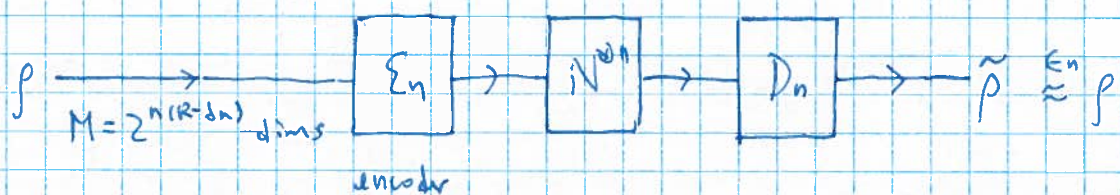
CO781 / QIC890 Lec 16 Nov 08, 2016

Transmitting quantum data via noisy quantum channel

Concepts concerning QECC & asymptotic similar to earlier discussions.

Def: Given a quantum channel $\mathcal{N}$, r is an achievable rate if $\forall n$, $\exists$ (M,n) code transmitting M-dim q states with n uses of $\mathcal{N}$, $M \geq 2^{n(r-\delta_n)}$, error ϵ_n, & $\delta_n, \epsilon_n \to 0$

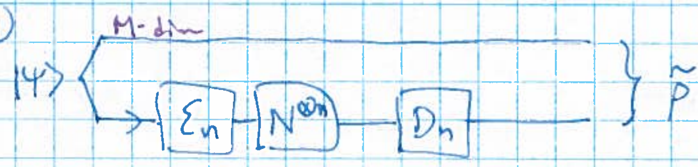


Def: Quantum capacity $Q(\mathcal{N})$ = supremum over achievable rates

see 2012 lec 12-13

How to define ϵ_n? Plausible options:

(1)



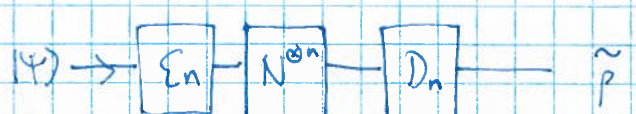
$\langle\psi|\rho|\psi\rangle \geq 1-\epsilon_n$

(a) for all $|\psi\rangle$ (*) sim of perfect channel in diamond norm. $nN \geq \log M$ qbits

(b) for $|\psi\rangle$ = MES only

NB: $\exists \mathcal{N}_1, \mathcal{N}_2$ s.t. $\|\mathcal{N}_1-\mathcal{N}_2\|_\diamond \gg \|I\otimes\mathcal{N}_1(\Phi) - I\otimes\mathcal{N}_2(\Phi)\|_1$

(2)



(a) $\min \langle\psi|\tilde\rho|\psi\rangle \geq 1-\epsilon_n$

(b) ave - - - - - -

(*) [(2a) with $\epsilon_n \Rightarrow$ (1a) with $\frac{3\epsilon_n}{2}$ BKN98 or NC p.429]

NB $\exists \mathcal{N}_1, \mathcal{N}_2$ s.t. $\|\mathcal{N}_1-\mathcal{N}_2\|_\diamond \gg \max_{|\psi\rangle} \|\mathcal{N}_1(|\psi\rangle\langle\psi|) - \mathcal{N}_2(|\psi\rangle\langle\psi|)\|_1$

In 9809010, 0311037, all 4 measures give the same $Q(\mathcal{N})$!

Barnum, Knill, Nielsen   Kretschmann, (R) Werner

Def: Coherent info for a quantum state

Let ρ be a state on RB.

$$I_c(R\rangle B)_\rho := \left[S(B) - S(RB)\right]_\rho$$

Aside: above $= -S(R|B)$, why a separate name?

I_c has well recognized operational meaning since 1996

$S(\cdot|\cdot)$ has little "status" before 2005.

Interpretation:

Let $|\psi\rangle_{RBE}$ be a purification of ρ.

