The framework of resource inequalities begs the Qn:

Is it possible for $Q(N \otimes I) > Q(N) + Q(I)$?

or for $D(\rho \otimes \Phi) > D(\rho) + D(\Phi)$?

$\uparrow$ ebit

ie can noiseless resource help beyond it's stated value?

If so, we have 2 diff quantum capacities

— one defined before

— another that allows borrowing & returning of a catalytic or linear amount of noiseless resources (such as deriving LSD from $\vec{\sigma}$).

$$\text{We will see} \quad Q, \quad Q_{\leftarrow}, \quad Q_{\leftrightarrow}, \quad \underbrace{D_{\rightarrow}, \quad D_{\leftarrow}}_{\text{same Qn}}, \quad D_{\leftrightarrow}$$

are all additive on noiseless resources.

Main idea (in BDSW96) is operational and applies to many capacities, but requires $Q(N) > 0$ to show $Q(N \otimes I_d) = Q(N) + \log d$ etc.

The remaining case: Solved in various informal discussions between Gottesman, Harrow, M. Horodecki, L, Oppenheim, Shor, Winter & never written up.

Thm: If $Q(N) > 0$ then $Q(N \otimes I) = Q(N) + Q(I)$

Pf:

Idea: If $Q(N \otimes I) > Q(N) + Q(I)$,

even without "I", you can make some using N

then use these fabricated I to boost capacity of N

– a contradiction.

Detail: Suppose $Q(N \otimes I_d) = Q(N) + \log d + \underset{\text{+ve const}}{\eta}$

$\exists\, n$ & a code C_1 using $(N \otimes I_d)^{\otimes n}$ to produce

$n\left[Q(N \otimes I_d) - \delta_n\right]$ qbits with error ε_n.

Using N alone, $\exists m$ & a code C_2 turning $N^{\otimes m}$ to $m[Q(N) - \delta'_m]$ qbits with error ε'_m

Now consider a code C_3 that uses N alone & does the following:

Run C_2 for some m using $N^{\otimes m}$ and then run C_1 for $n = m\left\lceil \frac{Q(N) - \delta'_m}{\log d} \right\rceil$ using the identity channels produced by C_2 & n uses of N.

Total error: $\delta'_m + \delta_n \longrightarrow 0$ as $m \to \infty$ $(n \to \infty)$

Total # N consumed: $m + n = m\left[1 + \frac{Q(N) - d'm}{\log d}\right]$

Total # of bit produced: $n\left[Q(N \otimes I_d) - dn\right]$

$$= m\left[\frac{Q(N) - d'm}{\log d}\right]\left[Q(N) + \log d + \eta - dn\right]$$

$$\text{Rate} = \frac{\dfrac{(Q(N) - d'm)}{\log d}\,(Q(N) + \log d + \eta - dn)}{1 + \dfrac{Q(N) - d'm}{\log d}}$$

$$= \frac{(Q(N) - d'm)\left(1 + \dfrac{Q(N) + \eta - dn}{\log d}\right)}{\left(1 + \dfrac{Q(N) - d'm}{\log d}\right)}$$

$$= \left(Q(N) - \delta_m'\right)\left[1 + \left[\frac{\frac{\eta + \delta_m' - \delta_n}{\log d}}{1 + \frac{Q(N) - \delta_m'}{\log d}}\right]\right]$$

$$\geq \left(Q(N) - \delta_m'\right)\left(1 + \frac{\eta + \delta_m' - \delta_n}{Q(N) + \log d}\right)$$

$$> Q(N) \text{ as } m \to \infty, \ \delta_n', \delta_m' \to 0$$

Similar argument works for $Q_{\leftarrow}$, $Q_{\leftrightarrow}$, $D_{\rightarrow}$, $D_{\leftrightarrow}$

when the noisy channel / state has nonzero capacity or distillable entanglement.

Remaining case: it is possible for

- $Q(N) = 0$ but $Q(N \otimes I_d) > \log d$?

