Decoupling Method in Quantum Shannon Theory

Toby Cubitt

Much of the following material (and more!) was originally proven in arXiv:quant-ph/0606225

These notes largely follow Section 10.9 of Preskill's wonderful lecture notes, with a (very) few changes / additions.

Before the decoupling method, results in quantum Shannon theory (capacity formulae etc.) were proven using ad-hoc methods. Each result had to be proven separately, the proofs were long & complicated*, and there was no unifying principle behind them (in the way random coding & typical sets serve as unifying principles classically).

*If you think the proofs in these notes are long, read the pre-decoupling proofs!

The decoupling method + the "Church of the larger Hilbert space" (i.e. always purify everything before analysing) provide those unifying principles. Using these, we can prove essentially <u>all</u>† results in quantum Shannon theory!

†Even the classical capacity formula, see arXiv:1207.0067

Fundamental intuition: "if we can decorrelate output from environment, we can communicate quantumly".

Notation & Definitions

$A, B \in \mathcal{M}_d$ (i.e. $d \times d$ matrices)

- $\|A\| = \|A\|_\infty := \sup_{|\psi\rangle \in \mathcal{H}} \frac{\|A|\psi\rangle\|}{\||\psi\rangle\|}$
  operator norm (Schatten ∞-norm)
  unitarily invariant: $\|UAU^\dagger\| = \|A\|$

- $\|A\|_1 := \operatorname{tr}|A| = \operatorname{tr}\sqrt{A^\dagger A}$
  trace norm (Schatten 1-norm)
  unitarily invariant; note for $A \geq 0$, $\|A\|_1 = \operatorname{tr} A$

- $\|A\|_p := (\operatorname{tr}|A|^p)^{1/p} = (\operatorname{tr}(A^\dagger A)^{p/2})^{1/p}$
  Schatten p-norm

- Recall all norms satisfy triangle inequality:
  $\|A+B\| \leq \|A\| + \|B\|$

- Submultiplicativity: $\|AB\|_p \leq \|A\|_p \|B\|_p$

- Monotonicity: $\forall\ 1 \leq p \leq q \leq \infty : \|A\|_p \geq \|A\|_q$

- Every norm defines a distance measure: $\|A - B\|$

- $H_p := \frac{1}{1-p} \log(\operatorname{tr}\sigma^p)$
  Renyi p-entropy of density matrix σ:

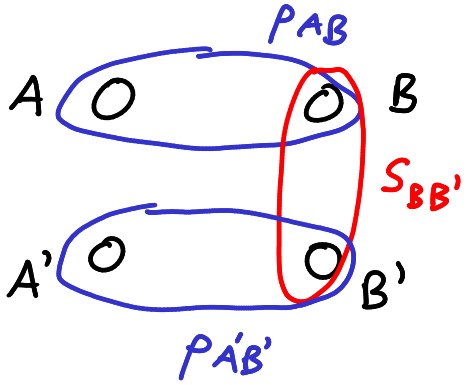
- $\lim_{p \to 1} H_p(\sigma) = H(\sigma)$ von Neumann entropy

- Monotonicity $\forall\ 1 \leq p \leq q \leq \infty : H_p(\sigma) \leq H_q(\sigma)$

Lemma ("Swap trick")

$$\mathrm{tr}(\rho_B^2) = \mathrm{tr}\left[(\mathbb{1}_{AA'} \otimes S_{BB'})(\rho_{AB} \otimes \rho_{A'B'}) \right]$$

where $S_{BB'} |\psi\rangle_B |\varphi\rangle_{B'} = |\varphi\rangle_B |\psi\rangle_{B'}$ Swap operation



Theorem (Uhlmann)

Fidelity $F(\rho,\sigma) := \mathrm{tr}\sqrt{\rho^{1/2}\sigma\rho^{1/2}}$.

$$F(\rho,\sigma) = \max_{|\psi\rangle_{AE}} \langle\psi|\varphi\rangle \quad \text{where} \quad \mathrm{tr}_E |\psi\rangle\langle\psi|_{AE} = \rho_A, \quad \mathrm{tr}_E |\varphi\rangle\langle\varphi|_{AE} = \sigma_A$$

$$= \max_{U_E} \langle\psi|U|\varphi\rangle \quad \text{for any fixed } |\psi\rangle, |\varphi\rangle \text{ s.t. } \mathrm{tr}_E |\psi\rangle\langle\psi|_{AE} = \rho_A, \quad \mathrm{tr}_E |\varphi\rangle\langle\varphi|_{AE} = \sigma_A$$