Then
$$I_c(R\rangle B)_\rho := \left[S(B) - S(RB)\right]_\rho$$
$$= \left[S(B) - S(E)\right]_{|\psi\rangle\langle\psi|}$$
$$= \frac{1}{2}\left[S(B:R) - S(E:R)\right]_{|\psi\rangle\langle\psi|}$$

$$S(B) + \cancel{S(R)} - S(BR) \qquad S(E) + \cancel{S(R)} - S(ER)$$

So $I_c(R\rangle B)_\rho$ is $\frac{1}{2}\times$ how much more B is correlated with R than E is.

e.g.	ρ_{RB}	$S(B)$	$S(E)$	$I_c(R\rangle B)$	$S(B:R)$	$S(E:R)$
	$\frac{1}{\sqrt{2}}(\|00\rangle + \|11\rangle)$	1	0	1	2	0
	$\frac{1}{2}(\|00\rangle\langle 00\| + \|11\rangle\langle 11\|)$	1	1	0	1	1
	$\|00\rangle\langle 00\|$	0	0	0	0	0
	$\frac{I}{2}\otimes\|0\rangle\langle 0\|$	0	1	-1	0	2
	$\|0\rangle\langle 0\|\otimes\frac{I}{2}$	1	1	0	0	0

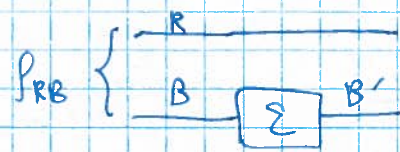
$\approx$ Q correlation $\qquad \approx$ total correlation

Properties of the coherent information $I_c(R\rangle B) := S(B) - S(RB)$

① Invariant under local unitaries (on R, B separately)

② Invariant under attaching / discarding local pure states

③ Nonincreasing under TCP maps on B

Pf: 

Note $I_c(R\rangle B) = S(B) - S(RB)$

$= S(B:R) - S(R)$

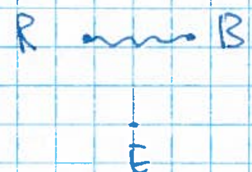
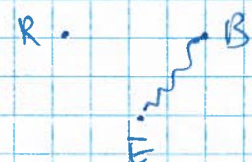
By monotonicity of QMI, $S(B:R)_\rho \geq S(B':R)_{I\otimes\mathcal{E}(\rho)}$

Meanwhile, ρ_R & $S(R)$ unchanged.

$\therefore I_c(R\rangle B)_\rho \geq I_c(R\rangle B')_{I\otimes\mathcal{E}(\rho)}$

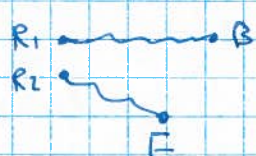
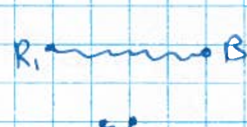
* This is called the quantum data processing inequality.

☆ ④ Discarding a subsystem of R may increase or decrease $I_c(R\rangle B)$:

eg 1  $\xrightarrow[\text{(give R to E)}]{\text{Discard R}}$ 

$\frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{RB}|0\rangle_E \longrightarrow |0\rangle_R \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{BE}$

$I_c(R\rangle B) = 1 \longrightarrow I_c(R\rangle B) = 0$

eg 2  $\xrightarrow{\text{Discard } R_2}$ 

$R_2 E = E'$

$I_c(R\rangle B) = 0$ $\qquad$ $I_c(R\rangle B) = 1$

$\quad\| \qquad\qquad\qquad\qquad \|$

$S(B) - S(E) = 1-1$ $\qquad$ $S(B) - S(E') = 1-0$

* So $I_c(R\rangle B)$ not monotonic wrt TCP maps on R!!

⑤ <u>Continuity</u>

<u>Recall the Fannes-Alicki ineq</u>

Let $\rho, \sigma \in B(\mathbb{C}^{d_A} \otimes \mathbb{C}^{d_B})$, $\|\rho - \sigma\|_1 \leq \delta$

