sigma_B)\}$$
$$H_{\min}(A|B)_\rho = \sup_{\sigma_B} H_{\min}(\rho_{AB}|\sigma_B)\,,$$

In general,

$$-\log|\mathcal{H}_B| \leq H_{\min}(A|B)_\rho \leq \log|\mathcal{H}_A|$$

- If $\sigma_B = \frac{\mathbb{1}_B}{|\mathcal{H}_B|}$, then $\rho_{AB} \preceq \lambda(\mathbb{1}_A \otimes \sigma_B)$ holds for $\lambda = |\mathcal{H}_B|$, hence $H_{\min}(\rho_{AB}|\sigma_B) \geq -\log|\mathcal{H}_B|$ (saturated by $|\Phi_{AB}\rangle$)
- We also have $1 = \mathrm{Tr}(\rho_{AB}) \leq \lambda|\mathcal{H}_A|\mathrm{Tr}(\sigma_B) = \lambda|\mathcal{H}_A|$, hence $H_{\min}(\rho_{AB}|\sigma_B) \leq \log|\mathcal{H}_A|$ (saturated by $\frac{\mathbb{1}_A}{|\mathcal{H}_A|} \otimes \rho_B$)

The Decoupling Approach (Cont.)

Smoothed min-entropy

$$H^{\varepsilon}_{\min}(A|B)_{\rho} = \max_{\sigma_{AB}\,:\,d_F(\rho_{AB},\sigma_{AB})\leq\varepsilon} H^{\varepsilon}_{\min}(A|B)_{\sigma}$$

Min-Entropy AEP [Tomamichel, Colbeck, and Renner 2008]

$$\frac{1}{n} H^{\varepsilon}_{\min}(A^n|B^n)_{\rho^{\otimes n}} \xrightarrow{n\to\infty} H(A|B)_{\rho}$$

The Decoupling Approach (Cont.)

Decoupling Theorem [Dupuis 2010]

Let θ_{A_1K} be a quantum state, $\mathcal{T}_{A_1\to E}$ a quantum channel, and $\varepsilon > 0$ arbitrary. Define

$$\omega_{AE} = \mathcal{T}_{A_1\to E}(\Phi_{A_1A}) \,.$$

Then, there exists a probability (Haar) measure on the set of all unitaries U_{A_1}, such that

$$\mathbb{E}_{U_{A_1}} \left\| \mathcal{T}_{A_1\to E}(U_{A_1}\rho_{A_1K}) - \omega_E \otimes \theta_K \right\|_1 \leq 2^{-\frac{1}{2}[H^{\varepsilon}_{\min}(A|E)_\omega + H^{\varepsilon}_{\min}(A_1|K)_\theta]} + 8\varepsilon$$

The Decoupling Approach (Cont.)

Decoupling Theorem [Dupuis 2010]

Let $\theta_{A_1 K}$ be a quantum state, $\mathcal{T}_{A_1 \to E}$ a quantum channel, and $\varepsilon > 0$ arbitrary. Define

$$\omega_{AE} = \mathcal{T}_{A_1 \to E}(\Phi_{A_1 A}) \,.$$

Then, there exists a probability (Haar) measure on the set of all unitaries U_{A_1}, such that

$$\mathbb{E}_{U_{A_1}} \left\| \mathcal{T}_{A_1 \to E}(U_{A_1} \rho_{A_1 K}) - \omega_E \otimes \theta_K \right\|_1 \leq 2^{-\frac{1}{2}[H^{\varepsilon}_{\min}(A|E)_{\omega} + H^{\varepsilon}_{\min}(A_1|K)_{\theta}]} + 8\varepsilon$$

Consequence

There exists $U_{A_1^n}$ such that

$$\mathcal{T}_{A_1^n \to E^n}(U_{A_1^n} \rho_{A_1^n K}) \approx \omega_E^{\otimes n} \otimes \theta_K \quad \text{if} \quad - H^{\varepsilon}_{\min}(A_1^n|K)_{\rho} < n(H(A|E)_{\omega} + \varepsilon')$$

