Lec10, June 8, 2010.

Note Title 07/06/2010

Last time: Quantum capacity of quantum channel

(1) Basic def (2) Diff measures of errors lead to same capacity

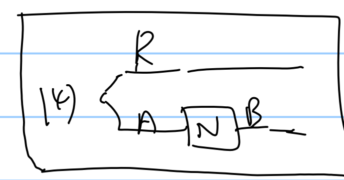
(3) Quantum error correcting code as a subspace, errors translate it to identical / orthogonal error spaces.

(4) Statement of LSD theorem: $Q(N) = \sup_n Q^n(N) = \sup_n \frac{1}{n} Q^{(1)}(N)$

& $Q^{(1)}(N) = \max_{|\psi\rangle} I_c(R\rangle B)$ $I\otimes N(|\psi\rangle)$

coherent info

$S(B) - S(RB) = \frac{1}{2}[I(R:B) - I(R:E)]$



(5) $I_c(R\rangle B)$ non increasing under local op on B

Discarding a subsys of R may increase / decrease it.

Proving the LSD theorem (ref 0702005 or Preskill Ph219 lec notes May 18 & Jun 1, 2009)

① Converse

② Derive from the exact converse the "decoupling condition" necessary for sucessful transmission

Show exact decoupling is sufficient for exact transmission
& approx - - - - - - - - approx - - -

③ Prove direct coding theorem based on random codes and approx decoupling

All parts revolve about error def ②a of entangling Bob & reference

① Converse:

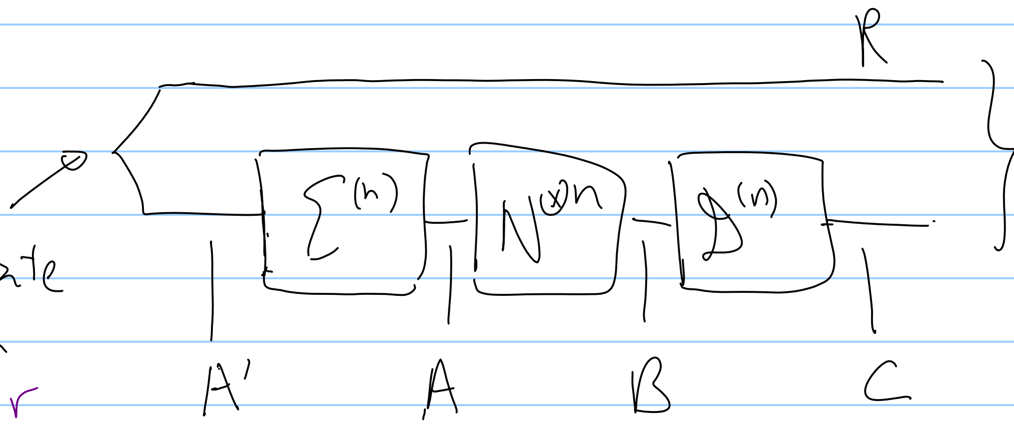
Suppose r is achievable (note lower case r)

Pick an arbitrary small error parameter ε.

$\exists n$ & $(2^{nr}, n)$ code

s.t.

max ent state of dim $2^{nr} \times 2^{nr}$



$\approx$ max ent state of dim $2^{nr} \times 2^{nr}$

By Quantum data processing ineq
(mono of I_c under local op on 2nd sys)

$$I_c(R\rangle A') \geq I_c(R\rangle A) \geq I_c(R\rangle B) \geq I_c(R\rangle C)$$

$nr = I_c(R\rangle A')$ ⟵ By def of achievable rate ⟶ $I_c(R\rangle C) \geq nr - f(\varepsilon)$

f vanishing function

$$\therefore \frac{1}{n} f(\varepsilon) + \frac{1}{n} I_c(R\rangle B) \gtrsim r$$

If $\frac{f(\varepsilon)}{n} \to 0$ as $n \to \infty$ then converse holds.

