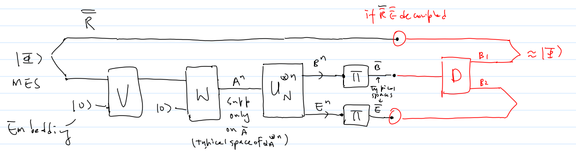
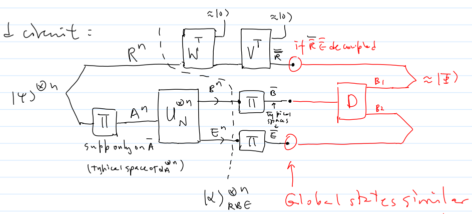
Lec 15, 2010

Note Title 24/06/2010

• Recall the coding protocol for the LSD theorem:



• A related circuit:

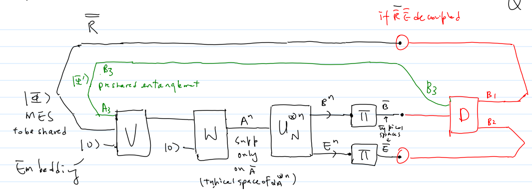


Global states similar on these 2 circuits
can analyze 2nd one

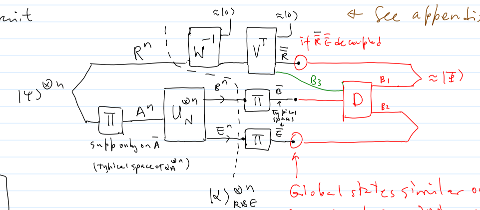
• The father protocol (direct coding): charged-entanglement assisted Q comm by Q channel

B3 need not be sent but cannot be op on by Alice

(noisy channel) ↓ noiseless channel)



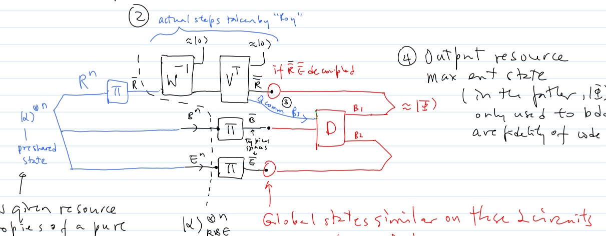
• A related circuit ← See appendix 1 for detail



[Choose basis for R s.t. $W^T = W^\dagger$]

Global states similar on these 2 circuits
can analyze 2nd one

• A protocol "mother" suggested by the related circuit:



② actual steps taken by "Eoy"

④ Output resource max ent state (in the father, $|\Phi\rangle$) only used to bdd are fidelity of code)

① The new given resource iid copies of a pure state on RBE (or mixed state on RB)

Global states similar on these 2 circuits
can analyze 2nd one

Mother: Mixed state entanglement purification (noisy ent → noiseless ent) using charged Q communication

Suffices to analyze mother (father follows with $|\alpha\rangle = I \otimes U_N |\phi\rangle$ same dim for $\bar{\bar{R}}$ & B_3).

Goal: max $\dim(\bar{\bar{R}})$ (Q comm or distillable entanglement obtained)

min $\dim(B_3)$ (Noiseless ent or Q communication spent)

while decoupling $\bar{\bar{R}}\,\bar{E}$ (to guarantee the job done right)

Recall approx decoupling lemma: (lecture 10 p 11)

If $\| \rho_{\bar{\bar{R}}\bar{E}} - \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}} \|_{tr} \le \varepsilon'$

then $\exists\, |\psi\rangle_{\bar{\bar{R}}\bar{E}B_1B_2}$ purifying $\rho_{\bar{\bar{R}}\bar{E}}$

s.t. $\| \operatorname{tr}_{\bar{E}B_2} |\psi\rangle\langle\psi|_{\bar{\bar{R}}\bar{E}B_1B_2} - \underbrace{|\Phi\rangle\langle\Phi|}_{\text{MES}}{}_{\bar{\bar{R}}B_1} \| \le 2\sqrt{\varepsilon'}$

