Proving result 1: Using 0702005 Thm III

Let: (1) ρ^{SE} max mixed on S

(2) $P^{S\to R}$ proj onto subspace $R \subseteq S$

(3) $\psi_U^{RE} := \frac{|S|}{|R|} (PU)^S \otimes I^E \; \rho^{SE} \, (U^\dagger P)^S \otimes I^E$

Then: (1) $\left\| \psi_U^{RE} - \frac{I_R}{|R|} \otimes \psi^E \right\|_2^2 = \mathrm{Tr}\left(\psi_U^{RE}\right)^2 - \frac{1}{|R|}\mathrm{Tr}\left(\psi^E\right)^2$

indep of U

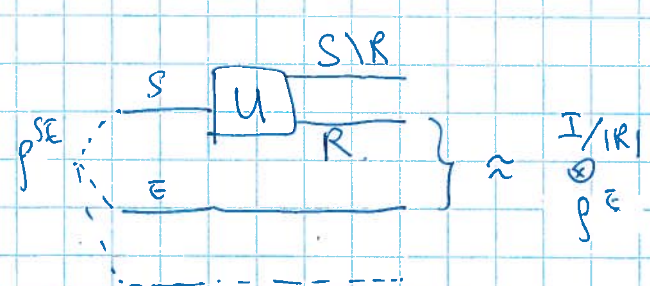
(2) $\int dU \left\| \psi_U^{RE} - \frac{I_R}{|R|} \otimes \psi^E \right\|_2^2 \leq \mathrm{tr}\left(\rho^{SE}\right)^2$

(3) $\int dU \left\| \psi_U^{RE} - \frac{I_R}{|R|} \otimes \psi^E \right\|_1^2 \leq |RE| \, \mathrm{tr}\left(\rho^{SE}\right)^2$.

Conclusion (1) $\leftrightarrow$ Eq (9) in ArXiv version

(2) $\leftrightarrow$ Eq before Eq (19).

(3) $\leftrightarrow$ Eq (19)



A useful lemma:

$$\mathrm{tr}_2\left(M_{12}\cdot\left(A_1 \otimes I_2\right)\right) = \left[\mathrm{tr}_2\left(M_{12}\right)\right]\cdot A_1$$

Pf: Since operators of the form $M_{12} = M_1 \otimes M_2$ form a basis, it suffices to prove lemma for them.

$$\text{LHS} = \mathrm{tr}_2\left(M_1 A_1 \otimes M_2\right) = M_1 A_1 \,\mathrm{tr}(M_2).$$

$$\text{RHS} = \left[\mathrm{tr}_2\left(M_1 \otimes M_2\right)\right]\cdot A_1 = M_1 \cdot A_1 \,\mathrm{tr}(M_2).$$

A useful corollary:

$$\mathrm{tr}_{(12)}\left(M_{12}\cdot\left(A_1 \otimes I_2\right)\right) = \mathrm{tr}_{(1)}\left[\left(\mathrm{tr}_2\left(M_{12}\right)\right) A_1\right]$$

Deriving 0702005 Thm III :

First note that Ψ_U^{RE} in assumption ③ is an exact state because of assumption ① :

Pf:

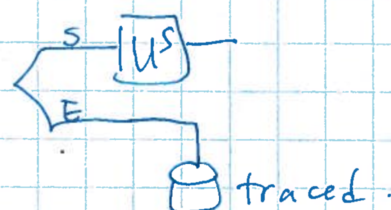
cyclic property of Tr and $P^2 = P$.

$$\mathrm{tr}\,\Psi_U^{RE} = \frac{|S|}{|R|}\,\mathrm{Tr}_{SE}\left[\left(U^S \otimes I^E\, \rho^{SE}\, U^{S\dagger} \otimes I^E\right)\left(P^S \otimes I^E\right)\right]$$

Cor with
$E \leftrightarrow 2$
$S \leftrightarrow 1$

$$= \frac{|S|}{|R|}\,\mathrm{Tr}_{(S)}\left[\underbrace{\left(\mathrm{tr}_E\left(U^S \otimes I^E\, \rho^{SE}\, U^{S\dagger} \otimes I^E\right)\right)} \cdot P^S\right]$$

