Quantum Channels: Transition from Classical to Quantum Channels

Himanshu Singh Raagav Ramakrishnan Shreyas Sinha Yash Seri

November 6, 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:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{1}$$

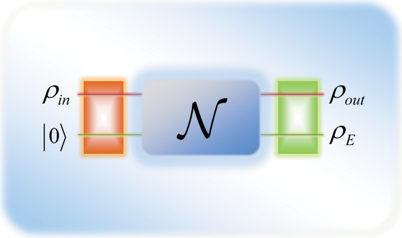
where ψ_i is the i^{th} state occuring with probability p_i

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.



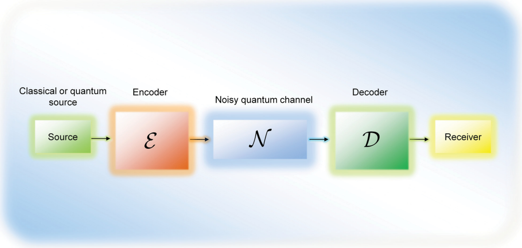


Figure: Illustrations of a quantum channel

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:

$$\mathcal{N}(\rho) = \sum_i K_i \rho K_i^\dagger \tag{2}$$

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:

$$S(\rho) = -Tr[\rho log(\rho)] \tag{3}$$

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:

$$S(\sigma) = H(p) = \sum_i p_i log(p_i) \tag{4}$$

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 ρ_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.

Holevo Bound

The Holevo bound is the upper bound of information that can be extracted from a quantum system, characterized by:

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

Derivation of the Holevo Bound

To prove this, consider a quantum system that encodes classical information represented by a distribution with probability p_x for each input x, allowing us to define the classical state ρ_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 $|x\rangle$.

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

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

The received combined state is represented as:

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

where tr_X represents the trace over ρ_{XQ}.

Derivation of the Holevo Bound

To bound the maximum obtainable information, we need to bound the mutual information $I(X:Y)$ with $I(X:Q)$. From the monotonicity of quantum mutual information, we have:

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

and similarly:

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

Combining these inequalities, we get:

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

Now, we simplify $I(X:Q)$ as follows to get the Holevo bound.

$$\begin{aligned} I(X:Q) &= S(X) + S(Q) - S(XQ) \\ &= S(X) + S(\rho) + \mathrm{tr}(\rho_{XQ} \log \rho_{XQ}) \\ &= S(\rho) + \sum_x p_x \, \mathrm{tr}(\rho_x \log \rho_x) \\ &= S(\rho) - \sum_x p_x S(\rho_x), \end{aligned}$$

Classical Context: Shannon's Source Coding Theorem

Shannon's Source Coding Theorem provides the foundation for **lossless data compression**, ensuring data can be encoded efficiently without information loss. According to this theorem:

- In the limit, as the length of a stream of i.i.d. random variable data tends to infinity, it is impossible to compress data such that the code rate (average bits per symbol) is less than the entropy of the source.
- The average number of bits needed per symbol is given by the source's entropy $H(X)$.

Schumacher's Compression

- In the quantum domain, we use **qubits**, which can exist in superpositions of states.
- A quantum state can be represented by a **density matrix** ρ, particularly when dealing with mixed states. For a source emitting states $\{|\psi_i\rangle\}$ with probabilities $\{p_i\}$, the density matrix ρ is given by:

$$\rho = \sum_i p_i |\psi_i\rangle\langle\psi_i| \tag{5}$$

- The von Neumann entropy, $S(\rho)$, is the quantum analogue of Shannon entropy. It measures the uncertainty or the amount of quantum information in ρ and is defined as:

$$S(\rho) = -\mathrm{Tr}(\rho \log \rho) \tag{6}$$

Statement of Schumacher's Quantum Noiseless Channel Coding Theorem

1. For a quantum source emitting states described by a density matrix ρ with entropy $S(\rho)$, the minimum number of qubits required to encode these states can be compressed to $n \cdot S(\rho)$ qubits for n copies of the state.
2. As $n \to \infty$, it is possible to compress the data with nearly perfect fidelity, occupying a subspace of dimension $2^{nS(\rho)}$.

