Quantum Project

Info Measures of Quantum Channels

Information measures of Quantum Channels

Team-9

Aryaman Basu Roy

Ayush Agrawal

L.Charan Sahit

Prerak Srivastava

Venika Annam

Vishnu Sai Gembali

Intro - What are quantum Channels ?

A quantum channel is a kind of communication channel that can send both quantum and classical information. The state of a qubit is an example of quantum information. It is like a linear map from density operators to density operators

The quantum channel conducts the superoperator or quantum operation, which is the transformation (mapping) of the initial density operator ρ to the final density operator ρ_f, represented as :

$$\xi : \rho \rightarrow \rho_f$$

Intro - Representation

Here, we talk about the operator-sum form of the final density operator :

$$\rho_f = \sum_k E_k \rho E_k^\dagger$$

It simply means that the final density operator is found by measuring state S' in basis of the initial state for a system that starts in pure state |ψ) and interacts with another state S'.

We average out all post measurement states that are possible changing the original density operator to ε(ρ).

Hence sender sends ρ and others receive ε(ρ) (modified state)

Intro - Properties

To understand decoherence which is the evolution of pure states to mixed states or to understand composition of 2 channels, some properties as below are important to state regarding quantum channels:

Linearity : $E(\alpha\rho 1 + \beta\rho 2) = \alpha E(\rho 1) + \beta E(\rho 2)$.

Preserves Hermiticity : $\rho = \rho^{\dagger}$ implies $E(\rho) = E(\rho)^{\dagger}$.

Preserves positivity : $\rho \geq 0$ implies $E(\rho) \geq 0$.

Preserves trace : $tr(E(\rho)) = tr(\rho)$.

Notice how these properties explain a part of “trace-preserving” completely positive map

Intro - Reversibility

- Reversibility is nothing but our ability to recover today's state (after applying unitary transformation on it) by applying unitary inverse to tomorrow's state
- Now for Unitary channels, we can in principle recover yesterday's state by applying $U^{\dagger}$ to today's state where $U^{\dagger}$ is the unitary inverse of a unitary transformation U.
- For general quantum channels that are not unitary, they cannot be inverted by another quantum channel.
- The process of decoherence is irreversible. We can't restore the damage to A if we don't have access to B after system A gets entangled with system B. Quantum information leaks into a system's environment due to decoherence, and since we can't control the environment, we can't retrieve it.

Intro - Quantum Operations

Quantum channels and generalized measurements are both particular examples of a larger concept known as a quantum operation.

A generalized measurement may be made by entangling a system with a meter and executing an orthogonal measurement on the meter, but a quantum channel can be created by measuring the meter but forgetting the measurement result. Imagine measuring the meter, then keeping part of the information about the result while discarding the rest in a quantum process.

Hence we need a much more general notion of quantum operation

$$\boldsymbol{\rho} \mapsto \frac{\mathcal{E}_{a_n} \circ \mathcal{E}_{a_{n-1}} \circ \cdots \circ \mathcal{E}_{a_2} \circ \mathcal{E}_{a_1}(\boldsymbol{\rho})}{\operatorname{tr} \mathcal{E}_{a_n} \circ \mathcal{E}_{a_{n-1}} \circ \cdots \circ \mathcal{E}_{a_2} \circ \mathcal{E}_{a_1}(\boldsymbol{\rho})}$$

Intro - Quantum Channel Positivity

We say that a channel is a positive map since its input as well as output is a non negative operator.

A channel is completely positive means that the channel remains positive even when we consider it to be acting on part of a larger system

Completely positive maps give a notion of quantum process that allows the description of probabilistic effects in quantum theory

We define it as follows :

ε is completely positive on A if $\varepsilon_a \otimes I_b$ is positive acting on AB (for any B)

Capacity of Quantum Channels

- A Quantum Channel can be viewed as a CPTP map which maps the input quantum state ρ1 to output state ρ2.
- If the output states are perfectly orthogonal, then the quantum channel is said to be noiseless.
- Capacity of a channel is the maximum rate at which information can be transferred with a reasonably small probability of error.
- Two types of capacities for Quantum Channels:
  - Classical Capacity
  - Quantum Capacity
- Classical Capacity refers to the capacity of quantum channels used for transmitting classical bits.
- Can be split into 3 categories: unentangled, private and entanglement assisted

Unentangled Classical Capacity

The Holevo-Schumacher-Westmoreland Capacity gives the least upper bound on the classical capacity of a quantum channel. (provided there is no entangled qubit shared between the sender and receiver)

$$C(\mathcal{N}) = \max_{all\ p_i,\rho_i} \chi = \max_{all\ p_i,\rho_i} \left[S(\sigma_{out}) - \sum_i p_i S(\sigma_i) \right]$$
$$= \max_{all\ p_i,\rho_i} \left[S\left(\mathcal{N}\left(\sum_i p_i \rho_i \right) \right) - \sum_i p_i S(\mathcal{N}(\rho_i)) \right]$$

The capacity is maximum for a noiseless quantum channel.

