8.S372/18.S996 Quantum Information Science III	**Fall 2020**

Lecture 19: November 5, 2020

Lecturer: Aram Harrow — *Scribe: Shreya Vardhan, Yogeshwar Velingker*

19.1 Schur-Weyl Duality

Recall from the previous lecture that $(\mathbb{C}^d)^{\otimes n}$ can be decomposed into irreps of $U^d \times S_n$ as:

$$(\mathbb{C}^d)^{\otimes n} \simeq \oplus_{\lambda \in \mathrm{Par}(n,d)} \, Q_\lambda \otimes P_\lambda \tag{19.1}$$

where $\mathrm{Par}(n,d)$ is the set of partitions of n into d elements, each Q_λ is an irrep of V_d, and each P_λ is an irrep of S_n.

In particular, for the $n = 2$ case, we have two possible partitions $\lambda = (2, 0)$, represented by $\square\square$, and $\lambda = (1, 1)$, represented by $\begin{smallmatrix}\square\\\square\end{smallmatrix}$. Corresponding to these, we get two terms in (19.1):

$$(\mathbb{C}^d)^{\otimes 2} \simeq Q_{\square\square} \otimes P_{\square\square} \;\oplus\; Q_{\begin{smallmatrix}\square\\\square\end{smallmatrix}} \otimes P_{\begin{smallmatrix}\square\\\square\end{smallmatrix}} \tag{19.2}$$

where $Q_{\square\square}$ is the $d(d+1)/2$-dimensional symmetric representation of V_d, $P_{\square\square}$ is the 1-dimensional trivial representation of S_2, $Q_{\begin{smallmatrix}\square\\\square\end{smallmatrix}}$ is the $d(d-1)/2$-dimensional antisymmetric representation of V_d, $P_{\square\square}$ is the 1-dimensional sign representation of S_2.

19.2 Application to merging

Recall from the last lecture that as a consequence of (19.2),

$$\begin{aligned} \mathbb{E}_U \; (U \otimes U) \; X \; (U \otimes U)^\dagger &= \text{projection of X onto } (\mathrm{span}\{\Pi_{\mathrm{sym}}, \Pi_{\mathrm{anti}}\} = \mathrm{span}\{I, F\}) \\ &= \frac{\mathrm{Tr}[X\Pi_{\mathrm{sym}}]}{\mathrm{Tr}\Pi_{\mathrm{sym}}} \Pi_{\mathrm{sym}} + \frac{\mathrm{Tr}\,[X\Pi_{\mathrm{anti}}]}{\mathrm{Tr}\,\Pi_{\mathrm{anti}}} \Pi_{\mathrm{anti}} \end{aligned} \tag{19.1}$$

This tells us that $\mathbb{E} \; (U \otimes U) \; X \; (U \otimes U)^\dagger$ has a simple block-diagonal structure when written in terms of the symmetric and antisymmetric subspaces, and is proportional to the identity within each block.

We consider the particular case of $X = \psi \otimes \psi$, and consider the setup for decoupling, shown in figure 19.1.

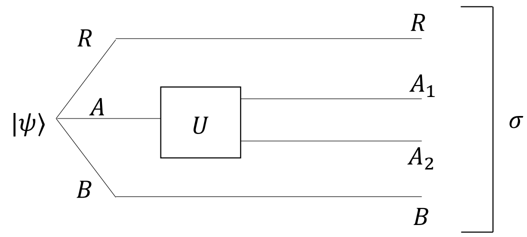

Figure 19.1: Setup for decoupling

Decoupling implies that $\sigma^{A_2R} \approx \sigma^{A_2} \otimes \sigma^R$. Let us see this by first looking at the distance in the Schatten 2-norm, which is mathematically easier to work with despite being less useful operationally:

$$\begin{aligned} &\mathbb{E}_U||\sigma_{A_2R} - \sigma_{A_2} \otimes \sigma_R||_2^2 \\ &= \mathbb{E}_U[\mathrm{tr}\sigma_{A_2R}^2 - 2\mathrm{tr}(\sigma_{A_2R}\sigma_{A_2} \otimes \sigma_R) + \mathrm{tr}\sigma_{A_2}^2\mathrm{tr}\sigma_R^2] \end{aligned} \tag{19.2}$$

