Lec 17, July 6, 2010

Note Title 02/07/2010

Surprising mixtures of resources:

(I) Superactivation

(II) Rocket channel.

Recall
$$Q(N) = \sup_n Q^{(n)}(N)$$
$$= \sup_n \frac{1}{n} Q^{(1)}(N^{\otimes n})$$
$$= \sup_n \frac{1}{n} I_c(R \rangle B^{\otimes n})_{I \otimes N^{\otimes n}(|\psi\rangle_{RA^{\otimes n}})}$$

Determining whether $Q(N) = 0$ or $Q(N) > 0$ is nontrivial.

(I) Superactivation

Result (1) : $\exists N_1, N_2$ s.t. $Q(N_1) = Q(N_2) = 0$

but $Q^{(1)}(N_1 \otimes N_2) > 0$

(2) : Q not convex

ie $\exists p_i, N_i$ s.t. $Q(\sum_i p_i N_i) > \sum_i p_i Q(N_i)$

(3) : Large gap between $Q^{(2)} - Q^{(1)}$

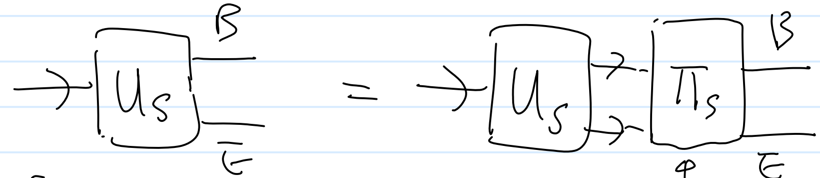
NB : (1) $\Rightarrow$ (2)

$\Rightarrow$ (3)

Ingredients for (1):

(1a) $Q(N) = 0$ if N antidegradable

$\Rightarrow Q(S) = 0$ if S symmetric



iso ext

proj onto the sym space

Special case of interest: $E_{\frac{1}{2}}$ erasure channel with error prob $\frac{1}{2}$

HHH 98 ?

(1b) $Q(N) = 0$ if N "entanglement binding"

ie $\forall |\psi\rangle$ $I_R \otimes N^{\otimes n}(|\psi\rangle)$ bound entangled

($D_{\leftrightarrow} = 0$)

Special case: if ρ_{RB} "PPT", then $D_{\leftrightarrow}(\rho) = 0$

"PPT" stands for positive partial transpose

eg $\begin{bmatrix} A & B \\ C & D \end{bmatrix} \xrightarrow{T_2} \begin{bmatrix} A^T & B^T \\ C^T & D^T \end{bmatrix}$

2 qubit

Consider $\Phi = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$, $\Phi^{T_2} = \frac{1}{2}\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$

$\mathrm{Spec}(\Phi^{T_2}) = \left(\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, -\frac{1}{2}\right)$

So Φ is not PPT.

eg. if ρ separable, $\rho = \sum_i p_i \, \underbrace{\omega_i \otimes \eta_i}_{\text{positive semidefinite}}$

$\rho^{T_2} = \sum_i p_i \, \underbrace{\omega_i \otimes \eta_i^T}_{\text{also positive semidefinite}}$

$\therefore \rho^{T_2} \geq 0 \qquad \therefore \rho$ PPT.

Facts: ① If ρ PPT, $\rho^{\otimes n}$ PPT.

② a state stays PPT under LOCC

③ If ρ distillable

$\exists$ LOCC protocol $\mathcal{D}$ s.t.

$$\mathcal{D}(\rho^{\otimes n}) \doteq \Phi^{\otimes n\alpha}$$

④ If ρ PPT, $\mathcal{D}(\rho^{\otimes n})$ PPT by ①, ②

If ρ distillable, $\mathcal{D}(\rho^{\otimes n})$ NPT contradiction

$\therefore$ ρ PPT $\Rightarrow$ ρ bound entangled

It turns out N only creates PPT states

$\Leftrightarrow$ Choi-Jamiołkowski state is PPT

$I \otimes N(\Phi)$

$\therefore$ $I \otimes N(\Phi)$ PPT gives a simple sufficient condition for $Q(N)=0$

(1c) $P(\mathcal{N})$ = private classical capacity of $\mathcal{N}$

$$= \sup_n \frac{1}{n} P^{(1)}(\mathcal{N}^{\otimes n})$$

where $$P^{(1)}(\mathcal{N}) = \max_{p_X, \rho_{XA}} \left[I(X:B) - I(X:Z) \right]$$

evaluated on

$$\sum_x p_x |x\rangle\langle x|_X \otimes \left(U_{\mathcal{N}} \rho_x U_{\mathcal{N}}^{\dagger} \right)_{BE}$$

This setting assumes the users (Alice / Bob) know the channel $\mathcal{N}$ & that it is iid. — (*)

QKD requires verifying (*) also.

