Lecture 23

3/29/2011

Recall direct part of EA classical capacity theorem. $\exists$ message set $\mathcal{M}$ & EA quantum codewords

$$U(s(m))^{A^n} |\varphi\rangle^{A^nB^n} \quad w/ \ |\mathcal{M}| \approx 2^{nI(A;B)},$$

& POVM $\{\Lambda_m^{B'^nB^n}\}$ such that

$$\forall m \quad \mathrm{Tr}\{\Lambda_m^{B'^nB^n} \mathcal{N}^{A'^n\to B'^n}(U(s(m))^{A^n} \varphi^{A^nB^n} [U^\dagger(s(m))]^{A^n})\} \geq 1-\epsilon$$

nice property of EA codewords is that $U(s(m))^{A^n} |\varphi\rangle^{A^nB^n} = U^T(s(m))^{B^n} |\varphi\rangle^{A^nB^n}$

Also, the protocol consumes entanglement at a rate equal to $H(A)_\varphi$. Thus, the resource inequality for the protocol is

$$\langle \mathcal{N} \rangle + H(A)_\varphi [qq] \geq I(A;B)_\rho [c\to c]$$

where $\rho^{AB} = \mathcal{N}^{A'\to B}(\varphi^{AA'})$

How to turn this into a protocol for entanglement-assisted quantum communication?

simple way is to use extra entanglement + teleportation:

$$\langle \mathcal{N} \rangle + \left(H(A)_\rho + \tfrac{1}{2} I(A;B)_\rho \right) [qq] \geq$$

$$I(A;B)_\rho [c \to c] + \tfrac{1}{2} I(A;B)_\rho [qq] \qquad \text{(EAC)}$$

$$\geq \tfrac{1}{2} I(A;B) [q \to q] \qquad \text{(teleportation)}$$

this rate of q. comm is provably optimal. Were it not so, then we could combine further w/ dense coding + beat EAC capacity...

though, protocol above uses too much entanglement...

can make more judicious use of entanglement w/ a different protocol that uses our EA code. will show how to achieve

$$\langle \mathcal{N} \rangle + H(A)_\rho [qq] \geq I(A;B)_\rho \underbrace{[q \to qq]}_{\text{coherent bits from Ch. 7}}$$

Consider state

$$|\psi\rangle^{RA_1} \equiv \sum_{l,m=1}^{D^2} \alpha_{l,m} \underbrace{|l\rangle^R |m\rangle^{A_1}}_{\text{some orthonormal bases...}}$$

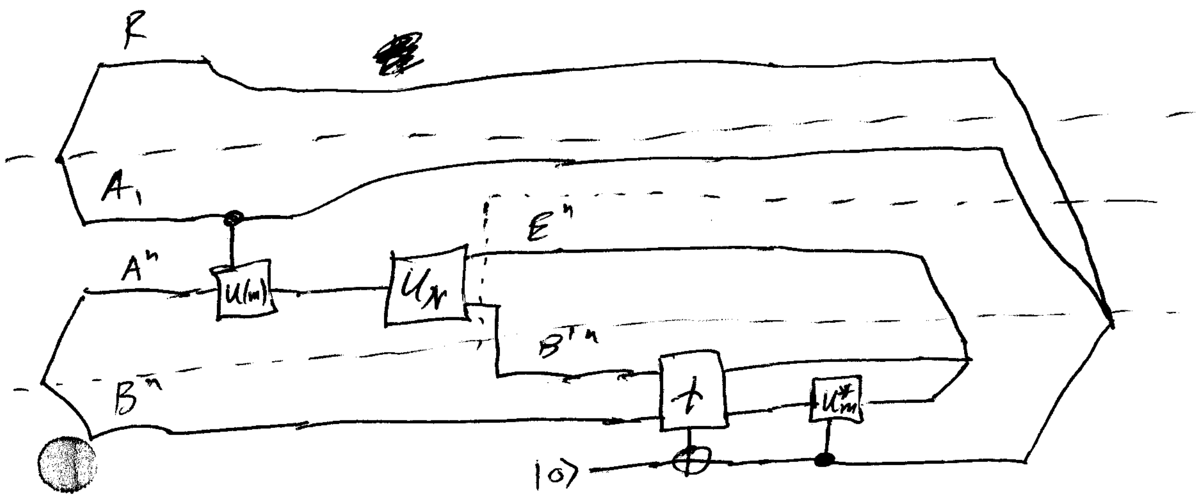
Alice & Bob implement coherent channel if they execute $|m\rangle^{A_1} \to |m\rangle^{A_1} |m\rangle^{B_1}$ & state above becomes

$$|\psi\rangle^{RA_1} \to \sum_{l,m=1}^{D^2} \alpha_{l,m} |l\rangle^R |m\rangle^{A_1} |m\rangle^{B_1}$$

they do so approximately if state is ϵ-close to the above state

3/29/2011

execute coherent version of EAC protocol w/ controlled unitaries and coherent measurements.