Let us now compute each of the terms in (19.2). The first term can be evaluated as follows:

$$\begin{aligned} \mathbb{E}\mathrm{tr}\sigma_{A_2R}^2 &= \mathbb{E}\mathrm{tr}(\sigma_{A_2R} \otimes \sigma_{A_2'R'})F^{A_2R} \\ &= \mathrm{tr}[\psi_{AR} \otimes \psi_{A'R'}\mathbb{E}(U^\dagger \otimes U^\dagger)F^{A_2R}(U \otimes U)] \end{aligned} \tag{19.3}$$

where for instance A' refers to a copy of the system A, and F_B for any subsystem B refers to the swap operator on two copies of B. F has a non-trivial evolution only in A_2, so we find

$$\mathbb{E}(U^\dagger \otimes U^\dagger)F^{A_2}(U \otimes U) = \alpha_+ \frac{\Pi_+}{\mathrm{Tr}[\Pi_+]} + \alpha_- \frac{\Pi_-}{\mathrm{Tr}[\Pi_-]}, \quad \Pi_\pm = \frac{I \pm F}{2} \tag{19.4}$$

where

$$\alpha_\pm = \mathrm{tr}[\Pi_\pm F^{A_2}] = \mathrm{tr}[\frac{I \pm F^{A_1}F^{A_2}}{2} F^{A_2}] = \mathrm{tr}\frac{[F^{A_2} \pm F^{A_1}]}{2} \tag{19.5}$$

so that

$$\begin{aligned} \mathbb{E}_{U_{A_1A_2}}(U^\dagger \otimes U^\dagger)F^{A_2}(U \otimes U) &= \frac{d_{A_1} + d_{A_2}}{d_A + 1}\Pi_+ + \frac{d_{A_1} - d_{A_2}}{d_A - 1}\Pi_- \\ &\equiv p\ \Pi_+ + q\ \Pi_- \\ &= \frac{p+q}{2}I + \frac{p-q}{2}F^A \end{aligned} \tag{19.6}$$

So overall,

$$\begin{aligned} \mathbb{E}\ \mathrm{tr}[\sigma_{A_2R}^2] &= \mathrm{tr}[(\psi_{AR} \otimes \psi_{A'R'})(\frac{p+q}{2}I + \frac{p-q}{2}F^A)F^R \\ &= \frac{p+q}{2}\mathrm{tr}\psi_R^2 + \frac{p-q}{2}\mathrm{tr}\psi_{AR}^2 \end{aligned} \tag{19.7}$$

Note that

$$\frac{p+q}{2} \approx d_{A_2}^{-1}, \quad \frac{p-q}{2} \approx d_{A_1}^{-1} \tag{19.8}$$

The last term in (19.2) is

$$\mathbb{E}[\mathrm{tr}\sigma_{A_2}^2 \mathrm{tr}\sigma_R^2] = \mathbb{E}[\mathrm{tr}\,\sigma_{A_2}^2]\ \mathrm{tr}\,\psi_R^2, \tag{19.9}$$

where

$$\begin{aligned}\mathbb{E}\mathrm{tr}\sigma_{A_2}^2 &= \mathbb{E}\,\mathrm{tr}(U_A \otimes U_{A'})(\psi_A \otimes \psi_{A'})(U_A \otimes U_{A'})^\dagger F^{A_2} \\ &= \mathrm{tr}(\psi_A \otimes \psi_{A'})(\frac{p+q}{2} I + \frac{p-q}{2} F^A) \\ &= \frac{p+q}{2} + \frac{p-q}{2}\mathrm{tr}(\psi_A^2) \leq p = \frac{d_A + d_{A_2}}{d_{A_1} d_{A_2} + 1} \approx \frac{1}{d_{A_2}}\end{aligned} \tag{19.10}$$

if $d_{A_1} > d_{A_2}$. This suggests σ_{A_2} is close to the maximally mixed state if $d_{A_1} > d_{A_2}$.

$$\begin{aligned}\mathbb{E}\,\mathrm{tr}\sigma_{A_2R}(\sigma_{A_2} \otimes \sigma_R) &= \mathbb{E}\,\mathrm{tr}(U_A \otimes U_{A'})(\psi_{AR})(U_A \otimes U_{A'})^\dagger F^{AR} \\ &= \mathrm{tr}(\psi_{AR} \otimes \psi_{A'} \otimes \psi_{R'})(\frac{p+q}{2} I + \frac{p-q}{2} F^A) F^R \\ &= \frac{p+q}{2}\mathrm{tr}\psi_R^2 + \frac{p-q}{2}\mathrm{tr}\psi_{AR}(\psi_A \otimes \psi_R)\end{aligned} \tag{19.11}$$

Putting all the terms together,

$$\mathbb{E}\,||\sigma_{A_2R_2} - \sigma_{A_2} \otimes \sigma_R||_2^2 = \frac{d_{A_1}(d_{A_2}^2 - 1)}{d_A^2 - 1}(\mathrm{tr}\psi_{AR}^2 - 2\mathrm{tr}\psi_{AR}(\psi_A \otimes \psi_R) + \mathrm{tr}\psi_A^2 \mathrm{tr}\psi_R^2) \tag{19.12}$$

Note that we have made no approximations so far, and this expression is exact. Moreover, we only used the fact that U is a “2-design.”