Lemma (equivalence of fidelity & trace-distance)

$$1 - F(\rho,\sigma) \leq \tfrac{1}{2}\|\rho-\sigma\|_1 \leq \sqrt{1-F(\rho,\sigma)^2}$$

Lemma (partial trace identity)

$$\mathrm{tr}_{AB}(\mathbb{1}_A \otimes M_B \cdot X_{AB}) = \mathrm{tr}_B(M_B \cdot \mathrm{tr}_A(X_{AB})).$$

Theorem (Stelnspring dilation)

CPTP map (aka quantum channel) $\mathcal{E}$.

$\mathcal{E}(\rho) = \mathrm{tr}_E \left(V_{A\to BE}\, \rho\, V_{A\to BE}^\dagger \right)$

for some Isometry V, i.e. $V^\dagger V = \mathbb{1}$

$= \mathrm{tr}_E \left(U\, \rho_A \otimes |0\rangle\langle 0|_E\, U^\dagger \right)$

for some unitary U, i.e. $U^\dagger U = U U^\dagger = \mathbb{1}$

Theorem (Choi-Jamiołkowski isomorphism)

CPTP map $\mathcal{E} : \mathcal{M}_d \to \mathcal{M}_d$ (i.e. acts on qudits)

Choi-Jam. state $\sigma := \mathcal{E} \otimes \mathcal{I}(\phi)$

where $|\phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle$ max ent., $\phi = |\phi\rangle\langle\phi|$.

Also, $\mathcal{E}(\rho) = d \cdot \mathrm{tr}_A \left(\rho^T \otimes \mathbb{1} \cdot \sigma \right)$

Lemma ("Transpose trick")

For any matrix $M \in \mathcal{M}_d$: (i.e. $d \times d$ matrix)

$$M \otimes \mathbb{1}\ |\phi\rangle = \mathbb{1} \otimes M^T\ |\phi\rangle$$

where $|\phi\rangle = \frac{1}{\sqrt{d}} \sum_{i=1}^{d} |ii\rangle$

Lemma (trivial, but will be used frequently w/out reference)

Pure state $|\psi\rangle_{AB}$: $H(\rho_A) = H(\rho_B)$

$\rho_A := \mathrm{tr}_B |\psi\rangle\langle\psi|_{AB}$, $\rho_B := \mathrm{tr}_A |\psi\rangle\langle\psi|_{AB}$

Proofs: Exercise!

(This means: "Go away & prove all of these yourself!")

The following Lemma is the key technical result behind the decoupling technique.

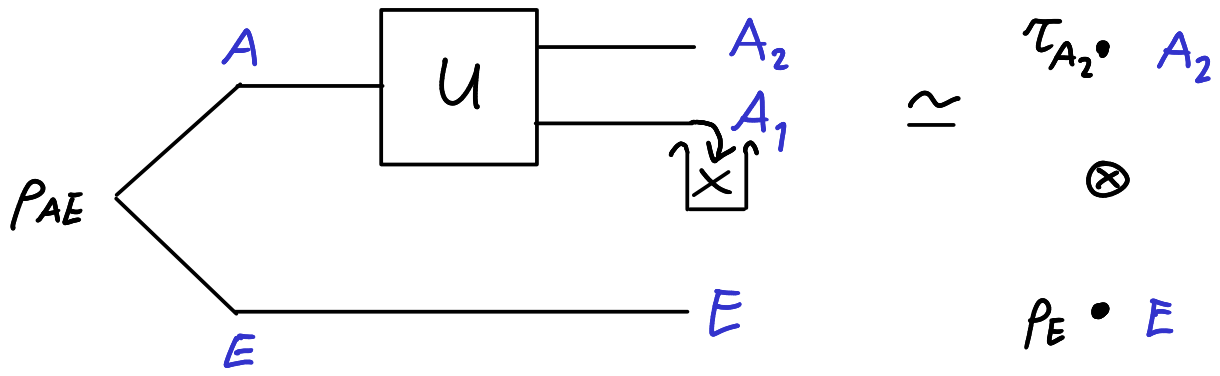
Lemma (Decoupling)

$$\mathbb{E}_U \left[\left\| \mathrm{tr}_{A_1} \left(\underbrace{(U_A \otimes \mathbb{1}_E)\, \rho_{AE}\, (U_A^\dagger \otimes \mathbb{1}_E)}_{\rho_{AE}^{(U)}} \right) - \tau_{A_2} \otimes \rho_E \right\|_1 \right]$$