Uhlmann's theorem [Uhlmann 1976]

For every pair of pure states $|\psi_{AB}\rangle$ and $|\theta_{AC}\rangle$ that satisfy

$$\|\psi_A - \theta_A\|_1 \leq \varepsilon \,,$$

there exists an isometry $F_{B\to C}$ such that

$$\|(\mathbb{1} \otimes F_{B\to C})\psi_{AB} - \theta_{AC}\|_1 \leq 2\sqrt{\varepsilon}$$

Proof

Conclusion

Achievability: Classical Capacity

Fix

- a distribution p_X
- a pure entangled state $|\phi_{G_1 G_2}\rangle$ on $\mathcal{H}_{A_0} \otimes \mathcal{H}_{A_0}$
- an isometry $F^{(x)}_{G_1 \to A}$

Classical Codebook

Select 2^{nR} independent sequences, $\{x^n(m)\}$, at random $\sim \prod_{i=1}^{n} p_X(x_i)$.

Achievability: Classical Capacity

Fix

- a distribution p_X
- a pure entangled state $|\phi_{G_1 G_2}\rangle$ on $\mathcal{H}_{A_0} \otimes \mathcal{H}_{A_0}$
- an isometry $F^{(x)}_{G_1 \to A}$

Classical Codebook

Select 2^{nR} independent sequences, $\{x^n(m)\}$, at random $\sim \prod_{i=1}^n p_X(x_i)$.

Denote

$$|\psi^x_{AG_2}\rangle = (F^{(x)}_{G_1 \to A} \otimes \mathbb{1}) |\phi_{G_1 G_2}\rangle$$
$$\rho^x_{BG_2} = (\mathcal{N}_{A \to B} \otimes \text{id})(\psi^x_{AG_2})$$

Achievability: Classical Capacity (Cont.)

Schmidt Decomposition

For every $|\psi_{AB}\rangle$, there exist orthonormal sets $\{|x\rangle_A\}$ and $\{|x\rangle_A\}$ such that

$$|\psi_{AB}\rangle = \sum_{x\in\mathcal{X}} \sqrt{p_X(x)}\,|x\rangle_A \otimes |x\rangle_B$$

for some probability distribution p_X.

Achievability: Classical Capacity (Cont.)

Schmidt Decomposition

For every $|\psi_{AB}\rangle$, there exist orthonormal sets $\{|x\rangle_A\}$ and $\{|x\rangle_A\}$ such that

$$|\psi_{AB}\rangle = \sum_{x\in\mathcal{X}} \sqrt{p_X(x)}\,|x\rangle_A \otimes |x\rangle_B$$

for some probability distribution p_X.

Let

$$\left|\psi^x_{AG_2}\right\rangle = \sum_{z\in\mathcal{Z}} \sqrt{p_{Z|X}(z|x)}\,|\xi_{x,z}\rangle \otimes \left|\xi'_{x,z}\right\rangle$$

Achievability: Classical Capacity (Cont.)

Heisenberg-Weyl Operators

$$\Sigma_X(D) = \sum_{k=0}^{D-1} |k \oplus 1\rangle\langle k|$$

$$\Sigma_Z(D) = \sum_{k=0}^{D-1} e^{-2\pi k i/D} |k\rangle\langle k|$$

Random Selection of Operators

For each message m', select a random operator

$$U(\gamma) = \bigoplus_{p \in \mathcal{P}_n(\mathcal{Z}|x^n(m))} (-1)^{c_p} (\Sigma_X(D_p))^{a_p} (\Sigma_Z(D_p))^{b_p}$$

$$D_p \equiv |\mathcal{T}(p|x^n(m))|$$

choosing $\gamma(m'|m) = (a_p, b_p, c_p)_p$ uniformly, $a_p, b_p \in \{0, \ldots, D_p - 1\}$, $c_p \in \{0, 1\}$.

MCQST

Achievability: Classical Capacity (Cont.)