$Q_{\leftarrow}$: $Q_{\leftarrow}$

$Q_{\leftrightarrow}$: $Q_{\leftrightarrow}$

$D_{\rightarrow}$ $D_{\rightarrow}$

$D_{\leftrightarrow}$ $D_{\leftrightarrow}$

Ans: no for all.

Thm 1: $D_{\to}(\rho \otimes \Phi^{\otimes m}) = D_{\to}(\rho) + m$

pf: $D_{\to}(\rho \otimes \Phi^{\otimes m}) = \lim_{n\to\infty} \frac{1}{n} \sup_{\mathcal{D} \in LOCC} I_c(A\rangle B)_{\mathcal{D}((\rho \otimes \Phi^{\otimes m})^{\otimes n})}$

$\forall m, \rho, \quad \sup_{\mathcal{D} \in LOCC_{\to}} I_c(A\rangle B)_{\mathcal{D}((\rho \otimes \Phi^{\otimes m})^{\otimes n})}$

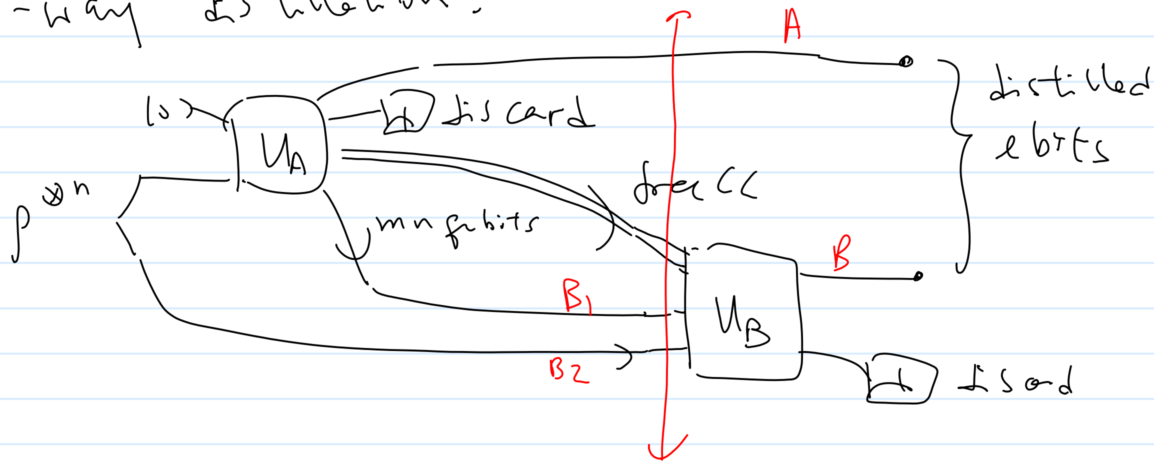
$= \sup_{\mathcal{D} \in LOCC_{\to} + mn \text{ qbits (forward)}} I_c(A\rangle B)_{\mathcal{D}(\rho^{\otimes n})}$

($\leq$ ED)

($\geq$ TP + free forward CL)

$$\leq \sup_{\mathcal{D} \in LOCC(\rightarrow)} I_c(A>B)_{\mathcal{D}(\rho^{\otimes n})} + mn$$

1-way distillation:



$I_c(A>B)$

$\leq I_c(A>B_2) + mn$

(1 qubit comm from A to B cannot increase $I_c(A>B)$ by more than 1)

$(I_c(A>B) = \underbrace{S(B)}_{\text{\uparrow by 1 at most}} - \underbrace{S(AB)}_{\text{inv}})$

