# Quantum Channels: Transition from Classical to Quantum Channels

Himanshu Singh     Raagav Ramakrishnan     Shreyas Sinha     Yash Seri

November 21, 2024

# Introduction

In this presentation, we will be discussing quantum channels and how they developed from classical channels. But before that, we need to define what quantum channels are and what they operate on.

Quantum channels operate on Density Matrices, which are mathematical constructs that hold all information about a quantum state. They can be defined as:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|$$

where $\psi_i$ is the $i^{th}$ state occuring with probability $p_i$

# Introduction

A quantum channel acts as a linear *Completely Positive Trace Preserving (CPTP)* map from one density matrix to the other. This means that the product state of the system and the environment stays positive throughout the transformation, and the trace remains constant. These two properties are essential for a channel to be physically viable and make sense in the real world.

It is usually denoted with $\mathcal{N}$ and the state generated after the application of the channel on the original state is $\mathcal{N}(\rho)$.

Generally, this channel is second one of the three steps that happen in the process of sending information from A to B, the others being encoding and decoding. These three steps have been illustrated in the following figures.

# Conditions for a Quantum Channel

A quantum channel must satisfy the following three conditions:

- Linearity

$$\mathcal{N}(\alpha X_A + \beta Y_A) = \alpha\mathcal{N}(X_A) + \beta\mathcal{N}(Y_A)$$

- Complete Positivity

  A linear map $\mathcal{M} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ is said to be completely positive if $id_R \otimes \mathcal{M}$ is positive map for a reference system $R$ of arbitrary size.

- Trace Preserving

  A map $\mathcal{N}$ is trace preserving if $Tr[X_A] = Tr[\mathcal{N}(X_A)]$, for all input $X_A \in \mathcal{L}(\mathcal{H}_A)$.

# Choi Operator

## Definition (Choi Operators)

Let $\mathcal{H}_R$ and $\mathcal{H}_A$ be isomorphic Hilbert spaces, and let $\{|i\rangle_R\}$ and $\{|i\rangle_A\}$ be orthonormal bases for $\mathcal{H}_R$ and $\mathcal{H}_A$, respectively. Let $\mathcal{H}_B$ be some other Hilbert space, and let $\mathcal{N} : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_B)$ be a linear map (written also as $N_{A\to B}$). The Choi operator corresponding to $N_{A\to B}$ and the bases $\{|i\rangle_R\}$ and $\{|i\rangle_A\}$ is defined as the following operator:

$$(id_R \otimes \mathcal{N}_{A\to B})(|\Gamma\rangle\langle\Gamma|_{RA}) = \sum_{i,j=0}^{d_A-1} |i\rangle\langle j|_R \otimes \mathcal{N}_{A\to B}(|i\rangle\langle j|_A)$$

where $d_A \equiv dim(\mathcal{H}_A)$ and $|\Gamma\rangle_{RA}$ is the unnormalized maximally entangled vector:

$$|\Gamma\rangle_{RA} \equiv \sum_{i=0}^{d_A-1} |i\rangle_R \otimes |i\rangle_A$$

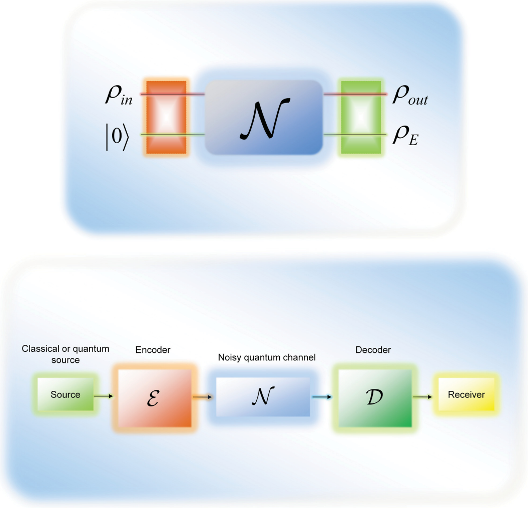



Figure: Illustrations of a quantum channel [1].