So we bound $\| \underbrace{\rho_{\bar{\bar{R}}\bar{E}} - \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}}}_{M} \|_{tr}$

Useful lemmas:

(L1) Cauchy-Schwarz inequality

$\|M\|_{tr}^2 \le \operatorname{rank}(M)\, \operatorname{tr}(M^\dagger M) = \operatorname{rank}(M)\, \|M\|_2^2$

(L2) $\operatorname{tr}(M^2) = \operatorname{tr}(\underbrace{\text{SWAP}}\; M \otimes M)$

the operator taking $|ij\rangle$ to $|ji\rangle$ eg $\begin{bmatrix} 1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1 \end{bmatrix}$

Pf: $\operatorname{tr}(M^2) = \sum_j \langle j| M\, I\, M |j\rangle$

$= \sum_{ij} \langle j|M|i\rangle\langle i|M|j\rangle$

$= \sum_{ij} \langle j|\langle i|\; M \otimes M\; |i\rangle|j\rangle$

Alternative proof in appendix 2

$$= \mathrm{tr}\Big(\underbrace{\sum_{ij} |ij\rangle\langle ji|}_{\mathrm{SWAP}}\ M\otimes M\Big)$$

(L3) Let $S_1 = S_{11}S_{12}\cdots S_{1s}$ be s 1-qubit systems

$S_2 = S_{21}S_{22}\cdots S_{2s}$ - - - - .

Then $$\mathrm{SWAP}_{S_1S_2} = \frac{1}{2^s}\sum_{P\in P_s} P\otimes P$$ $P_s = 4^s$ Pauli matrices on s qubits

Pf: $$\mathrm{SWAP}_{S_{1i}S_{2i}} = \frac{1}{2}(II+XX+YY+ZZ)_{S_{1i}S_{2i}} = \begin{bmatrix}1&0&0&0\\0&0&1&0\\0&1&0&0\\0&0&0&1\end{bmatrix}$$

$$\mathrm{SWAP}_{S_1S_2} = \bigotimes_{i=1}^{s} \mathrm{SWAP}_{S_{1i}S_{2i}} = \frac{1}{2^s}\sum_{P\in P_s} P\otimes P$$

(L4) $$\mathrm{Tr}(\overset{\text{state}}{\rho_1}\,\overset{\text{matrix}}{Q}) = \mathrm{Tr}(\overset{\text{extension of } \rho_1 \text{ ie } \mathrm{tr}_2\,\rho_{12}=\rho_1}{\rho_{12}}\ Q\otimes I_2)$$

(L5) $$\mathbb{E}\left(V^\dagger_{T_1S_1}\otimes V^\dagger_{T_2S_2}\right)\left(\overset{\text{each with } t \text{ qubits}}{I_{T_1T_2}}\otimes \mathrm{SWAP}_{S_1S_2}\right)\left(V_{T_1S_1}\otimes V_{T_2S_2}\right)$$

$V\in C_{s+t}$ = Clifford group on $s+t$ qubits

$$= \alpha\, I_{(T_1S_1)(T_2S_2)} + \beta\, \mathrm{SWAP}_{(T_1S_1)(T_2S_2)}$$

for $$\alpha = 2^s\left[\frac{4^t-1}{4^{s+t}-1}\right] \le \frac{1}{2^s} = \frac{1}{|S_1|}$$

$$\beta = 2^t\left[\frac{4^s-1}{4^{s+t}-1}\right] \le \frac{1}{2^t} = \frac{1}{|T_1|}$$

Pf: By (L3), LHS of (L5)

$$= \mathbb{E}_{V\in C_{s+t}} V^\dagger_{T_1S_1}\otimes V^\dagger_{T_2S_2}\left[I_{T_1T_2}\otimes\left(\sum_{P\in P_s} P_{S_1}\otimes P_{S_2}\right)\frac{1}{2^s}\right] V_{T_1S_1}\otimes V_{T_2S_2}$$