Bounding $f(\varepsilon)$:

Main Ingredient:

Fannes Inequality (see NC p512):

Let ρ_1, ρ_2 be density matrices supported on a d-dim space with $\|\rho_1 - \rho_2\|_{tr} = \Delta \leq \frac{1}{e}$

Then $|S(\rho_1) - S(\rho_2)| \leq \Delta \log d + H(\Delta)$

Fannes-Alicki Inequality (see 0312081):

Setting as above but bipartite ρ_1, ρ_2 on sys AB, $d = d_A d_B$

Then $|S(A|B)_{\rho_1} - S(A|B)_{\rho_2}| \leq 4\Delta \log d_A + 2H(\Delta)$

☆ Most useful if $d_A \ll d_B$ or d_B unknown!

For the converse: ρ_1 = max ent state on RC

ρ_2 = actual output on RC

$\Delta \leq \varepsilon$, $\quad d_R = d_C = 2^{nr}$

Upper bound $\left| \underset{\substack{\uparrow \\ \text{this is } nr}}{I_c(R\rangle C)_{\rho_1}} - \underset{\substack{\uparrow \\ \text{want lower bound}}}{I_c(R\rangle C)_{\rho_2}} \right|$

Recall $I_c(R\rangle C) = \underbrace{S(C) - S(RC)}_{①} = \underbrace{-S(R|C)}_{②}$

We can either use Fannes ineq to bound ①

or use Fannes-Alicki ineq to bound ②

Since $d_C \approx d_R$, the two methods give similar bounds

Bounding ① : $\|\mathrm{tr}_R(\rho_1) - \mathrm{Tr}_R(\rho_2)\|_{tr} \le \varepsilon$ by monotonicity of trace distance

$$\therefore \left| S(C)_{\mathrm{tr}_R(\rho_1)} - S(C)_{\mathrm{tr}_R(\rho_2)} \right|_{tr} \overset{\text{Fannes}}{\le} \underbrace{nr}_{\dim C = 2^{nr}} \varepsilon + H(\varepsilon)$$

$$\& \ \left| S(RC)_{\rho_1} - S(RC)_{\rho_2} \right| \le \underbrace{2nr}_{\dim RC = 2^{2nr}} \varepsilon + 2H(\varepsilon)$$

$$\text{So } \left| I_c(R\rangle C)_{\rho_1} - I_c(R\rangle C)_{\rho_2} \right|$$

$$\le \left| S(C)_{\mathrm{tr}_R(\rho_1)} - S(C)_{\mathrm{tr}_R(\rho_2)} \right| - \left| S(RC)_{\rho_1} - S(RC)_{\rho_2} \right|$$

$$\le 3nr\varepsilon + 3H(\varepsilon)$$

NB Bounding ② gives upp bdd: $4nr\varepsilon + 2H(\varepsilon)$

So $\quad I_c(R\rangle C)_{\rho_2} \geq \underbrace{I_c(R\rangle C)_{\rho_1}}_{nr} - 3nr\varepsilon - 3H(\varepsilon)$

Back to converse:

$$I_c(R\rangle B) \geq I_c(R\rangle C)_{\rho_2}$$

$$\geq nr - \underbrace{\left[3nr\varepsilon + 3H(\varepsilon)\right]}_{f(\varepsilon)}$$

$$\therefore \quad \frac{1}{n} I_c(R\rangle B) + \underbrace{\left[3r\varepsilon + 3\frac{H(\varepsilon)}{n}\right]}_{\to\, 0 \text{ as } \varepsilon \to 0.} \geq r$$

② Exact decoupling condition:

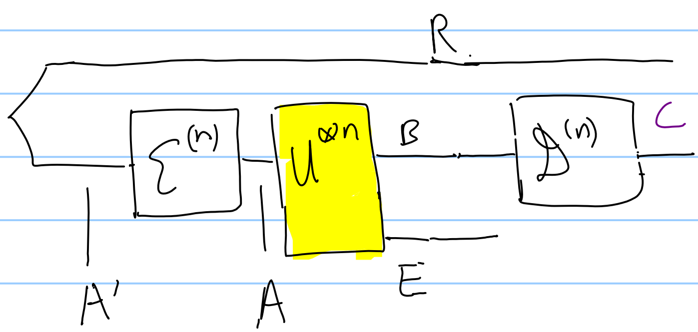
the code achieves $nr = I_c(R \rangle B)$ exactly $\iff$ RE are decoupled (E = Env for $N^{\otimes n}$ purifying RB)

because $nr = I_c(R\rangle B)$

$$\underset{H(R)}{\overset{\parallel}{nr}} = \underset{H(B)-H(RB) = H(RE) - H(E)}{\overset{\parallel}{I_c(R\rangle B)}}$$

$\iff H(R) + H(E) = H(RE)$

& RE in product state right after channel transmission.