(1d) $\boxed{\exists N_H \text{ s.t. } Q(N_H) = 0 \quad \text{but } P^{(1)}(N_H) > 0}$ ← HHHO03

NB1 Clearly $Q(N) \leq P(N) \quad \forall N$

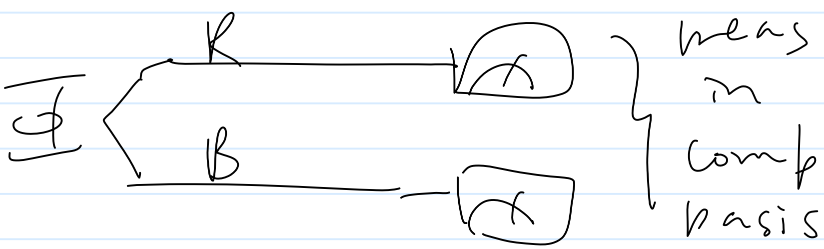
but for a long time, it wasn't clear whether entanglement is necessary for generating secret key.

NB2 0608195 shows that some of these channels can be verified and be used for QKD.

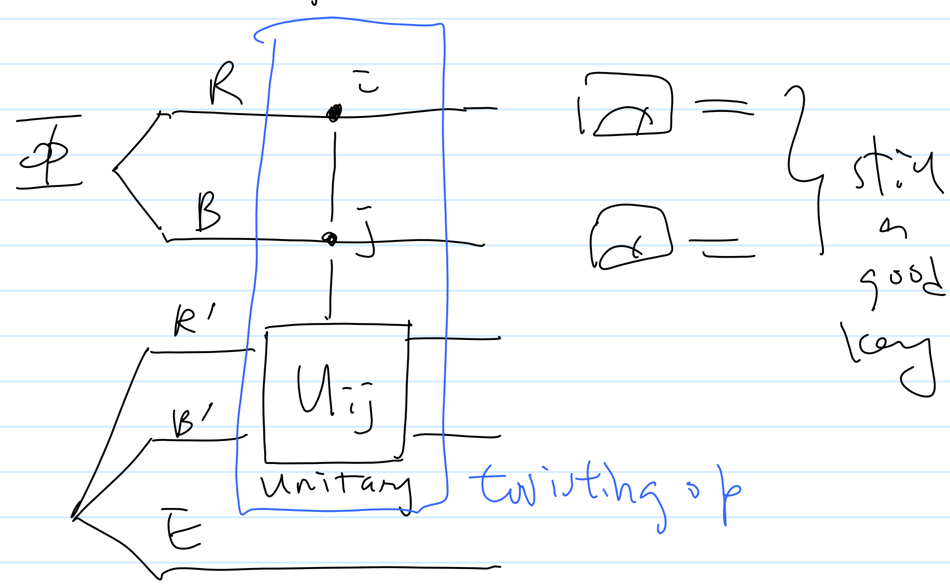
- Will discuss why these channels behave as such
- Write down a specific example of interest

Why NR exists :

If R & B have a max ent state they can generate a key



The most general state that gives a key is the "twisted ebit"



Eve's attack of the key via the "shield" R'B' does not affect the security of the key but ent % RR' & BB' is much reduced.

A concrete example of twisted ebits come from "data hiding" $\rho_{0\,R'B'}$ & $\rho_{1\,R'B'}$ ortho to one another but nearly indistinguishably by LOCC.

The state on $RB\ R'B' = \frac{1}{2}\left[\Phi \otimes \rho_0 + \Phi^- \otimes \rho_1\right]$

It is a labeled mixed of Φ & $\Phi^- = \frac{(|00\rangle - |11\rangle)(\langle 00| - \langle 11|)}{2}$

but the label ρ_0 vs ρ_1 cannot be read by Rob & Bob so they can't distill ebits. But the label ensures they're not sharing $\frac{1}{2}(|00\rangle\langle 00| + |11\rangle\langle 11|)$ which purifies to $\frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ on RBE.