- If $P=I$, $$\mathbb{E}_{V\in C_{s+t}} V^\dagger_{T_1S_1}\otimes V^\dagger_{T_2S_2}\left[I_{T_1T_2}\otimes I_{S_1S_2}\right] V_{T_1S_1}\otimes V_{T_2S_2}$$ $$= I_{T_1S_1T_2S_2}$$
- If $P\ne I$, $$\mathbb{E}_{V\in C_{s+t}} V^\dagger_{T_1S_1}\otimes V^\dagger_{T_2S_2}\left[(I_{T_1}P_{S_1})\otimes(I_{T_2}P_{S_2})\right] V_{T_1S_1}\otimes V_{T_2S_2}$$

see appendix 3

$$= \mathbb{E}_{V\in C_{s+t}} V^\dagger_{T_1S_1}(I_{T_1}P_{S_1})V_{T_1S_1}\otimes V^\dagger_{T_2S_2}(I_{T_2}P_{S_2})V_{T_2S_2}$$

The Clifford group permutes Pauli matrices by conjugation & acts transitively on all the non-identity Paulis.
(for any $P_1\ne I$, $P_2\ne I$, $\exists\, V$ s.t. $VP_1V^\dagger = P_2$)

$$= \frac{1}{4^{s+t}-1}\sum_{Q\in P_{s+t},\, Q\ne I} Q\otimes Q$$

$4^{s+t}-1$ = # of possible $Q = V^\dagger(I\otimes P)V \ne I$, $Q\in P_{s+t}$

(L3) $$= \left(\frac{1}{4^{s+t}-1}\right)\left(2^{s+t}\,\mathrm{SWAP}_{(T_1S_1)(T_2S_2)} - I\otimes I\right)$$

So LHS of (L5)

$$= \mathbb{E}_{V\in C_{s+t}} V^\dagger_{T_1S_1}\otimes V^\dagger_{T_2S_2}\left[I_{T_1T_2}\otimes\left(\sum_{P\in P_s} P_{S_1}\otimes P_{S_2}\right)\frac{1}{2^s}\right] V_{T_1S_1}\otimes V_{T_2S_2}$$

$$= \frac{1}{2^s}\left(P=I \text{ case}\right) + \frac{4^s-1}{2^s}\left(P\ne I \text{ case}\right)$$

$$= \frac{1}{2^s} I_{T_1S_1T_2S_2} + \frac{4^s-1}{2^s}\,\frac{1}{4^{s+t}-1}\left(2^{s+t}\,\mathrm{SWAP}_{(T_1S_1)(T_2S_2)} - I_{T_1S_1}I_{T_2S_2}\right)$$

$$= \underbrace{\frac{1}{2^s}\left(1-\frac{4^s-1}{4^{s+t}-1}\right)}_{\frac{1}{2^s}\left(\frac{4^{s+t}-4^s}{4^{s+t}-1}\right) = 2^s\left(\frac{4^t-1}{4^{s+t}-1}\right) = \alpha} I_{T_1S_2}I_{T_2S_2} + \underbrace{2^t\,\frac{4^s-1}{4^{s+t}-1}}_{\beta}\,\mathrm{SWAP}_{(T_1S_1)(T_2S_2)}$$

NB The average over Clifford group in (L5) same as average over V drawn over the Haar meas.

The above allows stabilizer codes (not random codes) to be used.

A slightly modified proof (appendix 3) shows that the Clifford group is a "2-design".

Back to $\| \rho_{\bar{\bar{R}}\bar{E}} - \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}} \|_2^2$

$$= \operatorname{tr}\left[\left(\rho_{\bar{\bar{R}}\bar{E}} - \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}}\right)\left(\rho_{\bar{\bar{R}}\bar{E}} - \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}}\right)\right]$$

$$= \operatorname{tr}\left(\rho_{\bar{\bar{R}}\bar{E}}^2\right) - 2\operatorname{tr}\left(\rho_{\bar{\bar{R}}\bar{E}} \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}}\right) + \operatorname{tr}\left(\left(\frac{I}{2^{nr}}\right)^2_{\bar{\bar{R}}} \otimes \rho_{\bar{E}}^2\right)$$