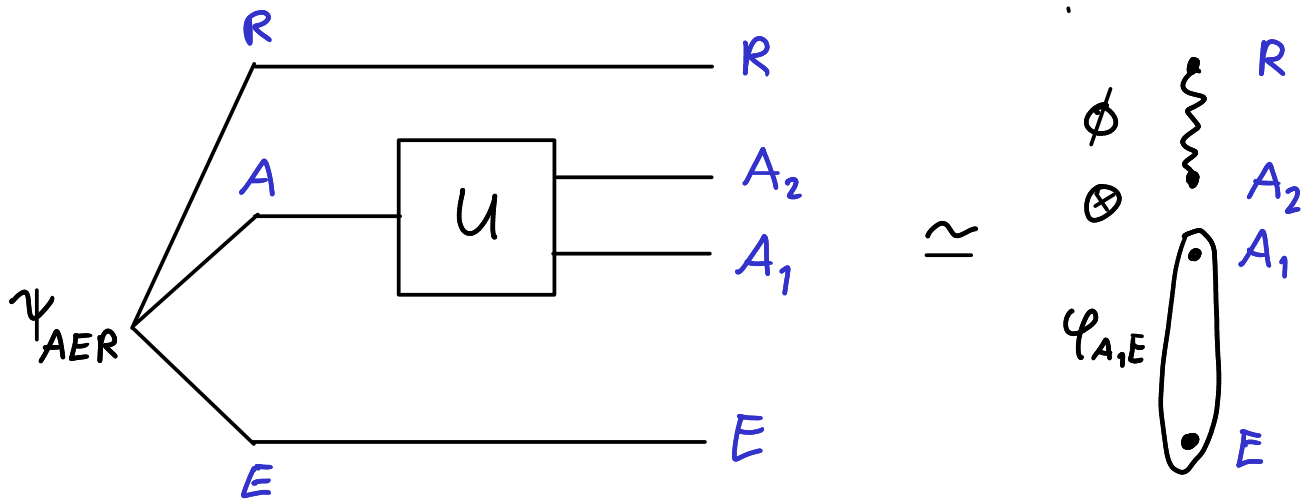
$$\leq \left(\frac{|A_2| \cdot |E|}{|A_1|}\, \mathrm{tr}(\rho_{AE}^2) \right)^{1/2}$$

where $\tau_X := \dfrac{\mathbb{1}_X}{|X|}$

In pictures:



or, taking purifications of everything:



Proof

$$\left(\mathbb{E}_u \left[\| \mathrm{tr}_{A_1}(\rho_{AE}^{(u)}) - \tau_{A_2} \otimes \rho_E \|_1 \right]\right)^2$$

$$\leq \mathbb{E}_u \left[\| \mathrm{tr}_{A_1}(\rho_{AE}^{(u)}) - \tau_{A_2} \otimes \rho_E \|_1^2 \right]$$

$f \geq 0 : (\mathbb{E}[f])^2 \leq \mathbb{E}[f^2]$

$$\leq |A_2| \cdot |E| \cdot \mathbb{E}_u \left[\| \mathrm{tr}_{A_1}(\rho_{AE}^{(u)}) - \tau_{A_2} \otimes \rho_E \|_2^2 \right]$$

$\|M_X\|_1^2 \leq |X| \cdot \|M\|_2^2$

$$\leq |A_2| \cdot |E| \cdot \mathbb{E}_u \left[\mathrm{tr} \left(\mathrm{tr}_{A_1}(\rho_{AE}^{(u)}) - \tau_{A_2} \otimes \rho_E \right)^2 \right]$$

$$= |A_2| \cdot |E| \cdot \mathbb{E}_u \left[\mathrm{tr} \left(\mathrm{tr}_{A_1}(\rho_{AE}^{(u)}) \right)^2 - \frac{1}{|A_2|} \mathrm{tr}(\rho_E^2) \right]$$

expanding & using $\mathrm{tr}(X_{AB} \cdot \mathbb{1}_A \otimes Y_B) = \mathrm{tr}(\mathrm{tr}_A(X_{AB}) Y_B)$

$$= |A_2| \cdot |E| \cdot \left(\mathbb{E}_u \left[\mathrm{tr} \left(\mathrm{tr}_{A_1} (\rho_{AE}^{(u)})^2 \right) \right] - \frac{1}{|A_2|} \mathrm{tr}(\rho_E^2) \right) \quad (*)$$

