Lec 14, Jun 21, 2010

Note Title 21/06/2010

Capacity of transmitting quantum / classical data, using N (many times) as the only nonlocal resource:

LSD: $Q(N) = \sup_n \frac{1}{n} \max_{|\psi\rangle_{RA^{\otimes n}}} I_c(R \rangle B^{\otimes n})_{I \otimes N^{\otimes n}(|\psi\rangle\langle\psi|)}$

HSW: $C(N) = \sup_n \frac{1}{n} \max_{\underbrace{\sum_x p_x |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_{A^{\otimes n}}}_{\rho_{in}}} S(R : B^{\otimes n})_{I \otimes N^{\otimes n}(\rho_{in})}$

- Consider "assisted" capacities instead, when some extra unlimited nonlocal resource is available for free.

eg $C_E(N)$, $Q_E(N)$, $Q_{\rightarrow}(N)$, $Q_{\leftarrow}(N)$, $Q_{\leftrightarrow}(N)$, $C_{\leftarrow}(N)$

free entanglement   free forward   backward   two-way classical communication

- Assisting resources shouldn't trivialize the task:

eg. entanglement is static – it's independent of the message

eg. classical communication by itself has no quantum capacity

eg. backward comm by itself cannot forward data.

- Motivations
  - upper bounds for unassisted capacities
  - operationally interesting (eg $Q_2(N)$)
  - pieces of a bigger simpler theory
  - inspires unexpected results (like superactivation of Q)

LSD: $Q(N) = \sup_n \frac{1}{n} \max_{|\psi\rangle_{RA^{\otimes n}}} I_c(R \rangle B^{\otimes n})_{I \otimes N^{\otimes n}(|\psi\rangle\langle\psi|)}$

HSW: $C(N) = \sup_n \frac{1}{n} \max_{\underbrace{\sum_x p_x |x\rangle\langle x|_R \otimes |\psi_x\rangle\langle\psi_x|_{A^{\otimes n}}}_{\rho_{in}}} S(R:B^{\otimes n})_{I \otimes N^{\otimes n}(\rho_{in})}$

BSST: $C_E(N) = \sup_n \frac{1}{n} \max_{|\psi\rangle_{RA^{\otimes n}}} S(R:B^{\otimes n})_{I \otimes N^{\otimes n}(|\psi\rangle\langle\psi|)}$

Bennett
Shor
Smolin
Thapliyal
0106052

$= \max_{|\psi\rangle_{RA}} S(R:B)_{I \otimes N(|\psi\rangle\langle\psi|)}$

BSST
Cerf & Adami 9609024
Childs, L, Lo 0506039

Shannon: $\underset{\text{Classical}}{C(N)} = \max_{\sum_x p_x |x\rangle\langle x| \otimes |x\rangle\langle x|} S(R:B)_{I \otimes N(\rho_{in})}$

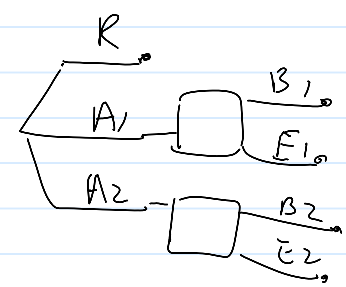
① Additivity:

[Recall lec 11, p18–19, in the proof of additivity of coherent info for degradable channels:
$S(B_1B_2|E_1E_2) \leq S(B_1|E_1) + S(B_2|E_2)$ (due to mono QMI)]

Let $f(N) = \max_{|\psi\rangle_{RA}} S(R:B)_{I\otimes N(|\psi\rangle\langle\psi|)}$

Claim: $f(N_1 \otimes N_2) = f(N_1) + f(N_2)$

Pf: $\text{LHS} = \max_{|\psi\rangle_{RA_1A_2}} S(R:B_1B_2)_{I\otimes N_1 \otimes N_2(|\psi\rangle\langle\psi|)}$



$= \max_{|\psi\rangle_{RA_1A_2}} S(R) + S(B_1B_2) - S(RB_1B_2)$

$= \max_{|\psi\rangle_{RA_1A_2}} S(B_1B_2E_1E_2) + S(B_1B_2) - S(E_1E_2)$

$$\overset{(*)}{=} \max_{|4\rangle_{RA_1A_2}} S(B_1\bar{B}_2|\bar{E}_1\bar{E}_2) + S(B_1B_2)$$