$$= \operatorname{tr}\left(\rho_{\bar{\bar{R}}\bar{E}}^2\right) - 2\left(\frac{1}{2^{nr}}\right) \underbrace{\operatorname{tr}\left(\rho_{\bar{\bar{R}}\bar{E}}\left(I_{\bar{\bar{R}}} \otimes \rho_{\bar{E}}\right)\right)}_{\downarrow \text{L4}} + \frac{1}{2^{nr}} \operatorname{tr} \rho_{\bar{E}}^2$$

$$\operatorname{tr}\left(\operatorname{tr}_{\bar{\bar{R}}}\left(\rho_{\bar{\bar{R}}\bar{E}}\right) \cdot \rho_{\bar{E}}\right) = \operatorname{tr}\left(\rho_{\bar{E}} \cdot \rho_{\bar{E}}\right)$$

$$= \operatorname{tr}\left(\rho_{\bar{\bar{R}}\bar{E}}^2\right) - \frac{1}{2^{nr}} \operatorname{tr} \rho_{\bar{E}}^2$$

Now bounding $\mathbb{E}_V \operatorname{tr}\left(\rho_{\bar{\bar{R}}\bar{E}}\right)^2$

$$\overset{\text{L2}}{=} \mathbb{E}_V \operatorname{tr}\left[\left(\rho_{\bar{\bar{R}}_1\bar{E}_1} \otimes \rho_{\bar{\bar{R}}_2\bar{E}_2}\right) \mathrm{SWAP}_{(\bar{\bar{R}}_1\bar{E}_1)(\bar{\bar{R}}_2\bar{E}_2)}\right]$$

$$\overset{\text{L4}}{=} \mathbb{E}_V \operatorname{tr}\left[\left(\underbrace{\rho_{B_{31}\bar{\bar{R}}_1\bar{E}_1}}_{V_{B_{31}\bar{\bar{R}}_1} \otimes I_{\bar{E}_1}\left(\alpha_{\bar{R}_1\bar{E}_1}\right) V^{\dagger}_{B_{31}\bar{\bar{R}}_1} \otimes I_{\bar{E}_1}} \otimes \underbrace{\rho_{B_{32}\bar{\bar{R}}_2\bar{E}_2}}_{\text{similarly}}\right)\left(I_{B_{31}B_{32}} \otimes \mathrm{SWAP}_{\bar{\bar{R}}_1\bar{\bar{R}}_2} \otimes \mathrm{SWAP}_{\bar{E}_1\bar{E}_2}\right)\right]$$

$$\boxed{\bar{R}_1 = \bar{\bar{R}}_1 B_3}$$

cyclic tr

$$= \mathbb{E}_V \operatorname{tr}\left[\left(\alpha_{\bar{R}_1\bar{E}_1} \otimes \alpha_{\bar{R}_2\bar{E}_2}\right) \times V^{\dagger}_{B_{31}\bar{\bar{R}}_1} \otimes V^{\dagger}_{B_{32}\bar{\bar{R}}_2} \otimes I_{\bar{E}_1\bar{E}_2}\left(I_{B_{31}B_{32}} \otimes \mathrm{SWAP}_{\bar{\bar{R}}_1\bar{\bar{R}}_2} \otimes \mathrm{SWAP}_{\bar{E}_1\bar{E}_2}\right) V_{B_{31}\bar{\bar{R}}_1} \otimes V_{B_{32}\bar{\bar{R}}_2} \otimes I_{\bar{E}_1\bar{E}_2}\right]$$

