Lecture 7

Purification is a technique whereby we replace a mixed-state evolution (noisy) by a pure state evolution on a larger space (noiseless). This allows us to use tools of analysis from the noiseless theory.

Purifying states given \( \rho_A \) and a pure state \( |\psi_{AR}\rangle \) on the joint space \( \mathcal{H}_A \otimes \mathcal{H}_R \), \( |\psi_{AR}\rangle \) is a purification of \( \rho_A \) if \( \rho_A = \text{Tr}_R \{ |\psi_{AR}\rangle \langle \psi_{AR}\} \} \) ("\( R \)" = "Reference"). We can construct a purification from any ensemble decomposition of \( \rho_A \):

\[
\rho_A = \sum_x \rho_x |\psi_x\rangle \langle \psi_x|,
\]

\[
|\psi_{AR}\rangle = \sum_x \sqrt{\rho_x} |\psi_x\rangle \otimes |x\rangle.
\]

In particular, if we diagonalize \( \rho_A \),

\[
\rho_A = \sum_k \lambda_k |\phi_k\rangle \langle \phi_k|, \quad \langle \phi_k| \phi_j\rangle = \delta_{kj},
\]

\[
|\psi_{AR}\rangle = \sum_k \sqrt{\lambda_k} |\phi_k\rangle \otimes |k\rangle.
\]

This is a Schmidt decomposition.

Provided the dimension of \( \mathcal{H}_R \) is high enough, we can switch to any ensemble decomposition of \( \rho_A \) by applying a unitary to \( R \):

\[
\sum_x \sqrt{\rho_x} |\psi_x\rangle \langle 1x| = (1 \otimes U) \sum_{x} \sqrt{\rho_x} |\psi_x\rangle \langle 1x|,
\]

\[
\rho_A = \sum_k \rho_k |\psi_k\rangle \langle \psi_k| = \sum_k \rho_k |\psi_k\rangle \langle \psi_k| = \sum_{x} \rho_x |\psi_x\rangle \langle \psi_x|.
\]
Isometries

An isometry is a linear map that preserves lengths and angles. We can think of it as an embedding into a higher dimensional space:

\[ |\psi_A\rangle \in \mathcal{H}_A \rightarrow U^{A\rightarrow B} |\psi_A\rangle \in \mathcal{H}_B, \quad d_B \geq d_A \]

\[(U^{A\rightarrow B})^\dagger U^{A\rightarrow B} = I_A, \quad U^{A\rightarrow B} (U^{A\rightarrow B})^\dagger = I_P\]

\[I_P^2 = I_P = I_P^\dagger, \quad \text{tr} I_P = d_A.\]

Any such isometry can be written as an embedding followed by a unitary:

\[U^{A\rightarrow B} = \begin{pmatrix} I \\ \mathbb{0}_{d_B} \end{pmatrix} \begin{pmatrix} \mathbb{0}_{d_A} \\ \mathbb{1}_{d_A} \end{pmatrix} \begin{pmatrix} \mathbb{1}_{d_A} \\ \mathbb{0}_{d_A} \end{pmatrix} \begin{pmatrix} I \\ \mathbb{0}_{d_B} \end{pmatrix} \]

\[U_B \text{ is not unique.}\]

A very common type of isometry in this class is appending a subsystem, followed by a joint unitary: \(U^{A\rightarrow BE}, \quad \mathcal{H}_E \cong \mathcal{H}_A\)

\[U^{A\rightarrow BE} = U^{BE} (I \otimes \text{10}\rangle)\]

\[(I \otimes \text{10}\rangle) |\psi \rangle = |\psi \rangle \otimes \text{10}\rangle\]

\[U^{A\rightarrow BE} |\psi \rangle = U^{BE} (|\psi \rangle \otimes \text{10}\rangle) \in \mathcal{H}_B \otimes \mathcal{H}_E\]

Of course we are not really "creating" subsystem \(E\) out of nothing... we are just including it in our description. \(E = \{\text{environment}\}\)

\(\text{Eve, the eavesdropper}\)
Isometric extension of a CPTP map

We can purify a general noisy map by a trick called Stinespring dilation or isometric extension. Suppose $\mathcal{K}_A \cong \mathcal{K}_B$ and

$$N^{A \rightarrow B}(\rho_A) = \sum_K A_K \rho_A A_K^+ . \sum_K A_K^+ A_K$$

Define an isometry

$$U^{A \rightarrow B \mathcal{E}} |\psi\rangle = \sum_K A_K |\psi\rangle \otimes |1_k\rangle_{\mathcal{E}}, \quad U^{A \rightarrow B \mathcal{E}} = U^{B \mathcal{E}} (I \otimes \mathcal{I})$$

$$U^{B \mathcal{E}} (|\psi\rangle \otimes |0\rangle) = \sum_A A_K |\psi\rangle \otimes |1_k\rangle$$

Some trick as in generalized measurement!

