Lec17, 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 $Q^{(2)} - Q^{(1)}$

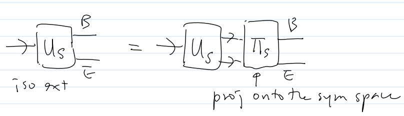
NB: (1) $\Rightarrow$ (2)

$\Rightarrow$ (3)

Ingredients for (1):

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

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



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

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

So Φ is not PPT.

positive semidefinite

eg. if ρ separable, $\rho = \sum_i p_i \omega_i \otimes \eta_i$

$\rho^{T_2} = \sum_i p_i \omega_i \otimes \eta_i^T$

also positive semidefinite

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

Facts: (·) If ρ PPT, $\rho^{\otimes n}$ PPT.

(··) a state stays PPT under LOCC

(∴) If ρ distillable

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

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

(∷) If ρ PPT, $\mathcal{D}(\rho^{\otimes n})$ PPT by (·), (··)

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-Jamiolkowski state is PPT

$I \otimes N(\Phi)$

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

(1c) $P(N)$ = private classical capacity of N

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

where $P^{(1)}(N) = \max_{p_x, \rho_{xA}} \left[I(X:B) - I(X:E) \right]$ evaluated on $\sum_x p_x |x\rangle\langle x|_X \otimes (U_N \rho_x U_N^\dagger)_{BE}$

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

QKD requires verifying (*) also.

(1d) $\boxed{\exists N_H \text{ s.t. } Q(N_H) = 0 \text{ but } P^{(1)}(N_H) > 0}$ HHHO 03

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

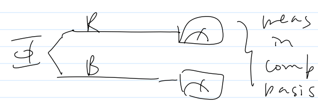
but for a long time, it wasn't clear whether entanglement is necessary for generating secret key.

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

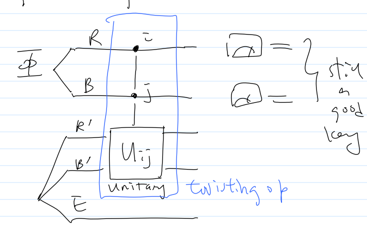
- Will discuss why these channels behave as such
- Write down a specific example of interest

Why N_H 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 indistinguishable by LOCC.

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

It's 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.)

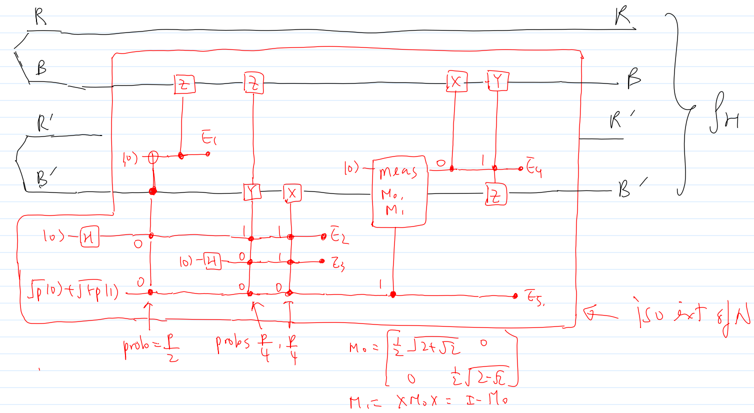
Some has max mixed reduced state on RR'

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

So $Q(N) = 0$ ($\because \rho_H$ PPT)

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

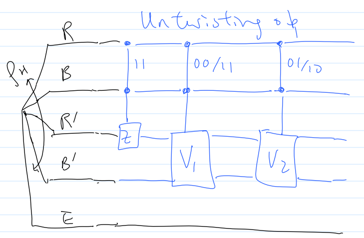
Specific example (see 0608195 Sec IV for detail):



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:



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

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

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

V_1 takes $|00\rangle \to |00\rangle$
$|11\rangle \to |11\rangle$
$|01\rangle + |10\rangle \to |01\rangle$
$|01\rangle - |10\rangle \to |10\rangle$

V_2 takes $|\chi_+\rangle \to |00\rangle$
$|\chi_-\rangle \to |11\rangle$
$|01\rangle + |10\rangle \to |01\rangle$
$|01\rangle - |10\rangle \to |10\rangle$