$$= \operatorname{tr}\left[\left(\alpha_{\bar{R}_1\bar{E}_1} \otimes \alpha_{\bar{R}_2\bar{E}_2}\right) \times \mathbb{E}_V V^{\dagger}_{B_{31}\bar{\bar{R}}_1} \otimes V^{\dagger}_{B_{32}\bar{\bar{R}}_2} \otimes I_{\bar{E}_1\bar{E}_2}\left(I_{B_{31}B_{32}} \otimes \mathrm{SWAP}_{\bar{\bar{R}}_1\bar{\bar{R}}_2} \otimes \mathrm{SWAP}_{\bar{E}_1\bar{E}_2}\right) V_{B_{31}\bar{\bar{R}}_1} \otimes V_{B_{32}\bar{\bar{R}}_2} \otimes I_{\bar{E}_1\bar{E}_2}\right]$$

$$= \operatorname{tr}\left[\left(\alpha_{\bar{R}_1\bar{E}_1} \otimes \alpha_{\bar{R}_2\bar{E}_2}\right) \times \mathbb{E}_V V^{\dagger}_{B_{31}\bar{\bar{R}}_1} \otimes V^{\dagger}_{B_{32}\bar{\bar{R}}_2}\left(I_{B_{31}B_{32}} \otimes \mathrm{SWAP}_{\bar{\bar{R}}_1\bar{\bar{R}}_2}\right) V_{B_{31}\bar{\bar{R}}_1} \otimes V_{B_{32}\bar{\bar{R}}_2} \otimes \mathrm{SWAP}_{\bar{E}_1\bar{E}_2}\right]$$

$$\overset{\text{L5}}{\leq} \operatorname{tr}\left[\left(\alpha_{\bar{R}_1\bar{E}_1} \otimes \alpha_{\bar{R}_2\bar{E}_2}\right) \times \left(\frac{1}{|\bar{\bar{R}}|} I_{B_{31}\bar{\bar{R}}_1 B_{32}\bar{\bar{R}}_2} + \frac{1}{|B_3|} \mathrm{SWAP}_{(B_{31}\bar{\bar{R}}_1)(B_{32}\bar{\bar{R}}_2)}\right) \otimes \mathrm{SWAP}_{\bar{E}_1\bar{E}_2}\right]$$

$\downarrow$ L4

$$= \frac{1}{|\bar{\bar{R}}|} \operatorname{tr}\left(\alpha_{\bar{E}_1} \otimes \alpha_{\bar{E}_2} \, \mathrm{SWAP}_{\bar{E}_1\bar{E}_2}\right) + \frac{1}{|B_3|} \operatorname{tr}\left(\alpha_{\bar{R}_1\bar{E}_1} \otimes \alpha_{\bar{R}_2\bar{E}_2}\right) \mathrm{SWAP}_{\bar{R}_1\bar{E}_1\,\bar{R}_2\bar{E}_2}$$

$$= \frac{1}{|\bar{\bar{R}}|} \operatorname{tr}\left(\alpha_{\bar{E}}^2\right) + \frac{1}{|B_3|} \operatorname{tr}\left(\alpha_{\bar{R}\bar{E}}^2\right)$$

$$\| \rho_{\bar{\bar{R}}\bar{E}} - \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}} \|_2^2 \leq \left(\frac{1}{|\bar{\bar{R}}|} \operatorname{tr}\left(\alpha_{\bar{E}}^2\right) + \frac{1}{|B_3|} \operatorname{tr}\left(\alpha_{\bar{R}\bar{E}}^2\right)\right) - \frac{1}{2^{nr}} \operatorname{tr} \rho_{\bar{E}}^2$$

$$= \frac{1}{|B_3|} \operatorname{tr}\left(\alpha_{\bar{R}\bar{E}}\right)^2$$

By L1, $$\| \rho_{\bar{\bar{R}}\bar{E}} - \left(\frac{I}{2^{nr}}\right)_{\bar{\bar{R}}} \otimes \rho_{\bar{E}} \|_{\mathrm{tr}}^2 \leq \frac{|\bar{R}\bar{E}|}{|B_3|} \underbrace{\operatorname{tr}\left(\alpha_{\bar{R}\bar{E}}\right)^2}$$