Encoder

To send the messages $(m, m') \in [1 : 2^{nR}] \times [1 : 2^{nR'}]$, apply the operators $\bigotimes_{i=1}^{n} F_{G_1 \to A}^{(x_i(m))}$ and $U(\gamma(m'|m))$ to $|\phi_{G_1 G_2}\rangle^{\otimes n}$, and transmit A^n through the channel.

Achievability: Classical Capacity (Cont.)

Encoder

To send the messages $(m, m') \in [1 : 2^{nR}] \times [1 : 2^{nR'}]$, apply the operators $\bigotimes_{i=1}^{n} F_{G_1 \to A}^{(x_i(m))}$ and $U(\gamma(m'|m))$ to $|\phi_{G_1 G_2}\rangle^{\otimes n}$, and transmit A^n through the channel.

Decoder

Bob receives the systems B^n in a state $\sigma_{B^n G_2^n}^{\gamma, x^n}$, and decodes as follows.

1. Measure B^n using a square-root measurement $\{D_m^*\}$. Denote the outcome $\hat{m}$.
2. If EA is absent, declare $\hat{m}$ as the message estimate.
3. If EA is present, measure $B^n G_2^n$ jointly using a second square-root measurement $\{\Delta_{m'|x^n(\hat{m})}\}_{m' \in [1:2^{nR'}]}$. Let $\hat{m}'$ be the outcome. Declare $(\hat{m}, \hat{m}')$.

Achievability: Classical Capacity (Cont.)

“Ricochet Property"

$$(U \otimes \mathbb{1}) |\Phi_{AB}\rangle = (\mathbb{1} \otimes U^T) |\Phi_{AB}\rangle$$

Using the “ricochet property" and the type-class decomposition, we show that Alice's operations for encoding the second message m' can be effectively reflected to Bob's side:

$$\sigma^{m,m'}_{B^n G_2^n} = (\mathbb{1} \otimes \Gamma^T(m'|m)) \rho^{x^n(m)}_{B^n G_2^n} (\mathbb{1} \otimes \Gamma^*(m'|m)) \,.$$

Achievability: Classical Capacity (Cont.)

“Ricochet Property"

$$(U \otimes \mathbb{1}) |\Phi_{AB}\rangle = (\mathbb{1} \otimes U^T) |\Phi_{AB}\rangle$$

Using the “ricochet property" and the type-class decomposition, we show that Alice's operations for encoding the second message m' can be effectively reflected to Bob's side:

$$\sigma_{B^n G_2^n}^{m,m'} = (\mathbb{1} \otimes \Gamma^T(m'|m)) \rho_{B^n G_2^n}^{x^n(m)} (\mathbb{1} \otimes \Gamma^*(m'|m)) \,.$$

First Decoding Step

Observe that the reduced state (without G_2^n) is

$$\sigma_{B^n}^{m,m'} = \rho_{B^n}^{x^n(m)}$$

Thus, the reduced output is not affected by the encoding operation $U(\gamma(m'|m))$, and we can use the standard results on classical communication over a quantum channel without assistance.

Achievability: Classical Capacity (Cont.)

Thus, the first probability of error tends to zero as $n \to \infty$, provided that

$$R < I(X;B)_\rho - \varepsilon_1$$

This can be obtained from the quantum packing lemma, with

$$\Pi \equiv \Pi^\delta(\rho_B) \quad , \quad \Pi_{x^n} \equiv \Pi^\delta(\rho_B|x^n)$$

Achievability: Classical Capacity (Cont.)

Second Decoding Step

Applying the quantum packing lemma with conditioning on $x^n(m)$, we have that the second probability of error tends to zero, if

$$R < I(G_2; B|X)_\rho - \varepsilon_2$$

This can be obtained from the quantum packing lemma, with

$$\Pi \equiv \Pi^\delta(\rho_B|x^n(m)) \otimes \Pi^\delta(\rho_{G_2}|x^n(m))$$
$$\Pi_\gamma \equiv (\mathbb{1} \otimes U^T(\gamma))\Pi^\delta(\rho_{BG_2}|x^n)(\mathbb{1} \otimes U^*(\gamma))$$

Finally, we let A_0, A_1 replace G_1, G_2, respectively. □

Achievability: Quantum Capacity

- Let $|\phi_{A_1 A_2 AJ}\rangle$ be a purification of $\varphi_{A_1 A_2 A}$.

