Quantum Cyber Security

Lecture 6: Quantum Information Part IV

Mina Doosti

In this lecture…

We learn about:

- Generalised quantum operations
  - CPTP maps / quantum channels
  - Examples of CPTP maps
  - The concept of “noisy quantum states”
- Some well-known quantum channels for qubits
- Purification
- Schmidt decomposition
- Steinspring Dilation

CPTP Maps / Quantum channels

We have seen how to transform a pure state into another pure state (unitary) and also a mixed state to another mixed state (again by applying a unitary)

But how do we map pure states to mixed states? We need a transformation other than unitary matrices.

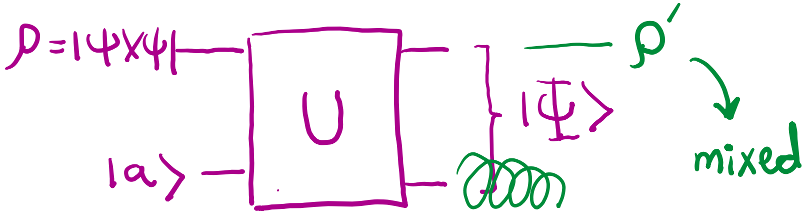
ρ — $\boxed{U}$ — $U\rho U^\dagger$ if $\rho = |\psi\rangle\langle\psi| \rightarrow \underline{U|\psi\rangle}\underline{\langle\psi|U^\dagger} = |\psi^{out}\rangle\langle\psi^{out}|$

We need some operations $\underset{\text{pure or mixed}}{\rho} \rightarrow \underbrace{\mathcal{E}}_{?}(\rho) = \rho'$ mixed

$Tr[\rho] = 1$

also a density matrix $Tr[\rho'] = 1$

1) It should be linear
2) It should be trace-preserving



Let's use the same idea of having a unitary on a larger space:

$$\mathcal{E}(\rho) = Tr_B[U(\rho \otimes |a\rangle\langle a|_B)U^\dagger]$$

CPTP Maps / Quantum channels with Krause operators

Let $|e_k\rangle$ be the orthogonal basis of the space B and $\rho = \sum_j \lambda_j |\psi_j\rangle\langle\psi_j|$ be the spectral decomposition of ρ.

$$\mathcal{E}(\rho) = \sum_k \sum_j \langle e_k | U [\lambda_j |\psi_j\rangle\langle\psi_j| \otimes |a\rangle\langle a|] U^\dagger | e_k\rangle$$

$$= \sum_{j,k} \lambda_j E_k |\psi_j\rangle\langle\psi_j| E_k^\dagger = \sum_k E_k \rho E_k^\dagger$$

Let's define $\langle e_k | U | a\rangle \equiv E_k$ as a linear operator

$$\forall |\phi\rangle \in \mathcal{H}_A : E_k |\phi\rangle = \langle e_k | U (|\phi\rangle \otimes |\psi\rangle) \in \mathcal{H}_A$$

Now we have a good way to define quantum channels.

CPTP map definition: A quantum channel is defined by the "superoperator" $\mathcal{E}$ which is a completely positive trace-preserving map.

positive $\mathcal{E}(\rho) \geq 0$ but also $(\mathcal{E} \otimes \mathbb{I}_{d'})\rho \geq 0$ $\forall$ dimensions d' $\downarrow$ positive for all subsystems

to produce density matrix

$$\mathcal{E} \in \mathcal{B}[\underbrace{\mathcal{B}[\mathcal{H}]}_{\text{space of density operators}}]$$

And it can be described by Kraus operators $E_k : \mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger$

This is also called operator-sum representation.

Note that the Kraus decomposition is not unique!

Unitary Channels and State Preparation Channels

Unitaries are CPTP maps:

$\mathcal{E}_U(\rho) = U\rho U^\dagger$ only one Kraus operator $E_1 = U$

Preparing a specific quantum state can also be described by a quantum channel:

We want to prepare state $|\psi\rangle \in \mathcal{H}$ $\rightarrow$ Let's define : $E_1 = |\psi\rangle\langle 0|$ $E_2 = |\psi\rangle\langle 1|$

check : $\sum_k E_k^\dagger E_k = I$ $\rightarrow$ $|0\rangle\underbrace{\langle\psi|\psi\rangle}_{1}\langle 0| + |1\rangle\underbrace{\langle\psi|\psi\rangle}_{1}\langle 1| = |0\rangle\langle 0| + |1\rangle\langle 1| = I$

$\mathcal{E}(|0\rangle\langle 0|) = E_1|0\rangle\langle 0|E_1^\dagger + E_2|0\rangle\langle 0|E_2^\dagger = |\psi\rangle\underbrace{\langle 0|0\rangle\langle 0|0\rangle}_{1}\langle\psi| + |\psi\rangle\underbrace{\langle 1|0\rangle\langle 0|1\rangle}_{0}\langle\psi| = |\psi\rangle\langle\psi|$ ✓