# Kraus Representation

Quantum channels are often represented in what is called the Kraus form (or the Choi-Kraus representation). In this form, quantum channels can be defined as linear combination in the following way:

$$\mathcal{N}(\rho) = \sum_i K_i \rho K_i^\dagger$$

where $\sum_i K_i^\dagger K_i = \mathbb{I}$

The Kraus representation is very useful in as a tool for analysing quantum channels, and makes several problens easier to solve. Kraus operators and their uses show up at many useful places throughout Quantum information theory. It makes channels easier to understand as well, by decomposing them into several ”sub-channels”.

## Von Neumann Entropy

The quantum analogue of the classical entropy is the Von Neumann Entropy. It is defined on the density operator as:

$$S(\rho) = -Tr[\rho log(\rho)]$$

Its maximum value is for the maximally mixed state and mimimum for a pure state.

Any quantum state can be spectrally decomposed to be written as $\sigma = \sum_i p_i |x_i\rangle\langle x_i|$ where $x_i$ are eigenvectors and $p_i$ are eigenvalues. Some algebraic manipulation can show that the quantum entropy ($S(\sigma)$) will be equivalent to the classical entropy of a probability distribution described by the eigenvalues:

$$S(\sigma) = H(p) = \sum_i p_i log(p_i)$$

# Other quantities

Several other quantities are defined for quantum systems analogous to the classical ones. Many of their properties are similar to their classical counterparts, but there are some striking exceptions as well. We define some of these here:

- Quantum Conditional Entropy

$$S(A|B) = S(\rho_{AB}) - S(\rho_B)$$

  where $\rho_B$ is the system with $A$ traced out. Interestingly, this quantity can be negative, something which is not seen in its classical counterpart.

## Other quantities

- Quantum Mutual Information

$$I(A:B) = S(\rho_A) + S(\rho_B) - S(\rho_{AB})$$

Quantum mutual information has a greater upper bound (by 2 times) compared to its classical counterpart.

- Quantum Relative Entropy

$$D(\rho||\sigma) = Tr[\rho(log(\rho) - log(\sigma))]$$

This is analogous to the classical Kullback-Liebler Divergence.

# Accessible Information

The Quantum no-cloning theorem establishes that quantum states cannot be perfectly cloned. This implies that there is an upper bound to the information that can be extracted from a quantum channel. The upper bound of information that is extractable from a quantum system is called the Holevo bound.

In classical systems, information is encoded deterministically, such as binary bits. In principle, all the encoded information can be accessed without limitations. In Quantum systems, however, information is encoded in quantum states, which can be superpositions or mixed states. This limits the amount of information that can be extracted from the system.

# Accessible Information

Let a sender(Alice) encode a classical variable X into a quantum state $\rho_x$.
The receiver(Bob) attempts to decode X by measuring the quantum state.
The accessible information is defined as the maximum classical mutual information between X and the output decoded Y:

$$I_{accessible} = \max I(X; Y)$$

Where the maximum is taken over all possible measurements that can be performed, represented by POVMs

# Holevo Bound

The Holevo bound is a fundamental result in quantum information theory that quantifies the maxiumum amount of classical information that can be extracted from a quantum system.

$$\chi = S(\rho) - \sum_i p_i S(\rho_i).$$

The proof for this is as follows:

Consider a quantum system that encodes classical information, which can be represented by a distribution with probability $p_x$ for each input $x$. This allows us to define the classical state $\rho_X$ as:

$$\rho_X := \sum_x p_x |x\rangle\langle x|,$$

(where $|x\rangle$ (ket $x$) represents a quantum state and $\langle x|$ (bra $x$) represents the Hermitian conjugate of $|x\rangle$.)

# Holevo Bound

Since each input is mapped to a quantum state $\rho_x$, the combined state can be written as:

$$\rho_{XQ} := \sum_x p_x |x\rangle\langle x| \otimes \rho_x,$$

where $\rho_x$ represents the density matrix of the quantum system.

