Lecture 19: November 12, 2024

Scribe: Mahdi Hamad *Quantum State Merging*

This lecture introduces the quantum state merging protocol, a foundational task in quantum information theory that generalizes Schumacher compression to the setting where the receiver has quantum side information. The protocol shows how communication costs can be reduced, and in some cases made negative, by leveraging pre-existing correlations.

19.1 Warm-up: Schumacher Compression with a Reference

We begin with a variant of Schumacher compression in which a reference system R is included. Suppose we have a pure state $|\psi\rangle_{RA}$ and we want to transfer the A part to Bob. The final state will be $|\psi\rangle_{RB}$, where Bob now holds the system that used to be A.

This can be visualized as a process in which only the ownership of the A system changes, while the global state remains the same:

$$|\psi\rangle_{RA} \longrightarrow |\psi\rangle_{RB}$$

with the notation $\psi_{RA} \to B$ denoting that the A part of the state is now controlled by Bob.

In the standard compression setting, Alice can Schumacher-compress A into $\approx S(A)$ qubits. Here, the inclusion of R ensures that entanglement with the reference is preserved.

19.2 Introducing Side Information: Toward Merging

Now consider the case where Bob already holds a quantum system B that is entangled with A. The global state is $|\psi\rangle_{RAB}$. The new task is for Alice to send A to Bob so that the final state is $|\psi\rangle_{RB'B}$, where B' replaces A and is now part of Bob's lab. The transformation is:

$$|\psi\rangle_{RAB} \longrightarrow |\psi\rangle_{RB'B}$$

This is the quantum analogue of classical compression with side information at the decoder (Slepian-Wolf compression).

Classically, this task can be done at a rate of $H(A|B)$. Quantumly, this motivates the notion of **quantum state merging**.

19.3 Defining the Merging Task

Let $|\psi\rangle_{RAB}$ be a pure tripartite state. Alice wishes to send A to Bob, who already holds B, such that the resulting state is $|\psi\rangle_{RB'B}$, preserving coherence with R.

Alice applies an encoding operation $\mathcal{E}_A$, transmits a message (quantum or classical) to Bob, who then performs a decoding operation $\mathcal{D}_{B,M}$. The figure below illustrates this setup.

19.4 Naive Approach and the Role of Decoupling

Alice could ignore Bob's side information and Schumacher-compress A as usual, at cost $S(A)$ qubits. But this fails to exploit correlations between A and B.

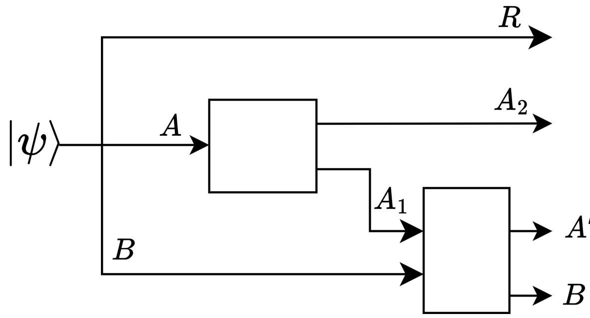

Figure 19.1: Quantum state merging protocol. Alice applies a random unitary to A, sends A_1 to Bob, and discards A_2. Bob applies a decoder using B and A_1.

The key insight is to use a **random unitary** on A that splits it into two subsystems: $A \to A_1A_2$. Alice sends A_1 to Bob and discards A_2.

If the discarded subsystem A_2 is nearly uncorrelated with the reference R, i.e.,

$$\rho_{RA_2} \approx \rho_R \otimes \rho_{A_2},$$

then the correlations between R and A have been preserved in the part sent to Bob, enabling him to reconstruct the original state. This is the **decoupling condition**.

19.5 Why Decoupling Implies Merging

Suppose $|\psi\rangle_{RAB}$ is transformed by the encoding U into:

$$|\sigma\rangle_{RA_1A_2B} = (U \otimes I_{RB})\,|\psi\rangle_{RAB}$$

Let σ_{RA_2} be the marginal state. If $\sigma_{RA_2} \approx \sigma_R \otimes \sigma_{A_2}$, then by Uhlmann's theorem, there exists an isometry $V : A_1B \to BB'B''$ such that:

$$(V \otimes I_R)\,|\sigma\rangle_{RA_1A_2B} \approx |\psi\rangle_{RB'B} \otimes |\phi\rangle_{A_2B''}$$

That is, Bob recovers the original state and obtains additional entanglement with Alice from A_2B''.