Alice first applies controlled unitary from A_1 to A^n:

$$\sum_m |m\rangle\langle m|^{A_1} \otimes U(s(m))^{A^n}$$

global state becomes

$$\sum_{l,m} \alpha_{l,m} |l\rangle^R |m\rangle^{A_1} \; U(s(m))^{A^n} \; |\varphi\rangle^{A^n B^n}$$

this is equivalent to

$$\sum_{l,m} \alpha_{l,m} \; |l\rangle^R |m\rangle^{A_1} \; U^T(s(m))^{B^n} \; |\varphi\rangle^{A^n B^n}$$

by properties of code

3/29/2011

Alice sends A^n through channel.
Consider isometric extension instead
so that

$$|\psi\rangle^{B'^n E^n B^n} = U_{\mathcal{N}}^{A\to B'E^n} |\varphi\rangle^{A^n B^n}$$

global state becomes

$$\sum_{l,m} \alpha_{l,m} |l\rangle^R |m\rangle^{A_1} U^T(s(m))^{B^n} |\psi\rangle^{B'^n E^n B^n}$$

Recall coherent measurement,
If $\forall k \quad \mathrm{Tr}\{\Lambda_k \rho_k\} \geq 1-\epsilon$
then

$$\langle\phi_k| \langle k| \left(\sum_{k'} \sqrt{\Lambda_{k'}} \otimes |k'\rangle \right) |\phi_k\rangle \geq 1-\epsilon$$

(identifies state & doesn't disturb too much)

So Bob can make coherent measurement

$$\sum_m \sqrt{\Lambda_m}^{B'^n B^n} \otimes |m\rangle^{B_1}$$

& resulting state is very close to

$$\sum_{l,m} \alpha_{l,m} |l\rangle^R |m\rangle^{A_1} U^T(s(m))^{B^n} |\psi\rangle^{B'^n E^n B^n} |m\rangle^{B_1}$$

Bob does controlled unitary

$$\sum_m |m\rangle\langle m|^{B_1} \otimes U^*(s(m))^{B^n}$$

& state becomes

$$\sum_{l,m} \alpha_{l,m} |l\rangle^R |m\rangle^{A_1} U^*(s(m))^{B^n} U^T(s(m))^{B^n} |\varphi\rangle^{B'^n E^n B^n} |m\rangle^{B_1}$$

$$= \underbrace{\left(\sum_{l,m} \alpha_{l,m} |l\rangle^R |m\rangle^{A_1} |m\rangle^{B_1}\right)}_{\text{they have implemented a coherent channel}} \otimes |\varphi\rangle^{B'^n E^n B^n}$$

How to make this protocol work for EA quantum communication?

use coherent communication identity: $2[q \to qq] = [qq] + [q \to q]$

$$\langle N \rangle + H(A)[qq] \geq I(A;B)[q \to qq]$$

$$\geq \frac{1}{2} I(A;B)[q \to q] + \frac{1}{2} I(A;B)[qq]$$

say that protocol is catalytic, where it consumes & generates same resource

Since $H(A) - \frac{1}{2} I(A;B) = \frac{1}{2} I(A;E)$

(from homework)

resource inequality is

$$\langle N \rangle + \frac{1}{2} I(A;E) \{qq\} \geq \frac{1}{2} I(A;B) \{q \to q\}$$

can combine further w/ entanglement distribution to get protocol for quantum communication:

$$\begin{aligned}\langle N \rangle + \frac{1}{2} I(A;E) \{qq\} &\geq \left[\frac{1}{2} I(A;B) - \frac{1}{2} I(A;E)\right] \{q \to q\} \\ &\quad + \frac{1}{2} I(A;E) \{q \to q\} \\ &\geq \left\{\frac{1}{2} I(A;B) - \frac{1}{2} I(A;E)\right\} \{q \to q\} \\ &\quad + \frac{1}{2} I(A;E) \{qq\}\end{aligned}$$

canceling resources + noting that

$$\frac{1}{2} I(A;B) - \frac{1}{2} I(A;E) = I(A \rangle B),$$ (from homework)

we get

$$\langle N \rangle \geq \underbrace{I(A \rangle B)}_{\text{coherent information}} \{q \to q\}$$

coherent information is achievable rate for quantum comm.

we proved this protocol in a catalytic way & you might not like this, but we can show this does not matter, by proving a converse theorem that demonstrates that catalytic use of entanglement & even classical communication cannot improve quantum capacity.