Then $|S(A|B)_\rho - S(A|B)_\sigma| \leq 4\delta \log d_A + 2h(\delta)$

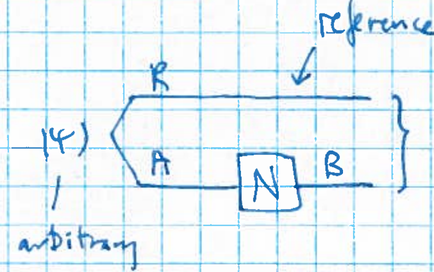
binary entropy function

Since $I_c(R\rangle B) = S(B) - S(RB) = -S(R|B)$

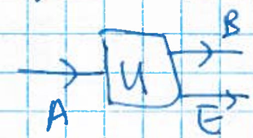
$\therefore \quad |I_c(R\rangle B)_\rho - I_c(R\rangle B)_\sigma| \leq 4\delta \log R + 2h(\delta)$

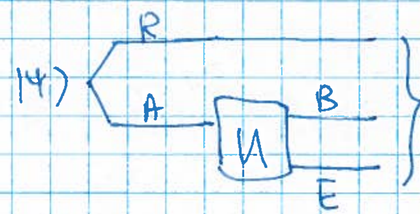
Coherent info for channels:

For the channel 

& 

$I\otimes N(|\psi\rangle\langle\psi|)$

use the isometric extension for N: 

and consider 

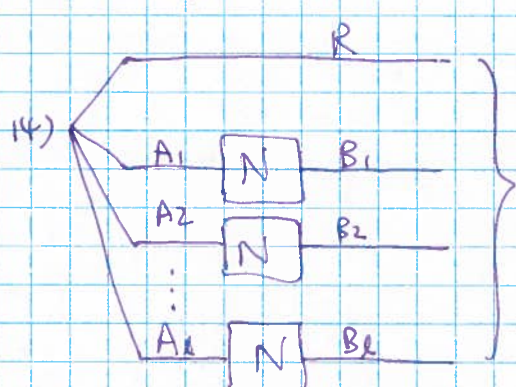
$(I\otimes U)|\psi\rangle = |\alpha\rangle_{RBE}$

Def: $Q^{(1)}(N) = \max_{|\psi\rangle} I_c(R\rangle B)_{I\otimes N(|\psi\rangle\langle\psi|)} = \max_{|\psi\rangle} [S_B - S_E]_{|\alpha\rangle}$

It is the max diff between $S(B{:}R)$ & $S(E{:}R)$ made possible by 1 use of N.
over initial state

Def: $Q^{(l)}(N) = \frac{1}{l} Q^{(1)}(N^{\otimes l})$

$$= \max_{|\psi\rangle_{RA_1A_2\ldots A_l}} I_c(R\rangle B_1\ldots B_l)_{I\otimes N^{\otimes l}(|\psi\rangle\langle\psi|)}$$



$I_R\otimes N^{\otimes l}(|\psi\rangle\langle\psi|)$

NB: Take $|\psi\rangle = |\psi_1\rangle_R |\psi_2\rangle_A$, then BE is in a pure state

so $I_c(R\rangle B) = 0$ $\therefore$ $Q^{(1)}(N) \geq 0$.

