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 following 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: 2cbit + 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 N.

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

(2) run the father protocol to transmit $\frac{n}{2} S(R:B)_\alpha$ qubits (consuming the borrowed ebits & n uses of N)

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

(3) run (2) l times

(4) return the borrowed ebits.

If the father protocol has error ε_n on perfect ebits

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

3rd $\leq 2\varepsilon_n$, $\leq 3\varepsilon_n$

⋮

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

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

slight rate deficit needed

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

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

As long as $\frac{ln}{ln + \text{const} \times n} \approx (1 - o(n))$ the asymptotic rate of $I(R\rangle B)_\alpha$ is still achieved (i.e. need l s.t. $\frac{\text{const}}{l} \approx o(n)$

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

we also have $l \leq \frac{1}{\varepsilon_n^{1/4}} \approx \exp(\sqrt{n})$

plenty of room to choose l).

In the resourcing framework, we put ♂ & ED (both proved) to get channel (direct) coding theorem:

$N + \frac{1}{2} S(R:E)_\alpha \text{ ebit} \overset{♂}{\geq} \frac{1}{2} S(R:B)_\alpha \text{ qbit} \overset{ED}{\geq} \frac{1}{2} I_c(R\rangle B)_\alpha \text{ qbits} + \frac{1}{2} S(R:E)_\alpha \text{ ebit}$

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

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

Will see later $\forall N$ $Q(N \otimes I) = Q(N) + Q(I)$

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

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

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

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

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

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

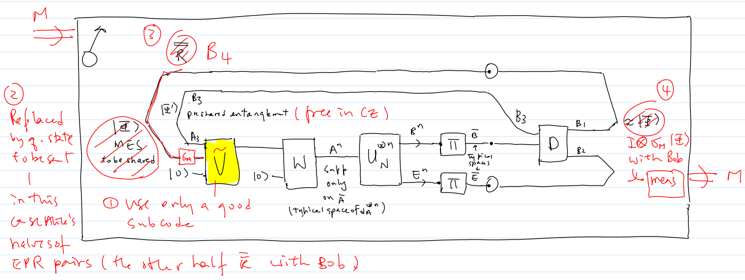
$\geq \frac{1}{2} S(R:B)_\alpha \text{ ebit} + \frac{1}{2} S(R:B)_\alpha \text{ qbit}$

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

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

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

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



Children of the mother:

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

(C1) Her first child was born with TP

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

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

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

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

$$\therefore S(R:B)_\alpha \text{ cbit} + \alpha_{RB} \geq \underset{\left[\frac{1}{2}S(R:B) - \frac{1}{2}S(R:E)\right]}{\underset{\shortparallel}{I_c(R\rangle B)_\alpha}} \text{ qbit}$$

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

(C2) The mother's second child uses TP to supply the qbit needed (LHS):

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

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

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

This child was famous years before its birth.

The "hashing inequality": $\infty \text{ cbit} + \alpha_{RB} \geq I_c(R\rangle B)_\alpha \text{ ebit}$ 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 (♀ + TP to send B_3)

(C3) A more similar sibling of NTP is NSD –

this time, the ebits from ♀ is used to do SD instead:

$$\tfrac{1}{2} S(R:B)_\alpha \text{ qbit} + \left[\alpha_{RB} + \tfrac{1}{2} S(R:E)_\alpha \text{ qbit}\right]$$
$$\overset{♀}{\geq} \tfrac{1}{2} S(R:B)_\alpha \text{ qbit} + \tfrac{1}{2} S(R:B)_\alpha \text{ ebit}$$
$$\overset{SD}{\geq} S(R:B)_\alpha \text{ cobit} \geq S(R:B)_\alpha \text{ cbit}$$

An aunt (or house keeper):

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

$$\therefore ♀ : \alpha_{RBE} + \tfrac{1}{2} S(R:E)_\alpha \text{ qbit} \geq \underbrace{\tfrac{1}{2} S(R:B)_\alpha \text{ ebit}}_{\text{desirable output}} + \underbrace{\alpha_{B_2 E}}_{\text{side product}}$$

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

$$\text{from } ♀ : \alpha_{RBE} + \underbrace{\tfrac{1}{2} S(R:E)_\alpha \text{ qbit}}_{\text{supply this using TP}} \geq \tfrac{1}{2} S(R:B)_\alpha \text{ ebit} + \alpha_{B_2 E}$$

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

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

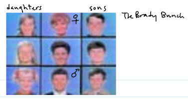
$$\therefore \text{Merging: } \alpha_{RBE} + S(R:E)_\alpha \text{ cbit} + \underbrace{S(R|B)}_{\substack{\text{if -ve it gives the \# ebits} \\ \text{left to RB after merging}}} \text{ ebit} \geq \alpha_{B_2 E}$$

if +ve, it represents how many ebits are consumed

Merging

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

↑ TP



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

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

↓ 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

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

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

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

↓ TP

Q(N)

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

↓ SD

$C_E(N)$

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

---

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 $|-\rangle$, Bob applies σ_Z to his qubit.

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

Consumes $S(R{:}E)_\alpha = 1$ cbit,

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

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

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

$\therefore\ \alpha + 1\ \text{cobit} \geq 1\ \text{ebit}$

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

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

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

Likewise, none of NTP, Hashing, NSD is nontrivial

(that's because α is absolutely rubbish as resource to make ebits).

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

Then merging reduces to data compression

$\underbrace{\alpha_{RBE} + \underbrace{S(R{:}E)_\alpha}_{2 \times S(R)}\ \text{cbit} + \underbrace{S(R|B)_\alpha}_{S(R)}\ \text{ebit}}_{S(R)\ \text{qbits}} \geq \alpha_{B_2E}$

---

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

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

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

$\therefore\ \alpha_{RBE} \geq E(|\phi\rangle)$ 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 ♂)

We will see Q, $Q_\leftarrow$, $Q_\leftrightarrow$, $D_\rightarrow$, $D_\leftarrow$, $D_\leftrightarrow$ are all additive on noiseless resources.

(same Qn: $D_\rightarrow$, $D_\leftarrow$)

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 : Gottesman, Harrow, M. Horodecki, L, Oppenheim, Shor, Winter & never written up .