Private Classical Capacity

The private classical capacity P (N) of a quantum channel N describes the maximum rate at which the channel is able to send classical information through the channel reliably and privately (i.e., without any information leaked about the original message to an eavesdropper). The single use capacity is given by:

$$P^{(1)}(\mathcal{N}) = \max_{all\ p_i,\rho_i} \left(I(A:B) - I(A:E) \right).$$

The asymptotic capacity is given by

$$P(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} P^{(1)}\left(\mathcal{N}^{\otimes n}\right) = \lim_{n\to\infty} \frac{1}{n} \max_{all\ p_i,\rho_i} \left(I(A:B) - I(A:E) \right).$$

Entanglement-assisted Classical Capacity

This measures the capacity of channel when the sender and receiver have shared entangled state(s) before the communication.

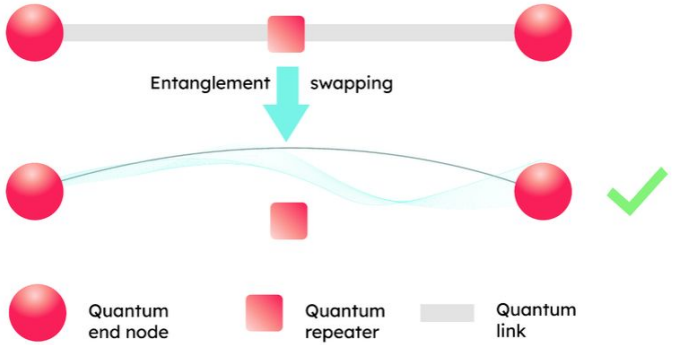
It can be expressed as: $$C_E\left(\mathcal{N}\right) = \max_{all\ p_i,\rho_i} I\left(A:B\right).$$

The maximum of the transmittable classical information is equal to the maximized quantum mutual information.

The asymptotic capacity is the same as single use capacity.

Quantum Repeaters

- Quantum repeaters just like classical repeaters are used to amplify quantum signals which are attenuated by the optic fibre cable while transmission.
- However, because of the no-cloning theorem they cannot work on the principle of classical repeaters (which copy and retransmit the signal).
- They achieve their goal through entanglement swapping.



Quantum capacity of a Quantum channel

Preserving Quantum Information

Apart from some fundamental differences encoding and decoding of quantum information are same. Here quantum information is encoded into non-orthogonal entangled quantum states $\{\rho_k\}$ chosen with probability $\{p_k\}$.

Input of encoder consists m states which are mapped to n joint intermediate states. These joint states are sent through independent instances of quantum channel $\mathcal{N}$ and then decoded by decoder which results in m output states. These output states are mixed based on the noise of the quantum channel.

Quantum states have to preserve their original superposition during the transmission without affecting original properties. But during the transmission quantum channels are entangled with environment which results in mixed states.

Quantum Coherent Information

- In case of the classical capacity C ($\mathcal{N}$) , the correlation between the input and the output is measured by the Holevo information and the quantum mutual information function.
- In case of the quantum capacity Q ($\mathcal{N}$) , we have a completely different correlation measure with completely different behaviors: it is called the quantum coherent information.
- The maximized quantum mutual information of a quantum channel $\mathcal{N}$ is always additive but the quantum coherent information is not.
- Entropy exchange is given by $S_E = S_E(\rho_A : \mathcal{N}(\rho_A)) = S(\rho_{PB})$
- Unitary transformation of input state and environment $U_{A \to BE}(A|0\rangle) = BE$

Connection between classical and Quantum Information

Quantum coherent information can be also can be expressed with the help of Holevo information $I_{coh}(\rho_A : \mathcal{N}(\rho_A)) = (\chi_{AB} - \chi_{AE})$

$$\chi_{AB} = S(\mathcal{N}_{AB}(\rho_{AB})) - \sum_i p_i S(\mathcal{N}_{AB}(\rho_i))$$

$$\chi_{AE} = S(\mathcal{N}_{AE}(\rho_{AE})) - \sum_i p_i S(\mathcal{N}_{AE}(\rho_i))$$

$$\rho_{AB} = \sum_i p_i \rho_i \qquad \rho_{AE} = \sum_i p_i \rho_i$$

Single use quantum capacity can be expressed as

$$Q^{(1)}(\mathcal{N}) = \max_{all\ p_i,\rho_i} (\chi_{AB} - \chi_{AE}) =$$

$$= \max_{all\ p_i,\rho_i} S\left(\mathcal{N}_{AB}\left(\sum_{i=1}^{n} p_i(\rho_i)\right)\right) - \sum_{i=1}^{n} p_i S(\mathcal{N}_{AB}(\rho_i))$$

$$- S\left(\mathcal{N}_{AE}\left(\sum_{i=1}^{n} p_i(\rho_i)\right)\right) + \sum_{i=1}^{n} p_i S(\mathcal{N}_{AE}(\rho_i)),$$