$$\boxed{\text{The LSD thm: } Q(N) = \sup_{\ell} Q^{(\ell)}(N)}$$

Lloyd 96 Shor 02 Devetak 04

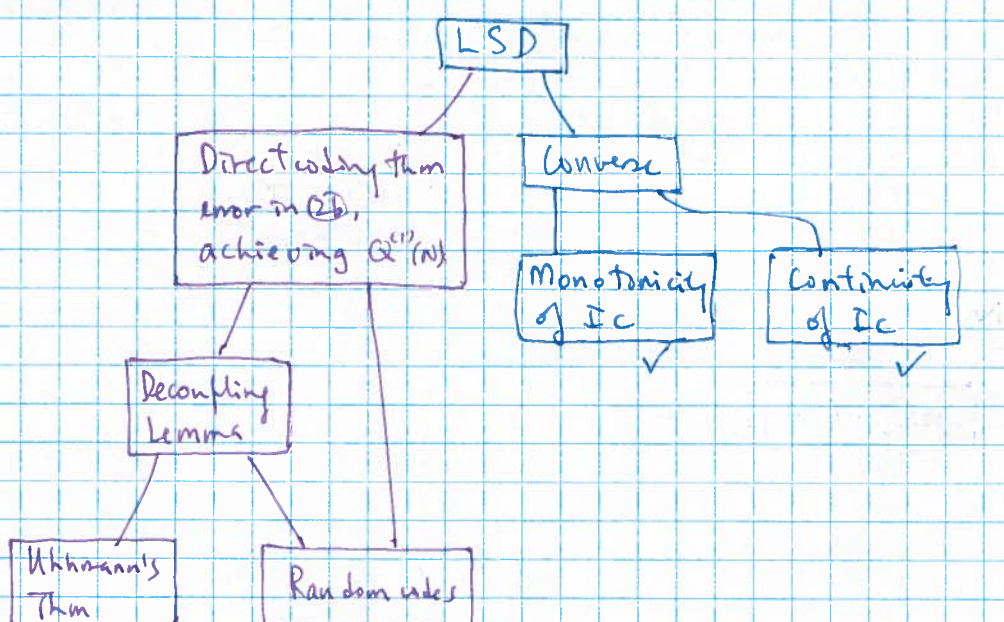
NB: for $C(N)$, we max $S(B:R)$ for $\rho_{RB} = \sum_x p_x |x\rangle\langle x|_R \otimes N^{\otimes \ell}(\rho_x)_B$ $B_1 B_2 \ldots B_\ell$.

for $Q(N)$, - . $S(B:R) - S(R:E)$ for $|\alpha\rangle_{RBE} = I \otimes U^{\otimes \ell}(|\psi\rangle_{RA})$ $E_1 \ldots E_\ell$ $A_1 \ldots A_\ell$

Interpretation: E cannot have info about R if Bob is to receive near perfect transmission. This follows from the "information gain implies disturbance" principle.

So Bob has to decorrelate E from R, by consuming an equal amount of his correlation with R.

Proof outline:



Direct quantum proof ...
Hayden et al 0702005

Also available in Watrous book, entanglement assisted version + BH model in Preskill's notes

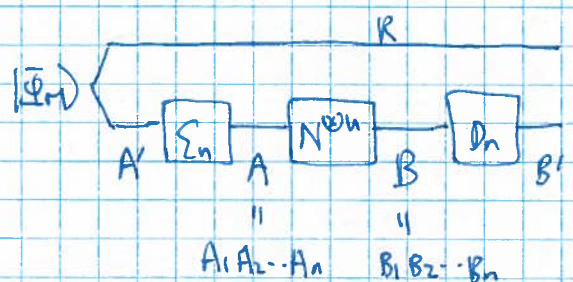
Converse:

Suppose r achievable.

Then $\exists\,(M, n)$ codes, $M = \lfloor 2^{n(r-\delta_n)} \rfloor$

s.t. $\left\| (I \otimes \mathcal{D}_n \circ \mathcal{N}^{\otimes n} \circ \mathcal{E}_n)(\Phi_M) - \Phi_M \right\|_1 \leq \epsilon_n \quad \leftarrow (*)$

where $\Phi_M = |\Phi_M\rangle\langle\Phi_M|$, $\quad |\Phi_M\rangle = \frac{1}{\sqrt{M}} \sum_{i=1}^{M} |i\rangle|i\rangle$.



We have:

$$I_c(R\rangle B)_{I \otimes \mathcal{N}^{\otimes n} \circ \mathcal{E}_n(\Phi_M)}$$

$$\overset{\text{mono}}{\geq} I_c(R\rangle B')_{I \otimes \mathcal{D}_n \circ \mathcal{N}^{\otimes n} \circ \mathcal{E}_n(\Phi_M)}$$

$$\overset{\text{cty}, (*)}{\geq} I_c(R\rangle B')_{\Phi_M} + 4\epsilon_n \log M + 2h(\epsilon_n)$$

$$= (1+4\epsilon_n)\underbrace{n(r-\delta_n)}_{\log M} + 2h(\epsilon_n)$$

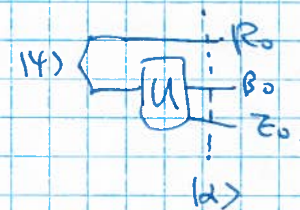
$$\therefore \max_{|\psi\rangle} \frac{1}{n} I_c(R\rangle B)_{I \otimes \mathcal{N}^{\otimes n}(|\psi\rangle\langle\psi|)} \geq \frac{1}{n} I_c(R\rangle B)_{I \otimes \mathcal{N}^{\otimes n}(\Phi_M)}$$

