8.372 Quantum Information Science III **Fall 2024**

Lecture 20: November 14, 2024

Scribe: Svyatoslav Filatov *Black holes as mirrors. Quantum capacity.*

From Lecture 19, recall the quantum state merging task, which involves transferring ownership of subsystem A, initially controlled by Alice, to Bob (Figure 20.1).

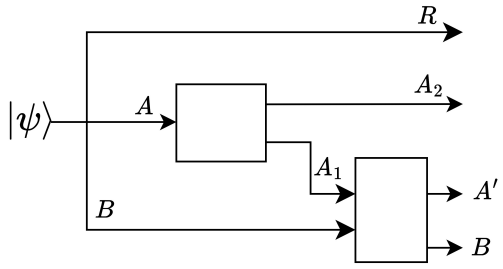

Figure 20.1: State Merging Scheme

The main result of Lecture 19 is that merging succeeds, i.e., $\psi_{RAB} \approx \rho_{R(A\to A')B}$, if the dimension d_{A_1} is sufficiently large:

$$d_A d_R(\operatorname{tr}\psi_{AR}^2 + \operatorname{tr}\psi_A^2\psi_R^2) \ll d_{A_1}^2 \tag{20.1}$$

Note that none of the terms can be discarded, as for different states ψ, either $\operatorname{tr}\psi_{AR}^2 \gg \operatorname{tr}\psi_A^2\psi_R^2$ or $\operatorname{tr}\psi_{AR}^2 \ll \operatorname{tr}\psi_A^2\psi_R^2$ can hold.

20.1 Application 1. Black Holes as Mirrors

Based on the paper arXiv:0708.4025. Hayden and Preskill (2007) made a theoretical argument: since black holes emit Hawking radiation and eventually evaporate over approximately 10^{80} years, any hypothetical "diary" thrown into the black hole must eventually emerge in the form of outgoing radiation. Even if the marginal state of each piece of radiation is thermal, the correlations can encode the information that was initially thrown in.

Hayden and Preskill take this example further, arguing that black holes can be viewed as mirrors — meaning that the information thrown in can emerge almost immediately. This holds under two conditions: first, the black hole is old or has emitted half of its entropy, and second, the observer throwing in the information must have collected all of the prior radiation.

Let's examine the merging part of the argument from the original paper. Consider the process illustrated in Figure 20.2. The initial pure system ρ consists of: i) the black hole (A) and all radiation emitted before (E); ii) a small diary (M) and a reference system (N).

The diary falls into the black hole (together denoted B), after which the diary is scrambled inside and subsequently radiates a small amount R. The resulting black hole is now denoted B', and the entire globally pure system is σ. We are interested in the conditions under which the initial information M can be recovered.

Consider quantity (20.2); we claim that if it is sufficiently small, systems B' and N are nearly decoupled. This implies that the purification of both B' and N resides in E and R. Therefore, there

exists a unitary rotation on the radiation that purifies N, which corresponds exactly to system M. In other words, if quantity (20.2) is small, the diary can be recovered from the radiation.

$$\mathbb{E}_U \left\| \sigma_{NB} - \sigma_N \otimes \sigma_B \right\|_1^2 \tag{20.2}$$

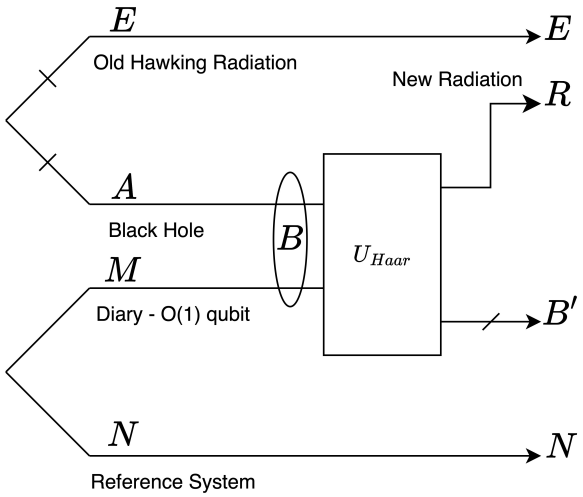

Figure 20.2: State Merging Scheme

Apply the merging formula (20.1) to upper-bound (20.2):

$$\mathbb{E}_U \left\| \sigma_{NB} - \sigma_N \otimes \sigma_B \right\|_1^2 \leq \frac{d_N d_{B'}}{d_R} \operatorname{tr} \rho_{BN}^2 \tag{20.3}$$