$$(\langle \psi_1 \otimes \langle 0_1 | (U^{B \mathcal{E}})^+ U^{B \mathcal{E}} (|\psi\rangle \otimes |0\rangle)$$

$$= \sum_{j,k} |\langle \psi_1 | A_j^+ A_k^+ |\psi\rangle \rangle_{\mathcal{E}} = \langle \psi | \sum_K A_K^+ A_K \otimes |1_k\rangle_{\mathcal{E}} = I\langle \psi |$$

We can now see that

$$N^{A \rightarrow B}(\rho_A) = \text{Tr}_E \left\{ U^{A \rightarrow B} \rho_A (U^{A \rightarrow B})^+ \right\}$$

$$= \text{Tr}_E \left\{ \sum_{j,k} A_j \rho_A A_k^+ \otimes |1_j\rangle \langle k| \right\}$$

$$= \sum_{j,k} \delta_{jk} A_j \rho_A A_k^+ = \sum_K A_K \rho_A A_K^+$$

(We can do the same kind of thing if $d_A \neq d_B$, but it's a little more complicated.)
If we purify both the state and the map, it looks like this:

$$\rho_A = \text{Tr}_R \{ |\psi_{AR}\rangle \langle \psi_{AR}| \}^2$$

$$N^{A\rightarrow B} (\rho_A) = \text{Tr}_B \{ (U^{A\rightarrow BE} \otimes I_R) |\psi_{AR}\rangle \langle \psi_{AR}| \} \times (U^{A\rightarrow BE} \otimes I_R)^+ \}^2$$

E.g.,

$$\rho \rightarrow (1-p) \rho + p |x\rangle \langle x|.$$

$$U^{A\rightarrow BE} |\psi\rangle = \sqrt{1-p} |\psi\rangle |0\rangle + \sqrt{p} |x\rangle |1\rangle.$$

**Complementary Channels**

If we trace over B instead of E we get the complementary channel:

$$(N^{E\rightarrow A} (\rho) = \text{Tr}_B \{ U^{A\rightarrow BE} \rho_A (U^{A\rightarrow BE})^+ \}^2$$

For our example

$$\rho_A \rightarrow (1-p) |0\rangle \langle 0| + p |1\rangle \langle 1| + \sqrt{p(1-p)} \langle x\rangle \rho \langle x|$$

$$= \frac{I}{2} + (1-2p) |2\rangle \langle 2| + \sqrt{p(1-p)} \langle x\rangle \rho \langle x|$$

For a CPTP map $\rho \rightarrow \sum A_j \rho A_j^+$,

1. The isometric extension

$$U^{A\rightarrow BE} |\psi\rangle = \sum_j A_j |\psi\rangle |j\rangle$$

2. The complementary map

$$\rho_A \rightarrow \text{Tr}_B \{ U^{A\rightarrow BE} \rho_A (U^{A\rightarrow BE})^+ \}^2 = \sum_{i,j} \text{Tr}_E \{ A_i \rho A_j \} |i\rangle \langle j|$$

Both of these are only unique up to an isometry on $E$. Note: starting from different Kraus decompositions obtained by a unitary $U$.
Generalized dephasing channel

A channel that preserves states diagonal in a particular basis \( \{1 \times \}^3 \) in a generalized dephasing channel:

\[
U_{A \rightarrow BE} |\psi\rangle = \sum_x 1 \times x \langle x | 1 \times \psi \rangle \otimes |\Phi_x \rangle_E
\]

where the states \( \{1 \times \}^3 \) need not be orthogonal.

The channel is

\[
N_D (\rho_A) = \sum_{x, x'} \langle x | 1 \times \rho_A | 1 \times x' \rangle \langle x' | 1 \times x \rangle
\]

The complementary channel is

\[
N_D^c (\rho_A) = \sum_x \langle x | 1 \times \rho_A | 1 \times x \rangle |\Phi_x \rangle_E \langle \Phi_x |
\]

This is an example of a classical-quantum channel: it is the same as measuring \( A \) is the basis \( \{1 \times \}^3 \) and then preparing the state \( |\Phi_x \rangle \) based on the outcome. Such a channel is entanglement-breaking: any entanglement \( A \) may have had is destroyed by the measurement.
Quantum Hadamard Channels

Any channel whose complement is entanglement-breaking is called a \underline{Hadamard channel}. They are so called because there is a choice of basis in which the channel can be written as the Hadamard product (element-wise) of \( p \) with a fixed matrix. For instance, the generalized dephasing channel can be written in the basis \( \{|x\rangle\} \) as the Hadamard product of \( p \) with the matrix \( M = [m_{xx'}] \), \( m_{xx'} = \langle \phi_x | \phi_{x'} \rangle \).

Hadamard channels are \underline{degradable}. A degradable channel has the property that Bob can simulate the complementary channel by applying a degrading map to his received state:

\[ E \otimes B^{\rightarrow E} \text{ s.t. } B^{\rightarrow E} \circ N^{A\rightarrow B} = (N^c)^{A\rightarrow E} \]

Degradable channels have a particularly nice structure in calculating their quantum channel capacity.