We can also prepare any ensemble state from classical basis $\{|e_j\rangle\}_{j=1}^n$

with Kraus operators $E_j = |\psi_j\rangle\langle e_j|$

Measurement Channels

POVMs can also be describes as a channel. They are also called quantum-to-classical channels (classical output)

$\{M_i\}_{i=1}^{K} \rightarrow$ POVM   Let's define $M_i = E_i^\dagger E_i \rightarrow$ Kraus operators

$$p_i = tr(M_i \rho) = tr(E_i \rho E_i^\dagger)$$

The outcome of a measurement should be a "classical" basis, let's say $\{|e_i\rangle\}_{i=1}^{K}$

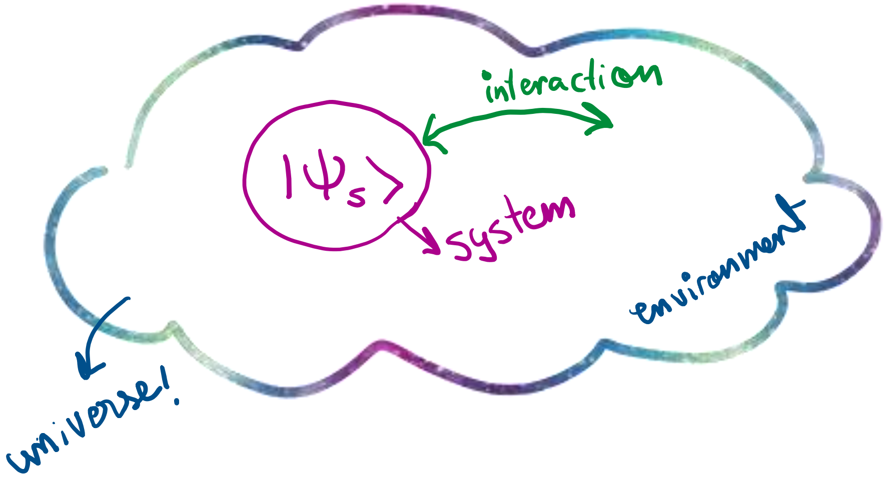
Now let's define $\bar{E}_i = \bar{E}_i|\psi\rangle = E_i|\psi\rangle \otimes |e_i\rangle$

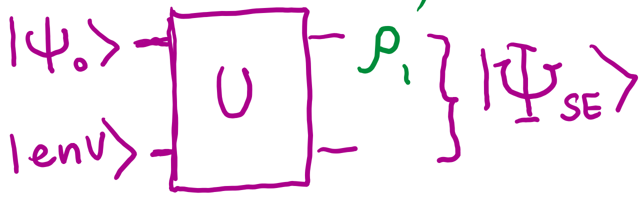
$$\mathcal{E}_{POVM} = \sum_{i=1}^{K} \bar{E}_i \rho \bar{E}_i^\dagger = \sum_{i=1}^{k} E_i \rho E_i^\dagger \otimes |e_i\rangle\langle e_i| = \sum_{i=1}^{k} \underbrace{\frac{E_i \rho E_i^\dagger}{tr(E_i \rho E_i^\dagger)}}_{\text{post-measurement state}} \otimes \underbrace{tr(E_i \rho E_i^\dagger)}_{p_i \,\to\, \text{prob. of outcome } i} \underbrace{|e_i\rangle\langle e_i|}_{\text{classical outcome}}$$

Noise: Interpretation of quantum channel output

We can interpret the mixedness of an output of a CPTP map as “quantum noise”.

$|\psi_0\rangle \xrightarrow{U} |\psi_1\rangle \xrightarrow{U} |\psi_2\rangle$





No longer pure of $|\psi_1\rangle$
↓
Noisy version

Another intuition: When states get mixed, you have less certainty (more noise). Why?

pure state $|\psi\rangle$ → There is a Measurement in which I know this is $|\psi\rangle$ with $p=1$

$$\mathcal{E}(|\psi\rangle\langle\psi|) = \rho = \underbrace{\tfrac{1}{2}|\psi\rangle\langle\psi| + \tfrac{1}{2}|\psi^{\perp}\rangle\langle\psi^{\perp}|}_{\text{uncertainty because of "mixedness"}}$$

Meet some famous quantum channels

① Bit-flip error $|0\rangle \to |1\rangle$, $|1\rangle \to |0\rangle$ $\quad |\psi\rangle \to X|\psi\rangle \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

phase flip error $|0\rangle \to |0\rangle$, $|1\rangle \to -|1\rangle$ $\quad |\psi\rangle \to Z|\psi\rangle \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$

both $\to Y$

→ Pauli depolarizing channel

$$\mathcal{E}(\rho) = (1-p)\rho + \underbrace{\frac{p}{3}(X\rho X + Y\rho Y + Z\rho Z)}_{\text{noise}}$$

$$\mathcal{E}(\rho) = (1-p)\rho + p\frac{I}{2}$$

② Dephasing channel

$$|0\rangle_A \longrightarrow \sqrt{1-p}\,|0\rangle_A|0\rangle_E + \sqrt{p}\,|0\rangle_A|1\rangle_E$$
$$|1\rangle_A \longrightarrow \sqrt{1-p}\,|1\rangle_A|0\rangle_E + \sqrt{p}\,|1\rangle_A|2\rangle_E$$

