Quantum Cyber Security
Lecture 6: Quantum Information Basics IV

Petros Wallden

University of Edinburgh

29th January 2026

This Lecture

- General quantum channels (operations)
- Examples
- Purification
- Schmidt Decomposition

General Quantum Channels and CPTP Maps

- We saw how to evolve states with unitaries
- Pure states remain pure!

General Quantum Channels and CPTP Maps

- We saw how to evolve states with unitaries
- Pure states remain pure!
- What if
  - evolve with some probability with U_1 and some other with U_2?
  - Discard a subsystem?
  - Measure a subsystem?
  - Prepare a specific state?

General Quantum Channels and CPTP Maps

- We saw how to evolve states with unitaries
- Pure states remain pure!
- What if
  - evolve with some probability with U_1 and some other with U_2?
  - Discard a subsystem?
  - Measure a subsystem?
  - Prepare a specific state?
- We need a more general concept of 'evolution', that we call a **quantum channel**
- It should be a map: $\mathcal{E}(\rho) = \rho'$, that is (i) linear, (ii) trace-preserving, (iii) maps density matrices to density matrices
- Most general: $\mathcal{E}(\rho) := \mathrm{Tr}_B \left(U(\rho \otimes |a\rangle \langle a|_B) U^\dagger \right)$

- Append an extra system, evolve (unitary), discard extra system!

General Quantum Channels and CPTP Maps

- Append an extra system, evolve (unitary), discard extra system!
- Can be defined in terms of the Kraus representation:

$$\mathcal{E}(\rho) = \sum_k E_k \rho E_k^\dagger \quad \text{where} \quad \sum_k E_k^\dagger E_k = \mathbb{I}$$

Unitary Channels and State Preparation Channels

- Unitaries are (simple) channels: $\mathcal{E}_U(\rho) = U\rho U^\dagger$

  with a single Kraus operator $E_1 = U$
- Check: obeys Kraus condition

Unitary Channels and State Preparation Channels

- Unitaries are (simple) channels: $\mathcal{E}_U(\rho) = U\rho U^\dagger$

  with a single Kraus operator $E_1 = U$
- Check: obeys Kraus condition
- Prepare state $|\psi\rangle \in \mathcal{H}$

- Define $E_1 = |\psi\rangle\langle 0|$, $E_2 = |\psi\rangle\langle 1|$
- Check: obeys Kraus condition, gives $\mathcal{E}(|x\rangle\langle x| = |\psi\rangle\langle\psi|)$ for both $x = 0, 1$

Measurement Channels

- Consider a measurement given by a POVM $\{M_i\}_i$ with Kraus operators $M_i = K_i^\dagger K_i$
- Consider a measurement device/register initiated at $|0\rangle\langle 0|_M$, taking i different values
- Define the channel: $E_i := K_i \otimes |i\rangle\langle 0|_M$

Measurement Channels

- Consider a measurement given by a POVM $\{M_i\}_i$ with Kraus operators $M_i = K_i^\dagger K_i$
- Consider a measurement device/register initiated at $|0\rangle \langle 0|_M$, taking i different values
- Define the channel: $E_i := K_i \otimes |i\rangle \langle 0|_M$

$$\mathcal{E}_{meas}(\rho \otimes |0\rangle \langle 0|) = \sum_i E_i \rho \otimes |0\rangle \langle 0| E_i^\dagger = \sum_i K_i \rho K_i^\dagger \otimes |i\rangle \langle i|$$

$$= \sum_i \left(\mathrm{Tr}(K_i \rho K_i^\dagger)\right) \left(\frac{K_i \rho K_i^\dagger}{\mathrm{Tr}(K_i \rho K_i^\dagger)}\right) \otimes (|i\rangle \langle i|)$$

Measurement Channels

- Consider a measurement given by a POVM $\{M_i\}_i$ with Kraus operators $M_i = K_i^\dagger K_i$
- Consider a measurement device/register initiated at $|0\rangle\langle 0|_M$, taking i different values
- Define the channel: $E_i := K_i \otimes |i\rangle\langle 0|_M$

$$\mathcal{E}_{meas}(\rho \otimes |0\rangle\langle 0|) = \sum_i E_i \rho \otimes |0\rangle\langle 0| E_i^\dagger = \sum_i K_i \rho K_i^\dagger \otimes |i\rangle\langle i|$$

$$= \sum_i \left(\mathrm{Tr}(K_i \rho K_i^\dagger)\right) \left(\frac{K_i \rho K_i^\dagger}{\mathrm{Tr}(K_i \rho K_i^\dagger)}\right) \otimes (|i\rangle\langle i|)$$

- Outcome i with prob $p(i) = \mathrm{Tr}(K_i \rho K_i^\dagger)$ and post-measurement state $\frac{K_i \rho K_i^\dagger}{\mathrm{Tr}(K_i \rho K_i^\dagger)}$

