Existence of an n-Copy Quantum Purification Channel: A Structured Proof

Theorem 1 (Existence of n-Copy Purification Channel)**.** *Let $\mathcal{H}_A$ be a finite-dimensional Hilbert space with $\dim(\mathcal{H}_A) = d < \infty$, and let $\mathcal{H}_B \cong \mathcal{H}_A$. For any integer $n \geq 1$, there exists a quantum channel $\Lambda_{\mathrm{purify}}^{(n)} : \mathcal{L}(\mathcal{H}_A^{\otimes n}) \to \mathcal{L}((\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n})$ such that for any density operator $\rho_A \in \mathcal{D}(\mathcal{H}_A)$:*

$$\Lambda_{\mathrm{purify}}^{(n)}(\rho_A^{\otimes n}) = \left[\mathbb{E}_U \left[(\mathrm{id}_A \otimes U_B) \left| \psi_\rho \right\rangle \left\langle \psi_\rho \right|_{AB} (\mathrm{id}_A \otimes U_B^\dagger) \right] \right]^{\otimes n}$$

where $\left| \psi_\rho \right\rangle_{AB}$ is the canonical purification $\left| \psi_\rho \right\rangle = (\sqrt{\rho} \otimes I) \left| \Omega \right\rangle$ with maximally entangled state $\left| \Omega \right\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d \left| i \right\rangle_A \left| i \right\rangle_B$, and $\mathbb{E}_U$ denotes the expectation over the Haar measure on the unitary group $U(d)$.

Assumptions.

A1: $\dim(\mathcal{H}_A) = d < \infty$.

A2: $\mathcal{H}_B \cong \mathcal{H}_A$.

A3: $n \geq 1$.

External Results.

E1. *Schur–Weyl Duality* [1]: For a representation of $U(d)$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ via $U \mapsto I_A \otimes U_B$, the commutant is $\mathcal{L}(\mathcal{H}_A) \otimes \mathbb{C} \cdot I_B$.

Proof.$\langle 1 \rangle 1$. **Purification Existence.** Every density operator $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ admits a purification $\left| \psi \right\rangle_{AB} \in \mathcal{H}_A \otimes \mathcal{H}_B$. *(Standard result; A1, A2)*

$\langle 1 \rangle 2$. **Canonical Purification.** Define $\left| \psi_\rho \right\rangle = (\sqrt{\rho} \otimes I) \left| \Omega \right\rangle$ where $\left| \Omega \right\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d \left| i \right\rangle_A \left| i \right\rangle_B$. *(Construction; A1, A2)*

$\qquad \langle 2 \rangle 1$. Let $\{ \left| i \right\rangle \}_{i=1}^d$ be an orthonormal basis for $\mathcal{H}_A \cong \mathcal{H}_B$.

$\qquad \langle 2 \rangle 2$. Define the maximally entangled state $\left| \Omega \right\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^d \left| i \right\rangle_A \left| i \right\rangle_B$.

$\qquad \langle 2 \rangle 3$. Set $\left| \psi_\rho \right\rangle = (\sqrt{\rho} \otimes I) \left| \Omega \right\rangle$.

$\qquad \langle 2 \rangle 4$. Verify $\mathrm{Tr}_B(\left| \psi_\rho \right\rangle \left\langle \psi_\rho \right|) = \rho_A$:

$\qquad \qquad \langle 3 \rangle 1$. $\mathrm{Tr}_B((\sqrt{\rho} \otimes I) \left| \Omega \right\rangle \left\langle \Omega \right| (\sqrt{\rho} \otimes I))$

$\qquad \qquad \langle 3 \rangle 2$. $= \sqrt{\rho} \left(\sum_i \left| i \right\rangle \left\langle i \right| \right) \sqrt{\rho}$ *(partial trace over B)*

$\qquad \qquad \langle 3 \rangle 3$. $= \sqrt{\rho} \cdot I \cdot \sqrt{\rho} = \rho$. $\left(\sum_i \left| i \right\rangle \left\langle i \right| = I \right)$

$\langle 1 \rangle 3$. **Purification Uniqueness.** Any two purifications of ρ_A differ by a local unitary $I_A \otimes W$ on $\mathcal{H}_B$. *(Uhlmann's theorem; $\langle 1 \rangle 1$, $\langle 1 \rangle 2$)*

$\langle 2 \rangle$1. Let $|\psi\rangle_{AB}$ and $|\psi'\rangle_{AB}$ be purifications of ρ_A.