$$\geq (1+4\epsilon_n)(r-\delta_n) + \frac{1}{n} 2h(\epsilon_n)$$

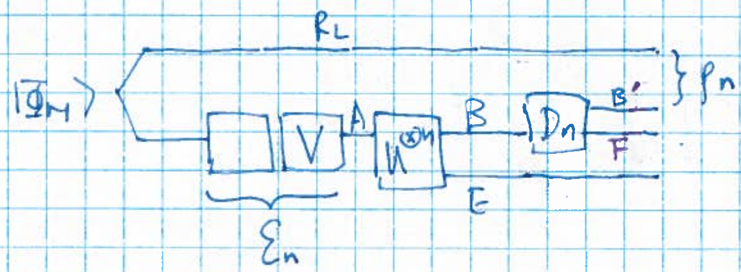
As $n \to \infty$, $\underbrace{\sup_n Q^{n}(\mathcal{N})}_{= Q(\mathcal{N})} \geq r$.

Direct coding thm:

- Let U = isometric extension of N.
- For any $|\psi\rangle_{R_0 A_0}$, let $|\omega\rangle = \underbrace{I_{R_0} \otimes U(|\psi\rangle)}_{\text{lives on } R_0 B_0 E_0}$



- We show $\exists (M,n)$ code achieving the following:



$A = A_1 \ldots A_n$, $B = B_1 \ldots B_n$, $E = E_1 \ldots E_n$

$M \geq 2^{n(r-\delta_n)}$, $\| \rho_n - \Phi_M \|_1 \leq \epsilon_n$

$r = I_c(R_0 \rangle B_0)_{|\omega\rangle}$

- We consider a random choice of codes where

  —[ ]— embeds $\mathbb{C}^M$ into $A = A_1 \ldots A_n$

  —[V]— is drawn according to the Haar measure, $V \in \mathcal{U}(A_1 \ldots A_n)$

Keep on board ?

⊙ To upper bound the error ϵ_n, we show the state on R_L & E is close to a product state, which implies $\exists D_n$ s.t., to good approx., R_L is purified by B' and E is purified by F, separately.

} Called the decoupling approach to showing the direct coding thm.

Requires : ① Why R_L & E decoupled $\Rightarrow$ separate purification

② Why on average over V, R_L & E decoupled approx

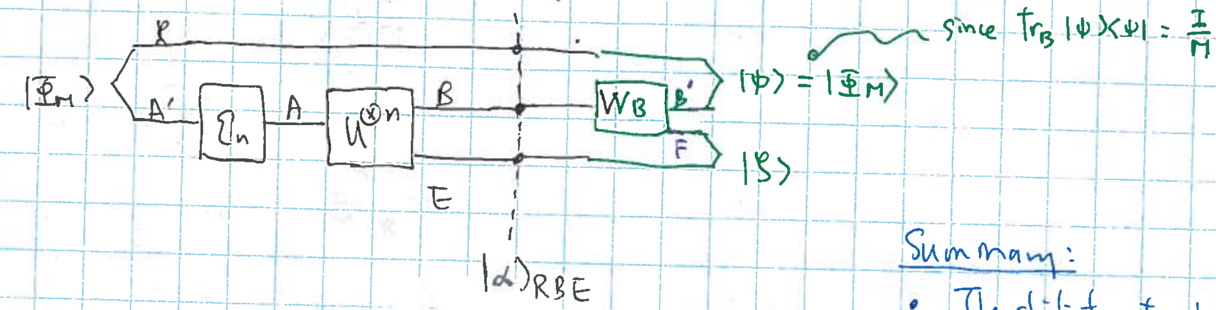
Together $\exists V$ s.t. R_L & E decoupled enough so R_L purified by B' resulting in the desirable Φ_M on R_L & B'.

- Replace N by $N^{\otimes \ell}$ and repeat the above argument gives the existence of codes attaining rate $Q^{(\ell)}(N)$ under the error meas (1b) (for creating max entangled states)

- Finally, apply 9809010 / 0311037 (trimming the code space) $Q^{(\ell)}(N)$ is achievable for error meas (1a).

