Lec 16, Jun 29, 2010

Note Title 27/06/2010

Last time, we proved the decoupling condition for both father & mother (the LSD theorem needs yet 1 more piece to complete).

So the follow resource inequalities hold approx & asymptotically:

♀ mother : $\forall \alpha_{RB}$, purified by E

$$\alpha_{RB} + \frac{1}{2} S(R:E)_\alpha \text{ qbit} \geq \frac{1}{2} S(R:B)_\alpha \text{ ebit}$$

♂ father : $\forall N, |\alpha\rangle_{RBE} = I \otimes U_N |\phi\rangle_{RA}$

$$N + \frac{1}{2} S(R:E)_\alpha \text{ ebit} \geq \frac{1}{2} S(R:B)_\alpha \text{ qbit}$$

Also, recall SD: qbit + ebit = 2 cobit $\geq$ 2 cbit

TP: 2 cbit + ebit $\geq$ qbit

ED: qbit $\geq$ ebit

This time: their children — Devetak, Harrow, Winter [PRL 93, 230504 (2004)]

Children of the father:

(C1) Suppose we want to transmit quantum data using $\mathcal{N}$.

If we ① borrow $\frac{n}{2} S(R:E)_\rho$ ebits between Alice & Bob

② run the father protocol to transmit $\frac{n}{2} S(R:B)_\rho$ qubits

(consuming the borrowed ebits & n uses of $\mathcal{N}$)

allocate $\begin{cases} \frac{n}{2} S(R:E)_\rho \text{ qubits to reestablish } \frac{n}{2} S(R:E)_\rho \text{ ebits} \\ \text{the remaining } \frac{n}{2}\left[S(R:B)_\rho - S(R:E)_\rho\right] = n I_c(R\rangle B)_\rho \text{ qubit} \\ \text{to transmit quantum data} \end{cases}$

③ run ② l times

④ return the borrowed ebits.

If the ℓ^{th} protocol has error ε_n on perfect ebits

the 2^{nd} run has ebits with error $\leq \varepsilon_n$, output with error $\leq 2\varepsilon_n$

3^{rd} $\leq 2\varepsilon_n$, $\leq 3\varepsilon_n$

$\vdots$

combined error of output $= \varepsilon_n(1+2+\cdots+\ell) = \frac{\ell(\ell+1)}{2}\varepsilon_n$

This transmits $\ell n\left(I_c(R\rangle B) - \delta_n\right)$ qubits with ℓn uses.

δ_n: slight rate deficit needed

Choosing $\ell = \frac{1}{\varepsilon_n^{\frac{1}{4}}}$, error $\approx \varepsilon_n^{\frac{1}{2}}$ still small.

Instead of borrowing & returning ebits, we can also generate $\frac{n}{2} S(R\rangle E)_\rho$ ebits inefficiently with const $\times n$ uses of N (self bootstrapping):

As long as $\frac{\ell n}{\ell n + \text{const} \times n} \approx (1 - o(n))$ the asymptotic rate

of $I(R\rangle B)_\rho$ is still achieved (i.e. need ℓ s.t. $\frac{\text{const}}{\ell} \approx o(n)$

$$\ell > \frac{\text{const}}{o(n)}$$

we also have $\ell \leq \frac{1}{\varepsilon n^{\frac{1}{4}}} \approx \exp(\sqrt{n})$

plenty of room to choose ℓ).

In the resourcing framework, we put δ & $\in D$ (both proved) to get channel (direct) coding theorem:

$$N + \tfrac{1}{2} S(R:E)_\rho \text{ ebit} \overset{\delta}{\geq} \tfrac{1}{2} S(R:B)_\rho \text{ qbit} \overset{\in D}{\geq} \tfrac{1}{2} I_c(R\rangle B)_\rho \text{ qbits} + \tfrac{1}{2} S(R:E)_\rho \text{ ebit}$$

$$\therefore N \geq \tfrac{1}{2} I_c(R\rangle B)_\rho$$

This gives an alternative to LSD theorem if $Q(N) > 0$.

We'll see later $\forall N \quad Q(N \circledast I) = Q(N) + Q(I)$

So either: $\begin{cases} Q(N) = 0 \text{ \& borrowing doesn't help} \\ \text{\& don't bother "fattening"} \\ \text{or} \\ Q(N) > 0 \text{ without borrowing \& self bootstrapping works} \end{cases}$

(C2): Suppose the goal is entanglement assisted classical capacity.