But $\mathrm{Tr}_E\left(U^S \otimes I^E\, \rho^{SE}\, U^{S\dagger} \otimes I^E\right) = \mathrm{Tr}_E\, \rho^{SE} \overset{\text{by assumption ①.}}{=} \frac{I_S}{|S|}$

[∵ ρ_{SE} 

and $\boxed{U^S}$ & trace E commute].

$$\therefore\ \mathrm{tr}\,\Psi_U^{RE} = \frac{|S|}{|R|}\,\mathrm{Tr}_S\, \frac{I^S}{|S|} \cdot P^S = \frac{|S|}{|R|}\,\frac{\mathrm{rank}\,(P^S)}{|S|} = 1.$$

Second, prove conclusion ①:

For any state ψ^{RE} on RE :

$$\left\| \psi^{RE} - \frac{I^R}{|R|} \otimes \psi^E \right\|_2^2$$

$$= \mathrm{tr}\left[\left(\psi^{RE} - \frac{I^R}{|R|} \otimes \psi^E\right)\left(\psi^{RE} - \frac{I^R}{|R|} \otimes \psi^E\right)\right]$$

$$= \mathrm{tr}\left[\left(\psi^{RE}\right)^2\right] - 2\,\mathrm{tr}\left[\psi^{RE} \cdot \left(\frac{I^R}{|R|} \otimes \psi^E\right)\right] + \mathrm{tr}\left[\left(\frac{I^R}{|R|} \otimes \psi^E\right)^2\right]$$

$$= \mathrm{tr}\left[\left(\psi^{RE}\right)^2\right] \underbrace{- 2\,\mathrm{tr}_E\left(\psi^E \cdot \psi^E\right)\frac{1}{|R|}}_{\text{by Cor, } 2 \leftrightarrow R,\ 1 \leftrightarrow E \text{ and } \psi^{RE} \text{ state.}} + \frac{1}{|R|} \cdot \mathrm{tr}\left[\left(\psi^E\right)^2\right].$$

$$= \mathrm{tr}\left[\left(\psi^{RE}\right)^2\right] - \frac{1}{|R|}\,\mathrm{tr}\left[\left(\psi^E\right)^2\right].$$

So, in particular, it applies to ψ_u^{RE} in 0702005 Thm III

Proving conclusion ②:

ⓐ $\int du \left\| \psi_u^{RE} - \frac{I_R}{|R|} \otimes \psi^E \right\|_2^2$

$= \int du \, tr\left[(\psi_u^{RE})^2\right] - \int du \frac{1}{|R|} \underbrace{Tr\left[(\psi^E)^2\right]}_{\text{indep of } u \text{ which acts on } S}$. by conclusion ①.

$= \left[\int du \, tr\left[(\psi_u^{RE})^2\right]\right] - \frac{1}{|R|} tr\left[(\psi^E)^2\right]$.

ⓑ "The SWAP lemma":

Let $F = \sum_{ij} |ij\rangle\langle ji|$. [it swaps the state in the 2 sys $F|ij\rangle = |ji\rangle$]

$A = \sum_{ij} |i\rangle\underbrace{\langle i| A |j\rangle}_{A_{ij}}\langle j| = \sum_{ij} A_{ij} |i\rangle\langle j|$. square matrix on 1 sys.

Then. $Tr\, A^\dagger A = Tr\,(A^\dagger \otimes A \cdot F)$

Pf: $Tr\,(A^\dagger \otimes A \; F) = tr\left(A^\dagger \otimes A \sum_{ij} |ij\rangle\langle ji|\right)$.

$= \sum_{ij} \langle j| A^\dagger |i\rangle \langle i| A |j\rangle$

$= \sum_{ij} (A^\dagger)_{ji} \cdot A_{ij} = \sum_{ij} |A_{ij}|^2 = tr(A^\dagger A)$.