This means we can compress the information carried by n copies of ρ into a smaller subspace without significant information loss.

Proof Outline for Schumacher's Theorem

Schumacher's theorem relies on the concept of a **typical subspace** within the Hilbert space of the system, similar to how Shannon's theorem relies on typical sequences.

1. **Typical Subspace Formation**: For a large number n of quantum states, we can identify a subspace of the Hilbert space that is typical for most of the states generated by the source, with dimension approximately $2^{nS(\rho)}$.
2. **High Probability in the Typical Subspace**: For n copies of the quantum state ρ, almost all the probability mass of the state distribution is concentrated within this typical subspace, and the probability of the n-state system lying within it approaches 1 as n increases.
3. **Compression to the Typical Subspace**: The theorem states that we can compress our n-copy quantum state into a subspace of dimension $2^{nS(\rho)}$, thereby reducing the number of qubits from n to $n \cdot S(\rho)$. This achieves high fidelity, with minimal information loss for large n.

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. It is denoted by $C(\mathcal{N})$ and measured in bits per channel use.

Types of Quantum Channels

Quantum channels may be **noisy**, meaning they can alter or degrade the transmitted quantum states. Noise can arise from decoherence, loss, or other environmental factors. Common examples include depolarizing channels, dephasing channels, and amplitude damping channels.

Formula for Classical Capacity

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

$$C(\mathcal{N}) = \lim_{n \to \infty} \frac{1}{n} \chi \left(\mathcal{N}^{\otimes n} \right) \tag{7}$$

where χ is the Holevo quantity, providing an upper bound on the amount of classical information that can be transmitted.

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.

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

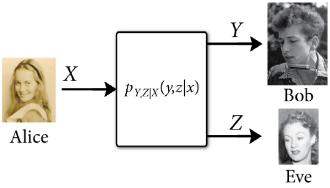


Figure: Classical wiretap channel.

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.

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

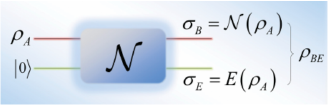


Figure: Private communication through a quantum channel.

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 $|\psi\rangle = U^{\mathcal{N}}_{A' \to BE}|\phi\rangle_{AA'}$).

$$
\begin{aligned}
Q(\mathcal{N}) &= \max_{\phi_{AA'}} [S(B)_\rho - S(AB)_\rho] \\
&= \max_{\phi_{AA'}} \left[S(B)_\psi - S(E)_\psi\right]
\end{aligned}
$$

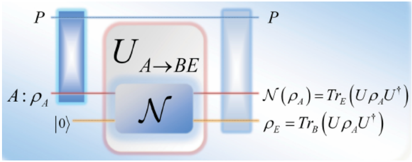


Figure: Quantum communication through a quantum channel.

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

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

Proof: Relation with other capacities

We will consider a pure state maximizing the coherent information. Let $\sigma_{XA'}$ denote the augmented classical-quantum state that correlates with index x.

$$\sigma_{XA'} = \sum_x p_X(x)|x\rangle\langle x| \otimes |\phi_x\rangle\langle\phi_x|_{A'}$$

$$\begin{aligned}
Q(\mathcal{N}) &= H(B)_\sigma - H(E)_\sigma \\
&= H(B)_\sigma - H(B|X)_\sigma - H(E)_\sigma + H(B|X)_\sigma \\
&= I(X;B)_\sigma - H(E)_\sigma + H(E|X)_\sigma \\
&= I(X;B)_\sigma - I(X;E)_\sigma \\
&\leq P(\mathcal{N}).
\end{aligned}$$

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 $1-p$:

$$\mathcal{N}_p(\rho) = (1-p)\rho + pX\rho X = K_0\rho K_0^\dagger + K_1\rho K_1^\dagger \tag{8}$$

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.