→ Environment "scatters" the qubits

$$E_0 = \sqrt{1-p}\,I \qquad E_1 = \sqrt{p}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \qquad E_2 = \sqrt{p}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$$

③ Amplitude damping channel

$$|0\rangle_A|0\rangle_E \longrightarrow |0\rangle_A|0\rangle_E$$
$$|1\rangle_A|0\rangle_E \to \sqrt{1-p}\,|1\rangle_A|0\rangle_E + \sqrt{p}\,|0\rangle_A|1\rangle_E$$

→ Models the loss of Energy in quantum systems

$$E_0 = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{1-p} \end{pmatrix} \qquad E_1 = \begin{pmatrix} 0 & \sqrt{p} \\ 0 & 0 \end{pmatrix}$$

Purification

Can we go back from a mixed state to a pure state? Can we purify mixed states?

What does it mean the purify a quantum state?

Purification Definition: Given a density matrix ρ_A, a pure state $|\psi_{AB}\rangle$ is a purification of ρ_A if $\rho_A = Tr_B[|\psi\rangle\langle\psi|_{AB}]$

How can we purify an arbitrary density matrix?

eigenvalues

eigenstates

1) let's diagonalize ρ_A $\rightarrow$ $\rho_A = \sum_{j=1}^{d_A} \lambda_j |\phi_j\rangle\langle\phi_j|$

2) let's add another system B with basis $\{|e_j\rangle_B\}_j^{d_B}$ but $d_B = d_A$

3) Let's make the pure state : $|\psi_{AB}\rangle = \sum_{j=1}^{d_A} \sqrt{\lambda_j} |\phi_j\rangle_A \otimes |e_j\rangle_B$ $\rightarrow$ purification

check: $Tr_B[|\psi_{AB}\rangle\langle\psi_{AB}|] = \sum_{k=1}^{d_B}\sum_{j=1}^{d_A} \langle e_k| \lambda_j |\phi_j\rangle\langle\phi_j|_A \otimes |e_j\rangle\langle e_j|_B |e_k\rangle = \sum_{j=1}^{d} \lambda_j |\phi_j\rangle\langle\phi_j|_A = \rho_A$

There is a mathematical tool that clarifies this better!

THE UNIVERSITY of EDINBURGH informatics

Schmidt decomposition

Schmidt decomposition: Suppose $|\psi_{AB}\rangle$ is a pure state of a composite system, AB. Then there exist orthonormal states $|i_A\rangle$ for system A, and orthonormal states $|i_B\rangle$ of system B such that

$$|\psi_{AB}\rangle = \sum_i \sqrt{\lambda_i}|i_A\rangle|i_B\rangle$$

where $\sqrt{\lambda_i}$ are non-negative real numbers satisfying $\sum_i \lambda_i = 1$ are known as Schmidt coefficients.

The number of non-zero values λ_i is called the **Schmidt rank** or **Schmidt number.**

Schmidt decomposition is the reason why we can do purification for any arbitrary state. → Now look again at the previous slide

Many interesting properties of quantum systems are related to Schmidt decomposition.

by Schmidt dec. $\rho_A = \sum_i \lambda_i |i_A\rangle\langle i_A|$ $\rho_B = \sum_i \lambda_i |i_B\rangle\langle i_B|$ → the reduced density matrices have same eigenvalues!

Schmidt decomposition also gives a method to measure entanglement. If the Schmidt rank is 1, the state is a product state

$|\psi_{AB}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ → Schmidt decomp.?

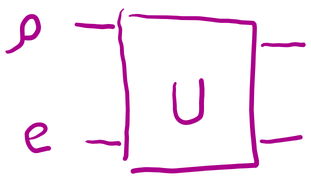
Stinespring Dilation or Isometric extension of a quantum channel

We saw that quantum channels can be described by unitaries on an expanded system. More generally:

Stinespring Theorem: For any CPTP map $\mathcal{E}\colon \mathcal{H}_1 \to \mathcal{H}_2$ There exists a linear map $V\colon \mathcal{H}_1 \to \mathcal{H}_2 \otimes \mathbb{C}^e$ such that:

$$\mathcal{E}(\rho) = Tr_e[V\rho V^\dagger]$$

If the dimensions are the same, V is a unitary and we have our original picture



$Tr_e[U(\rho \otimes |e\rangle\langle e|)U^\dagger]$

In general V is not unitary (if dimensions don't match), and it is an isometry, but this form is enough to compute Kraus operators and so get a quantum channel.

Resources

1. Quantum Computation and Quantum Information by *Nielsen & Chuang*: 8.2 , 8.3, 2.5

2. Introduction to Quantum Cryptography by *Thomas Vidick and Stephanie Wehner*: chapter 4: 4.2