Let us now see how this can be used to obtain an upper bound on the distance in the Schatten 1-norm, which is more operationally useful. Note that for a $d \times d$ matrix X,

$$||X||_2 \leq ||X||_1 \leq \sqrt{d}\ ||X||_2 \tag{19.13}$$

The latter inequality can be shown using the Cauchy-Schwarz inequality. Due to the factor of $\sqrt{d}$, to get a non-trivial bound, we often need $||X||_2$ to be exponentially small in the number of degrees of freedom.

Since the unitary operator does not act on R,

$$\sigma_R = \psi_R \tag{19.14}$$

As warm-up, let us find an upper bound on the 1-norm distance between σ_2 and the maximally mixed state $\tau_{A_2} = \frac{I_{A_2}}{d_{A_2}}$.

$$\begin{aligned} ||\sigma_{A_2} - \tau_{A_2}||_1^2 &\leq d_{A_2}\,\mathbb{E}\,||\sigma_{A_2} - \tau_{A_2}||^2 \\ &= d_{A_2}\,\mathbb{E}(\mathrm{tr}\sigma_{A_2}^2 - \frac{1}{d_{A_2}}) \\ &= d_{A_2}(\frac{p+q}{2} + \frac{p-q}{2}\mathrm{tr}\psi_A^2) - 1 \\ &= \frac{d_{A_2}}{d_{A_1}}\mathrm{tr}\psi_A^2 \\ &\leq \text{small if } d_{A_1} \gg d_{A_2} \end{aligned} \tag{19.15}$$

Similarly, the trace distance between σ_{A_2R} and $\sigma_{A_2} \otimes \sigma_R$ is upper-bounded by

$$\begin{aligned} \mathbb{E}\,||\sigma_{A_2R} - \sigma_{A_2} \otimes \sigma_R||_1^2 &\leq d_{A_2}d_R\,\mathbb{E}\,||\sigma_{A_2R} - \sigma_{A_2} \otimes \sigma_R||_2^2 \\ &\leq \frac{d_{A_2}d_R}{d_{A_1}}(\mathrm{tr}\psi_{AR}^2 + \mathrm{tr}\psi_A^2\ \mathrm{tr}\psi_R^2) \end{aligned} \tag{19.16}$$

Let us now try to estimate the sizes of the different terms in (19.16).

Let us now take n copies of our state. Take $|\psi\rangle$ to be a *typical purification* of $\rho_{AB}^{\otimes n}$. Given a purification $|\phi\rangle_{ABR}$ of ρ_{AB}, $|\psi\rangle$ is defined as

$$|\psi\rangle = c(\Pi^n_{\phi_A,\delta} \otimes \Pi^n_{\phi_B,\delta} \otimes \Pi^n_{\phi_B,\delta})\,|\phi\rangle_{ABR}^{\otimes n} \tag{19.17}$$

Then

$$\begin{aligned} \mathrm{tr}\psi_A^2 &\approx \exp(-nS(A)_\phi) = \exp(-nS(A)_\rho) \\ \mathrm{tr}\psi_R^2 &\approx \exp(-nS(R)_\phi) = \exp(-nS(AB)_\rho) \\ \mathrm{tr}\psi_{AR}^2 &\approx \exp(-nS(AR)_\phi) = \exp(-nS(B)_\rho) \geq \mathrm{tr}\psi_A^2\ \mathrm{tr}\psi_R^2 \end{aligned} \tag{19.18}$$

This means the second term in (19.16) can be ignored. Further, we can estimate

$$d_R \approx \exp(nS(AB)_\rho), \quad d_A \approx \exp(nS(A)_\rho) \tag{19.19}$$

So (19.16) is small if

$$\frac{d_A d_R}{d_{A_1^2}}\mathrm{tr}\psi_{AR}^2 \ll 1 \Rightarrow \log d_{A_1} \gg \frac{1}{2}\log(d_A d_R \mathrm{tr}\psi_{AR}^2) \approx \frac{1}{2}nI(A:R) \tag{19.20}$$

Let us now apply this to merging. The key idea is that due to the decoupling between A_2 and R when A_1 consists of $\frac{1}{2}nI(A:R)$ qubits, the final state can be rotated to purify R and A_2 separately.

We now have a "fully quantum Slepian wolf" protocol, where $\frac{1}{2}I(A:R)[q \to q]$ is used, to produce $\frac{1}{2}I(A:B)[qq]$.