$\alpha_{\bar{R}\bar{E}} = (\alpha_{RE})^{\otimes n}$ projected onto typical space of. Each eigvalue $\approx \frac{1}{2^{nS(RE)}}$ $\therefore \operatorname{tr}\left(\alpha_{\bar{R}\bar{E}}\right)^2 = \frac{1}{2^{nS(RE)}}$

If we choose $|\bar{\bar{R}}| = 2^{\frac{n}{2}[S(R:B)_\alpha - \delta]}$

$|B_3| = 2^{\frac{n}{2}[S(R:E)_\alpha + \delta]}$

then $$\| \cdot \|_{\mathrm{tr}}^2 \leq \frac{2^{\frac{n}{2}[S(R:B)_\alpha - \delta]}}{2^{\frac{n}{2}[S(R:E)_\alpha + \delta]}} \times \frac{2^{n(S(E)_\alpha + \varepsilon)}}{2^{n(S(RE)_\alpha - \varepsilon)}}$$

$$= 2^{\frac{n}{2}\left[\left(\cancel{S(R)} + S(B) - S(RE)\right)_\alpha - \left(\cancel{S(R)} + S(E) - S(RE)\right)_\alpha - 2\delta\right]} \cdot 2^{n\left(S(E)_\alpha - S(RE)_\alpha + 2\varepsilon\right)}$$

$$= 2^{n\left(\cancel{S(B)}_\alpha - \cancel{S(RE)}_\alpha - \delta\right)} \, 2^{n\left(\cancel{S(E)}_\alpha - \cancel{S(RE)}_\alpha + 2\varepsilon\right)}$$

$$= 2^{-n(\delta - 2\varepsilon)} \qquad \text{choose } \delta = 3\varepsilon$$

$\uparrow$ fixed by how good the typical spaces are

$$= 2^{-n\varepsilon} \to 0 \text{ as } n \to \infty$$

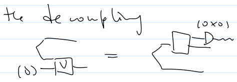
NB the unassisted case (the LSD thm) has $|B_3| = 1$

We choose $|\bar{\bar{R}}| = 2^{\frac{n}{2}(S(R:B)_\alpha - S(R:E)_\alpha - 2\delta)}$

$$= 2^{n[I_c(R\rangle B) - \delta]}$$

and the same decoupling condition for $\bar{\bar{R}}\bar{E}$ holds.

The mapping from the direct coding scheme to the decoupling condition based on $\alpha^{\otimes n}$ has a glitch:



For other recent outcomes, decoupling still works but the proof is involved (see 0702005 p9-10 pf of Thm IV), & omitted

Alt: just use the father to get LSD.

① mother:

$$n\{qq\} + \frac{n}{2}\left(S(R:E)+\delta\right)[q\to q] \geq \frac{n}{2}\left(S(R:B)-\delta\right)[qq]$$

noisy — static 2-party quantum resource (ψ_{RB} here) — evaluated on α — noiseless dynamical — qbit — ebits

Bob's full potential

the more Eve has the more assistance it takes to decouple her

② father:

$$n\{q\to q\} + \frac{n}{2}\left(S(R:E)+\delta\right)[qq] \geq \frac{n}{2}\left(S(R:B)-\delta\right)[q\to q]$$

noisy dynamical resource (N here) — eval on $I\otimes U_N|\phi\rangle = |\alpha\rangle$ — ebits — qbits

Note that we have asymptotic approximate resource inequalities here. Say, XXX >= YYY. We demand the output resource YYY (lesser side) to be close to the ideal resource in trace distance or diamond norm. This ensures the protocol underlying the resource inequality can be used as a subroutine in any other protocol to produce YYY (using XXX) and when YYY is consumed, it is basically as good as ideal.