Twisted ebits contain a perfect key & some distillable entanglement

In HHHO 03, the idea is to mix twisted ebits with a little garbage (max mixed state).

For well chosen twisted ebits, the new states ρ_H contain noisy but distillable key but no distillable entanglement.

(Need to show ρ_H PPT.)

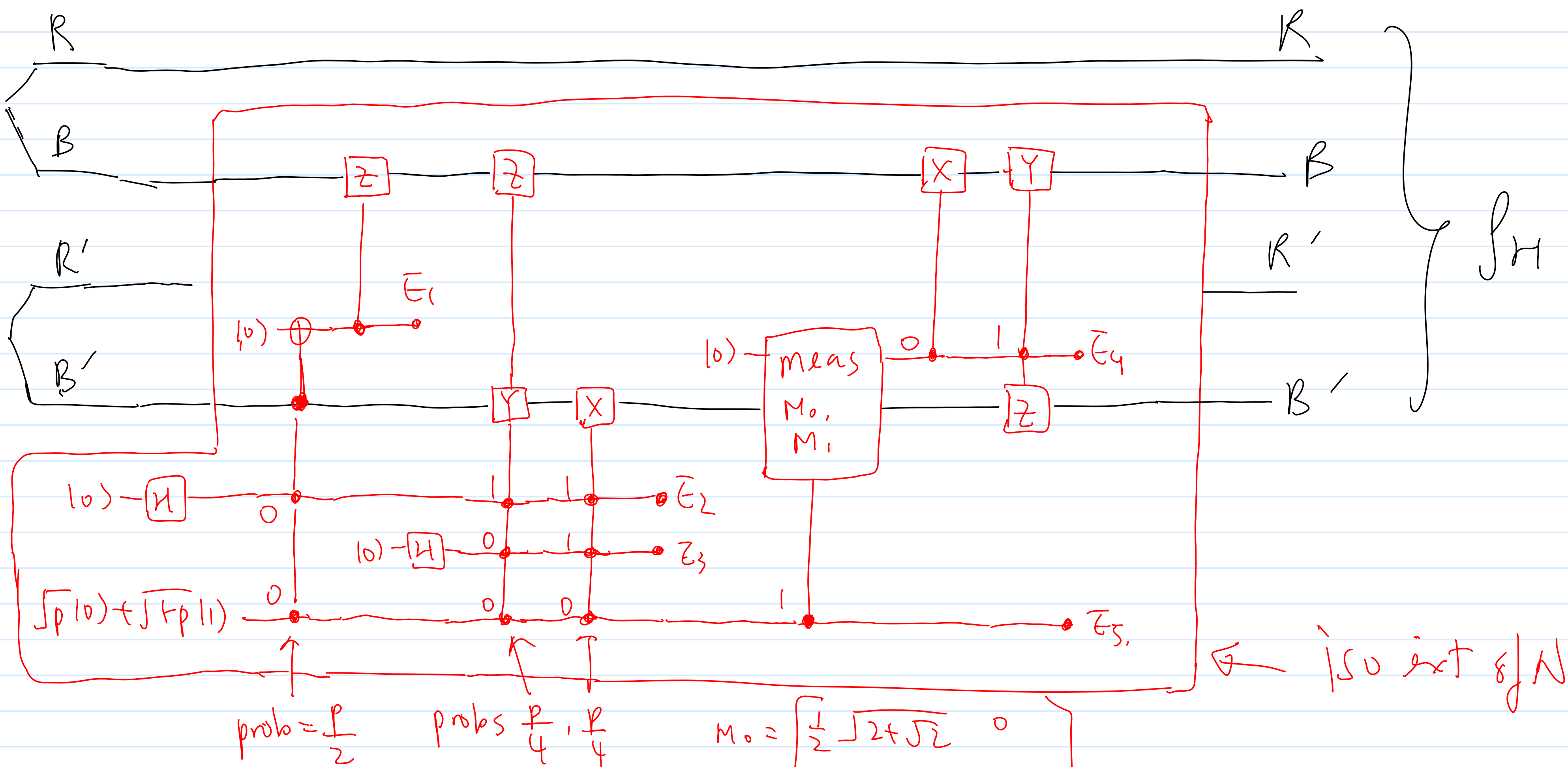
Same has max mixed reduced state on RR'

so $\rho_H = \left(\underset{RR'}{I} \otimes \underset{AA' \to BB'}{N}\right)\left(\Phi_{RB} \otimes \Phi_{R'B'}\right)$ for some channel N