Examples: "famous" channels

- Bit flip channel: $\mathcal{E}(\rho) = p\rho + (1-p)X\rho X$

  Which is the Kraus rep?
- Phase flip: $\mathcal{E}(\rho) = p\rho + (1-p)Z\rho Z$
- Depolarising: $\mathcal{E}(\rho) = (1-p)\rho + p\mathbb{I}/2$

  Equivalent with prob $p/4$ apply X, Y, Z and nothing with the rest $1 - 3p/4$ (see tutorial 2)

Examples: "famous" channels

- Bit flip channel: $\mathcal{E}(\rho) = p\rho + (1-p)X\rho X$

  Which is the Kraus rep?
- Phase flip: $\mathcal{E}(\rho) = p\rho + (1-p)Z\rho Z$
- Depolarising: $\mathcal{E}(\rho) = (1-p)\rho + p\mathbb{I}/2$

  Equivalent with prob $p/4$ apply X, Y, Z and nothing with the rest $1-3p/4$ (see tutorial 2)
- Dephasing: $E_0 = \sqrt{1-p}\mathbb{I}$; $E_1 = \sqrt{p}\,|0\rangle\langle 0|$; $E_2 = \sqrt{p}\,|1\rangle\langle 1|$

  Check its effect on $|0\rangle$ and $|+\rangle$ states!
- Amplitude damping:
  $E_0 = 1\,|0\rangle\langle 0| + \sqrt{(1-p)}\,|1\rangle\langle 1|$; $E_1 = \sqrt{p}\,|0\rangle\langle 1|$

Purification

- Assume we have a mixed state ρ. Can we find a pure state on a larger space that its reduced matrix is our state?

Purification

- Assume we have a mixed state ρ. Can we find a pure state on a larger space that its reduced matrix is our state?

Definition: purification

Given ρ_A, a pure state $|\psi\rangle_{AB}$ is a purification of ρ_A if
$\rho_A = \mathrm{Tr}_B \left(|\psi\rangle \langle\psi|_{AB} \right)$

Purification

- Assume we have a mixed state ρ. Can we find a pure state on a larger space that its reduced matrix is our state?

Definition: purification

Given ρ_A, a pure state $|\psi\rangle_{AB}$ is a purification of ρ_A if
$\rho_A = \mathrm{Tr}_B \left(|\psi\rangle \langle\psi|_{AB} \right)$

- Can we purify any mixed state? (yes)

- Diagonalise $\rho_A = \sum_i \lambda_i |\phi_i\rangle \langle\phi_i|$

  where $\lambda_i, |\phi_i\rangle$ eigenvalues and eigenvectors

- Add system B where $d_A = d_B$, and orthonormal basis $\{|e_i\rangle_B\}_i$

- Prepare the state: $|\psi_{AB}\rangle = \sum_i \sqrt{\lambda_i}\, |\phi_i\rangle_A \otimes |e_i\rangle_B$

Purification

- Assume we have a mixed state ρ. Can we find a pure state on a larger space that its reduced matrix is our state?

Definition: purification

Given ρ_A, a pure state $|\psi\rangle_{AB}$ is a purification of ρ_A if $\rho_A = \mathrm{Tr}_B\left(|\psi\rangle\langle\psi|_{AB}\right)$

- Can we purify any mixed state? (yes)

- Diagonalise $\rho_A = \sum_i \lambda_i |\phi_i\rangle\langle\phi_i|$

  where $\lambda_i, |\phi_i\rangle$ eigenvalues and eigenvectors

- Add system B where $d_A = d_B$, and orthonormal basis $\{|e_i\rangle_B\}_i$

- Prepare the state: $|\psi_{AB}\rangle = \sum_i \sqrt{\lambda_i}\,|\phi_i\rangle_A \otimes |e_i\rangle_B$

- This is a purification (check definition!)

Schmidt Decomposition

- A two-qubit pure state, can have all non-zero terms $\sum_{ij} c_{ij} |ij\rangle$
- Can find a basis that it only has "diagonal" terms:

Schmidt Decomposition

- A two-qubit pure state, can have all non-zero terms $\sum_{ij} c_{ij} |ij\rangle$
- Can find a basis that it only has "diagonal" terms:

Schmidt Decomposition

Suppose $|\psi\rangle_{AB}$ pure state. There exists orthonormal bases $|i_A\rangle, |i\rangle_B$ 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 $\sum_i \lambda_i = 1$ known as Schmidt coefficients

Schmidt Decomposition

- A two-qubit pure state, can have all non-zero terms $\sum_{ij} c_{ij} |ij\rangle$
- Can find a basis that it only has "diagonal" terms:

Schmidt Decomposition

Suppose $|\psi\rangle_{AB}$ pure state. There exists orthonormal bases $|i_A\rangle, |i\rangle_B$ 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 $\sum_i \lambda_i = 1$ known as Schmidt coefficients

- $\rho_A = \sum_i \lambda_i |i_A\rangle \langle i_A|$ and $\rho_B = \sum_i \lambda_i |i_B\rangle \langle i_B|$

  Reduced states have same eigenvalues!

  (related with entropy and information; see next lecture)