Interpretation:

RBE share a pure state:

$$|\psi\rangle_{RBE} = I_R \otimes U^{\otimes n} (|\psi\rangle_{RA})$$

- So B purifies RE.

- If RE in product state, $\rho_{RE} = \rho_R \otimes \rho_E$

  A particular purification is $|\phi\rangle_{RB_1} \otimes |\xi\rangle_{EB_2}$

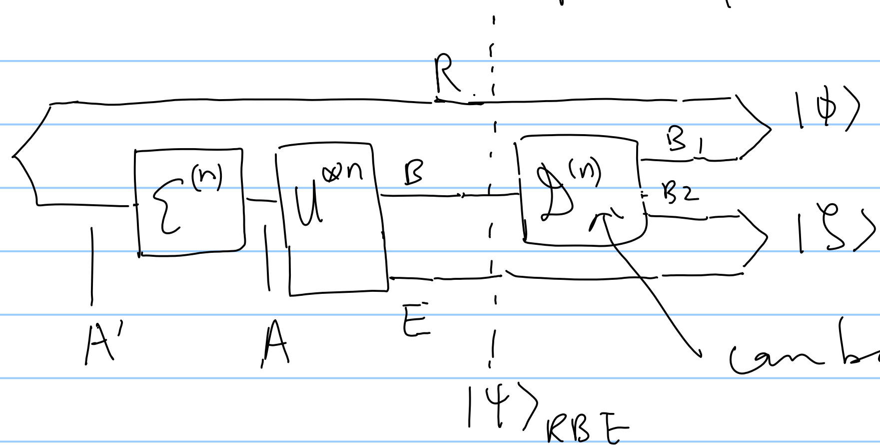
  where $|\phi\rangle_{RB_1}$ purifies ρ_R & $|\xi\rangle_{EB_2}$ purifies ρ_E.

- Recall that any 2 purifications diff by a unitary on the purifying sys.

  $\therefore \exists V_B$ s.t. $\left(V_B \otimes I_{RE}\right)|\psi\rangle_{RBE} = |\phi\rangle_{RB_1} \otimes |\xi\rangle_{EB_2}$

- "Purification of R has to be somewhere, and it has to be completely outside E $\therefore$ it's completely inside B."

- So



since R max mixed, RB_1 max ent & a unitary on B_1 will make it the standard max ent state.

can be chosen to be V_B

Approx decoupling condition (that implies approx transmission of max ent state MES):

Lemma:

If $\left\| \rho_{RE} - \left(\frac{I}{2^{nr}}\right)_R \otimes \rho_E \right\|_{tr} \leq \varepsilon'$

then $\exists\, |\psi\rangle_{REB}$ purifying ρ_{RE}, $B = B_1 B_2$

s.t. $\| \underbrace{\mathrm{tr}_{EB_2} |\psi\rangle\langle\psi|_{REB}}_{\text{final output in } RB_1} - \underbrace{|\Phi\rangle\langle\Phi|_{RB_1}}_{\text{MES}} \| \leq 2\sqrt{\varepsilon'}$.

Pf of Lemma:

Ingredients:

① Uhlmann's thm (p410 NC): density matrices ρ_1 & ρ_2

$$F(\rho_1, \rho_2) := \operatorname{tr}\sqrt{\rho_1^{\frac{1}{2}} \rho_2 \rho_1^{\frac{1}{2}}} \overset{\text{thm}}{=\!=} \underbrace{\max_{|\psi_1\rangle, |\psi_2\rangle}}_{\text{purify } \rho_1, \rho_2 \text{ respectively}} |\langle \psi_1 | \psi_2 \rangle|$$

Note that we can fix one purification & max the other.