If we ① run the father protocol to generate $\frac{n}{2} S(R:B)_\rho$ qbits
(consuming $n\,N$ & $\frac{n}{2} S(R:E)_\rho$ ebits)

② use these $\frac{n}{2} S(R:B)_\rho$ qbits & $\frac{n}{2} S(R:B)_\rho$ extra ebits
to do SD

We ends up with $n\,S(R:B)_\rho$ cobits (& surely cbits).

ie $\frac{1}{2} S(R:B)_\rho$ ebit + $\left[\frac{1}{2} S(R:E)_\rho \text{ ebit} + N \right]$

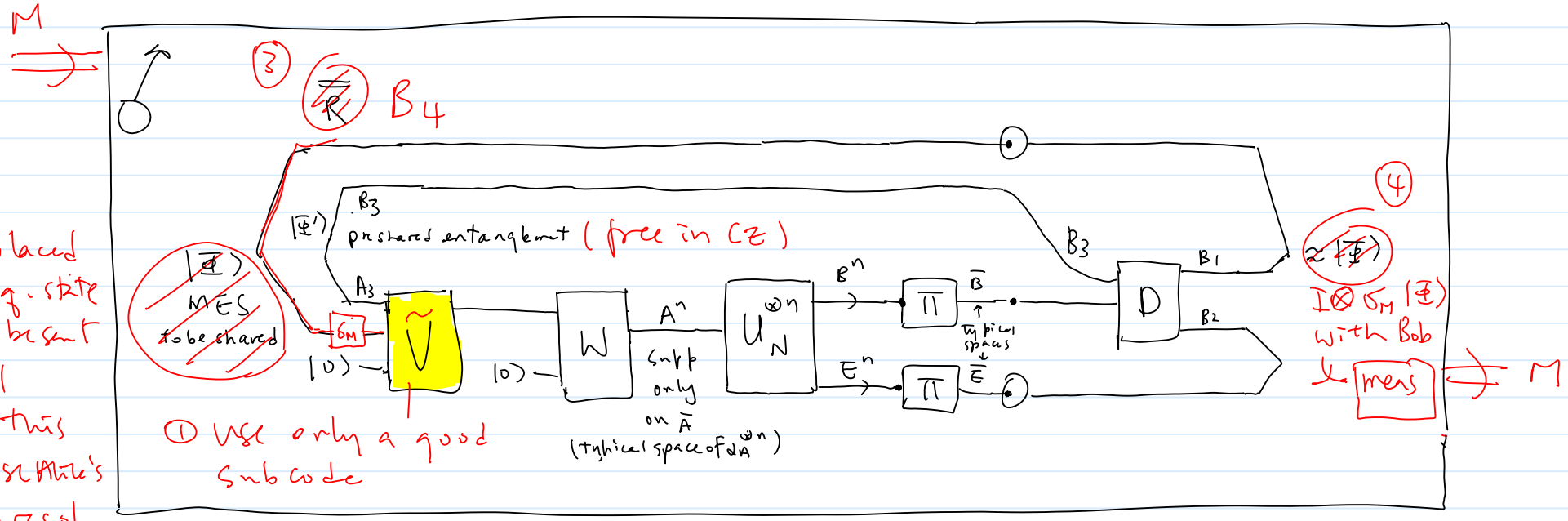
$\geq$ (by) $\frac{1}{2} S(R:B)_\rho$ ebit + $\frac{1}{2} S(R:B)_\rho$ qbit

$\overset{SD}{=} S(R:B)_\rho$ cobit $\geq S(R:B)_\rho$ cbit.

Tidying: $H(R)_\rho$ ebit + $N \geq S(R:B)_\rho$ cbit

The direct coding thm for $C_E(N)$ com.

Red: changes to code for $CE(N)$:



Children of the mother:

$$♀: \quad \alpha_{RB} + \tfrac{1}{2} S(R:\bar{E})_\alpha \text{ qbit} \geq \tfrac{1}{2} S(R:B)_\alpha \text{ ebit}$$

(C1) Her first child was born with TP

ie we use cbits & ebits from ♀ to transmit q. bits.

$$S(R:B)_\alpha \text{ cbit} + \left[\alpha_{RB} + \tfrac{1}{2} S(R:\bar{E})_\alpha \text{ qbit}\right]$$

$$\overset{♀}{\geq} S(R:B)_\alpha \text{ cbit} + \tfrac{1}{2} S(R:B)_\alpha \text{ ebit}$$

$$\overset{TP}{\geq} \tfrac{1}{2} (R:B)_\alpha \text{ qbit}.$$

By borrow $\frac{n}{2} S(R:\bar{E})_\alpha$ qbits & returning in the end, or by inefficiently producing it using const $\times n$ (cbits & copies of α) & repeating the above enough # times to offset this initial cost, we can cancel the

$\frac{1}{2} S(R:\bar{E})_\rho$ qbit on both sides of the resource inequality:

$$\therefore\ S(R:B)_\rho \text{ cbit} + \rho_{RB} \geq I_c(R\rangle B)_\rho \text{ qbit}$$

$$= \left[\tfrac{1}{2} S(R:B) - \tfrac{1}{2} S(R:E)\right]$$

This is call "noisy teleportation" (NTP) since mixed state ent is used with classical comm to send noiseless Q data.