Let us translate the bound obtained above for the trace distance to a bound on fidelity:

$$\frac{1}{2}||\sigma_{A_2R} - \sigma_{A_2} \otimes \sigma_R||_1 \leq \epsilon \Rightarrow F(\sigma_{A_2R}, \sigma_{A_2} \otimes \sigma_R) \geq 1 - \epsilon \tag{19.21}$$

We know that σ_{A_2R} is purified by $U_{A\to A_1A_2}\,|\psi\rangle_{ABR}$, while $\sigma_{A_2} \otimes \sigma_R$ can be purified by $|\Phi\rangle_{A_2\tilde{B}} \otimes |\psi\rangle_{B_AB_BR}$. By Uhlmann's theorem, this implies that there exists a unitary acting on the complement of A_2R, $V_{A_1}B \to \tilde{B}B_AB_B$, that achieves this fidelity.

Implications of this discussion for relations between various protocols and resource inequalities in quant-ph/0606225:

Let us first try to express the Fully Quantum Slepian Wolf(FQSW)/ merging protocol as a resource inequality. Suppose we have an isometry W from a source S to AB. We denote with $\langle W_{S\to AB} : \psi_S\rangle$ the ability to produce the state ρ_{AB} when the state on the source if ψ_S. Then we have

$$\langle W_{S\to AB} : \psi_S\rangle + \frac{1}{2}I(A:R)[q \to q] \geq \langle W_{S\to B_AB_B} : \psi_S\rangle + \frac{1}{2}I(A:B)[qq] \tag{19.22}$$

Using teleportation, we can equivalently write

$$\langle W_{S\to AB} : \psi_S\rangle + S(A|B)[q \to q] + I(A:B)[c \to c] \geq \langle W_{S\to B_AB_B} : \psi_S\rangle \tag{19.23}$$

Let us now run this protocol backwards. This gives us the FQRS, or the fully quantum reverse shannon protocol. While FQSW sends $\rho_{AB} \to \omega_{B'}$ where $B' = B_AB_B$, FQRS sends $\omega_{B'} \to \rho_{AB} = \mathcal{N}_{B'\to AB}(\omega)$, where $\mathcal{N}_{B'\to AB}$ is a channel from Bob (B') to Alice(A), where Alice keeps the environment. This can be seen as a protocol for *state splitting*,

$$\frac{1}{2}I(A:R)[q \leftarrow q] + \frac{1}{2}I(A:B)[qq] \geq \langle N_{B'\to AB} : \omega_B\rangle \tag{19.24}$$

Renaming the various parties, this can be written in a more standard form:

$$\frac{1}{2}I(A:B)[q \to q] + \frac{1}{2}I(B:E)[qq] \geq \langle N_{A'\to BE_A} : \omega_{A'}\rangle \tag{19.25}$$

Now recall the father protocol

$$\langle \mathcal{N}_{A'\to B} : \omega_{A'}\rangle + \frac{1}{2}I(A:E)[qq] \geq \frac{1}{2}I(A:B)[q \to q] \tag{19.26}$$

What if Alice keeps the environment? Then we have a channel $\mathcal{N}_{A'\to BE_A}$. Bob has purification, so $S(E)[qq]$ can be recovered. Net entanglement is

$$S(E) - \frac{1}{2}I(A:E) = \frac{1}{2}I(B:E) \tag{19.27}$$

$$\langle N_{A'\to BE_A} : \omega_{A'}\rangle = \frac{1}{2}I(A:B)[q \to q] + \frac{1}{2}I(B:E)[qq] \tag{19.28}$$

Shown in Devetak, quant-ph/0505138.

19.3 Merging and quantum error correction

Suppose we have a state with a ebits between Alice and Rebecca, and b ebits between Alice and Bob.

$$|\psi\rangle = |\phi\rangle_{A_1 R}^{\otimes a} |\phi\rangle_{A_2 B}^{\otimes b} \tag{19.1}$$

Merging requires a qubits from A to B, or b qubits from $A \to R$. Both tasks are quite trivial, and can be accomplished by simply handing over the right qubits to Bob or Rebecca.

If instead we use a Haar-random unitary to accomplish this task, then we can use *any* $a + \delta$ qubits sent or $b + \delta$ qubits sent to R. But now, the *same* unitary works for both receivers, and it does not matter which qubits are sent to B or R.

Conversely if Bob gets $a - \delta$ qubits, he is decoupled, or if Rebecca gets $b - \delta$ then she is decoupled, and the merging task cannot be accomplished.

Similar to a quantum error-correcting code.

Applications: Hayden and Preskill, "Black holes as mirrors" 0708.4025. Throw in one qubit. Can we recover it from the Hawking radiation?