Now,

$$\mathbb{E}_u \left[\mathrm{tr} \left(\mathrm{tr}_{A_1} (\rho_{AE}^{(u)}) \right)^2 \right]$$

$$= \mathbb{E}_u \left[\mathrm{tr} \left(\left(\mathbb{1}_{A_1 A_1'} \otimes S_{(A_2 E)(A_2' E')} \right) \left(\rho_{AE}^{(u)} \otimes \rho_{A'E'}^{(u)} \right) \right) \right]$$

Swap trick

$$= \mathbb{E}_u \left[\mathrm{tr} \left(\left(U_A^\dagger \otimes \mathbb{1}_E \otimes U_{A'}^\dagger \otimes \mathbb{1}_{E'} \right) \cdot \left(\mathbb{1}_{A_1 A_1'} \otimes S_{A_2 A_2'} \otimes S_{EE'} \right) \right.\right.$$

$$\left.\left. \cdot \left(U_A \otimes \mathbb{1}_E \otimes U_{A'} \otimes \mathbb{1}_{E'} \right) \cdot \rho_{AE} \otimes \rho_{A'E'} \right) \right]$$

$$= \mathrm{tr}\Big(\mathbb{E}_u \left[(U_A^\dagger \otimes U_{A'}^\dagger)\left(\mathbb{1}_{A_1A_1'} \otimes S_{A_2A_2'}\right)(U_A \otimes U_{A'}) \right] \otimes S_{E'E'} \cdot \rho_{AE} \otimes \rho_{A'E'} \Big)$$

linearity of $\mathbb{E}$, i.e. $\mathbb{E}\left[\mathrm{tr}(f)\right] = \mathrm{tr}\left(\mathbb{E}[f]\right)$

Note: $\mathbb{E}_u[\sim\!\!\sim]$ is now expectation of fixed operator $\rightarrow$ "just" calculate!

Turns out $\mathbb{E}_u[\sim\!\!\sim] = c_1 \mathbb{1}_{AA'} + c_2 S_{AA'}$

where $c_{1,2} = \frac{1}{|A_{2,1}|}\left(\frac{1 - 1/|A_{1,2}|}{1 - 1/|A|}\right) \leq \frac{1}{|A_{2,1}|}$

$$= \mathrm{tr}\left((c_1 \mathbb{1}_{AA'} + c_2 S_{AA'}) \otimes S_{EE'} \cdot \rho_{AE} \otimes \rho_{A'E'} \right)$$

$$= c_1 \, \mathrm{tr}\left((\mathbb{1}_{AA'} \otimes S_{EE'})(\rho_{AE} \otimes \rho_{A'E'}) \right) + c_2 \, \mathrm{tr}\left((S_{AA'} \otimes S_{EE'})(\rho_{AE} \otimes \rho_{A'E'}) \right)$$

$$= c_1 \, \mathrm{tr}(\rho_E^2) + c_2 \, \mathrm{tr}(\rho_{AE}^2) \qquad \text{Swap trick}^{-1}$$

$$\therefore \mathbb{E}_u\left[\mathrm{tr}\left(\mathrm{tr}_{A_1}(\rho_{AE}^{(u)}) \right)^2 \right] \leq \frac{1}{|A_2|}\mathrm{tr}(\rho_E^2) + \frac{1}{|A_1|}\mathrm{tr}(\rho_{AE}^2).$$

Using this in (*) we are done. □

Lemma (entanglement distribution $\Rightarrow$ q. communication)

Quantum channel $\mathcal{E}: \mathcal{M}_d \to \mathcal{M}_d$ (CPTP map).

If $\| \mathcal{E} \otimes \mathcal{I} (\phi) - \phi \|_1 \leq \delta$, then

$\forall \rho \quad \| \mathcal{E}(\rho) - \rho \|_1 \leq d\,\delta$.