Reasoning for ①:

Decoupling (exact case):



NB: E purifies RB & $\underbrace{B \text{ purifies } RE}_{|\alpha\rangle_{RBE} \text{ purifies } \rho_{RE}}$

Summary:

- The ability to perfectly generate $|\Phi\rangle$ on RB' $\Rightarrow \rho_{RE} = \left(\frac{I}{M}\right)_R \otimes \rho_E$ ($\because U_B$ exists ...)
- If $\rho_{RE} = \left(\frac{I}{M}\right)_R \otimes \rho_E$ then, $\exists\, W_B$ to generate $|\Phi\rangle$ on RB'

Observation:

- If $\rho_{RE} = \rho_R \otimes \rho_E$

  then we have another purification: $|\phi\rangle_{RB'} \otimes |\xi\rangle_{EF}$

  where $B = B'F$, $|\phi\rangle_{RB'}$ purifies ρ_R

  $|\xi\rangle_{EF}$ .. ρ_E.

- Recall any 2 purifications differ by a unitary on the purifying system. (Sec 2.5 NC Ex 2.81).

- $\exists W_B$ s.t. $(W_B \otimes I_{RE}) \underbrace{|\alpha\rangle_{RBE} = |\phi\rangle_{RB'} \otimes |\xi\rangle_{EF}}_{\text{both are purifications of } \rho_{RE}}$

- See diagram

Interpretation: ① purification of R is BE, and ② E contains none of it
$\therefore$ B contains the entire purification

Decoupling (exact) $\Leftrightarrow$ $\mathcal{E}_n$ works & $\frac{1}{n}\log M$ achievable.

Approx decoupling $\Rightarrow$ approx transmission of $|\Phi_M\rangle$

<u>Lemma</u>:

If $\| \rho_{RE} - \left(\frac{I}{M}\right)_R \otimes \rho_E \|_1 \le \varepsilon'$

then $\exists\, |\alpha\rangle_{REB}$ purifying ρ_{RE}, for $B = B'F$

s.t. $\| \mathrm{tr}_{EF}\, |\alpha\rangle\langle\alpha|_{REB} - |\Phi_M\rangle\langle\Phi_M|_{RB'} \|_1 \le 2\sqrt{\varepsilon'}$

Pf: (tr dist $\Rightarrow$ F $\Rightarrow$ F of purification $\Rightarrow$ tr dist)

- Recall $1 - F(\mu, \nu) \le \frac{1}{2} \| \mu - \nu \|_1$ ($\forall\, \mu, \nu$ states)

  $\therefore\ F\left(\rho_{RE}, \left(\frac{I}{M}\right)_R \otimes \rho_E\right) \ge 1 - \frac{\varepsilon'}{2}$

- Recall [Uhlmann] $F(\mu, \nu) = \max\limits_{\substack{|\alpha\rangle, |\beta\rangle \\ \text{purifies } \mu \quad \text{purifies } \nu}} |\langle\alpha|\beta\rangle| = \max\limits_{\substack{|\alpha\rangle \\ \text{purifies } \mu}} |\langle\alpha|\beta_0\rangle|$ — fixed purification of ν.

  since any $|\beta\rangle = U \otimes I |\beta_0\rangle$, absorb U into $\langle\alpha|$

- Choose $|\beta_0\rangle = |\Phi\rangle_{RB'} \otimes |\xi\rangle_{EF}$, $\nu = \left(\frac{I}{M}\right)_R \otimes \rho_E$, $\mu = \rho_{RE}$

  Then: $\exists\, |\alpha\rangle_{REB}$ attaining the max in $F(\mu, \nu)$

  $\therefore\ 1 - \frac{\varepsilon'}{2} \le F\left(\rho_{RE}, \left(\frac{I}{M}\right)_R \otimes \rho_E\right) = F\left(|\Phi_M\rangle_{RB'} \otimes |\xi\rangle_{EF}, |\alpha\rangle_{REB}\right)$