Achievability: Quantum Capacity

- Let $|\phi_{A_1 A_2 AJ}\rangle$ be a purification of $\varphi_{A_1 A_2 A}$.
- The corresponding channel output is

$$|\omega_{A_1 A_2 BEJ}\rangle = U^{\mathscr{N}}_{A\to BE} |\phi_{A_1 A_2 AJ}\rangle \ ,$$

where $\mathcal{U}^{\mathscr{N}}_{A\to BE}$ is a Stinespring dilation, $\mathcal{U}^{\mathscr{N}}_{A\to BE}(\rho_A) = U^{\mathscr{N}} \rho_A \, (U^{\mathscr{N}})^{\dagger}$.

Achievability: Quantum Capacity

- Let $|\phi_{A_1 A_2 AJ}\rangle$ be a purification of $\varphi_{A_1 A_2 A}$.
- The corresponding channel output is

$$|\omega_{A_1 A_2 BEJ}\rangle = U^{\mathcal{N}}_{A\to BE} |\phi_{A_1 A_2 AJ}\rangle \ ,$$

where $\mathcal{U}^{\mathcal{N}}_{A\to BE}$ is a Stinespring dilation, $\mathcal{U}^{\mathcal{N}}_{A\to BE}(\rho_A) = U^{\mathcal{N}} \rho_A \, (U^{\mathcal{N}})^\dagger$.

Consider a message state $|\theta_{MK}\rangle \otimes |\xi_{\bar{M}\bar{K}}\rangle$, and suppose that Alice and Bob share an entangled state $|\Phi_{G_A G_B}\rangle$,

$$|\mathcal{H}_M| = |\mathcal{H}_K| = 2^{nQ}$$

$$|\mathcal{H}_{\bar{M}}| = |\mathcal{H}_{\bar{K}}| = 2^{n(Q+Q')}$$

$$|\mathcal{H}_{G_A}| = |\mathcal{H}_{G_B}| = 2^{nR_e} \quad , \quad R_e = \frac{1}{2}[H(A_2)_\omega + H(A_2|B)_\omega]$$

Achievability: Quantum Capacity (Cont.)

Let $V^{(1)}_{M\to A_1^n}$ and $V^{(2)}_{\bar{M}G_A\to A_2^n}$ be arbitrary full-rank partial isometries. That is, each operator has 0-1 singular values with a rank of 2^{nQ} and $2^{n(Q+Q')}$, respectively. Denote

$$\left|\psi^{(1)}_{A_1^n K}\right\rangle = V^{(1)}_{M\to A_1^n} \left|\theta_{MK}\right\rangle \,,$$

$$\left|\psi^{(2)}_{A_2^n G_B \bar{K}}\right\rangle = V^{(2)}_{\bar{M}G_A\to A_2^n}\left(\left|\xi_{\bar{K}\bar{M}}\right\rangle \otimes \left|\Phi_{G_A,G_B}\right\rangle\right).$$

Achievability: Quantum Capacity (Cont.)

Given a pair of Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ with orthonormal bases $\{|i_A\rangle\}$ and $\{|j_B\rangle\}$, respectively, define the operator

$$\text{op}_{A\to B}(|i_A\rangle \otimes |j_B\rangle) \equiv |j_B\rangle\langle i_A|$$

Consider the operators

$$\Pi_{A_2\to A_1AJ} = \sqrt{|\mathcal{H}_{A_2}|}\text{op}_{A_2\to A_1AJ}(\phi_{A_1A_2AJ})$$
$$\Pi_{A_1\to A_2AJ} = \sqrt{|\mathcal{H}_{A_1}|}\text{op}_{A_1\to A_2AJ}(\phi_{A_1A_2AJ})$$

Achievability: Quantum Capacity (Cont.)