Asymptotic quantum capacity can be expressed as

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

$$= \lim_{n\to\infty} \frac{1}{n} \max_{all\ p_i,\rho_i} I_{coh}(\rho_A : \mathcal{N}^{\otimes n}(\rho_A))$$

$$= \lim_{n\to\infty} \frac{1}{n} \max_{all\ p_i,\rho_i} (\chi_{AB} - \chi_{AE}).$$

Lloyd-Shor-Devatak Formula

- Quantum coherent information can be used to express asymptotic quantum capacity $Q(\mathcal{N})$) of quantum channel $\mathcal{N}$ called the Lloyd-Shor-Devatak (LSD) capacity as follows

$$Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} Q^{(1)}\left(\mathcal{N}^{\otimes n}\right)$$
$$= \lim_{n\to\infty} \frac{1}{n} \max_{all\ p_i,\rho_i} I_{coh}\left(\rho_A : \mathcal{N}^{\otimes n}\left(\rho_A\right)\right)$$
$$= \lim_{n\to\infty} \frac{1}{n} \max_{all\ p_i,\rho_i} \left(\mathrm{S}\left(\rho_B\right) - \mathrm{S}\left(\rho_E\right)\right),$$

  where $Q^{(1)}(\mathcal{N})$ represents the single-use quantum capacity

- $Q(\mathcal{N})$ can also be expressed using the Holevo information

$$Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_{all\ p_i,\rho_i} \left(\chi_{AB} - \chi_{AE}\right),$$

χ_{AB} , χ_{AE} denotes the classical

The Assisted Quantum Capacity

- Assisted capacity measures quantum capacity of a pair of channels that contains different channel models.
- For a quantum channel $\mathcal{N}$, we can find a symmetric channel A that results in following assisted quantum capacity $Q_{\mathcal{A}}(\mathcal{N}) = Q(\mathcal{N} \otimes \mathcal{A})$.

$Q_{\mathcal{A}}(\mathcal{N})$ makes it possible to realize superactivation of zero-capacity quantum channel.

The Zero-error Quantum Capacity

- In case of quantum zero-error capacities, encoding and decoding process differ from classical zero-error capacity
- Single use zero-error capacity is defined as $Q_0^{(1)}(\mathcal{N}) = \log(K(\mathcal{N}))$
- Asymptotic zero-error capacity is defined as $Q_0(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \log\left(K\left(\mathcal{N}^{\otimes n}\right)\right)$
- Here $K\left(\mathcal{N}^{\otimes n}\right)$ is max number of n-length mutually non-adjacent quantum messages that quantum channel can transmit with zero-error
- Also $Q_0(\mathcal{N}) \leq Q(\mathcal{N})$.

Relation between Classical and Quantum capacities of Quantum channels

- When classical capacity is measured with entangled inputs and joint measurement $C(\mathcal{N}) >= Q(\mathcal{N})$
- When classical capacity is measured by a classical encoder and a single measurement setting $C(\mathcal{N}) < Q(\mathcal{N})$

Capacity	*Type of information*	*Correlation measure between input and output*	*Measure of the Asymptotic channel capacity*
Classical	Classical information	Holevo information (Maximum of Quantum Mutual Information)	Holevo-Schumacher-Westmoreland formula
Private Classical	Private information (Classical)	Private information (Difference of Quantum Mutual Information functions)	Li-Winter-Zou-Guo, Smith-Smolin formula
Entanglement Assisted Classical	Classical information	Quantum mutual information	Bennett-Shor-Smolin-Thapliyal formula (Equal to single-use quantum mutual information.)
Quantum	Quantum information	Quantum Coherent Information	Lloyd-Shor-Devetak formula

TYPES OF QUANTUM CHANNELS

Unital and Non-Unital model

A unital quantum channel $\mathcal{N}$ transforms the identity transformation I to itself.

This condition does not hold true for a non unital quantum channel.

That is for a unital quantum channel, $\mathcal{N}(I) = I$

For a non unital quantum channel, $\mathcal{N}(I) \neq I$

The main difference between unital and non-unital channels is that the non-unital channels do not preserve the average state in the center of the Bloch sphere

Unital channel maps can be expressed as convex combinations of the four unitary Pauli operators (X, Y, Z and I), hence unital quantum maps are also called Pauli channels

Bloch Sphere

Let us understand the bloch sphere to easily visualise what happens in each type of channel and what the noise does to the input.

The north and south poles of the Bloch sphere are typically chosen to correspond to the standard basis vectors |0> and |1> , respectively.

The points on the surface of the sphere correspond to the pure states of the system, whereas the interior points correspond to the mixed states.