So $Q(N) = 0$ ($\because \rho_{r1}$ PPT)

Finally, simple choices of ρ_X, ρ_X lower bounds $P^{(1)}(N)$

Specific example (see 0608195 Sec IV for detail):



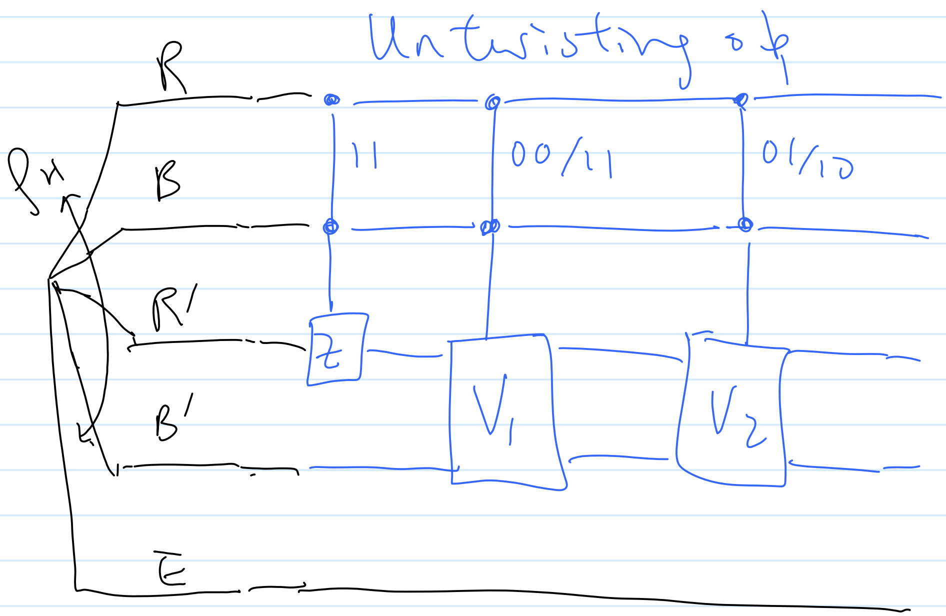
$$M_0 = \begin{bmatrix} \frac{1}{2}\sqrt{2+\sqrt{2}} & 0 \\ 0 & \frac{1}{2}\sqrt{2-\sqrt{2}} \end{bmatrix}$$

$$M_1 = X M_0 X = I - M_0$$

So N_H has 4-dim input & output.

When $p = \frac{\sqrt{2}}{1+\sqrt{2}} \doteq 0.5858$, ρ_H PPT

We can also verify that ρ_H is a noisy twisted ebit by:



$$= p\,\Phi + (1-p)\left(\frac{|01\rangle+|10\rangle}{\sqrt{2}}\right)\left(\frac{\langle 01|+\langle 10|}{\sqrt{2}}\right)$$

for $p > \frac{1}{2}$

$P^{(1)}(\rho_H)$ or $P^{(1)}(N_H) \geq 0.0213$

V_1 takes $|00\rangle \rightarrow |00\rangle$

$|11\rangle \rightarrow |11\rangle$

$|01\rangle + |10\rangle \rightarrow |01\rangle$

$|01\rangle - |10\rangle \rightarrow |10\rangle$

V_2 takes $|\chi_+\rangle \rightarrow |00\rangle$

$|\chi_-\rangle \rightarrow |11\rangle$

$|01\rangle + |10\rangle \rightarrow |01\rangle$

$|01\rangle - |10\rangle \rightarrow |10\rangle$

$$|\chi_\pm\rangle = \frac{1}{2}\left(\sqrt{2 \pm \sqrt{2}}\,|00\rangle \pm \sqrt{2 \mp \sqrt{2}}\,|11\rangle\right)$$

1e General theorem:

sym channel

Q capacity assisted by free sym channel

$$\frac{1}{2} P^{(1)}(N) \le \frac{1}{2} P(N) \le Q^{(1)}(N \otimes S) = Q_{ss}(N)$$

def.