The received combined state is represented as:

$$\rho := \mathrm{Tr}_X(\rho_{XQ}) = \sum_x p_x \rho_x,$$

where $\mathrm{Tr}_X$ represents the trace of $\rho_{XQ}$.

To bound the maximum information obtainable, we need to bound the mutual information $I(X : Y)$ with $I(X : Q)$, where $X$ is the input, $Y$ is the output, and $Q$ is the quantum state.

# Holevo Bound

From the monotonicity of quantum mutual information, quantum mutual information does not increase under quantum operations. Hence, we get:

$$I(X : Q'Y) \leq I(X : Q).$$

Similarly,

$$I(X : Y) \leq I(X : Q'Y).$$

From these two inequalities, we get:

$$I(X : Y) \leq I(X : Q).$$

Simplifying $S(X : Q)$, we arrive at the Holevo bound.

$$I(X : Q) = S(X) + S(Q) - S(XQ),$$

$$= S(X) + S(\rho) - \mathrm{Tr}(\rho_{XQ} \log \rho_{XQ}),$$

$$= S(\rho) - \sum_x p_x S(\rho_x).$$

# Shannon's Source Coding Theorem

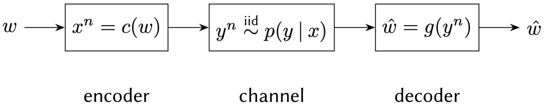
**Classical Context:** Shannon's theorem provides the foundation for lossless data compression:

- It ensures data can be encoded efficiently without losing information.
- In the limit of long sequences, the average number of bits required per symbol equals the entropy of the source $H(X)$.

**Formula:**

$$H(X) = -\sum_{x \in \mathcal{X}} P(x) \log_2 P(x),$$

where $P(x)$ is the probability of symbol $x$.




$p(y \mid x)$ probability of transmitted symbol $x$ being receved as $y$.

Figure: Shannon's Noisy Channel Theorem [2]

# Schumacher's Compression Theorem

Schumacher's theorem extends Shannon's ideas to quantum systems, enabling lossless compression of quantum states.

## Key Idea

- Use **qubits**, the fundamental units of quantum information.
- Compress $n$-copy quantum states described by a density matrix $\rho$ to occupy a subspace of dimension $2^{nS(\rho)}$, where $S(\rho)$ is the von Neumann entropy.

**Theorem Statement:**

1. For a source emitting states described by $\rho$, the minimum qubits needed for $n$ copies is $nS(\rho)$.
2. The data can be compressed with nearly perfect fidelity as $n \to \infty$.

# Quantum States and Density Matrices

- A quantum state is described by a density matrix $\rho$, particularly for mixed states.
- If a source emits states $\{|\psi_i\rangle\}$ with probabilities $\{p_i\}$, the density matrix is:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|.$$

- The von Neumann entropy $S(\rho)$ measures the quantum uncertainty:

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho).$$

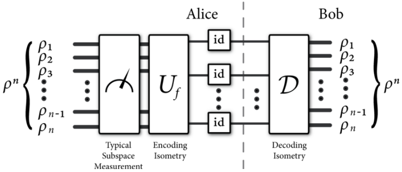



Figure: Schumacher Info Picture [3]

# Typical Subspaces

**Key Concept:** The typical subspace captures the most probable sequences emitted by a quantum source.

## Definition

An $\epsilon$-typical sequence $(i_1, i_2, \ldots, i_n)$ satisfies:

$$\left| -\frac{1}{n} \log p_{i_1 i_2 \ldots i_n} - S(\rho) \right| < \epsilon,$$

where $p_{i_1 i_2 \ldots i_n} = p_{i_1} p_{i_2} \cdots p_{i_n}$.