Given a pair of unitaries, $U^{(1)}_{A_1^n}$ and $U^{(2)}_{A_2^n}$, define the following quantum states,

$$\left|\omega^{U^{(2)}}_{A_1^n A^n J^n \bar{K} G_B}\right\rangle = \Pi^{\otimes n}_{A_2 \to A_1 A J} U^{(2)}_{A_2^n} V^{(2)}_{\bar{M} G_A \to A_2^n} \left(|\xi_{\bar{K}\bar{M}}\rangle \otimes |\Phi_{G_A, G_B}\rangle \right),$$

$$\left|\omega^{U^{(1)}}_{A_2^n A^n J^n K}\right\rangle = \Pi^{\otimes n}_{A_1 \to A_2 A J} U^{(1)}_{A_1^n} V^{(1)}_{M \to A_1^n} |\theta_{MK}\rangle .$$

The corresponding channel outputs are then

$$\left|\omega^{U^{(2)}}_{A_1^n B^n E^n J^n \bar{K} G_B}\right\rangle = (U^{\mathcal{N}}_{A \to BE})^{\otimes n} \left|\omega^{U^{(2)}}_{A_1^n A^n J^n \bar{K} G_B}\right\rangle$$

$$\left|\omega^{U^{(1)}}_{A_2^n B^n E^n J^n K}\right\rangle = (U^{\mathcal{N}}_{A \to BE})^{\otimes n} \left|\omega^{U^{(1)}}_{A_2^n A^n J^n K}\right\rangle$$

Achievability: Quantum Capacity (Cont.)

Using the decoupling theorem, we show that there exist $U^{(1)}_{A_1^n}$ and $U^{(2)}_{A_2^n}$ such that

1) $\mathrm{Tr}_{A^n J^n}\left[\Pi^{U^{(2)}}_{A_1^n \to A^n J^n \bar{K} G_B} U^{(1)}_{A_1^n} \psi^{(1)}_{A_1^n K}\right] \approx \theta_K \otimes \omega^{U^{(2)}}_{\bar{K} G_B}$ if $Q < H(A_1|A_2)_\omega - \varepsilon_{1,n}$

2) $\omega^{U^{(2)}}_{\bar{K} G_B} \approx \xi_{\bar{K}} \otimes \Phi_{G_B}$ if $Q + Q' + R_e < H(A_2)_\omega - \varepsilon_{4,n}$

3) $\mathcal{T}^{\otimes n}_{A_1 A_2 \to ED}\left(U^{(1)}_{A_1^n} \psi^{(1)}_{A_1^n K} \otimes U^{(2)}_{A_2^n} \psi^{(2)}_{A_2^n \bar{K} G_B}\right) \approx \theta_K \otimes \omega^{U^{(2)}}_{E^n J^n \bar{K}}$ if $Q < I(A_1\rangle B)_\omega - \varepsilon_{2,n}$

4) $\mathcal{T}^{\otimes n}_{A_1 A_2 \to ED}\left(U^{(1)}_{A_1^n} \psi^{(1)}_{A_1^n K} \otimes U^{(2)}_{A_2^n} \psi^{(2)}_{A_2^n \bar{K}}\right) \approx \xi_{\bar{K}} \otimes \omega^{U^{(1)}}_{E^n J^n K}$ if $Q + Q' - R_e < I(A_2\rangle B)_\omega - \varepsilon_{3,n}$

Achievability: Quantum Capacity (Cont.)

Encoding

$$1), 2) \quad \Rightarrow \quad \mathrm{Tr}_{A^n J^n}\left[\Pi^{U^{(2)}}_{A_1^n \to A^n J^n \bar{K} G_B} U^{(1)}_{A_1^n} \psi^{(1)}_{A_1^n K}\right] \approx \theta_K \otimes \xi_{\bar{K}} \otimes \Phi_{G_B}$$

Thus, by Uhlmann's theorem, $\exists$ an isometry $F_{M\bar{M}G_A \to A^n J^n}$ such that

$$5) \Pi^{U^{(2)}}_{A_1^n \to A^n J^n \bar{K} G_B} U^{(1)}_{A_1^n} \psi^{(1)}_{A_1^n K} \approx F_{M\bar{M}G_A \to A^n J^n}(\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B})$$

Achievability: Quantum Capacity (Cont.)