?? proved where

Smith Smolin Winter 0607039

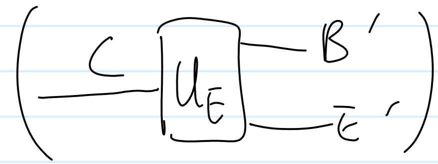
A more specific theorem (proved next page)

$$\frac{1}{2} P^{(1)}(N) \le Q^{(1)}(N \otimes E_{\frac{1}{2}})$$

Thm (Smith & Yard 0807.4935)

Given (i) any channel $\mathcal{N}$ 

(ii) any ensemble $\{p_x, \rho_{xA}\}$

let $\mathcal{E}_{\frac{1}{2}}$ = erasure channel with prob error $\frac{1}{2}$ 

$\dim(C) = \sum_x \operatorname{rank}(\rho_{xA})$

$\dim(B') = \dim(E') = 2\dim(C)$

Then $\exists\ |\psi\rangle_{RAC}$ s.t.

$$\underset{I_R \otimes \mathcal{N} \otimes \mathcal{E}_{\frac{1}{2}}(|\psi\rangle_{RAC})}{I_c(R\rangle BB')} = \frac{1}{2}\underset{I_X \otimes U_N\left(\sum_x p_x |x\rangle\langle x|_X \otimes \rho_{xA}\right)}{\left[I(X:B) - I(X:E)\right]}$$

Cor: $Q^{(1)}(\mathcal{N} \otimes \mathcal{E}_{\frac{1}{2}}) \geq \text{LHS} = \text{RHS} \underset{\text{when max RHS over } \Sigma}{=} P^{(1)}(\mathcal{N})$

Pf Let $|\psi\rangle_{RAC} = \sum_x \sqrt{p_x}\, |x\rangle_R |\psi_x\rangle_{AC}$

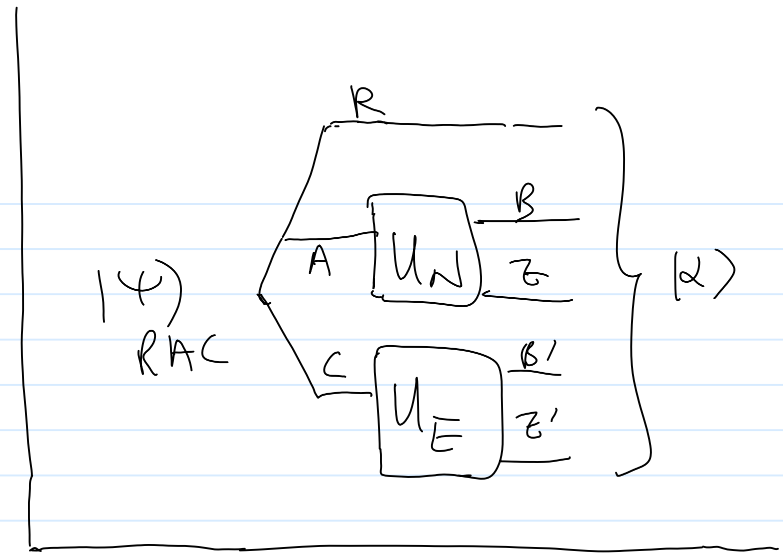
where $\forall x$ $\mathrm{tr}_C |\psi_x\rangle\langle\psi_x| = \rho_{xA}$

$\{\mathrm{tr}_A |\psi_x\rangle\langle\psi_x|\}$ has mutually disjoint support

ie for each ρ_{xA}, it is purified by C

and diff ρ_{xA} has purification supported on a diff subspace of C.

$I_c(R > BB')$



$$I_R \otimes N \otimes E_{\frac{1}{2}}\left(|\psi\rangle_{RAC}\right)$$

$$= \left(S_{BB'} - S_{ZZ'}\right)_{|\alpha\rangle}$$

Note B', Z' both include a register stating $C \to B'$ or $C \to Z'$

$$= \Big(\underbrace{1}_{H(\frac{1}{2})} + \tfrac{1}{2}\underbrace{S_{BC}}_{\text{when } C\to B'} + \tfrac{1}{2}\underbrace{S_B}_{\text{when } C\to Z'}\Big) - \Big(\underbrace{1}_{H(\frac{1}{2})} + \tfrac{1}{2}\underbrace{S_{ZC}}_{\text{when } C\to Z'} + \tfrac{1}{2}\underbrace{S_Z}_{\text{when } C\to B'}\Big)$$