You proved (in hwk) that any achievable rate Q for q. comm. obeys

$$Q \leq \underbrace{Q(\mathcal{N}^{\otimes n})}_{\text{coherent info of channel}}$$

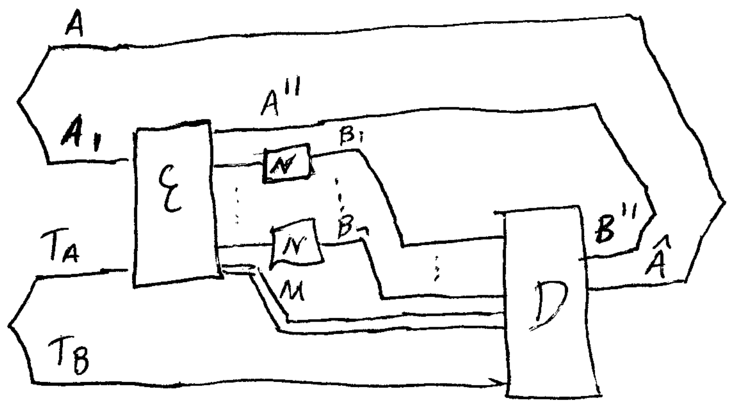
$$Q(\mathcal{N}) = \max_{\phi^{AA'}} I(A \rangle B)_\rho$$

where $\rho^{AB} = \mathcal{N}^{A' \to B}(\phi^{AA'})$

we will prove the same bound for catalytic & classical-assisted protocols:

3/29/2011

protocol for catalytic & classical-assisted entanglement generation:



begin w/ (size 2^{nE}) (size 2^{nE_c})

$$\Phi^{AA_1} \otimes \Phi^{T_A T_B}$$

encode

$$\omega^{AA''A'^n M T_B} = \mathcal{E}^{A_1 T_A \to A'' A'^n M}\left(\Phi^{AA_1} \otimes \Phi^{T_A T_B}\right)$$

send through channel:

$$\omega^{AA''B^n M T_B} = \mathcal{N}^{A'^n \to B^n}\left(\omega^{AA''A'^n M T_B}\right)$$

then decode

$$(\omega')^{A\hat{A}A''B''} = \mathcal{D}^{B^n M T_B \to B''\hat{A}}\left(\omega^{AA''B^n M T_B}\right)$$

protocol is good if

$$\left\| \omega' - \Phi^{A\hat{A}} \otimes \Phi^{A''B''} \right\|_1 \leq \epsilon$$

where $E_c = E_G$

demand to have size 2^{nE_G}

3/29/2011

$$n(E + E_G) = I(A \rangle \hat{A})_{\Phi} + I(A'' \rangle B'')_{\Phi}$$

$$= I(AA'' \rangle \hat{A}B'')_{\Phi\otimes\Phi} \quad \text{(b/c product states)}$$

$$\leq I(AA'' \rangle \hat{A}B'')_{\omega'} + n\epsilon' \quad \text{(Alicki-Fannes')}$$

$$\leq I(AA'' \rangle B^n M T_B)_{\omega} + n\epsilon' \quad \text{(QDP)}$$

$$= H(B^n M T_B)_{\omega} - H(AA'' B^n M T_B)_{\omega} + n\epsilon'$$

$$\leq H(B^n M)_{\omega} - H(AA'' B^n M T_B)_{\omega} + H(T_B)_{\omega} + n\epsilon'$$

$$= I(AA'' T_B \rangle B^n M)_{\omega} + H(T_B)_{\omega} + n\epsilon'$$

$$\leq I(AA'' T_B \rangle B^n M)_{\omega} + nE_C + n\epsilon'$$

$\therefore$

$$nE \leq I(AA'' T_B \rangle B^n M)_{\omega} + n\epsilon'$$

b/c $E_G = E_C$ (we demanded this)

state ω is of form

$$\frac{1}{|M|} \sum_m |m\rangle\langle m|^M \otimes \omega_m^{AA'' T_B \, B^n}$$

particular state of form

$$\sum_x p(x) |x\rangle\langle x|^X \otimes \mathcal{N}^{A'^n \to B^n}(\rho_x^{AA'^n})$$

3/29/2011

$\therefore$

$$nE \leq \max_{\rho^{XAA'^n}} I(A\rangle B^n X) + n\epsilon'$$

take spectral decomp. of

$$\rho_x^{AA'^n} = \sum_y p(y|x)\, \psi_{y,x}^{AA'^n}$$

+ define

$$\sum_{x,y} p(x)\, p(y|x)\, |x\rangle\langle x|^X \otimes |y\rangle\langle y|^Y \otimes \mathcal{N}^{A'^n\to B^n}(\psi_{x,y}^{AA'^n})$$

$$\therefore \max_{\rho^{XAA'^n}} I(A\rangle B^n X) \leq \max_{\rho^{XYAA'^n}} I(A\rangle B^n XY)$$

$\therefore$ sufficient to consider pure states

Also since $I(A\rangle BX) = \sum_x p(x)\, I(A\rangle B)_{\psi_x}$

we have our final statement

$$nE \leq \max_{\phi^{AA'^n}} I(A\rangle B^n) + n\epsilon'$$

$\Leftrightarrow$

$$nE \leq Q(\mathcal{N}^{\otimes n}) + n\epsilon'$$