Since, density matrices can be expressed in terms of Bloch vectors, hence the map of a quantum channel also can be analyzed in the geometrical picture

Bloch Sphere

The shrinked ellipsoid is the plot of the the pure and mixed states, after they transformation due to the noise occurs.

For a unital quantum channel, the center of the geometrical interpretation of the channel ellipsoid is equal to the center of the Bloch sphere.

This means that a unital quantum channel preserves the average of the system states

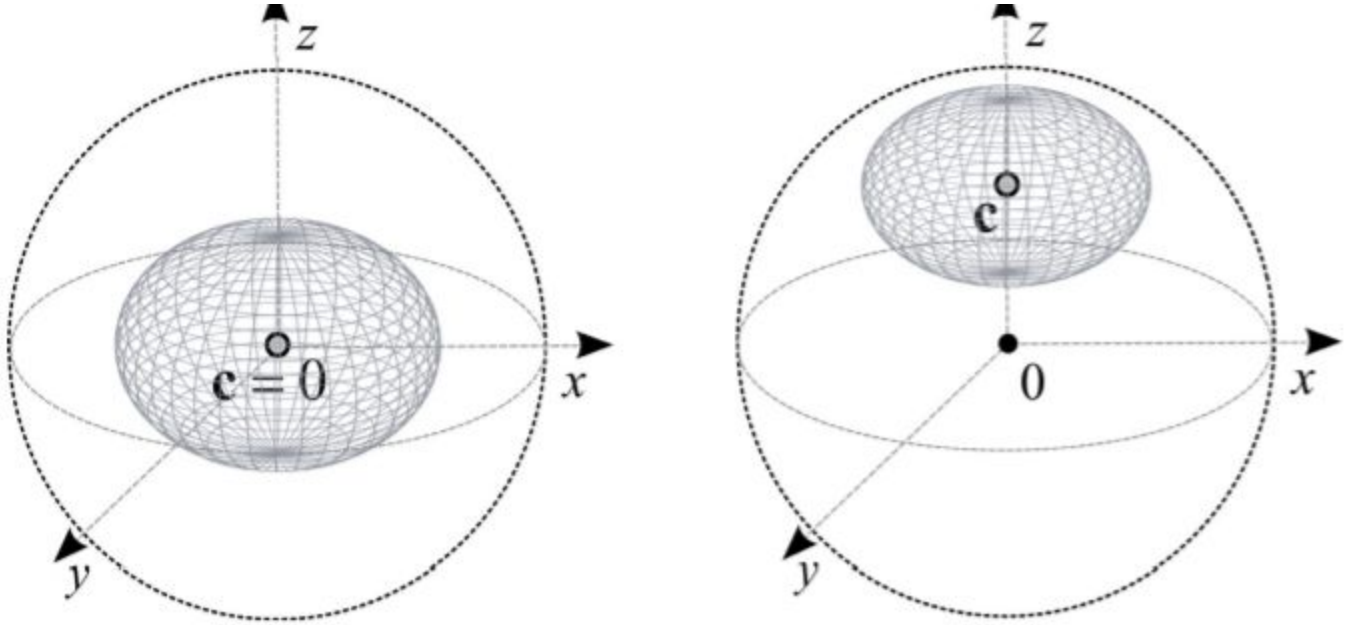
Bloch Sphere

On the other hand, for a non-unital quantum channel, the center of the channel ellipsoid will differ from the center of the Bloch sphere.

The main difference between unital and non-unital channels is that the non-unital channels do not preserve the average state in the center of the Bloch sphere.

Non-unital quantum channels shrink both the original Bloch sphere and move the center of the ball from the origin of the Bloch sphere.

Bloch Sphere



The geometrical interpretation of a unital and a non-unital quantum channels

Types of channel maps

- Flipping Channel Model
- Depolarizing Channel Model
- Amplitude Damping Channel
- Pancake Map

Flipping Channel Model

The bit flip model is defined through the help of the pauli transformation X, σ_X

The bit flip changes the probability amplitude of the input qubit.

The map of the bit flip channel can be represented as

$$\mathcal{N}(\rho) = p(\sigma_X \rho \sigma_X) + (1-p)\rho$$

For phase flip quantum channel, the pauli transformation Z σ_Z is being applied.

The phase flip changes the relative phase of input qubit.

Its map can be represented by, $\mathcal{N}(\rho) = p(\sigma_Z \rho \sigma_Z) + (1-p)\rho$

Flipping Channel Model

In physics realisations, phase flip channel map is also called as phase-damping channel model.

If the channel applies simultaneously both the bit flip and the phase flip, then it is called a s bit–phase flip model.