Proof

$$\| \mathcal{E}(\rho) - \rho \|_1$$

$$= \| d \cdot tr_A \left(\rho^T \otimes \mathbb{1} \cdot \mathcal{E} \otimes \mathcal{I} (\phi) \right) - \rho \|_1 \qquad \text{Choi-Jam.}$$

$$= \| d \cdot tr_A \left(\rho^T \otimes \mathbb{1} \cdot (\phi + \mathcal{E} \otimes \mathcal{I}(\phi) - \phi) \right) - \rho \|_1$$

$$\leq \| d \cdot tr_A (\rho^T \otimes \mathbb{1} \cdot \phi) - \rho \|_1 + d \cdot \| \mathcal{E} \otimes \mathcal{I} (\phi) - \phi \|_1$$

triangle inequality

$$\leq \| d \cdot tr_A (\mathbb{1} \otimes \rho \cdot \phi) - \rho \|_1 + d\delta \qquad \text{transpose trick}$$

$$= \| d \cdot \rho \cdot tr_A(\phi) - \rho \|_1 + d\delta$$

$$= \| \rho \cdot \mathbb{1} - \rho \|_1 + d\delta$$

$$= d\delta \qquad \square$$

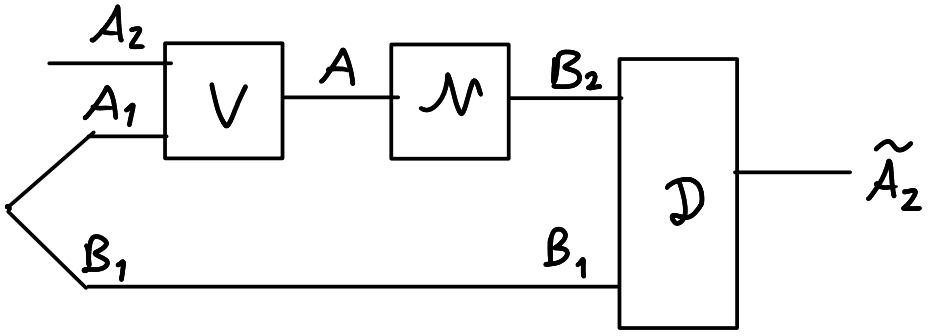
Thm (Father protocol)

$$\langle \mathcal{N}^{A\to B} : \rho_A \rangle + \tfrac{1}{2} I(R;E)[qq] \geq \tfrac{1}{2} I(R;B)[q \to q]$$

I.e. $\forall \varepsilon \; \exists n_0 \; \forall n > n_0$:

n channel uses + $\frac{1}{2} I(R;E)$ e-bits $\Big\lfloor$ $\frac{1}{2} I(R;B)$ qubits of q. communication

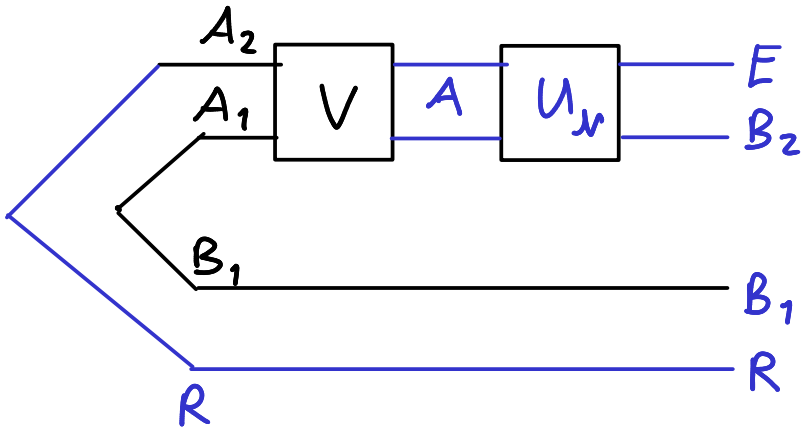
can simulate to fidelity $\geq \varepsilon$