Assume that initially E and A were maximally entangled; therefore, BN is maximally mixed, and

$$\operatorname{tr} \rho_{BN}^2 = \frac{1}{d_A} = \frac{d_N}{d_B} \tag{20.4}$$

Also, apply $d_B = d_{B'} d_R$ to obtain:

$$\mathbb{E}_U \left\| \sigma_{NB} - \sigma_N \otimes \sigma_B \right\|_1^2 \leq \frac{d_N^2}{d_R^2} \tag{20.5}$$

In this new formula, all large dimensions are eliminated, leaving only the new radiation and the dimension of the diary. Now, we simply need to wait for enough radiation to emerge to make this quantity small — a process that does not scale with the size of the black hole.

20.2 Application 2. Quantum Error Correction Codes

In this section, we demonstrate the application of merging, using the argument that random subspaces yield good error correction codes. Recall that, in general, $\frac{I(A:R)}{2}$ qubits of communication are required to obtain $\frac{I(A:B)}{2}$ qubits. Similarly, merging on state (20.5) requires a qubits to be transferred from $A \to B$ and yields b ebits. However, this process requires very specific a qubits to be transmitted.

In general, merging states that if we scramble the entire A subsystem and choose **any** $a+\delta$ qubits, we can generate b ebits with high probability.

$$|\Psi\rangle = |\Phi\rangle_{RA_1}^{\otimes a} |\Phi\rangle_{A_2B}^{\otimes b} \tag{20.6}$$

Connection to QECC. Quantum error correction (QECC) posits that for certain codes, errors affecting a small number of qubits do not prevent the recovery of the entire encoded information (e.g., the 9-qubit Shor code can recover from an error on one qubit). Merging guarantees that any subset of $a+\delta$ qubits is sufficient to recover the entire initial state, which closely mirrors the guarantee provided by QECC.

20.3 Application 3. Quantum Channel Coding

20.3.1 Quantum Capacity Definition

Let's examine a more sophisticated QECC protocol. In Lecture 8, we defined the Holevo quantity — the classical capacity of a quantum channel. Now, we are ready to define quantum capacity. Suppose we have a quantum channel $\mathcal{N}$:

$$\mathcal{N} : A' \to B \tag{20.7}$$
$$V_{\mathcal{N}} : A' \to BE \tag{20.8}$$
$$\mathcal{N} : \mathrm{tr}_E \circ V_{\mathcal{N}} \tag{20.9}$$

We express the quantum capacity of channel $\mathcal{N}$ in terms of *coherent information*:

$$I_c(\phi_A, \mathcal{N}) = S(B)_\gamma - S(E)_\gamma \tag{20.10}$$
$$\gamma = I_A \otimes V_{\mathcal{N}}^{A' \to BE} |\phi\rangle_{AA'} \tag{20.11}$$

This is a familiar setup: $|\phi\rangle_{AA'}$ is a purification of some density matrix ϕ_A. The subsystem A' undergoes isometry, splitting into subsystems B and E, resulting in the pure state γ.

If the channel is perfect (e.g., the identity or a unitary channel), no qubits are lost to Eve, and the coherent information is large, indicating successful transmission of the message. Conversely, if all qubits go to Eve, the coherent information becomes negative. The quantum capacity of channel $\mathcal{N}$ is defined as the regularized maximal coherent information:

$$Q(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n} \max_\rho I(\rho, \mathcal{N}^{\otimes n}) \tag{20.12}$$

The inner term $\max_\rho$ ensures that $Q(\mathcal{N}) \geq 0$.