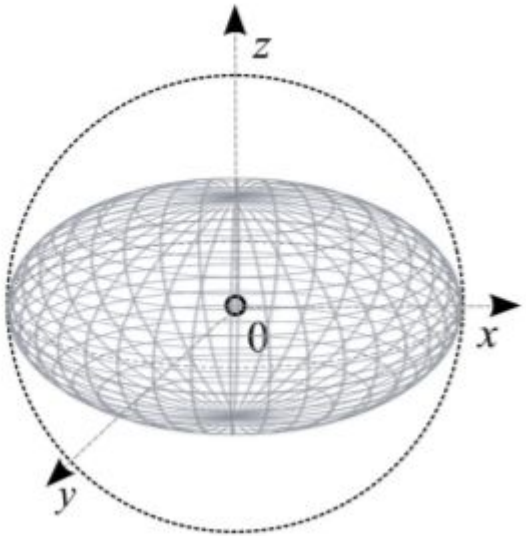
Both the effects of bit flip and phase flip, can be represented with the help of σ_Y

The effective map is given as,

$$\mathcal{N}(\rho) = p(\sigma_Y \rho \sigma_Y) + (1-p)\rho.$$

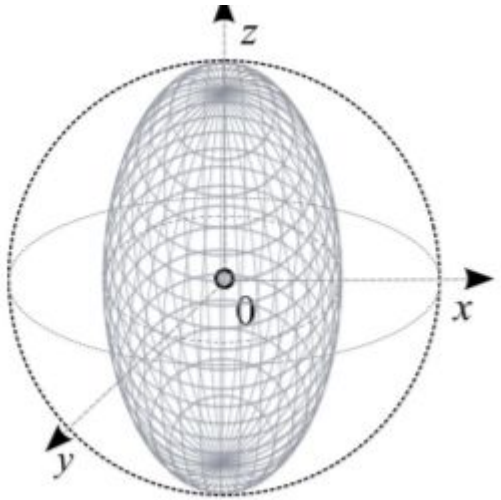
Flipping Channel Model

In the geometric representation of bit flip, this channel map shrinks the original Bloch sphere along the y and z axes, by the factor 1 -2 p .



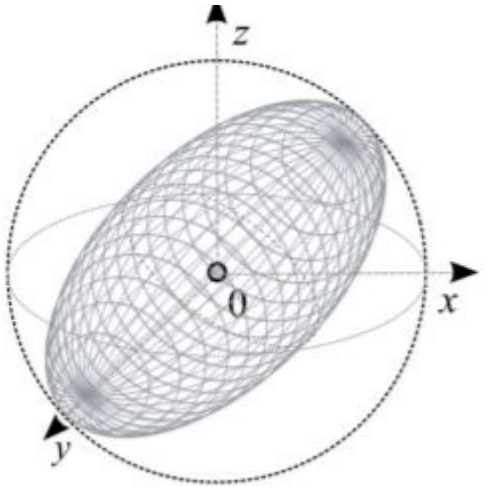
Flipping Channel Model

In the Bloch sphere representation in phase flip means that the width of the original Bloch sphere will be reduced by a factor of 1 -2 p in its equatorial plane.



Flipping Channel Model

The geometric interpretation of the bit-phase flip channel is depicted,



Depolarizing Channel Model

Depolarizing channel performs the following transformation,

$$\mathcal{N}(\rho_i) = p\frac{I}{2} + (1-p)\rho_i$$

where p is the depolarizing parameter of the channel.

if Alice uses two orthogonal states ρ_0 and ρ_1 for the encoding then the mixed input state is,

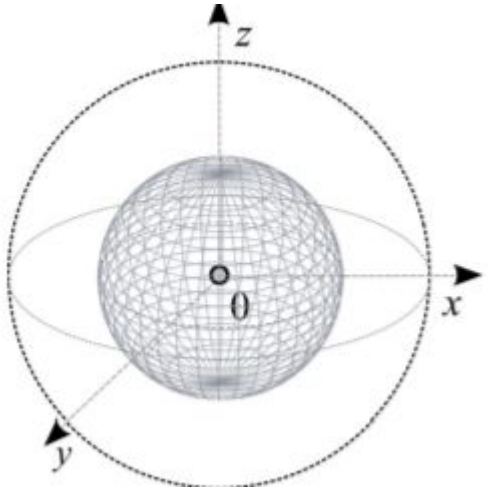
$$\rho = \left(\sum_i p_i \rho_i\right) = p_0\rho_0 + (1-p_0)\rho_1$$

$$\mathcal{N}(\rho) = \mathcal{N}\left(\sum_i p_i\rho_i\right) = \mathcal{N}\left(p_0\rho_0 + (1-p_0)\rho_1\right)$$

$$= p\frac{1}{2}I + (1-p)\left(p_0\rho_0 + (1-p_0)\rho_1\right)$$

Depolarizing Channel Model

Geometrically, the map of the depolarizing quantum channel shrinks the original Bloch sphere in every direction by 1 - p . The effect of the depolarizing quantum channel is shown,