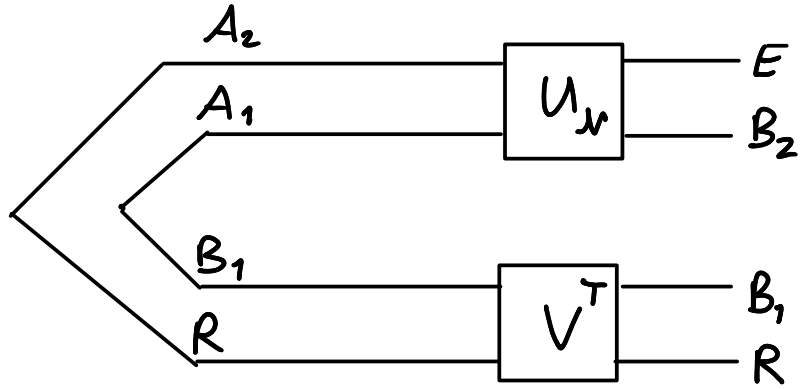
Proof

One-shot version

Purify & ignore decoder:

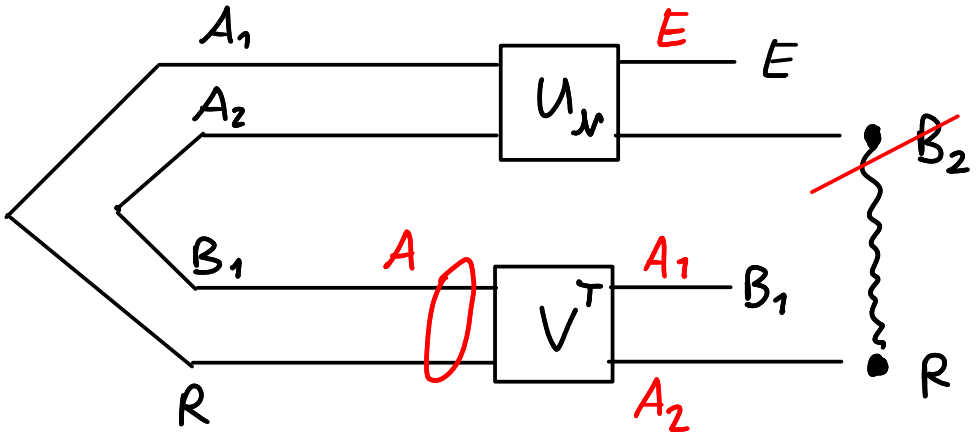


=



in decoupling ineq.

$=$



if R, E decouple ($\equiv$ q. communication by ent. dist. $\Rightarrow$ q. comm. Lemma)

Choose Haar-random V^T ($\Rightarrow V$ Haar-random).

$$\mathbb{E}_V \left[\left\| \mathrm{tr}_{B_1} \left[\mathcal{N} \circ V_{A_1 A_2} \left(\phi_{A_2 R} \otimes \phi_{A_1 B_1} \right) \right] - \phi_{B_2 R} \right\|_1 \right]$$

$$= \mathbb{E}_V \left[\left\| \mathrm{tr}_{B_1} \left((V_{B_1 R} \otimes \mathbb{1}_E) \rho_{B_1 R E} (V_{B_1 R} \otimes \mathbb{1}_E) \right) - \tau_R \otimes \rho_E \right\|_1 \right]$$

$$\leq \left(\frac{|R| \cdot |E|}{|B_1|} \mathrm{tr} \left(\rho_{B_1 RE}^2 \right) \right)^{1/2}$$ decoupling

$$= \left(\frac{|R| \cdot |E|}{|B_1|^2} \mathrm{tr} \left(\rho_{RE}^2 \right) \right)^{1/2}$$ B_2 purifies $B_1 RE$