② $1 - F(\rho_1, \rho_2) \underset{ⓐ}{\leq} \frac{1}{2} \|\rho_1 - \rho_2\|_{tr} \underset{ⓑ}{\leq} \sqrt{1 - F(\rho_1, \rho_2)^2}$

(p416 NC) "=" for pure ρ_1, ρ_2

Back to proving lemma:

If $\left\| \rho_{RE} - \left(\frac{I}{2^{nr}}\right)_R \otimes \rho_E \right\|_{tr} \leq \varepsilon'$ (hypothesis)

then $F\left(\rho_{RE}, \left(\frac{I}{2^{nr}}\right)_R \otimes \rho_E\right) \overset{(2a)}{\geq} 1 - \frac{\varepsilon'}{2}$

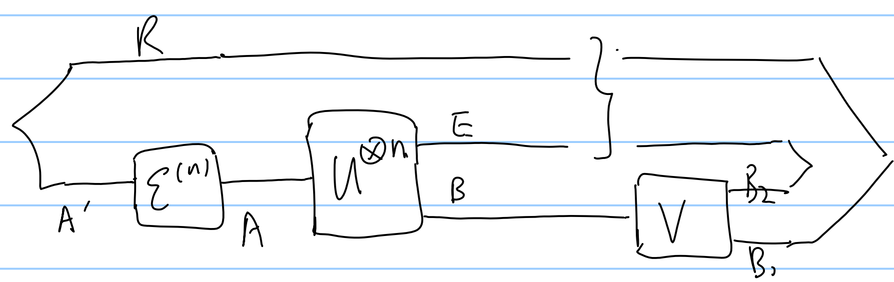
By Uhlmann's thm, $\exists\ |\psi\rangle_{REB}$

s.t. $F(\underbrace{|\psi\rangle_{REB}}_{\text{maximized}}, \underbrace{|\Phi\rangle_{RB_1} \otimes |\xi\rangle_{B_2E}}_{\text{fixed purification of 2nd state}}) \geq 1 - \frac{\varepsilon'}{2}$

$$\therefore \left\| |\psi\rangle\langle\psi|_{REB} - |\Phi\rangle\langle\Phi|_{RB_1} \otimes |\xi\rangle\langle\xi|_{B_2E} \right\|_{tr}$$

$$\overset{(26)}{=} 2\sqrt{1-f^2} \le 2\sqrt{1-\left(1-\frac{\varepsilon'}{2}\right)^2} = 2\sqrt{\left(\frac{\varepsilon'}{2}\right)\left(2-\frac{\varepsilon'}{2}\right)} \le 2\sqrt{\varepsilon'}$$

The lemma says that a code to establish max ent state w/ R & C provably works if $\rho_{RE} \approx \frac{I}{2^{nr}} \otimes \rho_E$ in trace distance.



③ Direct coding:

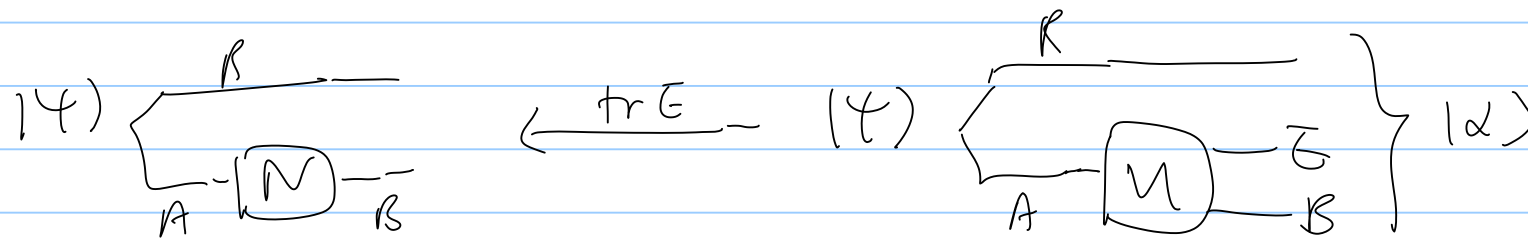
Suffices to show $Q^{(1)}(N) = \max_{|\psi\rangle_{RA}} I_c(R\rangle B)_{I\otimes N(|\psi\rangle)}$

is achievable asymptotically ($Q^{(m)}(N) = Q^{(1)}(N^{\otimes m})$ achievable)

(i) fix an arbitrary $|\psi\rangle_{RA}$

then $|\alpha\rangle = I_R \otimes U(|\psi\rangle_{RA})$ is now fixed.