**Properties:**

- High probability: Most of the probability mass lies in the typical subspace.
- Dimension:

$$2^{n(S(\rho)-\epsilon)} \leq \dim(\mathcal{H}_{\text{typ}}) \leq 2^{n(S(\rho)+\epsilon)}.$$

# Proof of Achievability

**Goal:** Achieve asymptotically perfect fidelity for $R > S(\rho)$.

1. **Projector Construction:**

$$\Pi_{n,\epsilon} = \sum_{(i_1,\ldots,i_n)\in T_{n,\epsilon}} |\psi_{i_1} \otimes \cdots \otimes \psi_{i_n}\rangle\langle\psi_{i_1} \otimes \cdots \otimes \psi_{i_n}|.$$

2. **Encoding Channel:** Map states into the typical subspace:

$$E_n(\rho^{\otimes n}) = \begin{cases} V_{n,\epsilon}\rho^{\otimes n}V_{n,\epsilon}^\dagger, & \text{if } \rho^{\otimes n} \in \mathcal{H}_{\text{typ}}; \\ |0\rangle\langle 0|, & \text{otherwise.} \end{cases}$$

3. **Decoding Channel:** Recover states from the typical subspace:

$$D_n(Y) = V_{n,\epsilon}^\dagger Y V_{n,\epsilon}.$$

# Fidelity

The fidelity between the original state and the reconstructed state satisfies:

$$F(D_n \circ E_n, \rho^{\otimes n}) \geq \mathrm{Tr}[\Pi_{n,\epsilon}\rho^{\otimes n}] \to 1 \quad \text{as } n \to \infty.$$

**Achievable Compression Rate:**

- Number of qubits required: $m_n = \lceil \log_2 \dim(\mathcal{H}_{\text{typ}}) \rceil$.
- Compression rate:
$$R = \lim_{n\to\infty} \frac{m_n}{n} \leq S(\rho) + \epsilon.$$
- For $R > S(\rho)$, choose $\epsilon > 0$ sufficiently small to achieve high fidelity.

# Proof of Converse

**Goal:** Show that $R < S(\rho)$ results in fidelity $\to 0$.

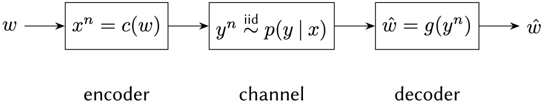
## Key Idea

- The compressed space $\dim = 2^{n_k R}$ is exponentially smaller than the typical subspace $\dim = 2^{n_k S(\rho)}$.
- Kraus decomposition bounds fidelity:

$$F(D_k \circ E_k, \rho^{\otimes n_k}) \leq \sqrt{\sum_{l=1}^{L_k} q_l \cdot \mathrm{Tr}[\Pi_l \rho^{\otimes n_k}]}.$$

Since $R < S(\rho)$, it follows:

$$\mathrm{Tr}[\Pi_l \rho^{\otimes n_k}] \to 0 \quad \Longrightarrow \quad F(D_k \circ E_k, \rho^{\otimes n_k}) \to 0.$$




$p(y \mid x)$ probability of transmitted symbol $x$ being receved as $y$.

Figure: Shannon's Noisy Channel Theorem [2]

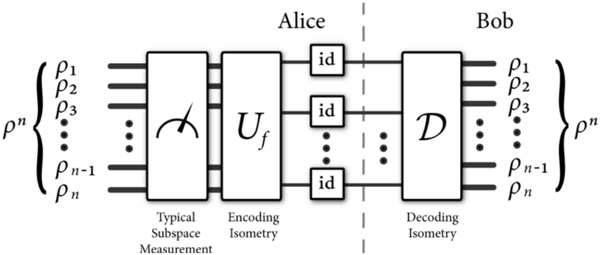



Figure: Schumacher Info Picture [3]

# Definition of Classical Capacity

The classical capacity of a quantum channel $\mathcal{N}$ is the maximum amount of classical information that can be transmitted per use of the channel with arbitrarily low error, as the number of channel uses goes to infinity.

## Key Points

- $C(\mathcal{N})$: Measures the effective transmission limit of classical data through a quantum channel.
- Ensures arbitrarily low error with sufficient channel uses and encoding strategies.
- Measured in bits per channel use.