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

(1e) General theorem:

$$\frac{1}{2} P^{(1)}(N) \underset{\text{def.}}{\leq} \frac{1}{2} P(N) \underset{\text{?! proved where}}{\leq} Q^{(1)}(N \otimes \underset{\text{sym channel}}{S}) \underset{\text{Smith Smolin Winter 0607039}}{=} \underset{\text{Q capacity assisted by free sym channel}}{Q_{ss}}(N)$$

A more specific theorem (proved next page)

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

Thm (Smith & Yard 0807.4935)

Given (i) any channel N ($\xrightarrow{A} \boxed{U_N} \to B, E$)

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

let $E_{\frac{1}{2}}$ = erasure channel with prob error $\frac{1}{2}$ ($\xrightarrow{C} \boxed{U_E} \to B', E'$)

$\dim(C) = \sum_x \operatorname{rank}(\rho_{xA})$
$\dim(B') = \dim(E') = 2\dim(C)$

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

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

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

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

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

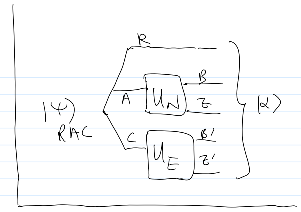
$\{\operatorname{tr}_A |\psi_x\rangle\langle\psi_x|\}$ has mutually disjoint support

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

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

$I_c(R\rangle BB')$
$\quad I_R \otimes N \otimes \mathcal{E}_{\frac{1}{2}}(|\psi\rangle_{RAC})$

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



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

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

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

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

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

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

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

Choose $N_1 = N_H$, $N_2 = \mathcal{E}_{\frac{1}{2}}$

- by (1a) (1b) $Q(N_1) = Q(N_2) = 0$
- by (1c) (1d) $P^{(1)}(N_1) \geq 0.0213$
- by (1e) $Q^{(1)}(N_1 \otimes N_2) \geq \frac{1}{2} P^{(1)}(N_1) = 0.01065 > 0$

NB tensoring 2 sym channel gives another sym channel
$\qquad\qquad\quad$ PPT $\qquad\qquad\qquad\qquad\qquad$ PPT.

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

NB Whether 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 $Q(\sum_i p_i N_i) \leq \sum_i p_i Q(N_i)$.

The possibility of superactivation challenges such intuition:

if $N = p\, N_H \otimes |0\rangle\langle 0|_B + (1-p)\, \mathcal{E}_{\frac{1}{2}} \otimes |1\rangle\langle 1|_B$ ← tells Bob which channel occurs.

Then having multiple access to N
$\quad$ resembles having access to some N_H & some $\mathcal{E}_{\frac{1}{2}}$

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 & $\mathcal{E}_{\frac{1}{2}}$).

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, $\mathcal{E}_{\frac{1}{2}}$ occurs in each use of N.

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

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

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

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

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

NB1. last term $= 0$ $\because$ $\mathcal{E}_{\frac{1}{2}}^{\otimes 2}$ sym wrt B_1B_2 & Z_1Z_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. 2nd term $\geq p(1-p)\, 0.0213$, the 1st & 3rd 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 2nd & 3rd term equal & positive

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

$\geq -p^2\, 2\log 6$ ← #kraus ops in N_H

Idea:

① choose $|\psi\rangle_{RA_1A_2}$ sym in A_1A_2 (∴ 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 $= p^2\, I_c(R\rangle B^{\otimes 2})_{I_R\otimes N_H^{\otimes 2}(|\psi\rangle_{RA_1A_2})}$

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

6 ← #kraus op in N & dim of env for N

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

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

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

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

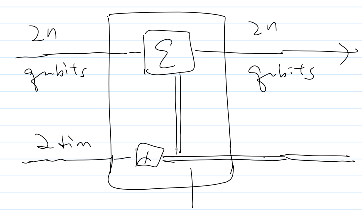
∴ $Q(N) \geq Q^{(2)}(N)$

$\underset{\neq}{\geq} p\, Q(N_H\otimes|0\rangle\langle 0|) + (1-p)\, Q(\mathcal{E}_{\frac{1}{2}}\otimes|1\rangle\langle 1|)$

$= 0$

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

Refine N as:



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

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

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