Cor1: $Q_{\to}(N \otimes I_d) = Q_{\to}(N) + Q_{\to}(I_d)$

Cor2: $Q(N \otimes I_d) = Q(N) + Q(I_d)$

Pf (cor1): $Q_{\to}(N) = \sup_n \frac{1}{n} \max_{|\psi\rangle_{A'B^n}} D_{\to}\left(I_{A'} \otimes N^{\otimes n}\left(|\psi\rangle_{A'B^n}\right)\right)$

$$Q_{\to}(N \otimes I_d) = \sup_n \frac{1}{n} \underbrace{\max_{|\tilde{\psi}\rangle} D_{\to}\left(I_{A'} \otimes N^{\otimes n} \otimes I_d^{\otimes n}(|\tilde{\psi}\rangle)\right)}_{=\ \max_{|\psi\rangle} D_{\to}\left(I_{A''} \otimes N^{\otimes n}(|\psi\rangle) \otimes \Phi^{\otimes n \log d}\right)}$$

Reason:

Given $I_d^{\otimes n}$, one can create $\Phi^{\otimes n \log d}$.

On the other hand, given $\Phi^{\otimes n \log d}$, one can create $I_d^{\otimes n}$ using free forward CC & teleportation (& define $A'' = A \otimes \mathbb{C}^{d \otimes n}$, $|\tilde{\psi}\rangle = |\psi\rangle$))

$$\therefore Q_{\to}(N \otimes I_d) = \sup_n \frac{1}{n} \max_{|\psi\rangle} D_{\to}\left(I_A' \otimes N^{\otimes n}(|\psi\rangle) \otimes \Phi^{\otimes n \log d}\right)$$

$$(\text{by Thm } 1) = \left[\sup_n \frac{1}{n} \max_{|\psi\rangle} D_{\to}\left(I_A' \otimes N^{\otimes n}(|\psi\rangle)\right)\right] + \log d$$

$$= Q_{\to}(N) + Q_{\to}(I_d)$$

Pf (Cor 2): $\forall N$, $Q_{\to}(N) = Q(N)$.

$\therefore$ Cor 2 follows from Cor 1.

Thm 2. $\forall \rho$ $D_{\leftrightarrow}(\rho \otimes \bar{\Phi}^{\otimes m}) = D_{\leftrightarrow}(\rho) + D_{\leftrightarrow}(\bar{\Phi}^{\otimes m})$

Pf: Suffices to consider $D_{\leftrightarrow}(\rho) = 0$.

Will prove by contradiction

ie assume $D_{\leftrightarrow}(\rho \otimes \bar{\Phi}^{\otimes m}) > m$ and deduce $D_{\leftrightarrow}(\rho) > 0$.

Suppose $D_{\leftrightarrow}(\rho \otimes \bar{\Phi}^{\otimes m}) = m(1+\delta)$ for some const $\delta > 0$

Then $\forall \varepsilon > 0$ $\exists n$ & a protocol P_n that uses n copies of $\rho \otimes \bar{\Phi}^{\otimes m}$ & 2-way CC to generate

depends on ε

$\sigma \approx \bar{\Phi}^{\otimes m(1+\delta) \cdot n}$ (up to trace distance ε).

Abusing notation, we write $P_n(\rho^{\otimes n} \otimes \bar{\Phi}^{\otimes mn}) = \sigma$ (ie we denote the TCP map induced by P_n by the same symbol).

Now we provide a protocol to distill ebits from $\rho_{AB}^{\otimes n}$ with nonzero rate (which gives the desired contradiction).

First consider a protocol to check entanglement using random hashing:

Let the 4 bell states on 2 qubit be labeled by 00, 01, 10, 11 where 00 corresponds to Φ

Suppose Alice & Bob each has k qubits. The 4^k Bell states form a basis for their joint Hilbert space. Represent each basis state as a 2k-bit string.

In BDSW96, the following can be done by 2 way CC:

① If Alice & Bob share σ_{AB}, they can turn it to a mixture of Bell states, so their state is a classical distribution of "2k-bit" strings

② Learn the parity of any subset of the 2k bits by measuring 1 qubit on each side.