Decoding without Assistance

Applying the channel to 5), we obtain

$$6)\mathcal{T}^{\otimes n}_{A_1 A_2 \to ED}(U^{(1)}_{A_1^n}\psi^{(1)}_{A_1^n K} \otimes U^{(2)}_{A_2^n}\psi^{(2)}_{A_2^n \bar{K} G_B}) \approx$$
$$\mathrm{Tr}_{B^n}\left[(U^{\mathcal{N}}_{A\to BE})^{\otimes n} F_{M\bar{M}G_A \to A^n J^n}(\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B})\right]$$

Hence, by 3),

$$\mathrm{Tr}_{B^n}\left[(U^{\mathcal{N}}_{A\to BE})^{\otimes n} F_{M\bar{M}G_A \to A^n J^n}(\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B})\right] \approx \theta_K \otimes \omega^{U^{(2)}}_{E^n J^n \bar{K}}$$

Then, by Uhlmann's theorem, $\exists$ an isometry $D^*_{B^n \to M J_1}$, such that

$$D^*_{B^n\to MJ_1}(U^{\mathcal{N}}_{A\to BE})^{\otimes n} F_{M\bar{M}G_A \to A^n J^n}(\theta_{MK} \otimes \xi_{\bar{M}\bar{K}} \otimes \Phi_{G_A G_B}) \approx \theta_{MK} \otimes \hat{\omega}_{E^n J^n \bar{K} G_B J_1}$$

Achievability: Quantum Capacity (Cont.)

By tracing over $E^n J^n \bar{K} G_B J_1$, we deduce that there exist an encoding map $\mathcal{F}_{M\bar{M}G_A \to A^n}$ and a decoding map $\mathcal{D}^*_{B^n \to M}$, such that

$$(\mathcal{D}^*_{B^n \to MJ_1} \circ \mathcal{N}^{\otimes n}_{A \to B} \circ \mathcal{F}_{M\bar{M}G_A \to A^n})(\theta_{MK} \otimes \xi_{\bar{M}} \otimes \Phi_{G_A}) \approx \theta_{MK}$$

Achievability: Quantum Capacity (Cont.)

Decoding with EA

By 4) and 6),

$$\mathrm{Tr}_{B^n G_B}\left[(U^{\mathcal{N}}_{A\to BE})^{\otimes n} F_{M\bar{M}G_A\to A^n J^n}(\theta_{MK}\otimes\xi_{\bar{M}\bar{K}}\otimes\Phi_{G_A G_B})\right]\approx\xi_{\bar{K}}\otimes\omega^{U^{(1)}}_{E^n J^n K}$$

Then, by Uhlmann's theorem, $\exists$ an isometry $D_{B^n G_B\to\bar{M}G'_A G'_B J_2}$, such that

$$D_{B^n G_B\to\bar{M}G'_A G'_B J_2}(U^{\mathcal{N}}_{A\to BE})^{\otimes n} F_{M\bar{M}G_A\to A^n J^n}(\theta_{MK}\otimes\xi_{\bar{M}\bar{K}}\otimes\Phi_{G_A G_B})\approx$$
$$\xi_{\bar{M}\bar{K}}\otimes\Phi_{G_A G_B}\otimes\hat{\omega}_{E^n J^n K J_2}$$

Thus, $\mathcal{F}_{M\bar{M}G_A\to A^n}$ and $\mathcal{D}_{BG_B\to\bar{M}}$ satisfy

$$\mathcal{D}_{B^n G_B\to\bar{M}}\circ\mathcal{N}^{\otimes n}_{A\to B}\circ\mathcal{F}_{M\bar{M}G_A\to A^n}(\theta_M\otimes\xi_{\bar{M}\bar{K}}\otimes\Phi_{G_A G_B})\approx\xi_{\bar{M}\bar{K}}\qquad\square$$