$\langle 2 \rangle$2. Write spectral decomposition $\rho = \sum_i \lambda_i |e_i\rangle \langle e_i|$.

$\langle 2 \rangle$3. Express $|\psi\rangle = \sum_i \sqrt{\lambda_i} |e_i\rangle_A |f_i\rangle_B$ and $|\psi'\rangle = \sum_i \sqrt{\lambda_i} |e_i\rangle_A |f_i'\rangle_B$.

$\langle 2 \rangle$4. There exists unitary W on $\mathcal{H}_B$ with $W |f_i\rangle = |f_i'\rangle$ for all i.

$\langle 2 \rangle$5. Hence $|\psi'\rangle = (I_A \otimes W) |\psi\rangle$.

$\langle 1 \rangle$4. **Haar Twirl Identity.** For any pure state $|\psi\rangle_{AB}$:

$$\mathbb{E}_U \left[(I_A \otimes U) |\psi\rangle \langle\psi| (I_A \otimes U^\dagger) \right] = \rho_A \otimes \frac{I_B}{d}$$

where $\rho_A = \mathrm{Tr}_B(|\psi\rangle \langle\psi|)$. *(Schur–Weyl; E1)*

$\langle 2 \rangle$1. Define $\mathcal{T}(\sigma) = \mathbb{E}_U[(I \otimes U)\sigma(I \otimes U^\dagger)]$ (the twirl map).

$\langle 2 \rangle$2. By Schur–Weyl duality (E1), the commutant of $\{I \otimes U : U \in U(d)\}$ is $\mathcal{L}(\mathcal{H}_A) \otimes \mathbb{C} \cdot I_B$.

$\langle 2 \rangle$3. Therefore $\mathcal{T}(|\psi\rangle \langle\psi|) = X_A \otimes I_B$ for some $X_A \in \mathcal{L}(\mathcal{H}_A)$.

$\langle 2 \rangle$4. The twirl map commutes with partial trace: $\mathrm{Tr}_B \circ \mathcal{T} = \mathrm{Tr}_B$.

$\langle 2 \rangle$5. Compute: $\mathrm{Tr}_B(X_A \otimes I_B) = d \cdot X_A$.

$\langle 2 \rangle$6. Also: $\mathrm{Tr}_B(|\psi\rangle \langle\psi|) = \rho_A$.

$\langle 2 \rangle$7. Hence $d \cdot X_A = \rho_A$, giving $X_A = \rho_A/d$.

$\langle 2 \rangle$8. Therefore $\mathcal{T}(|\psi\rangle \langle\psi|) = \rho_A \otimes I_B/d$.

$\langle 1 \rangle$5. **Single-Copy Purification Map.** Define $P : \mathcal{D}(\mathcal{H}_A) \to \{\text{pure states on } \mathcal{H}_A \otimes \mathcal{H}_B\}$ by $P(\rho) = |\psi_\rho\rangle \langle\psi_\rho|$. *($\langle 1 \rangle$2)*

$\langle 1 \rangle$6. **Single-Copy Channel Definition.** Define $\Lambda : \mathcal{L}(\mathcal{H}_A) \to \mathcal{L}(\mathcal{H}_A \otimes \mathcal{H}_B)$ by:

$$\Lambda(\rho) = \rho_A \otimes \frac{I_B}{d}$$

($\langle 1 \rangle$4)

$\langle 1 \rangle$7. **Linear Extension.** Λ extends linearly to all of $\mathcal{L}(\mathcal{H}_A)$. *(linearity of tensor product)*

$\langle 1 \rangle$8. **Λ is Completely Positive (CP).** *(Kraus representation)*

$\langle 2 \rangle$1. Write $\Lambda(\rho) = \rho \otimes I_B/d$.

$\langle 2 \rangle$2. Define Kraus operators $K_i = \frac{1}{\sqrt{d}} |i\rangle_B$ for $i = 1, \dots, d$.

$\langle 2 \rangle$3. Then $\Lambda(\rho) = \sum_i (I_A \otimes K_i)\rho(I_A \otimes K_i^\dagger)$.

$\langle 2 \rangle$4. Kraus representation implies complete positivity.

$\langle 1 \rangle$9. **Λ is Trace-Preserving (TP).** *(direct computation)*

$\langle 2 \rangle$1. $\mathrm{Tr}(\Lambda(\rho)) = \mathrm{Tr}(\rho_A \otimes I_B/d) = \mathrm{Tr}(\rho_A) \cdot \mathrm{Tr}(I_B/d)$.