U takes A to BE



Let $\alpha_R, \alpha_B, \alpha_E, \alpha_{RB}, \alpha_{RE}$ be reduced density matrices.

S_R, S_B etc ... vN entropies.

To be done

(ii) Define a set of $(2^{nr}, n)$ codes based on $|\psi\rangle / |\alpha\rangle$ with $r = I_c(R\rangle B)_{|\alpha\rangle} - \delta_n$

(iii) Show that average over these codes

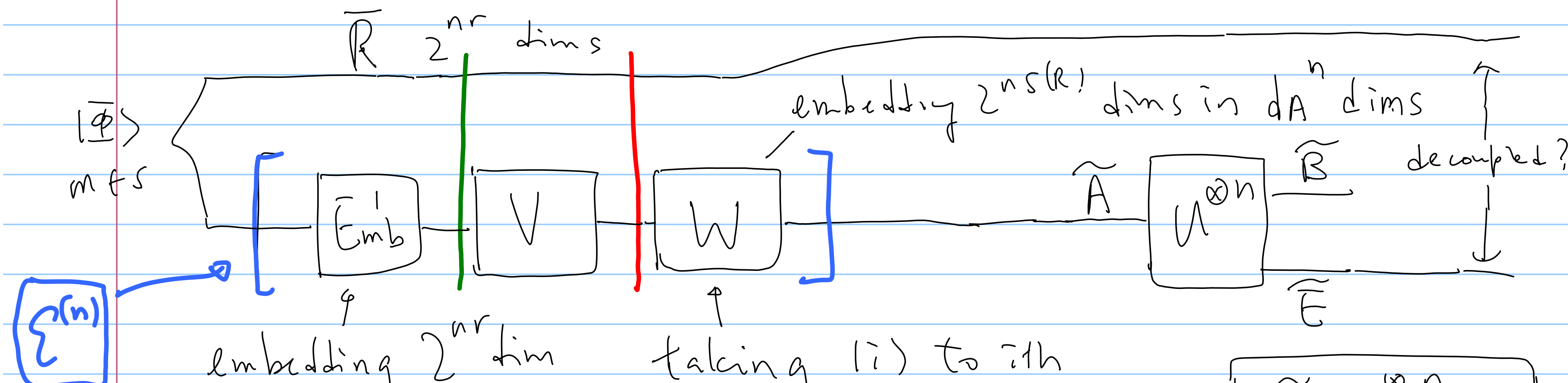
$$\mathop{\mathbb{E}}_{\text{codes}} \left\| \alpha_{RE} - \frac{I}{2^{nr}} \otimes \alpha_E \right\|_{tr} \leq 2^{n(2\xi - \delta_n)}$$

(iv) So at least one code will achieve the above.
For this code, the approx decoupling condition implies the existence of a unitary on B that gives a $\approx$ max ent state on RB_1.

(v) $I_c(R\rangle B)$ achievable $\forall |\psi\rangle$ $\therefore$ take max over $|\psi\rangle$.

Detail on (ii): $(2^{nr}, n)$ codes with $r = I_c(R\rangle B)_{|\alpha\rangle} - \delta_n$

Each code (a subspace of the n input spaces) is specified by a random unitary V on $2^{nS(R)}$ dims.
Call this code C_V.