So if they measure s qubits each to find the parity of s random subsets

$$\text{prob (all parity even} \mid \underbrace{\operatorname{tr}(\sigma_{AB}\,\Phi^{\otimes n})=0}_{\text{2k bit string} \neq 00\cdots00}) \leq \frac{1}{2^s}$$

They output "pass" if all parities are even, else they output "fail".

Let $\tilde{F}_{k,s}$ denote the above map taking $2k$ qubits to $2(k-s)$ qubits.

$$\tilde{F}_{k,s}\left(\Phi^{\otimes k}\right) = \Phi^{\otimes (n-k)} \otimes \text{"pass"}$$

$\forall \rho$ s.t. $\mathrm{tr}\left(\Phi^{\otimes k} \sigma\right) = 0$,

$$\tilde{F}_{k,s}(\sigma) = \frac{1}{2^s}\,\tilde{\sigma} \otimes \text{"pass"} + \left(1-\frac{1}{2^s}\right)\tilde{\tilde{\sigma}} \otimes \text{"fail"}$$

where $\tilde{\sigma}, \tilde{\tilde{\sigma}}$ are $2(k-s)$ qubit states.

The distillation protocol for ρ:

let m, n be as defined before.

let $\Psi = \left[\frac{|00\rangle\langle 00| + |11\rangle\langle 11|}{2}\right]^{\otimes mn} = \frac{\Phi^{\otimes mn}}{2^{mn}} + \left(1 - \frac{1}{2^{mn}}\right)\Gamma$

where $\mathrm{tr}(\Gamma\, \Phi^{\otimes mn}) = 0$, $\Gamma \geq 0$, $\mathrm{tr}\,\Gamma = 1$.

① Alice & Bob apply P_n to $\rho^{\otimes n}$ & Ψ:

Output $= P_n(\rho^{\otimes n} \otimes \Psi)$

$= \frac{1}{2^{mn}} P_n(\rho^{\otimes n} \otimes \Phi^{\otimes mn}) + \left(1 - \frac{1}{2^{mn}}\right) P_n(\rho^{\otimes n} \otimes \Gamma)$

$= \frac{1}{2^{mn}}\, \sigma + \left(1 - \frac{1}{2^{mn}}\right) P_n(\rho^{\otimes n} \otimes \Gamma)$

$\therefore$ σ ε-closed to $\Phi^{\otimes mn(1+\delta)}$

Output $\frac{\varepsilon}{2^{mn}}$-closed to $\frac{1}{2^{mn}} \Phi^{\otimes mn(1+\delta)} + \left(1-\frac{1}{2^{mn}}\right) P_n(\rho^{\otimes n} \otimes \Gamma)$

(2) Alice & Bob apply $F_{k,s}$ for $k = mn(1+\delta)$.

Output $\frac{\varepsilon}{2^{mn}}$-closed to

$$\left[\frac{1}{2^{mn}} \Phi^{\otimes mn(1+\delta)-s} + \left(1-\frac{1}{2^{mn}}\right)\frac{1}{2^s} \widetilde{P_n(\rho^{\otimes n} \otimes \Gamma)}\right] \otimes \text{"Pass"}$$

$$+ \left(1-\frac{1}{2^{mn}}\right)\left(1-\frac{1}{2^s}\right) \widetilde{\widetilde{P_n(\rho^{\otimes n} \otimes \Gamma)}} \otimes \text{"fail"}$$

③ Repeat ① & ② N times for $N \gg 2^{mn}$.

④ Postselect on states flagged by "Pass".

This gives $\approx N\left(\frac{1}{2^{mn}} + \frac{1}{2^s} - \frac{1}{2^{mn+s}}\right)$ copies of

$$\rho' \doteq \frac{1}{2^{mn}} \Phi^{\otimes mn(1+\delta)-s} + \left(1 - \frac{1}{2^{mn}}\right) \frac{1}{2^s} P_n(\rho^{\otimes n} \otimes \Gamma)$$

⑤ It is known that ρ' is distillable if

$$\frac{1}{2^{mn}} > \frac{1}{2^{mn(1+\delta)-s}} + \frac{\varepsilon}{2^{mn}} \quad \text{ie} \quad 1 \geq 2^{s-mn\delta} + \varepsilon$$

(singlet fidelity $> \frac{1}{\dim(A)}$, adjusted by error of ρ'.)