$\langle 2 \rangle$2. $= \mathrm{Tr}(\rho_A) \cdot 1 = \mathrm{Tr}(\rho_A)$.

$\langle 2 \rangle$3. For $\rho \in \mathcal{D}(\mathcal{H}_A)$, $\mathrm{Tr}(\rho_A) = 1$, so $\mathrm{Tr}(\Lambda(\rho)) = 1$.

$\langle 1 \rangle$10. **Λ is CPTP.** Λ is a valid quantum channel. *($\langle 1 \rangle$8, $\langle 1 \rangle$9)*

$\langle 1 \rangle$11. **Output Equals Twirled Purification.** For any purification $|\psi\rangle$ of ρ:

$$\Lambda(\rho) = \mathbb{E}_U \left[(I_A \otimes U) |\psi\rangle \langle\psi| (I_A \otimes U^\dagger) \right]$$

$$(\langle 1 \rangle 4,\ \langle 1 \rangle 6)$$

$\langle 2 \rangle$1. By $\langle 1 \rangle 4$, the Haar twirl of any purification gives $\rho_A \otimes I_B/d$.

$\langle 2 \rangle$2. By $\langle 1 \rangle 6$, $\Lambda(\rho) = \rho_A \otimes I_B/d$.

$\langle 2 \rangle$3. Hence $\Lambda(\rho) = \mathbb{E}_U[(I \otimes U) |\psi\rangle \langle\psi| (I \otimes U^\dagger)]$.

$\langle 2 \rangle$4. **Haar Invariance:** For $|\psi'\rangle = (I \otimes W) |\psi\rangle$:

$\langle 3 \rangle$1. $\mathbb{E}_U[(I \otimes U) |\psi'\rangle \langle\psi'| (I \otimes U^\dagger)]$

$\langle 3 \rangle$2. $= \mathbb{E}_U[(I \otimes UW) |\psi\rangle \langle\psi| (I \otimes W^\dagger U^\dagger)]$

$\langle 3 \rangle$3. $= \mathbb{E}_U[(I \otimes V) |\psi\rangle \langle\psi| (I \otimes V^\dagger)]$ *(right-invariance: $V = UW$)*

$\langle 3 \rangle$4. Result is independent of purification choice.

$\langle 1 \rangle$12. **Output Independent of Purification.** The Haar twirl gives the same result for any purification of ρ.   *($\langle 1 \rangle 3$, $\langle 1 \rangle 11$)*

$\langle 1 \rangle$13. **n-Copy Channel Definition.** Define $\Lambda^{(n)} = \Lambda^{\otimes n}$:

$$\Lambda^{(n)} : \mathcal{L}(\mathcal{H}_A^{\otimes n}) \to \mathcal{L}((\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n})$$

$$(A3)$$

$\langle 1 \rangle$14. $\Lambda^{(n)}$ **is CPTP.**   *(tensor product of CPTP maps)*

$\langle 2 \rangle$1. Λ is CPTP by $\langle 1 \rangle 10$.

$\langle 2 \rangle$2. The tensor product of CPTP maps is CPTP.

$\langle 2 \rangle$3. Hence $\Lambda^{(n)} = \Lambda^{\otimes n}$ is CPTP.

$\langle 1 \rangle$15. **Final Result.**

$$\Lambda^{(n)}(\rho^{\otimes n}) = \left[\mathbb{E}_U \left[(I_A \otimes U) |\psi_\rho\rangle \langle\psi_\rho| (I_A \otimes U^\dagger) \right] \right]^{\otimes n}$$

$$(\langle 1 \rangle 11,\ \langle 1 \rangle 13,\ \langle 1 \rangle 14)$$

$\langle 2 \rangle$1. By definition, $\Lambda^{(n)}(\rho^{\otimes n}) = \Lambda(\rho)^{\otimes n}$.

$\langle 2 \rangle$2. By $\langle 1 \rangle 11$, $\Lambda(\rho) = \mathbb{E}_U[(I \otimes U) |\psi_\rho\rangle \langle\psi_\rho| (I \otimes U^\dagger)]$.

$\langle 2 \rangle$3. Substituting: $\Lambda^{(n)}(\rho^{\otimes n}) = \left[\mathbb{E}_U[(I \otimes U) |\psi_\rho\rangle \langle\psi_\rho| (I \otimes U^\dagger)] \right]^{\otimes n}$.

$\langle 2 \rangle$4. This completes the proof. $\square$

References

[1] W. Fulton and J. Harris, *Representation Theory: A First Course*, Graduate Texts in Mathematics, vol. 129, Springer-Verlag, New York, 1991.