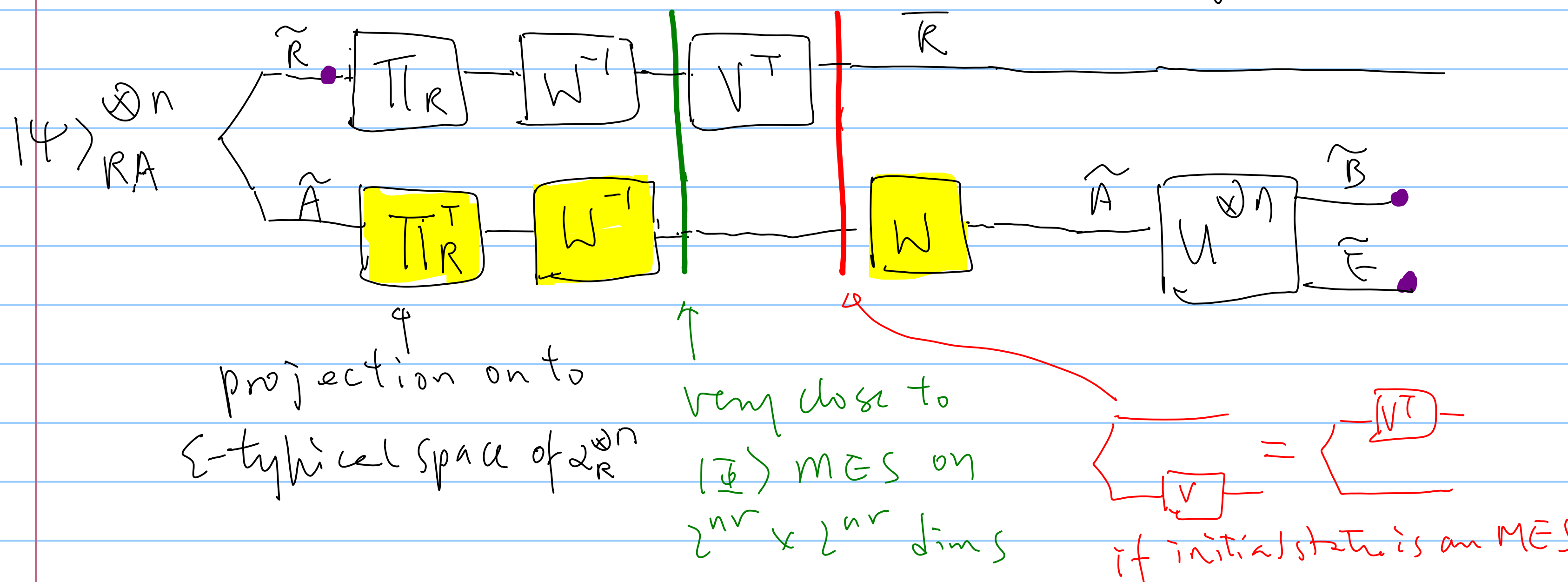


embedding 2^{nr} dim in $2^{n(S(R)+\epsilon)}$ dim but $r \approx S(R) \approx I_c(R\rangle B)$ $\therefore \mathrm{Emb}' = I$

taking $|i\rangle$ to ith basis state of ϵ, δ typical space of $\alpha_R^{\otimes n}$. ie W^{-1} compresses $\alpha_R^{\otimes n}$.

$\tilde{X} = X^{\otimes n}$ for $X = R, A, B, E$

What's the state of $\tilde{R}\,\tilde{B}\,\tilde{E}$? Very close to:



- But the highlighted boxes don't change $|\psi\rangle_{RA}^{\otimes n}$
- So if all ops on the lower branch & none on upper branch are applied, state on $\tilde{R}\,\tilde{B}\,\tilde{E}$ (labeled by the 3 purple dots) is

$\approx \left[(I_R \otimes U)|\psi\rangle\right]^{\otimes n} \approx |\alpha\rangle^{\otimes n}$.

- The ops on the upper branch projects $\tilde{R}$ onto the $\approx$ max mixed state on 2^{nr} dims, and unitarily transforms the latter by V^T.