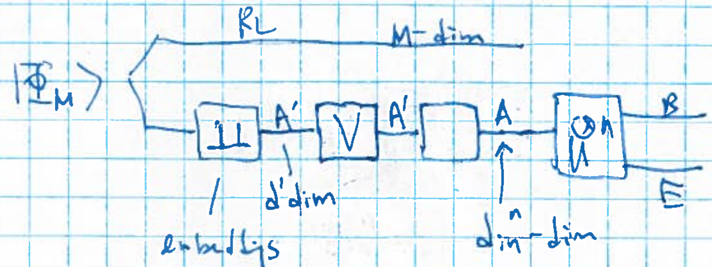
- Recall $\frac{1}{2} \| \mu - \nu \|_1 = \sqrt{1 - F(\mu, \nu)^2}$ if μ, ν pure. Apply to the 2 purifications:

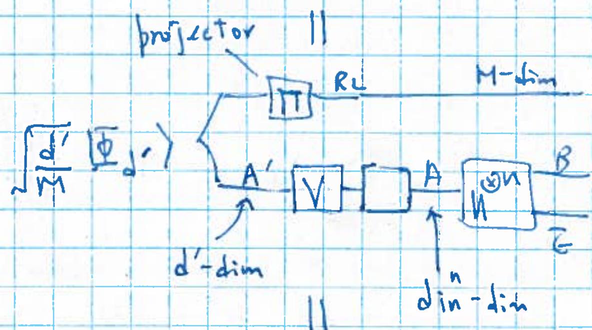
  $\therefore\ \| |\alpha\rangle\langle\alpha|_{REB} - |\Phi_M\rangle\langle\Phi_M|_{RB'} \otimes |\xi\rangle\langle\xi|_{EF} \|_1$

  $= 2\sqrt{1 - F\left(|\alpha\rangle_{REB}, |\Phi_M\rangle_{RB'} |\xi\rangle_{FE}\right)^2}$ $\quad [(1-f^2) = (1-f)(1+f)]$

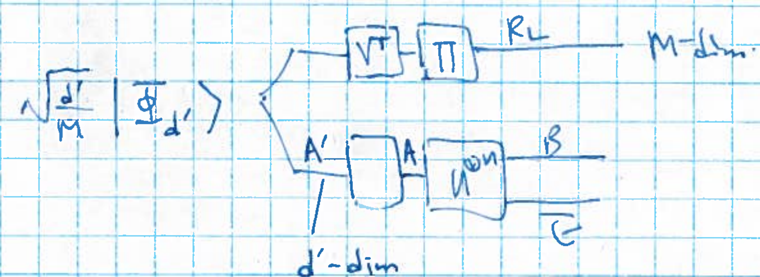
  $\le 2\sqrt{2}\sqrt{1-F} \le 2\sqrt{\varepsilon'}$, Finally, Tracing out EF, $\|\ \|_1$ non increasing.

② Why on average over V, R_L & E decoupled approx:





(by transpose trick)



Lemma: (0702005 Thm III)

Let ① ρ^{SE} be max mixed on S

② $P^{S\to R}$ be a projector into 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 $\left\| \psi_U^{RE} - \frac{I_R}{|R|} \otimes \psi^E \right\|_2^2 = \mathrm{Tr}\left(\psi_U^{RE}\right)^2 - \frac{1}{|R|} \mathrm{Tr}\left(\psi^E\right)^2$