In other words, if R is decoupled from A_2, then R must be fully purified by the remainder of the system, which is under Bob's control. Thus, the global state has been reconstructed and the merging has succeeded.

The goal now is to analyze the decoupling condition quantitatively. Let U be a random unitary drawn from an approximate 2-design over $\mathcal{H}_A$, and let $A \to A_1A_2$ as before. We examine the trace distance between σ_{RA_2} and $\sigma_R \otimes \sigma_{A_2}$:

$$\mathbb{E}_U\,\|\sigma_{RA_2} - \sigma_R \otimes \sigma_{A_2}\|_1$$

This is bounded using the 2-norm via:

$$\|X\|_1^2 \leq d \cdot \|X\|_2^2,$$

where $d = d_R d_{A_2}$. Define $\sigma = (U \otimes I_{RB})\psi_{RAB}(U^\dagger \otimes I_{RB})$, then:

$$\|\sigma_{RA_2} - \sigma_R \otimes \sigma_{A_2}\|_2^2 = \operatorname{tr}(\sigma_{RA_2}^2) - 2\operatorname{tr}(\sigma_{RA_2}\sigma_R \otimes \sigma_{A_2}) + \operatorname{tr}(\sigma_R^2)\operatorname{tr}(\sigma_{A_2}^2)$$

We evaluate each term using the replica trick. For the first term, introduce a second copy ψ' and write:

$$\operatorname{tr}(\sigma_{RA_2}^2) = \operatorname{tr}\left[\sigma_{RA_2} \otimes \sigma'_{R'A'_2} F_{A_2} F_R\right]$$

Here F_{A_2} and F_R are the swap operators on A_2, A'_2 and R, R' respectively.

This reduces to:

$$\operatorname{tr}\left[(U \otimes U)(\psi_{RA} \otimes \psi_{R'A'})(U^\dagger \otimes U^\dagger)(F_{A_2} \otimes F_R)\right]$$

and the Haar integral:

$$\mathbb{E}_U[U^{\otimes 2} X U^{\dagger \otimes 2}] = \Pi_{\text{sym}}(X) \in \operatorname{span}\{I, F\}$$

projects onto the symmetric subspace. We expand this into:

$$\alpha_+ \Pi_+ + \alpha_- \Pi_-$$

where $\Pi_\pm = \frac{1}{2}(I \pm F)$ are symmetric/antisymmetric projectors. The coefficients are:

$$\alpha_\pm = \frac{\operatorname{tr}(\Pi_\pm F_{A_2})}{\operatorname{tr}(\Pi_\pm)} = \frac{\operatorname{tr}(F_{A_2}) \pm \operatorname{tr}(F_A F_{A_2})}{d_A^2 \pm d_A}$$

One finds:

$$\mathbb{E}_U \operatorname{tr}(\sigma_{RA_2}^2) = \frac{1}{d_{A_1}} \left(\operatorname{tr}(\psi_{RA}^2) + \operatorname{tr}(\psi_R^2) \operatorname{tr}(\psi_A^2)\right)$$

We now compute the remaining two terms:

$$\mathbb{E}_U \operatorname{tr}(\sigma_{RA_2} \sigma_R \otimes \sigma_{A_2}) = \frac{1}{d_{A_1}} \left(\operatorname{tr}(\psi_R^2) + \operatorname{tr}(\psi_A^2) \operatorname{tr}(\psi_R^2)\right)$$

$$\mathbb{E}_U \operatorname{tr}(\sigma_R^2) \operatorname{tr}(\sigma_{A_2}^2) = \operatorname{tr}(\psi_R^2) \cdot \left(\frac{1}{d_{A_1}} + \frac{\operatorname{tr}(\psi_A^2)}{d_{A_1}}\right)$$

Substituting and simplifying:

$$\mathbb{E}_U \left\|\sigma_{RA_2} - \sigma_R \otimes \sigma_{A_2}\right\|_1 \leq \sqrt{\frac{d_R d_{A_2}}{d_{A_1}}} \left(\sqrt{\operatorname{tr}(\psi_{RA}^2)} + \sqrt{\operatorname{tr}(\psi_R^2) \operatorname{tr}(\psi_A^2)}\right)$$

This upper bound shows that the decoupling error decays as d_{A_1} grows, provided ψ_{RA} has low purity.

We now apply the decoupling bound to the i.i.d. setting. Let ρ_{AB} be a bipartite state and $|\phi\rangle_{RAB}$ a purification. Consider $\psi = \phi^{\otimes n}$. To avoid unnecessarily large dimensions from unused subspaces, we first restrict to the typical subspace.