$(S_{BC} = S_{RZ})$ $\qquad$ $(S_{ZC} = S_{RB})$

$$= \frac{1}{2}\left(S_{RZ} + S_B - S_{RB} - S_Z\right) = \frac{1}{2}\left[I(R:B) - I(R:Z)\right]_{|\alpha\rangle}$$

$$= \frac{1}{2}\left[I(X:B) - I(X:Z)\right]_{I_X \otimes U_N\left(\sum_x p_x |x\rangle\langle x|_X \otimes \rho^x_A\right)}$$

because "which x" is also recorded in C (or $B'Z'$)

Putting (1a) (1b) (1c) (1d) (1e) together to get superactivation eg:

Choose $\mathcal{N}_1 = \mathcal{N}_H$, $\mathcal{N}_2 = \mathcal{E}_{\frac{1}{2}}$

- by (1a) (1b) $Q(\mathcal{N}_1) = Q(\mathcal{N}_2) = 0$
- by (1c) (1d) $P^{(1)}(\mathcal{N}_1) \geq 0.0213$
- by (1e) $Q^{(1)}(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq \frac{1}{2} P^{(1)}(\mathcal{N}_1) = 0.01065 > 0$

NB tensoring 2 sym / PPT channel gives another sym / PPT channel.

but tensoring a sym channel with a PPT channel can break both properties, allowing them to activate each other.

NB Whether $\mathcal{N}$ has zero / nonzero q. capacity is context dependent.

② Quantum capacity is not convex

Intuitively a channel $N = \sum_i p_i N_i$ which is a mixture of other channels communicates no better than the average of the constituents. It is natural to conjecture that Q is convex ie $Q\left(\sum_i p_i N_i\right) \leq \sum_i p_i Q(N_i)$.

The possibility of super activation challenges such intuition: if $N = p\, N_H \otimes |0\rangle\langle 0|_B + (1-p)\, E_{\frac{1}{2}} \otimes |1\rangle\langle 1|_B$ — tells Bob which channel occurs.

then having multiple access to N resembles having access to some N_H & some $E_{\frac{1}{2}}$

So possibly $Q(N) > 0$, disproving convexity of Q.

To show $Q(N) > 0$, suffices to show $Q^{(k)}(N) > 0$ for some k. ie find some input $|\psi\rangle_{RA^{\otimes k}}$ and bound $I_c(R \rangle B^{\otimes k})$ on $I \otimes N^{\otimes k}(|\psi\rangle)$.

Try $k=2$ (lowest to get both N_H & $Z_{\frac{1}{2}}$).

Recall if there are events distinguishable on the receiver's system, the coherent info is the average (coherent info given each event).

Here Bob knows which of N_H, $Z_{\frac{1}{2}}$ occurs in each use of N.

$$\therefore I_c(R \rangle B^{\otimes 2})_{I_R \otimes N^{\otimes 2}(|\psi\rangle_{RA_1A_2})}$$

$$= p^2 \, I_c(R \rangle B^{\otimes 2})_{I_R \otimes N_H^{\otimes 2}(|\psi\rangle_{RA_1A_2})}$$

$$+ p(1-p) \, I_c(R \rangle B^{\otimes 2})_{I_R \otimes N_H \otimes E_{\frac{1}{2}}(|\psi\rangle_{RA_1A_2})}$$

$$+ p(1-p) \, I_c(R \rangle B^{\otimes 2})_{I_R \otimes E_{\frac{1}{2}} \otimes N_H(|\psi\rangle_{RA_1A_2})}$$

$$+ (1-p)^2 \, I_c(R \rangle B^{\otimes 2})_{I_R \otimes E_{\frac{1}{2}}^{\otimes 2}(|\psi\rangle_{RA_1A_2})}$$

NB! last term $= 0$ $\because$ $E_{\frac{1}{2}}^{\otimes 2}$ sym wrt $B_1 B_2$ & $E_1 E_2$

NB2. We're stuck with the same $|\psi\rangle_{RA_1A_2}$ for all terms so when max one term, other terms can turn negative. So despite the theorem in part ① stating that $\exists\ |\psi\rangle_{RA_1A_2}$ s.t. 2^{nd} term $\geq p(rp)\ 0.0213$, the 1^{st} & 3^{rd} term can be negative on that state and $I_c(R\rangle B^{\otimes 2})_{I_R \otimes N^{\otimes 2}(|\psi\rangle_{RA_1A_2})}$ need not be positive.