Amplitude Damping Channel

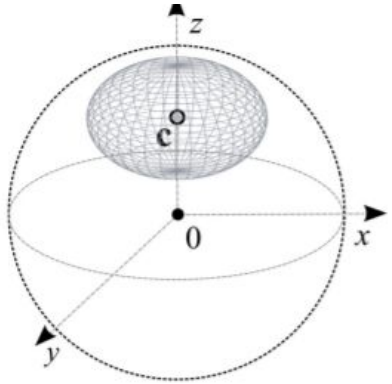
One of the most important type of channel map to describe decoherence is called the amplitude damping channel (or decay) map

Quantum decoherence is the loss of quantum coherence(difference in quantum state). If we leave the system isolated it would forever be in coherence, but even during measurement the system looses coherence which is similar to energy loss due to friction in classical case.

The amplitude damping channel map shrinks the Bloch sphere in the two directions of the equatorial plane – similarly to the phase flip channel, but it also moves the center of the ellipsoid from the center of the Bloch sphere. Therefore, this channel map is not unital. The height of the scaled ellipsoid will be given by the scaling factor 1/2 - p . The direction of the shift can be upward or downward.

Amplitude Damping Channel

Therefore, this channel map is not unital. The height of the scaled ellipsoid will be given by the scaling factor 1 - 2p . The direction of the shift can be upward or downward. On the other hand, the width of the ellipsoid will differ from the previous cases, namely by to the factor $\sqrt{1-2p}$



Amplitude Damping Channel

Any quantum channel can be described in the Kraus-representation, , using a set of Kraus matrices $\mathcal{A}=\{A_i\}$ in the following form,

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

Where, $\sum_i A_i^\dagger A_i = I$ For an amplitude damping quantum channel,

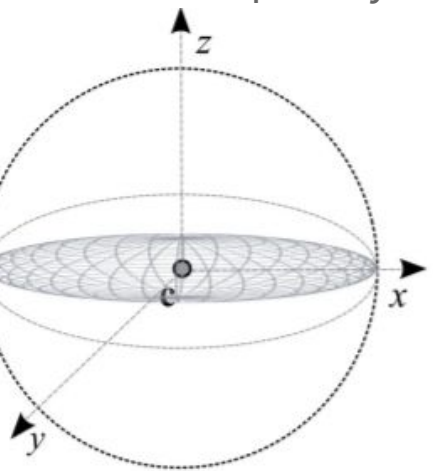
$$A_1=\begin{bmatrix}\sqrt{p} & 0\\ 0 & 1\end{bmatrix}, \text{ and } A_2=\begin{bmatrix}0 & 0\\ \sqrt{1-p} & 0\end{bmatrix}$$

where p represents the probability that the channel leaves input state |0> unchanged

Pancake Map

Pancake map is an example for physically not allowed (nonphysical, non-CP) transformations.

The non-CP property means, that there exists no Completely Positive Trace Preserving map, which preserves some information along the equatorial spanned by the x and y axes of the Bloch sphere, while it completely demolishes any information along the z axis.



The unitary maps in the maps which are discussed:

- Flipping Channel Model
- Depolarizing Channel Model

Non unitary maps:

- Amplitude Damping map

We can come to this conclusion by observing the centr eof the t=shrinked bloch sphere.

Shannon's Entropy

- It is the key concept of classical information theory.
- It measures how much information we gain of a random variable X after we learn of it or the uncertainty of how much info can be gained from the variable before knowing of the variable.
- The entropy is defined as the function of probabilities of different possible values of the random variable.

$$H(X) = H(p_1, p_2, ..p_n) = -\Sigma(p_x log(p_x))$$

- The best reason to use entropy is that, it quantifies the resources used to store information.

Von Neumann Entropy

- Shannon's Entropy is used for measuring the uncertainty in classical information theory. The quantum states are described in the same fashion by replacing the probability with the density operators.
- Von Neumann defined the entropy of a quantum state ρ by the formula

$$S(\rho) \equiv -\mathrm{tr}(\rho \log \rho).$$

- In this formula logarithms are taken to base two, as usual. If λ x are the eigenvalues of ρ then von Neumann's definition can be re-expressed

$$S(\rho) = -\sum_x \lambda_x \log \lambda_x$$

Data Compression

It determines the **minimal physical requirements** required to store an information source. Various techniques are used in both quantum and classical information theory that turn out to have more applications than mere data compression.

Some technique used are :

- Shannon’s noiseless channel coding theorem
- Schumacher’s quantum noiseless channel coding theorem

Shannon's noiseless channel coding theorem

- Shannon's noiseless channel coding theorem quantifies the extent to which we can compress the information being produced by a classical information source.
- The key idea behind Shannon's theorem is to divide the possible sequences of values x1 , . . . , xn for the random variables X1 , . . . , Xn up into two types – sequences which are highly likely to occur, known as typical sequences, and sequences which occur rarely, known as atypical sequences.
- Suppose {Xi } is an i.i.d. information source with entropy rate H(X). Suppose R > H(X). Then there exists a reliable compression scheme of rate R for the source. Conversely, if R < H(X) then any compression scheme will not be reliable.