Luckily, $m = \text{const}$ $\therefore$ we can choose $s = n(md) \times 2$ to ensure the above (& $D_{\leftrightarrow}(\rho') = \eta > 0$)

Now n depends on ε we're done with ε (as long as $D_{\leftrightarrow}(\rho') > 0$). So n is also a const.

⑥ Alice & Bob distill their $N\left(\frac{1}{2^{mn}} + \frac{1}{2^s} - \frac{1}{2^{mn+s}}\right)$ copies of ρ' to get $\approx \eta N\left(\frac{1}{2^{mn}} + \frac{1}{2^s} - \frac{1}{2^{mn+s}}\right)$ ebits.

They've used nN copies of ρ.

$$\therefore D_{\leftrightarrow}(\rho) \geq \frac{\eta}{n}\left(\frac{1}{2^{mn}} + \frac{1}{2^s} - \frac{1}{2^{mn+s}}\right) > 0$$

$\blacksquare$

☺

NB Previous version of lecture notes failed to stop n from growing so we didn't get $D_{\leftrightarrow}(\rho) > 0$.

(Rewording etc didn't help either.)

Also the alt proof in 9908070 has a problem:

In 9908070v3 lemma 4, it was proved that there is no $S_1 \in$ LOCC s.t. $S_1(\Phi^{\otimes n} \otimes \rho^{\otimes k}) = \Phi^{\otimes 3n}$

But we're concerned with the existence of a family of protocols $S_1^{(n)}(\Phi^{\otimes n} \otimes \rho^{\otimes k}) \doteq \Phi^{\otimes n(3-\delta_n)}$ where acc is measured by trace distance ε_n

Then single fraction of output when sub $\Phi^{\otimes n}$ by $\frac{1}{4^n} = \frac{1}{4^n} \pm \varepsilon_n$

and $\varepsilon_n \ll \frac{1}{4^n}$ to ensure the above $\geq \frac{1}{8^n}$ for the needed contradiction.

Cor: $Q_{\leftrightarrow}(N \otimes I_d) = Q_{\leftrightarrow}(N) + Q_{\leftrightarrow}(I_d)$

Pf: $Q_{\leftrightarrow}(N) = \sup_n \frac{1}{n} D_{\leftrightarrow}\left(I_{A'} \otimes N^{\otimes n} (|\psi\rangle_{A'B^n}) \right)$

$$Q_{\leftrightarrow}(N \otimes I_d) = \sup_n \frac{1}{n} D_{\leftrightarrow}\Big(\underbrace{I_{A'} \otimes N^{\otimes n} \otimes I_d^{\otimes n} (|\tilde{\psi}\rangle)}_{\text{WLOG} \ \shortparallel} \Big)$$

$$I_{A'} \otimes N^{\otimes n}(|\psi\rangle) \otimes \Phi^{\otimes n \log d}$$

Since the ebits can be converted to I_d by TP & be used in any other way

$= Q_{\leftrightarrow}(N) + Q_{\leftrightarrow}(I_d)$ by Thm on $D_{\leftrightarrow}$

Cor. $Q_{\leftarrow}(N \otimes I_d) = Q_{\leftarrow}(N) + \log d$.

Pf: suffices to consider $Q_{\leftarrow}(N) = 0$

But $Q_{\leftarrow}(N) = 0 \Rightarrow Q_{\leftrightarrow}(N) = 0$

because if $Q_{\leftrightarrow}(N) \neq 0$, $D_{\leftrightarrow}(N) \neq 0$

then use N to general forward classical communication

($C(N) \neq 0$ if $Q_{\leftrightarrow}(N) \neq 0$) to teleport q-data

(this assumes comm in 2-way distillation is at most

linear and I think this is true).