Let's justify formula (20.12). Consider the globally pure state γ and apply the typical projector to ϕ_A:

$$|\Gamma\rangle_{SBE} = \left(\Pi_{\phi_A,\delta}^n \otimes I_{BE}\right) |\gamma\rangle^{\otimes n} \quad \text{where S is a typical subspace of } A \subseteq A^n, \text{ or:} \tag{20.13}$$
$$|\Gamma\rangle_{SBE} = \left(I_S \otimes V_{S'\to BE}^n\right) |\phi\rangle_{SS'} \tag{20.14}$$

Analogous to classical random codebooks, we use a random subspace $R \subset S$ with a projector $P_{S\to R}$. To randomize, we sample from $U_S \sim$ Haar and apply the projector P. Define the new state $|\Psi\rangle_{RB^nE^n}$:

$$|\Psi\rangle_{RB^nE^n} = \sqrt{\frac{d_S}{d_R}} \left(P U_{\text{Haar}} \otimes I_{BE}\right) |\Gamma\rangle \tag{20.15}$$

Since we started with a maximally entangled state, we can transpose U to the other side:

$$|\Psi\rangle_{RB^nE^n} = \sqrt{\frac{d_S}{d_R}} \left(PU_{\text{Haar}} \otimes I_{BE}\right) \left(I_S \otimes V^n_{S'\to BE}\right) |\phi\rangle_{SS'} \tag{20.16}$$

$$= \sqrt{\frac{d_S}{d_R}} \left(P \otimes V^n U^T\right) |\phi\rangle_{SS'} \tag{20.17}$$

$$= \sqrt{\frac{d_S}{d_R}} \sqrt{\frac{d_R}{d_S}} \left(I_R \otimes V^n U^T\right) |\phi\rangle_{RR'} \tag{20.18}$$

$$= \sqrt{\frac{d_R}{d_S}} \left(I_R \otimes V^n U^T\right) |\phi\rangle_{RR'} \tag{20.19}$$

To ensure R is decoupled from R', Bob must be able to decode Alice's original message. Returning to the merging formula (simplified as the right-hand side is small compared to the left):

$$\mathbb{E}_U \left\|\Psi_{RE^n} - \Psi_R \otimes \Psi_{E^n}\right\|_1^2 \leq d_R \,\text{rank}\Psi_{E^n} \left(\text{tr}\Psi^2_{SE}\right) \tag{20.20}$$

By typicality:

$$d_R \,\text{rank}\Psi_{E^n} \left(\text{tr}\Psi^2_{SE^n}\right) \approx d_R \,\exp(nS(E)_\gamma) \left(\text{tr}\Psi^2_{B^n}\right) = d_R \,\exp(nS(E)_\gamma - nS(B)_\gamma) \tag{20.21}$$

This holds if:

$$\log d_R \ll nS(B)_\gamma - nS(E)_\gamma = nI(\phi_A, \mathcal{N}) \tag{20.22}$$

Related Fact. Distillable entanglement refers to the number of EPR pairs derivable from n copies of the state ρ_{AB}:

$$E_D(\rho_{AB}) = \lim_{n\to\infty} \max_{\mathcal{E}:A^n\to A^n} S(B^n) - S(A^nB^n) \tag{20.23}$$

20.3.2 Example of Quantum Capacity

Consider the depolarizing channel with parameter η:

$$\mathcal{D}_\eta(\rho) = (1-\eta)\rho + \frac{\eta}{3}(X\rho X + Y\rho Y + Z\rho Z)$$

First, compute the coherent information:

$$I_c\left(\frac{I}{2}, \mathcal{D}_\eta\right) = 1 - H_2(\eta) - \eta \log 3 \quad \text{, where} \tag{20.24}$$

$$|\gamma\rangle = \sqrt{1-\eta}\,|0\rangle_E\,|\Phi_{AB}\rangle + \sqrt{\frac{\eta}{3}}\left(|1\rangle_E \left(I \otimes X\right)|\Phi_{AB}\rangle\right) + \cdots \tag{20.25}$$

This result represents a combination of the entropy from applying mixing operations and the entropy of the actual mixing process.
Note that for sufficiently large η, this quantity becomes negative. Entangled inputs can mitigate this effect. Without delving into extensive numerical details, consider a degenerate code that maps a single logical qubit to five physical qubits:

$$\eta > 0.19 \Rightarrow I_c\left(\frac{I}{2}, \mathcal{D}_\eta\right) < \frac{1}{5} I_c\left(\frac{|0\rangle^5\langle 0|^5 + |1\rangle^5\langle 1|^5}{2}, \mathcal{D}_\eta\right)$$