# Types of Quantum Channels

Quantum channels often introduce errors due to interactions with the environment or system imperfections. These errors are referred to as **noise**.

## Examples of Quantum Channels

- **Depolarizing Channel:** Randomly replaces the state with a completely mixed state.
- **Dephasing Channel:** Reduces coherence by degrading off-diagonal terms in the density matrix.
- **Amplitude Damping Channel:** Models energy loss, such as photon loss in optical communication.

# Formula for Classical Capacity

The classical capacity $C(\mathcal{N})$ of a quantum channel $\mathcal{N}$ is determined by the **regularized Holevo capacity**:

$$C(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\chi\left(\mathcal{N}^{\otimes n}\right), \tag{1}$$

where:

- $\mathcal{N}^{\otimes n}$: Denotes $n$ channel uses.
- $\chi$: The Holevo quantity, bounding the extractable classical information.

## Holevo Quantity

$$\chi(\mathcal{N}, \{p_i, \rho_i\}) = S\left(\sum_i p_i \mathcal{N}(\rho_i)\right) - \sum_i p_i S\left(\mathcal{N}(\rho_i)\right),$$

where $S(\rho) = -\mathrm{Tr}(\rho \log \rho)$ is the von Neumann entropy.

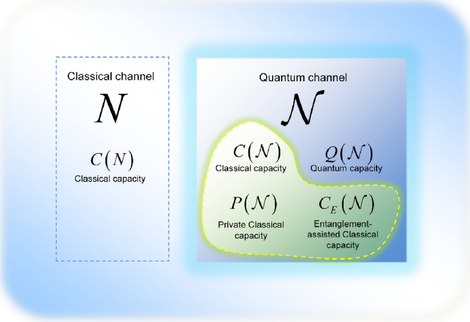



Figure: Properties of the Quantum Channel [4]

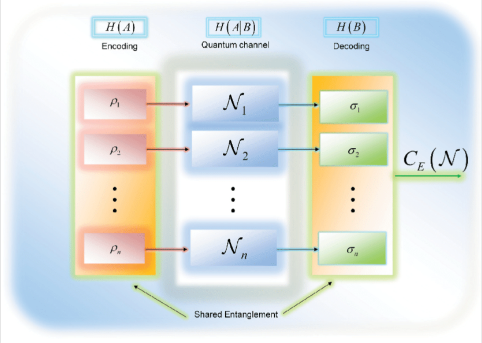



Figure: Classical Capacity Illustration [5]

# Private Capacity of a Wiretap Channel

The private capacity $P(\mathcal{N})$ of a classical wiretap channel $\mathcal{N} = p_{Y,Z|X}$ is defined as follows.

$$P(\mathcal{N}) = \max_{p_{U,X}(u,x)} [I(U;Y) - I(U;Z)]$$

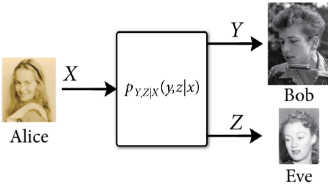



Figure: Classical wiretap channel [6].

# Properties: Private Capacity of a Wiretap Channel

- Non-negativity

$$P(\mathcal{N}) \geq 0$$

- Additivity

$$P(\mathcal{N} \otimes \mathcal{M}) = P(\mathcal{N}) + P(\mathcal{M})$$

- Equivalence of asymptotic and single use capacity

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

# Private Capacity of a Quantum Channel

Consider a classical-quantum state of the form given below.

$$\rho_{XA'} = \sum_x p_X(x)|x\rangle\langle x|_X \otimes \rho_{A'}^x$$

The private capacity $P(\mathcal{N})$ of a quantum channel $\mathcal{N}$ is defined as follows.

$$P(\mathcal{N}) = \max_{\rho_{XA'}} [I(X;B)_\rho - I(X;E)_\rho]$$

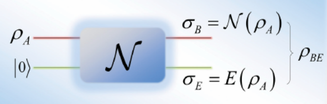



Figure: Private communication through a quantum channel [1].