Say, XXX + ZZZ >= YYY + ZZZ >= KKK

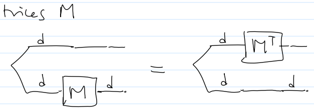
The first inequality only holds if XXX >= YYY is given by a protocol producing sufficiently

Appendix 1:

Let $\underset{d}{\overset{d}{\langle}}$ denote $\sum_{i=1}^{d}|i\rangle|i\rangle = \sqrt{d}\times$ max ent state

The well-known transpose trick says the following:

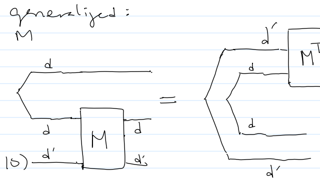
$\forall$ $d\times d$ matrices M



(This holds also for MES)

This can be generalized:

$\forall$ $dd' \times d'd$ M



(projection onto $|0\rangle\langle 0|$)

(remember to re-insert the normalization when applying this to max ent states)

Pf The output of the LHS

$= I\otimes V\left(\sum_i |i\rangle|i\rangle\right)|0\rangle$ $\quad$ [Let $V|ij\rangle = \sum_{rs} V_{ij\,rs}|rs\rangle$]

$= \sum_i |i\rangle \sum_{rs} V_{i0\,rs}|rs\rangle$

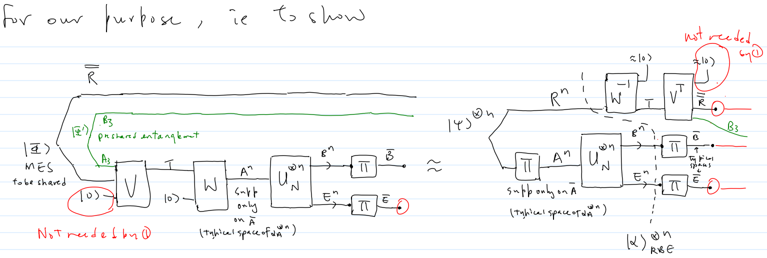
$= \sum_{rs}\left(\sum_i V_{i0\,rs}|i\rangle\right)|rs\rangle$

[$\therefore V^T|rs\rangle = \sum_{ij} V_{ij\,rs}|ij\rangle$]

$= \sum_{rs}(I\otimes\langle 0|)\left(V^T|rs\rangle\right)\otimes|rs\rangle$

$= (I\otimes\langle 0|\otimes I)(V^T\otimes I)\sum_{rs}|rs\rangle|rs\rangle$ = output of RHS

For our purpose, ie to show

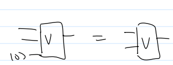


we don't need the above generalization of the transpose trick.

① In the end, $\dim(\bar{R}) = 2^{\frac{n}{2}[S(R:B)_\alpha - \delta]}$

$\dim(B_3) = 2^{\frac{n}{2}[S(R:E)_\alpha + \delta]}$

So $\dim(\bar{R}B_3) = \dim(T) = 2^{n(S(R)+\epsilon)}$ and



(if necessary add ϵ terms to $\dim(B_3)$)

(For the unassisted case (the LSD thm with $|B_3|=0$) moving V to the upper register requires an actual proj on the upper register. We can have a meas effecting one out of many possible projections. Thm IV of 0702005 is needed to ensure any outcome gives the same decoupling condition.)

② To move W: note initial state on RHS $\approx$ MES on $2^{nS(R)}$ dims not 2^{nd_R} dims. So moving W to W^T only requires the original transpose trick.

Appendix 2:

Alt proof for L2: $\quad tr(M^2) = tr(\text{SWAP } M\otimes M)$

Pf: $tr(\text{SWAP } M\otimes M)$

$= tr(\text{SWAP } M\otimes I \cdot I\otimes M)$

$= tr(\underbrace{\text{SWAP } M\otimes I \text{ SWAP}} \text{ SWAP } I\otimes M)$

$= tr(\quad I\otimes M \quad \text{SWAP } I\otimes M)$

$= tr(\text{SWAP } I\otimes M^2) \overset{(2.4)}{=} Tr\big[\underbrace{(tr_1 \text{ SWAP})}_{\overset{\shortparallel}{I}} M^2\big]$

$= tr(M^2)$ $\qquad$ (see next page)

NB $Tr_1(\text{SWAP}) = I$

Pf: $\text{SWAP} = \sum_{ij} |ji\rangle\langle ij|$, $\; tr(|j\rangle\langle i|) = \delta_{ij}$ — kronecker δ-fcn.