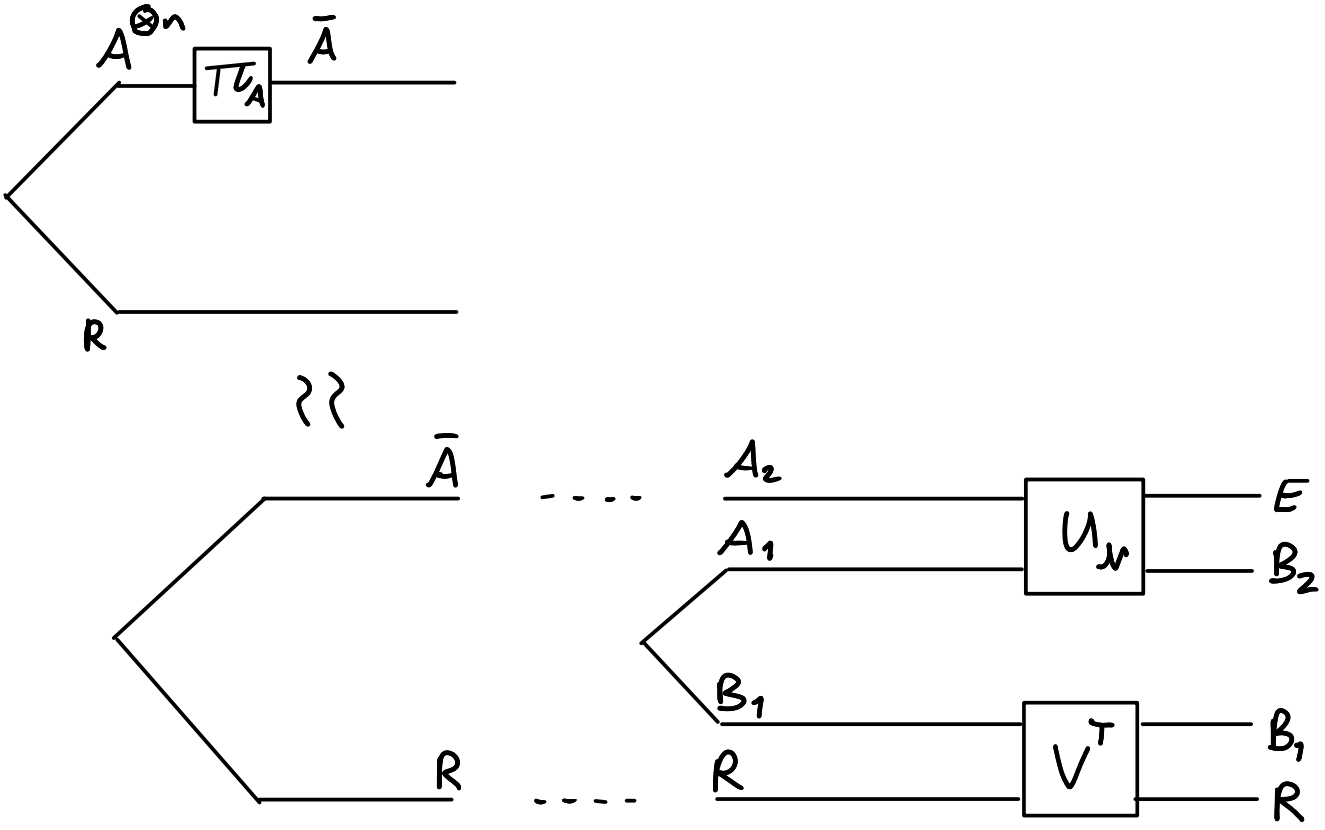
$\therefore$ Obtain high fidelity with max-ent. state $\phi_{B_2 R}$, averaged over V, if

$$|B_1| \gg |R| \cdot |E| \cdot \mathrm{tr} \left(\rho_{B_2}^2 \right)$$

$\therefore \exists V$ achieving this.

iid version:

- Input: $A^{\otimes n}$
- Project $A^{\otimes n}$ onto typical subspace $\bar{A}$
  - Succeeds w.h.p.
  - Typical subspace $\approx$ max mixed
    $\Rightarrow$ purification $\approx$ max entangled.
- Plug result into one-shot Father:



$$\mathbb{E}_V \left[\left\| \operatorname{tr}_{B_1} \left[\mathcal{N} \circ V_{A_1 A_2} (\phi_{A_1 R}) \right] - \phi_{B_2 R} \right\|_1 \right]$$

$$\leq \frac{|R| \cdot |E|}{|B_1|^2} \operatorname{tr}(\rho_B^2) = \frac{|R| \cdot |E|}{|B_1|^2} 2^{-\underbrace{\frac{1}{2-1} \log(\operatorname{tr} \rho_B^2)}_{H_2(\rho_B)}}$$

$$\leq \frac{|R|\cdot|E|}{|B_1|^2}\, 2^{-H(B)}$$

monotonicity of Renyi entropy: $H_2(\rho) \geq H(\rho)$

$$= \frac{2^{n(H(R)+H(E)-H(B)+o(1))}}{|B_1|^2}$$

$H(RE)$

typical subspace

$$= \frac{2^{n(I(R;E)+o(1))}}{|B_1|^2}$$

∴ For error $\to 0$ as $n \to \infty$, need $|B_1|^2 = 2^{n(I(R;E)+o(n))}$.