# Properties: Private Capacity of a Quantum Channel

- Non-negativity

$$P(\mathcal{N}) \geq 0$$

- Lower bounded by quantum capacity

$$P(\mathcal{N}) \geq Q(\mathcal{N})$$

- Non-additivity

$$P(\mathcal{N} \otimes \mathcal{M}) \neq P(\mathcal{N}) + P(\mathcal{M})$$

# Quantum Capacity of a Quantum Channel

The quantity capacity $Q(\mathcal{N})$ of a quantum channel is defined as follows (where $|\psi\rangle = U^{\mathcal{N}}_{A' \to BE}|\phi\rangle_{AA'}$).

$$Q(\mathcal{N}) = \max_{\phi_{AA'}} [S(B)_\rho - S(AB)_\rho]$$

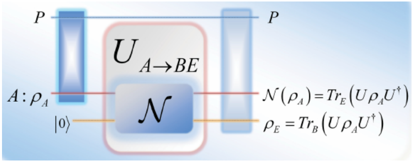



Figure: Quantum communication through a quantum channel [1].

## Properties: Quantum Capacity of a Quantum Channel

- Non-negativity

$$Q(\mathcal{N}) \geq 0$$

- Non-additivity

$$Q(\mathcal{N} \otimes \mathcal{M}) \neq Q(\mathcal{N}) + Q(\mathcal{M})$$

- Relation with other capacities

$$Q(\mathcal{N}) \leq P(\mathcal{N}) \leq C(\mathcal{N})$$

# Degradable Quantum Channels

A channel $\mathcal{N} : \mathcal{H}_A \to \mathcal{H}_B$ is called degradable when it may be degraded to its complementary channel $\mathcal{N}^c : \mathcal{H}_A \to \mathcal{H}_E$, i.e. when there exists a CPTP map $T : \mathcal{H}_B \to \mathcal{H}_E$ such that

$$\mathcal{N}^c = T \circ \mathcal{N}$$

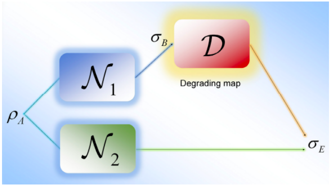



Figure: The concept of a degradable quantum channel [4].

# Properties: Degradable Quantum Channels

- Additivity of Private Capacity

$$P(\mathcal{N} \otimes \mathcal{M}) = P(\mathcal{N}) + P(\mathcal{M})$$

- Additivity of Quantum Capacity

$$Q(\mathcal{N} \otimes \mathcal{M}) = Q(\mathcal{N}) + Q(\mathcal{M})$$

- Equivalence of Private and Quantum Capacity

$$Q(\mathcal{N}) = P(\mathcal{N})$$

# Superadditivity

Superadditivity in quantum information theory refers to the phenomenon where certain types of quantum capacities increase when multiple uses of a quantum channel are considered together, rather than treating each channel use independently. This property arises because quantum entanglement and correlations can enhance the effectiveness of the channel when used in a collective or joint manner.

This superadditivity is the result of entanglement and other exotic correlation phenomena that arises in quantum systems. Superadditivity enhances communication capabilities of quantum channels and allows more communication than what their classical counterparts could (sometimes even through zero capacity channels).

# Superadditivity of various quantities

- Coherent information of a quantum channel:

$$Q(\mathcal{N} \otimes \mathcal{M}) \geq Q(\mathcal{N}) + Q(\mathcal{M})$$

  or

$$(Q(\mathcal{N}^{\otimes m}) > mQ(\mathcal{N}))$$

  where $Q(\mathcal{N}) = \max_{\phi_{AA'}} I(A\rangle B)_\rho$ and $\phi_{AA'}$ are all possible input states

- Holevo information:

$$\chi(\mathcal{N} \otimes \mathcal{M}) \geq \chi(\mathcal{N}) + \chi(\mathcal{M})$$

- Private capacity (over $m$ applications of the channel):

$$P(\mathcal{N}^{\otimes m}) > mP(\mathcal{N})$$

Since Holevo information and Coherent information are superadditive, Classical capacity and Quantum capacity are, by extension, also superadditive.