$\therefore Tr_1(\text{SWAP}) = \sum_{ij} \delta_{ij} \; |i\rangle\langle j| = I$ (on 2nd sys)

Appendix 3:

Let $\mathcal{T}(M) = \underset{V\in C_{s+t}}{\mathbb{E}} V\otimes V \; M \; V^\dagger\otimes V^\dagger$ $\quad$ $V \in C_{s+t}$ (Clifford group on s+t qubits)

① if $P \neq I$, $P \in P_{s+t}$ (Pauli group on s+t qubits)

then $\mathcal{T}(P\otimes P) = \frac{1}{4^{s+t}-1} \sum_{\substack{Q\in P_{s+t}\\ Q\neq I}} Q\otimes Q$

Pf: Note that C_{s+t} is transitive on $P_{s+t} - \{I\}$

ie for any $Q_1, Q_2 \in P_{s+t} - \{I\}$

$\exists \; W \in C_{s+t}$ s.t. $\; W Q_1 W^\dagger = Q_2$

Also, $\forall \; V \in C_{s+t}$, $\; V(P_{s+t} - \{I\}) V^\dagger$ only permutes elements of $P_{s+t} - \{I\}$.

So $\mathcal{T}(P\otimes P) = \sum_{Q\in P_{s+t}-\{I\}} \mu(Q) \, Q\otimes Q$ for some distribution $\mu(Q)$

If $\mu(Q)$ not uniform, then $\exists \, Q_1, Q_2$ s.t. $\mu(Q_1) \lneq \mu(Q_2)$

let $W' Q_1 W'^\dagger = Q_2$

then $\mathcal{T}(P\otimes P) = W' \, \mathcal{T}(P\otimes P) \, W'^\dagger$ $\quad \left(\text{this merely changes } \underset{V\in C_{s+t}}{\mathbb{E}} \text{ to } \underset{WV\in C_{s+t}}{\mathbb{E}}\right)$

$\left.\begin{array}{l} Q_2\otimes Q_2 \text{ has weight } \mu(Q_2) \text{ on LHS} \\ Q_2\otimes Q_2 \; - - \; \mu(Q_1) \text{ on RHS} \end{array}\right\} (\ast)$

($\because W'$ is a permutation on $P_{s+t} - \{I\}$, the $Q_2\otimes Q_2$ term in the 2nd line can only come from the $Q_1\otimes Q_1$ term before conjugation by W.)

But $\{Q\otimes Q\}$ is trace orthonormal.

$\therefore$ $(\ast)$ is a contradiction $\therefore$ $\mu(Q)$ has to be uniform

② $\mathcal{T}(P\otimes Q) = 0 \qquad \forall \; P\neq Q, \; P, Q \in P_{s+t}$

Pf. WLOG $P \neq I$ $\qquad$ (at least one of $P, Q \neq I$)

There are 4^{s+t-2} Pauli's anti commuting with P & commuting with Q

Let R be one of them

$$\mathcal{T}(P\otimes Q) = \underset{V\in C_{s+t}}{\mathbb{E}} V\otimes V \; P\otimes Q \; V^\dagger\otimes V^\dagger$$

$$= \frac{1}{2}\Big[\underset{V\in C_{s+t}}{\mathbb{E}} V\otimes V \; P\otimes Q \; V^\dagger\otimes V^\dagger + \underset{V\in C_{s+t}}{\mathbb{E}} VR\otimes VR \; P\otimes Q \; (VR)^\dagger\otimes(VR)^\dagger\Big]$$

$= 0$.

So $\forall M$, $\; \mathcal{T}(M) =$ linear combination of $I I$ & SWAP.

It easy to show that the coeffs are same as that of

$\int_{du} U\otimes U \; M \; U^\dagger\otimes U^\dagger$ $\quad$ (average U over Haar meas.)

(see Q. data hiding paper DiVincenzo, L. Terhal for detail.)