

# Lecture 7

①

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 decomp. of  $\rho$ :

$$\rho_A = \sum_x p_x |\psi_x\rangle \langle \psi_x|$$

$$|\Psi_{AR}\rangle = \sum_x \sqrt{p_x} |\psi_x\rangle \otimes |x\rangle$$

↑  
Orthonormal set  
of states

In particular, if we diagonalize  $\rho_A$ ,

$$\rho_A = \sum_k \lambda_k |\phi_k\rangle \langle \phi_k| \quad \langle \phi_k | \phi_j \rangle = \delta_{kj}$$

$$|\Psi_{AR}\rangle = \sum_k \sqrt{\lambda_k} |\phi_k\rangle |k\rangle$$

↳ this is a Schmidt decomp.

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

$$\sum_x \sqrt{p_x} |\psi_x\rangle |x\rangle = (I \otimes U) \sum_x \sqrt{q_x} |\psi'_x\rangle |x\rangle$$

$$\rho_A = \sum_x p_x |\psi_x\rangle \langle \psi_x| = \sum_x q_x |\psi'_x\rangle \langle \psi'_x|$$

# Isometries

(2)

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

$$|\psi\rangle \in \mathcal{H}_A \xrightarrow{U^{A \rightarrow B}} U^{A \rightarrow B} |\psi\rangle \in \mathcal{H}_B, d_B \geq d_A$$

$$(U^{A \rightarrow B})^\dagger U^{A \rightarrow B} = I_A, U^{A \rightarrow B} (U^{A \rightarrow B})^\dagger = P$$

$$P^2 = P = P^\dagger, \text{tr } P = d_A.$$

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

$$U^{A \rightarrow B} = U^B \begin{pmatrix} I & & \\ & \dots & \\ 0 & \dots & 0 \\ & \dots & \\ & & 0 & \dots & 0 \end{pmatrix} \begin{matrix} \} d_A \\ \} d_B - d_A \end{matrix}$$

$d_B \times d_B$        $d_A$

$U^B$  is not unique.

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

$$U^{A \rightarrow BE} = U^{BE} (I \otimes |0\rangle)$$

$$(I \otimes |0\rangle) |\psi\rangle = |\psi\rangle \otimes |0\rangle$$

$$U^{A \rightarrow BE} |\psi\rangle = U^{BE} (|\psi\rangle \otimes |0\rangle) \in \mathcal{H}_B \otimes \mathcal{H}_E$$

Of course we are not really "creating" subsystem E out of nothing... we are just including it in our description.

$E = \begin{cases} \text{environment} \\ \text{Eve, the eavesdropper} \end{cases}$

## Isometric extension of a CPTP map

③

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

$$N^{A \rightarrow B}(\rho_A) = \sum_k A_k \rho_A A_k^\dagger, \quad \sum_k A_k^\dagger A_k$$

Define an isometry

$$U^{A \rightarrow BE} |\psi\rangle = \sum_k A_k |\psi\rangle_B \otimes |k\rangle_E, \quad U^{A \rightarrow BE} = U^{BE} (I \otimes |0\rangle)$$

$$U^{BE} (|\psi\rangle \otimes |0\rangle) = \sum_A A_k |\psi\rangle \otimes |k\rangle$$

same trick as in generalized measurement!

$$(\langle \psi | \otimes \langle 0 |) (U^{BE})^\dagger U^{BE} (|\psi\rangle \otimes |0\rangle)$$

$$= \sum_{j,k} \langle \psi | A_j^\dagger A_k | \psi \rangle \underbrace{\langle j | k \rangle}_{\delta_{jk}} = \langle \psi | \underbrace{\sum_k A_k^\dagger A_k}_{I} | \psi \rangle = 1.$$

We can now see that

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

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

$$= \sum_{j,k} \delta_{jk} A_j \rho_A A_k^\dagger = \sum_k A_k \rho_A A_k^\dagger.$$

(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  $\textcircled{A}$  it looks like this:

$$\rho_A = \text{tr}_R \{ |\Psi_{AR}\rangle \langle \Psi_{AR}| \}$$

$$\mathcal{N}^{A \rightarrow B}(\rho_A) = \text{tr}_{RE} \left\{ (U^{A \rightarrow BE} \otimes I_R) |\Psi_{AR}\rangle \langle \Psi_{AR}| \times (U^{A \rightarrow BE} \otimes I_R)^\dagger \right\}$$

e.g.,

$$\rho \rightarrow (1-p)\rho + pX\rho X.$$

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

Note: starting from different Kraus decomps gives different isometries, related by a unitary on E.

### Complementary Channels

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

$$(\mathcal{N}^c)^{A \rightarrow E}(\rho) \equiv \text{tr}_B \left\{ U^{A \rightarrow BE} \rho_A (U^{A \rightarrow BE})^\dagger \right\}$$

For our example

$$\begin{aligned} \rho_A &\rightarrow (1-p) |0\rangle \langle 0| + p |1\rangle \langle 1| + \sqrt{p(1-p)} \langle X \rangle_\rho (|0\rangle \langle 1| + |1\rangle \langle 0|) \\ &= \frac{I}{2} + (1-2p)Z + \sqrt{p(1-p)} \langle X \rangle_\rho X \end{aligned}$$

For a CPTP map  $\rho \rightarrow \sum_j A_j \rho A_j^\dagger$ , we get

$\textcircled{1}$  The isometric extension

$$U^{A \rightarrow BE} |\psi\rangle_A = \sum_j A_j |\psi\rangle_B |j\rangle_E$$

Both of these are only unique up to an isometry on E

$\textcircled{2}$  The complementary map

$$\rho_A \rightarrow \text{tr}_B \left\{ U^{A \rightarrow BE} \rho_A (U^{A \rightarrow BE})^\dagger \right\} = \sum_{ij} \text{tr} \{ A_j \rho_A A_j^\dagger \} |i\rangle \langle j|_E$$

## Generalized dephasing channel

⑤

A channel that preserves states diagonal in a particular basis  $\{|x\rangle\}$  in a generalized dephasing channel:

$$\cup_{A \rightarrow BE} |\psi\rangle = \sum_x |x\rangle_B \langle x|\psi\rangle_E \otimes |\phi_x\rangle_E$$

where the states  $\{|\phi_x\rangle\}$  need not be orthogonal.

The channel is

$$N_D(\rho_A) = \sum_{x,x'} \langle x|\rho_A|x'\rangle |x\rangle_B \langle x'|$$

$$\langle \phi_{x'}|\phi_x\rangle$$

has an arbitrary phase  $\leq 1$

The complementary channel is

$$\rightarrow N_D^c(\rho_A) = \sum_x \langle x|\rho_A|x\rangle |\phi_x\rangle_E \langle \phi_x|$$

This is an example of a classical-quantum channel: it is the same as measuring  $A$  in the basis  $\{|x\rangle\}$  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

⑥

Any channel whose complement is entanglement-breaking is called a Q 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  $\rho$  with a fixed matrix. For instance, the generalized dephasing channel can be written in the basis  $\{|\phi_x\rangle\}$  as the Hadamard product of  $\rho$  with the matrix  $M = [m_{xx'}]$ ,  $m_{xx'} = \langle \phi_{x'} | \phi_x \rangle$ .

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

$$\exists \mathcal{D}^{B \rightarrow E} \text{ s.t. } \mathcal{D}^{B \rightarrow E} \circ \mathcal{N}^{A \rightarrow B} = (\mathcal{N}^c)^{A \rightarrow E}$$

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