(2) The mother's second child uses TP to supply the qbit needed (LHS):

$$\rho_{RB} + \left[\tfrac{1}{2} S(R:\bar{E})_\rho \text{ ebit} + S(R:\bar{E})_\rho \text{ cbit}\right] \geq \tfrac{1}{2} S(R:B)_\rho \text{ ebit}$$

$$\therefore\ \rho_{RB} + S(R:\bar{E})_\rho \text{ cbit} \geq I_c(R\rangle B)_\rho \text{ ebit}$$

(if we take NTP to create ebits, $S(R:B)_\rho$ cbits will be needed.)

This child was famous years before its birth.
The "hashing inequality": ∞ cbit + $\alpha_{RB} \geq I_c(R\rangle B)_\alpha$ ebit
was conjectured to hold for years, and is concerned with the traditional task to distill entanglement with free forward CC.

The current proof is easy, and gives a bound on how many cbits are need. and gives an actual protocol (Q + TP to send B_3)

(C3) A more similar sibling of NTP is NSD -
this time, the ebits from Q is used to do SD instead:

$\frac{1}{2} S(R:B)_\alpha$ qbit + $\left[\alpha_{RB} + \frac{1}{2} S(R:E)_\alpha \text{ qbit}\right]$

$\overset{Q}{\geq}$ $\frac{1}{2} S(R:B)_\alpha$ qbit + $\frac{1}{2} S(R:B)_\alpha$ ebit

$\overset{SD}{\geq}$ $S(R:B)_\alpha$ cobit $\geq$ $S(R:B)_\alpha$ cbit

An aunt (or house keeper):

Note that at the end of the mother protocol, Bob purifies Eve,

$$\therefore \quad \psi : \alpha_{RBE} + \frac{1}{2} S(R:\bar{E})_\alpha \text{ qubit} \geq \underbrace{\frac{1}{2} S(R:B)_\alpha \text{ ebit}}_{\text{desirable output}} + \underbrace{\alpha_{B\bar{E}}}_{\text{side product}}$$

Merging is a task in which RBE share iid copies of a pure state α and R wants to give B his share, preserving the correlation with Eve. This requires comm between R & B.

Idea: count cbits from R to B & # of ebits used

From φ : $\alpha_{RBE} + \underbrace{\frac{1}{2} S(R:E)_\alpha \text{ qbit}}_{\text{subbing this using TP}} \geq \frac{1}{2} S(R:B)_\alpha \text{ ebit} + \alpha_{B_2 E}$

$$\alpha_{RBE} + \left[S(R:E)_\alpha \text{ cbit} + \tfrac{1}{2} S(R:E)_\alpha \text{ ebit} \right] \geq \tfrac{1}{2} S(R:B)_\alpha \text{ ebit} + \alpha_{B_2 E}$$

But $\frac{1}{2} S(R:E)_\alpha - \frac{1}{2} S(R:B)_\alpha = -I_c(R\rangle B) = -(S(B)-S(RB))$

$$= S(RB) - S(B) = S(R|B)$$

$\therefore$ Merging: $\alpha_{RBE} + S(R:E)_\alpha \text{ cbit} + \underbrace{S(R|B) \text{ ebit}}_{\text{if -ve it gives the \# ebits left to RB after merging}} \geq \alpha_{B_2 E}$

if +ve, it represents how many ebits are consumed

Merging

$$\alpha_{RBE}{}^{\dagger}\ S(R:E)_{\alpha}\ \text{cbit} + S(R|B)_{\alpha}\ \text{ebit} \geq \alpha_{B_2E}$$

↑ TP

♀ mother : $\forall \alpha_{RB}$, purified by E

$$\alpha_{RB}{}^{\dagger}\ \tfrac{1}{2} S(R:E)_{\alpha}\ \text{qbit} \geq \tfrac{1}{2} S(R:B)_{\alpha}\ \text{ebit}$$