(c). $\int du \ \mathrm{tr}\left[\left(\varphi_u^{RE}\right)^2\right]$.

$$= \int du \ \mathrm{tr}\left[\varphi_u^{RE} \otimes \varphi_u^{\tilde R \tilde E} \cdot F^{RE \leftrightarrow \tilde R \tilde E}\right] \qquad \text{by SWAP lemma}$$

$$= \left(\frac{|S|}{|R|}\right)^2 \underbrace{\int du}_{\text{over } S} \mathrm{tr}\left[\begin{pmatrix} \left[(PU)^S \otimes I^E \ \ \rho^{SE} \ \ (U^\dagger P)^S \otimes I^E\right] \\ \otimes \\ \left[(PU)^{\tilde S} \otimes I^{\tilde E} \ \ \rho^{\tilde S \tilde E} \ \ (U^\dagger P)^{\tilde S} \otimes I^{\tilde E}\right] \end{pmatrix} \cdot \begin{pmatrix} F^{R\tilde R} \\ \otimes \\ F^{E\tilde E} \end{pmatrix}\right]$$

Cyclic prop of trace

$$= \left(\frac{|S|}{|R|}\right)^2 \int du \ \mathrm{tr}\left[\rho^{SE} \otimes \rho^{\tilde S \tilde E} \times \left[\begin{matrix} (U^\dagger P)^S \otimes (U^\dagger P)^{\tilde S} \ F^{R\tilde R} \ (PU)^S \otimes (PU)^{\tilde S} \\ \otimes \ F^{E\tilde E} \end{matrix}\right]\right]$$

$$= \left(\frac{|S|}{|R|}\right)^2 \mathrm{tr}\left(\rho^{SE} \otimes \rho^{\tilde S \tilde E}\right) \times \left(G^{S\tilde S} \otimes F^{E\tilde E}\right)$$

where $G^{S\tilde S} = \int du \ (U^\dagger P)^S \otimes (U^\dagger P)^{\tilde S} \ F^{R\tilde R} \ (PU)^S \otimes (PU)^{\tilde S}$.

$$U^\dagger P : \ |S| \overset{|R|}{\boxed{\ \diagup\ }} \ , \qquad F^{R\tilde R} : \ \overset{|R|^2}{\boxed{\qquad}} \ |R|^2$$

rectangular

Setup:

- Let V be the VS of bdd lin ops on $S\tilde{S}$ with inner product $\langle A, B\rangle = \mathrm{tr}(A^{+}B)$.
- Since $I^{S\tilde{S}}$ & $F^{S\tilde{S}} \in V$ are lin indep, define V' as ortho complemt of span $\{I^{S\hat{S}}, F^{S\hat{S}}\}$ in V.
- Pick an o.n basis for V', add $I^{S\hat{S}}$ & $F^{S\hat{S}}$ to make a basis for V
- Then, any $M \in V$ can be written as

$$M = aI + bF + Q \qquad \text{where} \quad Q \in V'$$

$$a = \frac{|S|\,\mathrm{tr}(M) - \mathrm{tr}(MF)}{|S|^3 - |S|}$$

$$b = \frac{|S|\,\mathrm{tr}(MF) - \mathrm{tr}(M)}{|S|^3 - |S|}$$

Pf: Consider $\mathrm{tr}(M) = a|S|^2 + b|S|$ $\left(\because \mathrm{tr}\, I = |S|^2, \ \mathrm{tr}\, F = |S|,\ \mathrm{tr}\, Q = 0\right)$

$\mathrm{tr}(MF) = a|S| + b|S|^2$ $\left(\because F^2 = I,\ \mathrm{tr}(QF) = 0\right)$

Solving for a, b gives the above.

The twirling lemma:

$$\forall M \in V, \quad \int dU \; U \otimes U \, M \, U^\dagger \otimes U^\dagger = a I^{SS'} + b F^{SS'}.$$

- This uses the fact the LHS projects M onto span$\{I, F\}$, and leaves I, F invariant.

- dU denotes the Haar meas.
- dU can be replaced by "any unitary 2 designs." which satisfies: $\forall M \in V$, $\int dU \; U \otimes U \, M \, U^\dagger \otimes U^\dagger = \sum_k p(k) \, U_k \otimes U_k \, M \, U_k^\dagger \otimes U_k^\dagger$

(d) $$G^{S\tilde{S}} = \int du \, (U^\dagger P)^S \otimes (U^\dagger P)^{\tilde{S}} \; F^{R\tilde{R}} \; (PU)^S \otimes (PU)^{\tilde{S}}$$

$$= \int du \; U^{\dagger S} \otimes U^{\dagger \tilde{S}} \; \underbrace{P^S \otimes P^{\tilde{S}} \; F^{R\tilde{R}} \; P^S \otimes P^{\tilde{S}}}_{\substack{\text{SWAP on } R\tilde{R}. \\ \text{"0" else where in } S\tilde{S}.}} \; U^S \otimes U^{\tilde{S}}$$