$\therefore$ Output from both circuits $\approx \left((V_T W^{-1} \Pi_R)_{\tilde{R}} \otimes I_{\tilde{B}\tilde{E}} (|\alpha\rangle) \right)^{\otimes n}$

trace $\tilde{B}$

Next, show approx decoupling "for the average V_T":

Let $\rho_{\bar{R}\tilde{E}} = \mathrm{Tr}_{\hat{B}} (V_T W^{-1} \Pi_R)_{\tilde{R}} \otimes I_{\tilde{B}\hat{B}} (|\alpha\rangle\langle\alpha|)^{\otimes n} (V_T W^{-1} \Pi_R)^{\dagger}_{\tilde{R}} \otimes I_{\tilde{B}\hat{B}}$

Claim: $\underbrace{\int dV}_{\text{Haar meas}} \left\| \rho_{\bar{R}\tilde{E}} - \frac{I}{2^{nr}} \otimes \rho_{\tilde{E}} \right\|_{tr}^2 \leq (\dim \bar{R}\tilde{E}) \, \mathrm{Tr}(\rho_{\bar{R}\tilde{E}})^2$

conjugated by V_T, a little like randomizing $\bar{R}$.

$\boxed{\text{Explain RHS.}}$

(Proof: see reference 0702005 or Preskill's notes.)

If we project $\tilde{E}$, $\tilde{B}$ onto ε - typical spaces for $\alpha_E^{\otimes n}$, $\alpha_B^{\otimes n}$

Call these $\bar{E}$, $\bar{B}$, the joint state is nearly unchanged.

$\therefore$ ① $\dim \bar{R}\bar{E} \approx 2^{nr} \times 2^{n(S(E)+\varepsilon)}$

② $(\rho_{\bar{R}\bar{E}})^2$ has same spectrum as $(\rho_{\bar{B}})^2$

$\rho_{\bar{B}}$'s spectrum : eigenvalue of $\approx 2^{-nS(B)}$ $\approx 2^{nS(B)}$ times

$(\rho_{\bar{B}}^2)$ spectrum : eigenvalue of $\approx 2^{-2nS(B)}$ $\approx 2^{nS(B)}$ times

$\therefore \operatorname{tr}(\rho_{\bar{B}})^2 \approx 2^{-nS(B)}$

$\therefore \int dV \left\| \rho_{\bar{R}\tilde{E}} - \frac{I}{2^{nr}} \otimes \rho_{\tilde{E}} \right\|_{tr}^2 \leq (\dim \bar{R}\tilde{E}) \, \mathrm{Tr}(\rho_{\bar{R}\tilde{E}})^2$

$$\leq 2^{nr} \, 2^{n(S(E)+\delta)} \cdot 2^{-n(S(B)-\varepsilon)}$$

$$= 2^{n[r - I_c(R>B) + 2\varepsilon]}. \qquad (I_c(R>B)_\alpha = S(B)_\alpha - S(E)_\alpha)$$

$\therefore$ if $r = I_c(R>B) - \delta_n$ for $\delta_n = \frac{1}{\sqrt{n}}$, averaged over V,

then $\bar{R}\tilde{E}$ decoupled (to trace distance $\leq 2^{-\sqrt{n}+2\varepsilon}$).

$\therefore \exists$ at least one V achieving that.

$\therefore$ by part 2, $\bar{B}$ can be decoded (unitarily) to

B_1 (max ent w/ $\bar{R}$) & B_2 (max ent w/ $\tilde{E}$) with error $2\sqrt{2^{-\sqrt{n}+2\varepsilon}}$.

$\therefore\ \forall\, |\psi\rangle_{RA}\ ,\ I_c(R\rangle B)_{I\otimes N(|\psi\rangle)}$ achievable

$\therefore\ Q^{(1)}(N) = \max_{|\psi\rangle} I_c(R\rangle B)_{I\otimes N(|\psi\rangle)}$ achievable

$\therefore\ Q^{(m)}(N) = \frac{1}{m} Q^{(1)}(N^{\otimes m})$ achievable $\forall m$

$\therefore\ Q(N) \geq \sup_m Q^{(m)}(N)$

$=$

due to converse.

Note: we're analyzed $Q(N)$ by considering the task of generating entanglement between reference & Bob.

(Reference keeps half of MES & gives half to Alice who encodes & transmits it via n uses of N.)

To transmit quantum data with small worse case error, a good subcode should be used, but the rate essentially unchanged.

Summary:

- Coherent info
- Fannes Ineq, Alicki-Fannes Ineq.
- Decoupling condition
- Uhlmann's Theorem
- 3rd class of random codes.
- LSD theorem