Ebits used $= \log|A_1|$

$= \log|B_1| = \frac{n}{2} I(R;E) + o(n)$.

Qubits transmitted

= ent. generated − ent. used

Lemma

$$= \log|\bar{A}| - \frac{n}{2} I(R;E) - o(n)$$

$$= nH(A) - \frac{n}{2}(H(R) + H(E) - H(RE)) - o(n)$$

$H(E) = H(RB)$, $H(RE) = H(B)$

$$= nH(R) - \frac{n}{2}(H(R) + H(RB) - H(B)) - o(n)$$

$$= \frac{n}{2} I(R;B) - o(n).$$

$$\therefore n\langle \mathcal{N}^{A\to B}:\rho_A\rangle + \frac{n}{2} I(R;E)[qq] \geq \frac{n}{2} I(R;B)[q\to q]$$

□

Corollary (ent.-assisted capacity, C_E)

$$C_E(\mathcal{N}) \geq \max_A I(R;B)$$

Proof

Super-dense coding: $[q \to q] + [qq] \geq 2[c \to c]$

Father: $\langle \mathcal{N} : \rho_A \rangle + \frac{1}{2} I(R;E)[qq] \geq \frac{1}{2} I(R;B)[q \to q]$

$$\therefore \langle \mathcal{N} : \rho_A \rangle + \tfrac{1}{2} I(R;E)[qq] + \tfrac{1}{2} I(R;B)[q \to q]$$

$$\geq \tfrac{1}{2} I(R;B)\left([q \to q] + [qq]\right) \quad \text{Father}$$

$$\geq I(R;B)[c \to c] \quad \text{super-dense}$$

LHS:

$$\langle \mathcal{N} : \rho_A \rangle + \tfrac{1}{2} I(R;E)[qq] + \tfrac{1}{2} I(R;B)[q \to q]$$

$$= \langle \mathcal{N} : \rho_A \rangle + \tfrac{1}{2}\big(H(R) + H(E) - H(RE) + H(R) + H(B) - H(RB) \big)[q \to q]$$

$$= \langle \mathcal{N} : \rho_A \rangle + H(R)[qq]$$

$\therefore C_E(\mathcal{N}) \geq I(R;B)$, using $H(R) = H(A)$ ebits. $\square$

Corollary (quantum capacity, Q)

$$Q(\mathcal{N}) \geq I_c(A\rangle B) := H(B) - H(E)$$

Proof

Trivially: $[q \to q] \geq [qq]$ — use q.comm. to generate ent.

Father: $\langle \mathcal{N} : \rho_A \rangle + \frac{1}{2} I(R;E)[qq] \geq \frac{1}{2} I(R;B)[q \to q]$

$$\therefore \langle \mathcal{N} : \rho_A \rangle + \frac{1}{2} I(R;E)[qq]$$

$$\geq \tfrac{1}{2}(I(R;B) - I(R;E))[q \to q] + \tfrac{1}{2} I(R;E)[qq]$$

Father + ent. gen.

$$= \tfrac{1}{2}\left(\cancel{H(R)} + H(B) - \underbrace{H(RB)}_{=H(E)} - \cancel{H(R)} - H(E) + \underbrace{H(RE)}_{=H(B)} \right)[q \to q] + \tfrac{1}{2} I(R;E)[qq]$$

$$= (H(B) - H(E))[q \to q] + \tfrac{1}{2} I(R;E)[qq]$$

"Subtracting $\frac{1}{2} I(R;E)[qq]$ from both sides

$$\Rightarrow Q(\mathcal{N}) \underset{(*)}{\geq} H(B) - H(E) = I_c(A\rangle B)" \quad \square$$

Interpretation (*):

If we start with $\frac{1}{2} I(R;E)$ ebits, can use it to obtain $I_c(A\rangle B)$ of quantum communication and get all the ebits back at the end.

→ Get Q. capacity catalysed by entanglement

(More sophisticated use of decoupling can prove $Q(\mathcal{N}) \geq I_c(A\rangle B)$ without catlysis.)