TP ↓

NTP

$$\alpha_{RB} + S(R:B)_{\alpha}\ \text{cbit} \geq I_c(R\rangle B)_{\alpha}\ \text{qbit}$$

EP ↓

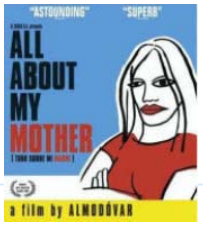
Hashing Ineq

$$\alpha_{RB} + S(R:E)_{\alpha}\ \text{cbit} \geq I_c(R\rangle B)_{\alpha}\ \text{ebit}$$

SD ↓

NSD

$$\alpha_{RB} + S(R)_{\alpha}\ \text{qbit} \geq S(R:B)_{\alpha}\ \text{cbit}$$



The Brady Bunch

♂ father : $\forall N, |\Omega\rangle_{RBE} = I \otimes U_N |\Phi\rangle_{RA}$

$$N^{\dagger}\ \tfrac{1}{2} S(R:E)_{\alpha}\ \text{ebit} \geq \tfrac{1}{2} S(R:B)_{\alpha}\ \text{qbit}$$

TP ↓

Q(N)

$$N \geq I_c(R\rangle B)_{\alpha}\ \text{qbit}$$

SD ↓

CE(N)

$$N + S(R)_{\alpha}\ \text{ebit} \geq S(R:B)_{\alpha}\ \text{cbit}$$

eg. $|\alpha\rangle_{RBE} = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$ (Classical correlation between BE)

$= \frac{1}{2}|+\rangle_R(|00\rangle+|11\rangle)_{BE} + \frac{1}{2}|-\rangle_R(|00\rangle-|11\rangle)_{BE}$

How to do Merging: R meas in $|\pm\rangle$ basis, tells B the ans.

If $(-)$, Bob applies δ_Z to his qubit.

Final state: $\frac{1}{2}(|++\rangle + |--\rangle_{RB'}) \otimes \frac{1}{\sqrt{2}}(\underbrace{|00\rangle+|11\rangle}_{|\alpha\rangle})_{B_2E}$

Consumes $S(R|E)_\alpha = 1$ cbit,

$S(R|B) = S(RB) - S(B) = 1 - 1 = 0$ ebits

How to get Mother: If R sends meas outcome with cobits:

final state $= \frac{1}{\sqrt{2}}(|++\rangle+|--\rangle)_{RB'} \otimes \frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{B_2E}$

$\therefore$ α + 1 cobit $\geq$ 1 ebit

$\alpha + \frac{1}{2}$ qbit $\geq \frac{1}{2}$ ebit

$\frac{1}{2} S(R=E)_\alpha = \frac{1}{2}$ $\quad$ $\frac{1}{2} S(R=B)_\alpha = \frac{1}{2}$

Here, α useless since $\frac{1}{2}$ qbit $\geq \frac{1}{2}$ ebit even without α around.

Likewise, more of NTP, Hashing, NSD is nontrivial (that's because α is absolutely nonsense as resource to make ebits).

eg. $|\alpha\rangle_{RBE} = |0\rangle_B |\phi\rangle_{RE}$.

Then merging reduces to data compression

$$\alpha_{RBE}^{\dagger} \underbrace{S(R=E)_\alpha \text{ cbit}}_{2 \times S(R)} + \underbrace{S(R|B)_\alpha \text{ ebit}}_{S(R)} \geq \alpha_{B_2 E}$$

$S(R)$ qbits

eg. $|\alpha\rangle_{RBE} = |\phi\rangle_{RB} |0\rangle_E$

Merging is simbly entanglement concentration of $|\phi\rangle_{RB}$.

$$\alpha_{RBE}^{\dagger} \underbrace{S(R:E)_\alpha}_{0} \text{ cbit} + \underbrace{S(R|B)_\alpha}_{-S(R) = -E(|\phi\rangle)} \text{ ebit} \geq \alpha_{B_2E}$$

$\therefore \alpha_{RBE} \geq E(|\phi\rangle)$ ebits $+ \alpha_{B_2E}$

The framework of resource inequalities beg the Qn:

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

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

↑ 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 (catalytic) resources (such as LSD derived from $\bar{0}$)

same Qn

We will see Q, $Q_{\leftarrow}$, $Q_{\leftrightarrow}$, $D_{\rightarrow}$, $D_{\leftarrow}$, $D_{\leftrightarrow}$ are all additive on no-signaling resources.

Main idea (in BPSW96) 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: Gottesman, Hamrow, M. Horodecki, L, Oppenheim, Shor, Winter & never written up.