# Examples of quantum channels - Bit Flip channel

We present the **Bit Flip** channel.

The Bit flip channel, as its name suggests, flips a qubit from $|0\rangle$ to $|1\rangle$ (or $|1\rangle$ to $|0\rangle$) with probability $p$, and does nothing with probability $1 - p$:

$$\mathcal{N}_p(\rho) = (1-p)\rho + pX\rho X = K_0\rho K_0^\dagger + K_1\rho K_1^\dagger \tag{2}$$

Where $X$ is the Pauli X operator: $X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$

and $K_0 = (\sqrt{1-p})\mathbb{I}$ and $K_1 = (\sqrt{p})X$ are the Kraus operators.

More channel examples will be produced soon along with analyses on the various capacities of these channels.

# Example - Erasure channel

The erasure quantum channel $\mathcal{N}_p$ "erases" the input state $\rho$ with probability $p$ or transmits the state unchanged with probability $(1-p)$

$$\mathcal{N}_p(\rho) \rightarrow (1-p)\rho + (p|e\rangle\langle e|) \tag{3}$$

where $|e\rangle$ is the "erasure state". The classical capacity of this channel is given by:

$$C(\mathcal{N}_p) = (1-p)\log(d) \tag{4}$$

Here $d$ is the dimension of the input system. This demonstrates that the channel can transmit some classical information only for $0 \leq p < 1$, otherwise the classical capacity is 0.

On the other hand, its quantum capacity is:

$$Q(\mathcal{N}_p) = (1-2p)\log(d) \tag{5}$$

This is similar to classical capacity, except that information can only be transferred if $0 \leq p < 1/2$.

# Example - Phase Erasure Channel

The Phase Erasure channel ”erases” (as the name indicates) the phase of its inputs with probability $p$ but does not affect the amplitude. The map is expressed as:

$$\mathcal{N}(\rho) \to (1-p)\rho \otimes |0\rangle\langle 0| + p\frac{\rho + Z\rho Z^{\dagger}}{2} \otimes |1\rangle\langle 1| \tag{6}$$

The classical capacity of this channel is:

$$C(\mathcal{N}) = 1 \tag{7}$$

The quantum capacity of this channel is:

$$Q(\mathcal{N}) = (1-p)\log(d) \tag{8}$$

where the variables hold the same meaning as the last example.

# Superadditivity

Graeme Smith and Jon Yard's example:

A private Horodecki channel and a Symmetric channel may be combined to give a quantum channel with non-zero Quantum capacity, even though the individual channels have zero quantum capacity individually.

# References I


[1] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Communications Surveys & Tutorials*, vol. 20, no. 2, pp. 1149–1205, 2018, ISSN: 2373-745X. DOI: 10.1109/comst.2017.2786748. [Online]. Available: http://dx.doi.org/10.1109/COMST.2017.2786748.

[2] Anonymous, *Shannon's noisy channel-coding theorem*, [Online]. Available: https://jahoo.github.io/2020/12/16/noisy-channel-coding.html.

[3] B. Schumacher, "Quantum coding," *Phys. Rev. A*, vol. 51, pp. 2738–2747, 4 Apr. 1995. DOI: 10.1103/PhysRevA.51.2738. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevA.51.2738.

[4] L. Gyongyosi and S. Imre, "Properties of the quantum channel," *ArXiv*, vol. abs/1208.1270, 2012. [Online]. Available: https://api.semanticscholar.org/CorpusID:11482137.

[5] C. E. Shannon, "A mathematical theory of communication," *The Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948. DOI: 10.1002/j.1538-7305.1948.tb01338.x.

[6] M. M. Wilde, "Quantum information theory," in Cambridge University Press, Nov. 2016. DOI: 10.1017/9781316809976.001. [Online]. Available: http://dx.doi.org/10.1017/9781316809976.001.