- Suppose an independent and identically distributed information source is producing bits X1 , X2 , X3 , . . ., each being equal to zero with probability p, and equal to one with probability 1 − p.
- As n gets large, we expect that with high probability a fraction p of the symbols output from the source will be equal to zero, and that a fraction 1 − p will be equal to one. The sequences x 1 , . . . , x n for which this assumption is correct are known as typical sequences.
- We now have the tools to understand a simple scheme for data compression. Suppose the output from the source is x 1 , . . . , x n . To compress this output, we check to see whether x 1 , . . . , x n is a typical sequence. If it's not, we give up – declare an error.

Schumacher's quantum noiseless channel coding theorem

- The key technical idea making the quantum noiseless channel coding theorem possible is a quantum version of the idea of typical sequences.
- Let {H, ρ} be an i.i.d. quantum source. If $R > S(\rho)$ then there exists a reliable compression scheme of rate R for the source {H, ρ}. If $R < S(\rho)$ then any compression scheme of rate R is not reliable.

Errors in Quantum Channels and Error Correction

Transmission over Noisy Quantum Channels

What is Quantum Noise? It is basically external factors that could affect the transmission of data over a quantum channel.

Quantum Information Processing relies on **superposition states**, which are extremely sensitive to the external environment. It they do come in contact, it could result in **decoherence**.

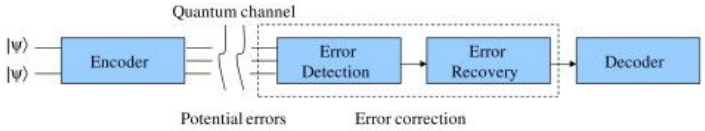
The 4 major steps in Quantum Error Correction are:

- Encoding
- Error Detection
- Error Recovery
- Decoding

Errors : Causes and Effects

Transmission of data over Quantum Channels can prove to be more difficult than transmission over Classical Channels for the following reasons

- **No-cloning Theorem** states that it is impossible to make a copy of any arbitrary quantum state.
- Quantum errors are **continuous** and a qubit that is meant to be transmitted can be in any superposition of the 2 base states.
- The measurement of any quantum information destroys that information.



Example: Quantum Key Distribution

We can study the errors that occur while transmitting data over quantum channels using the example of Quantum Key Distribution.In quantum cryptography, two authorized parties can send a secret key at the quantum level which can be used for data encryption and decryption.

The exchange between the sender and receiver takes place as follows:

- **Key Exchange (Encoding and Error Detection):**

  The sender generates the key and sends it using qubits. The bit value is attached to each photon by polarization.

  The sender polarizes photons based on 4 different types of polarization and bit values. The different polarization of a photon can be provided by a horizontal, vertical, -45 degrees and +45 degrees diagonal. Using this, each bit can be either polarized orthogonally or diagonally.

  Then, this sequence of photons is sent through a quantum channel. For each photon, the receiver randomly chooses the orthogonal or diagonal filter, also known as the **beam splitter**, to distinguish between the 2 polarization states.

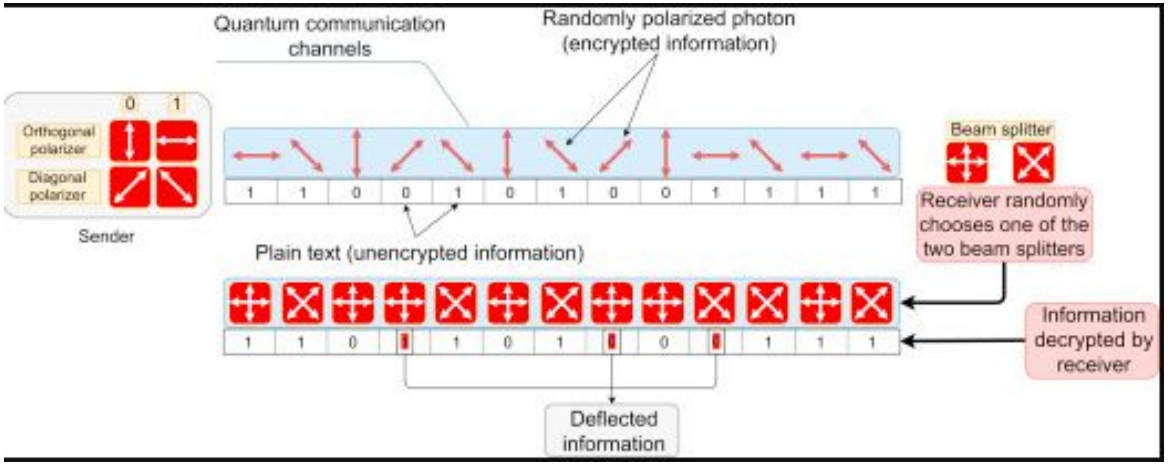
Example: Quantum Key Distribution

- **Key Sifting (Error Recovery and Decoding):**

  The receiver's job is to translate all the quantum states to a sequence of bits when all the photons are received. Some of these bit values are off because of the **randomness of the beam splitter.** Hence, the sender and receiver go through a process of **key-sifting** to find the identical secure key.