Idea: make 2^{nd} & 3^{rd} term equal & positive

Now, 1^{st} term $\geq p^2 \times (-S_{E_1E_2})$

$$\geq -p^2 2\log 6$$

$\leftarrow$ # Kraus ops in N_H

Idea:

① choose $|\psi\rangle_{RA_1A_2}$ sym in A_1A_2 ($\therefore$ 2nd term = 3rd term $= p(1-p)\alpha$)

for $\alpha = I_c(R\rangle B^{\otimes 2})_{I_R \otimes N_H \otimes \mathcal{E}_{\frac{1}{2}}(|\psi\rangle_{RA_1A_2})}$

In fact $\alpha > 0$ for $|\psi\rangle_{RA_1A_2} = \frac{|000\rangle + |111\rangle}{\sqrt{2}} \otimes \frac{|00\rangle + |11\rangle}{\sqrt{2}}$

on R, 1st qubit of A_1, 1st qubit of A_2 — on 2nd qubit of A_1 & A_2

② 1st term $= p^2 \, I_c(R\rangle B^{\otimes 2})_{I_R \otimes N_H^{\otimes 2}(|\psi\rangle_{RA_1A_2})}$

$\geq p^2 \, (-S_{E_1E_2}) \geq p^2 \, (-\log 6) \times 2$

Kraus op in N & dim of env for N

Since α constant, when p small enough ($p < 0.0041$)

the 2^{nd} & 3^{rd} term ($\sim p(1-p) \times$ positive const)

dominates the 1^{st} term ($\sim -p^2 \times$ negative const)

$$\therefore \; I_c(R\rangle B^{\otimes 2})_{I_R \otimes N^{\otimes 2}(|\Psi\rangle_{RA_1A_2})} \underset{\neq}{>} 0$$

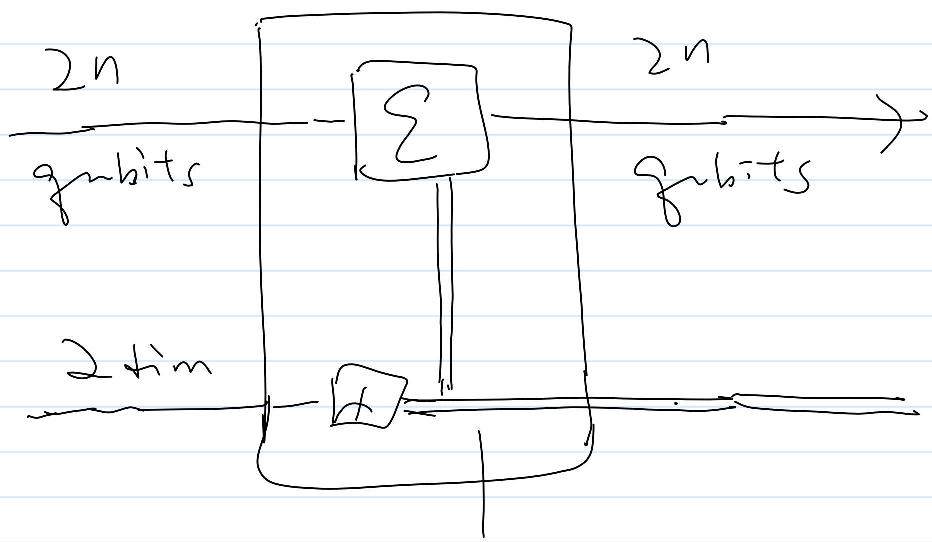
$$\therefore \; Q(N) \geq Q^{(2)}(N)$$

$$\underset{\neq}{>} p\, Q(N_H \otimes |0\rangle\langle 0|) + (1-p)\, Q(E_{\frac{1}{2}} \otimes |1\rangle\langle 1|)$$

$$= 0$$

③ $Q^{(2)}(N)$ can be much smaller than $Q^{(1)}(N)$

Refine N as :



if $i=0$, $\Sigma = N_H^{\otimes n}$

$i=1$, $\Sigma = \mathcal{E}_{\frac{1}{2}}^{\otimes n}$

$Q^{(1)}(N) = 0$, $Q^{(2)}(N) \geq n\, Q^{(1)}(N_H \otimes \mathcal{E}_{\frac{1}{2}}) = 0.00213\, n$