Applying the twirling lemma to $M = P^S \otimes P^{\tilde{S}} \; F^{R\tilde{R}} \; P^S \otimes P^{\tilde{S}}$:

$$\operatorname{tr} M = |R|$$

$$\operatorname{tr}\big(\underbrace{F^{S\tilde{S}} \; M}_{I^{R\tilde{R}}, \text{ 0's else where}}\big) = |R|^2$$

$$\therefore G^{S\tilde{S}} = a \, I^{S\tilde{S}} + b \, F^{S\tilde{S}}$$

where $$a = \frac{|S|\,|R| - |R|^2}{|S|^3 - |S|} = \frac{|R|}{|S|^2}\left(\frac{1 - \frac{|R|}{|S|}}{1 - \frac{1}{|S|^2}}\right)$$

$$b = \frac{|S|\,|R|^2 - |R|}{|S|^3 - |S|} = \frac{|R|^2}{|S|^2}\left(\frac{1 - \frac{1}{|R|\,|S|}}{1 - \frac{1}{|S|^2}}\right)$$

3.9

(e) $\int du \, \mathrm{tr}\left[\left(\psi_u^{RE}\right)^2\right]$

$$= \frac{|S|^2}{|R|^2} \mathrm{tr}\left[\left(\rho^{SE} \otimes \rho^{\tilde{S}\tilde{E}}\right)\right]\left[\left(a I^{S\tilde{S}} + b F^{S\tilde{S}}\right) \otimes F^{E\tilde{E}}\right]$$

$$= \frac{|S|^2}{|R|^2} \; a \left\{ \mathrm{tr}_{(E\tilde{E})} \left[\mathrm{tr}_{S\tilde{S}} \left(\rho^{SE} \otimes \rho^{\tilde{S}\tilde{E}}\right)\right] \cdot F^{E\tilde{E}} \right\}$$

$$+ \frac{|S|^2}{|R|^2} \; b. \left\{ \mathrm{tr} \left(\rho^{SE} \otimes \rho^{\tilde{S}\tilde{E}}\right) \left(F^{SE \leftrightarrow \tilde{S}\tilde{E}} \right) \right\}$$

$$= \frac{|S|^2}{|R|^2} \left\{ a \; \mathrm{tr}_{(E\tilde{E})} \left(\rho^{E} \otimes \rho^{\tilde{E}}\right) \cdot \left(F^{E\tilde{E}}\right) + b \; \mathrm{tr}\left(\rho^{SE} \otimes \rho^{\tilde{S}\tilde{E}}\right) \cdot F^{SE \leftrightarrow \tilde{S}\tilde{E}} \right\}$$

SWAP lemma

$$= \frac{|S|^2}{|R|^2} \left\{ a \; \mathrm{tr}\left[\left(\rho^E\right)^2\right] + b \; \mathrm{tr}\left[\left(\rho^{SE}\right)^2\right] \right\}$$

(f) $$\int du \, \left\| \psi_u^{RE} - \frac{I_R}{|R|} \otimes \psi^E \right\|_2^2$$ 3.10

P3.3

$$= \frac{|S|^2}{|R|^2} a \, \mathrm{tr}(\rho^E)^2 + \frac{|S|^2}{|R|^2} b \, \mathrm{tr}(\rho^{SE})^2 - \frac{1}{|R|} \mathrm{tr}(\rho^E)^2$$

Sub vals of a, b from P3.8

$$= \left[\frac{1}{|R|} \left(\frac{1 - \frac{|R|}{|S|}}{1 - \frac{1}{|S|^2}} \right) - \frac{1}{|R|} \right] \mathrm{tr}(\rho^E)^2$$ ← negative

$$+ \left(\frac{1 - \frac{1}{|R||S|}}{1 - \frac{1}{|S|^2}} \right) \mathrm{tr}(\rho^{SE})^2$$ ← pre factor < 1.

$$\leq \mathrm{tr}(\rho^{SE})^2$$