  - The receiver sends a sequence of beam splitters which are used for decryption.
  - The sender compares this sequence with the sequence of polarizers used for encryption.
  - The sender tells the receiver which beam splitters are right.
  - Based on this, the receiver keeps the corresponding bits and discards the deflected bits.
  - The remaining is called the **sifted key**, which is accepted as a secure shared key.

Example: Quantum Key Distribution

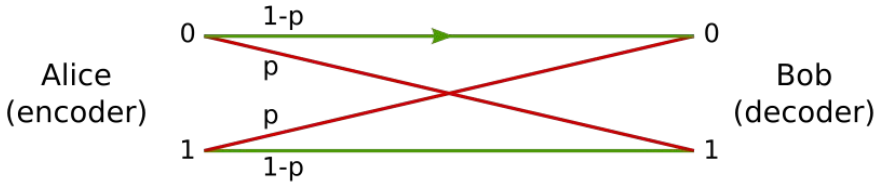


Error Correction

- In classical channels, to avoid corruption of data which is being transmitted over a noisy channel, we encode classical bits to be represented by multiple bits. When these bits are received, the bit which is in majority is that transmitted bit, or the representative bit of that received stream of bits. This is known as **Repetition Code**.
- We can use the **repetition code** in a classical channel, but this fails to work in quantum channels because of the **no cloning theorem.**
- But it is possible to spread the information of one qubit onto a highly entangled state of several (physical) qubits. Peter Shor first discovered this method of formulating a quantum error correcting code by storing the information of one qubit onto a highly entangled state of nine qubits.
- Asher Peres in 1985 proposed a method to protect against quantum errors, **the three-qubit bit flip.**

Binary Symmetric Channels

- It is a common communications channel model used in coding and information theory.
- Binary Symmetric Channels are used as models to model error and is used in the **three-qubit bit flip.**



Three-Qubit Bit Flip Code

- This technique uses entanglement and syndrome measurements and is comparable in performance with the repetition code.
- Let us take the example, where we want to transmit a single qubit through a noisy quantum channel, where the probability that this channel flips the qubit is p (Here p is considered to be small, so any higher powers of p are considered negligible). Therefore, without any error correcting protocol, the transmitted state will be correctly transmitted with probability of 1 - p.

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

$$\varepsilon(\psi) = (1-p)\psi + pX\psi X$$

Three-Qubit Bit Flip

- The probability of correct transmission can be improved however, by **encoding** the state into multiple qubits, so that the errors in these qubits can be identified and corrected.
- For this example. We encode the qubit as follows

$$|\psi'\rangle = \alpha|000\rangle + \beta|111\rangle$$

Three-Qubit Bit Flip

- This channel acts on this encoded qubit, possibly flipping some subset of its qubits.
- **Error Detection and Recovery:**
  - Since p is small, the probability of more than 1 qubit flip is negligible.
  - Since we are not allowed to query for the values which have been transmitted, we can only check which qubits differ from the other. For this we have to perform 4 projective measurements.

$$
\begin{aligned}
P_0 &= |000\rangle\langle 000| + |111\rangle\langle 111| \\
P_1 &= |100\rangle\langle 100| + |011\rangle\langle 011| \\
P_2 &= |010\rangle\langle 010| + |101\rangle\langle 101| \\
P_3 &= |001\rangle\langle 001| + |110\rangle\langle 110|
\end{aligned}
$$

Three-Qubit Bit Flip

- The measurement operators shown above correspond to the probability of either finding no bit flipped(shown by P_0) or one bit flipped (shown by P_1,P_2,P_3)
- Since all these vectors are mutually orthogonal, therefore they can be distinguished with certainty. Hence we know which bit was flipped, without knowing the state precisely.
- If the state corresponds to no bit flipped then we do nothing, however if the state corresponds to the first bit being flipped , we apply the pauli x gate on the first bit (given by $\sigma_x \otimes I \otimes I$), similarly if the second and third bits where flipped we apply the necessary transformations.

Three-Qubit Bit Flip

Therefore, in general, we can write the correction procedure using the following equation.

$$\varepsilon_{corr}(\rho) = P_0 \rho P_0 + \sum_{i=1}^{3} X_i P_i \rho P_i X_i$$

Thank You