Let Π_A, Π_R, and Π_{AB} be the typical projectors for the corresponding reduced density matrices of ϕ. Define:

$$\tilde{\psi}_{R^n A^n B^n} = \frac{(\Pi_R \otimes \Pi_A \otimes \Pi_B)\psi(\Pi_R \otimes \Pi_A \otimes \Pi_B)}{\operatorname{tr}(\cdot)}$$

Then $\tilde{\psi}$ is supported on a space of dimension:

$$\dim \mathcal{H}_A = 2^{n(S(A)+\delta)}$$
$$\dim \mathcal{H}_R = 2^{n(S(AB)+\delta)}$$
$$\dim \mathcal{H}_{RA} = 2^{n(S(B)+\delta)}$$

by purity and standard typicality bounds. Also:

$$\mathrm{tr}(\psi_{RA}^2) \approx 2^{-nS(B)}$$
$$\mathrm{tr}(\psi_{R}^2) \approx 2^{-nS(AB)}$$
$$\mathrm{tr}(\psi_{A}^2) \approx 2^{-nS(A)}$$

Substituting into the trace norm bound:

$$\|\sigma_{RA_2} - \sigma_R \otimes \sigma_{A_2}\|_1 \leq \sqrt{\frac{2^{n(S(AB)+S(A)+2\delta)}}{2^{nR}}} \left(2^{-nS(B)/2} + 2^{-n(S(AB)+S(A))/2}\right)$$

Combine exponents in the first term:

$$2^{n(S(AB)+S(A)-R+2\delta-\frac{1}{2}S(B))} = 2^{-n\left(\frac{R-S(AB)-S(A)-2\delta+\frac{1}{2}S(B)}{}\right)}$$

The dominant term in the parentheses is:

$$\frac{R-(S(AB)+S(A))}{2}$$

and since $I(R:A) = S(R) + S(A) - S(RA) = S(AB) + S(A) - S(B)$ by purity, we conclude:

$$\|\sigma_{RA_2} - \sigma_R \otimes \sigma_{A_2}\|_1 \leq 2^{-n\left(\frac{R-I(R:A)}{2} - o(1)\right)}$$

Thus, for any $\varepsilon > 0$, we can achieve trace distance at most ε if we set:

$$R \geq I(R:A) + 2\varepsilon'$$

which corresponds to sending $\frac{1}{2}I(R:A)$ qubits per copy. Since the communication cost is $\log d_{A_1}$, the required number of qubits sent by Alice is:

$$\boxed{\frac{1}{2}I(R:A)}$$

Entanglement Yield

Let $d_A = d_{A_1} d_{A_2}$. Then:

$$\log d_{A_2} = \log d_A - \log d_{A_1} = nS(A) - \frac{1}{2}nI(R:A)$$

Now recall that:

$$I(A:B) = S(A)+S(B)-S(AB) \quad \text{and} \quad I(R:A) = S(A)+S(R)-S(RA) = S(A)+S(AB)-S(B)$$

Subtracting:

$$I(A:B) = 2S(A) - I(R:A) \Rightarrow \log d_{A_2} = \frac{1}{2}nI(A:B)$$

Thus, Bob ends up entangled with Alice via A_2 and some ancilla $\tilde{B}$. They share $\frac{1}{2}I(A:B)$ EPR pairs.

Net Entanglement Cost and $S(A|B)$

If classical communication is free, then via teleportation, each ebit can be converted into one qubit of communication. Hence:

$$\text{Net cost} = \frac{1}{2}I(R:A) - \frac{1}{2}I(A:B)$$

We now simplify:

$$I(R:A)-I(A:B) = S(R)+S(A)-S(RA)-S(A)-S(B)+S(AB) = S(R)-S(B)+S(AB)-S(RA)$$

Using purity:

$$S(R) = S(AB), \quad S(RA) = S(B) \Rightarrow I(R:A) - I(A:B) = 2(S(AB) - S(B))$$

So the net cost is:

$$\text{Net cost} = \frac{1}{2}I(R:A) - \frac{1}{2}I(A:B) = S(AB) - S(B) = S(A|B)$$

This quantity can be negative. That is, merging can generate entanglement when $S(A|B) < 0$.

Summary

Quantum state merging allows Alice to send her share A of a state $|\psi\rangle_{RAB}$ to Bob while preserving entanglement with a reference R. The communication cost is $\frac{1}{2}I(R:A)$ qubits, and the entanglement yield is $\frac{1}{2}I(A:B)$ ebits. The net entanglement cost is:

$$\boxed{S(A|B)}$$

This operationally interprets the quantum conditional entropy as the cost of merging.