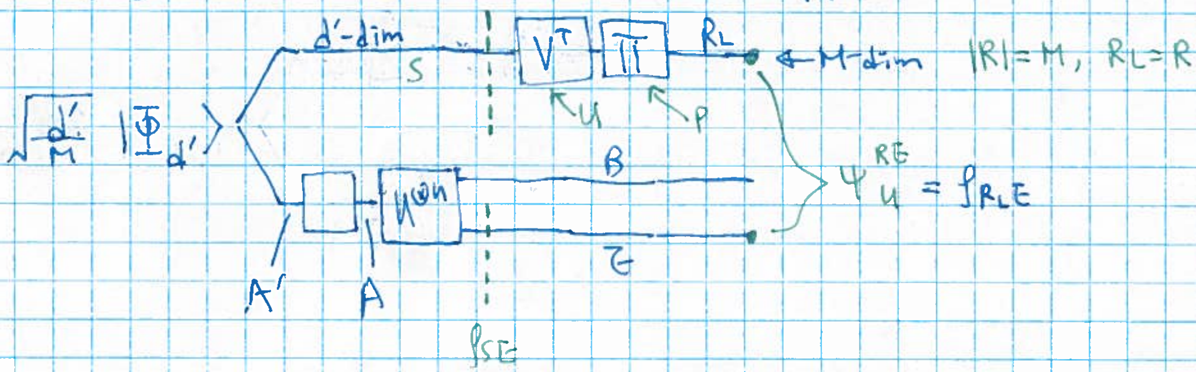
② $\int dU \left\| \psi_U^{RE} - \frac{I_R}{|R|} \otimes \psi^E \right\|_2^2 \leq \mathrm{Tr}\left(\rho^{SE}\right)^2$

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

Pf: See supp notes on course website.

(or Watrous book)

Identifying objects in lemma w/ decoupling problem:

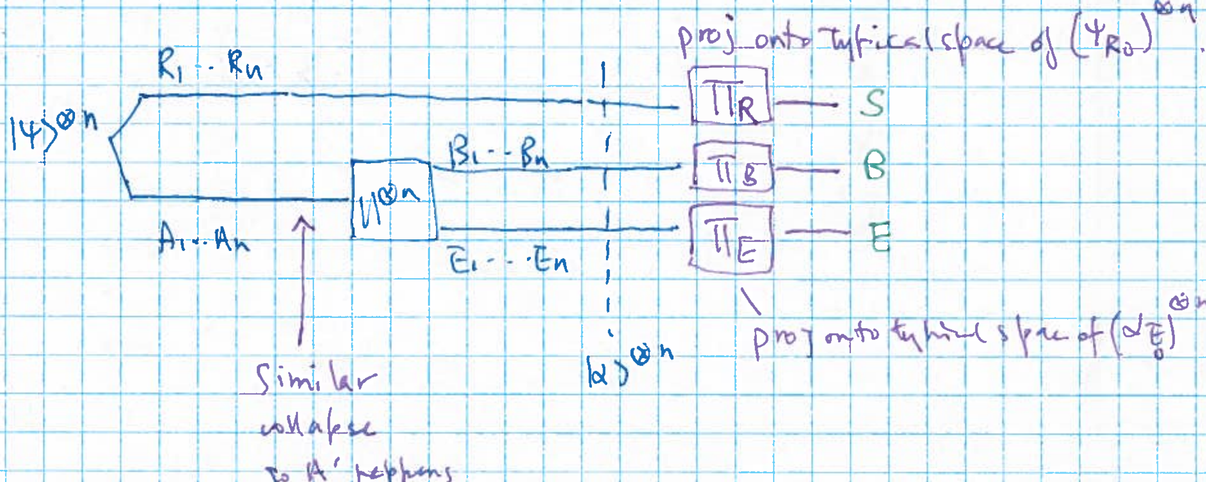


(if LHS is $|\Phi_{d'}\rangle$ w/o the factor $\sqrt{\frac{d'}{M}}$)

So conclusion ① gives:

$$\int dV^T \ \left\| \rho_{R_L E} - \left(\frac{I}{M}\right)_{R_L} \otimes \rho_E \right\|_1^2 \overset{(\ddagger)}{\leq} M \cdot |E| \ tr\left(\rho^{SE}\right)^2$$

Next: Replace the state @ the green dotted line (whose reduction on SE is ρ_{SE}) by the following (as a first step):



$\left(tr\left(\frac{I}{d}\right)^2 = \frac{1}{d} \right)$

Then ρ_{SE} "almost" max on S, Π_R, Π_B, Π_E succeeds whp, and state largely unchanged by the GML.

Then, $\dim E \approx 2^{-n S(E_0)_\alpha}$, $tr(\rho_B)^2 \approx 2^{-n S(B_0)_\alpha}$
$\approx$ max mixed.

$\therefore M \leq 2^{n[I_c(R_0 \rangle B_0)_\psi - \delta_n]}$ makes RHS of $(\ddagger)$ vanish.