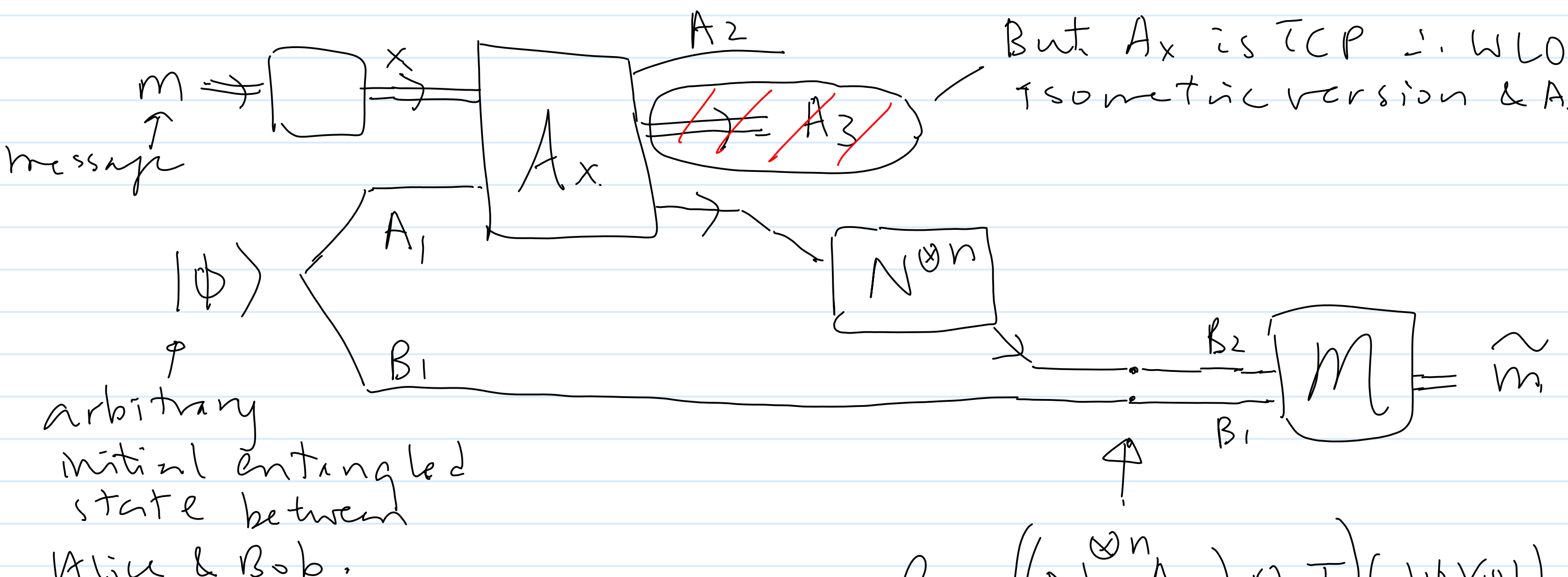
$$\leq \max_{|4\rangle_{RA_1A_2}} S(B_1|E_1) + S(B_2|E_2) + S(B_1) + S(B_2)$$

similar to (*) reversed

$$= \max_{|4\rangle_{RA_1A_2}} S(\underbrace{R_1}_{RB_2E_2} : B_1) + S(\underbrace{R_2}_{RB_1E_1} : B_2)$$

$$\leq f(N_1) + f(N_2)$$

② General protocol for entanglement assisted classical comm



But A_x is TCP ∴ WLOG can use isometric version & A3 not needed

$$\rho_x = \left(\left(N^{\otimes n} A_x\right) \otimes I\right)\left(|\psi\rangle\langle\psi|\right)$$

(Without $A_2 A_3 A_1 B_1$, above reduces to an unassisted protocol)

NB. Lack of feedback from Bob to Alice gives the simple structure of the protocol.

③ Converse:

ie no A_2

ⓐ Prove sufficiency of considering unitary encoding only

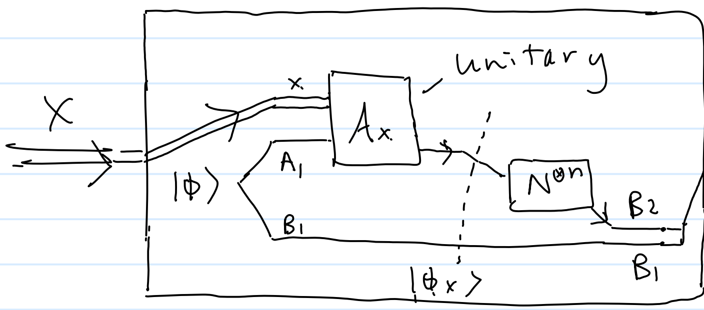
ⓑ Prove converse for unitary encoding

Pf ⓐ For Bob, the most general protocol is same as one in which A_2 is sent to him via R (the completely randomizing map).

By additivity, $C_E(N \otimes R) = C_E(N) + \cancel{C_E(R)}$ 0

$\therefore$ We can always analyze $N \otimes R$ instead & focus on unitary encodings

(b) The most general protocol with n uses gives a Q-box:



$$\left(I \otimes N^{\otimes n} A_x\right)\left(|\phi\rangle\langle\phi|\right) = \rho_{x\,B_1 B_2}$$

By the HSW theorem, the classical capacity

$$= \sup_n \frac{1}{n} \max_{A_x,\, p_x} \chi\{p_x, \rho_x\} \quad \forall x,\ (\rho_x)_{B_1} = \rho$$

Facts useful later:

$$\forall x,\quad \rho_{x B_1} = \mathrm{tr}_{A_1} |\phi\rangle\langle\phi| ,$$

$$S(\rho_{x B_1}) = S\left(\mathrm{tr}_{A_1} |\phi\rangle\langle\phi|\right) \overset{\text{unitarity of } A_x}{=} S\left(\mathrm{tr}_{B_2} |\phi_x\rangle\langle\phi_x|\right)$$

$$\chi(\{p_x, \rho_{x\,B_1B_2}\}) = S\left(\sum_x p_x \rho_{x\,B_1B_2}\right) - \sum_x p_x S(\rho_{x\,B_1B_2})$$

sub add $$\leq S\left(\sum_x p_x \rho_{x\,B_1}\right) + S\left(\sum_x p_x \rho_{x\,B_2}\right) - \sum_x p_x S(\rho_{x\,B_1B_2})$$

fact $$= \underbrace{\sum_x p_x S(\rho_{x\,B_1}) - \sum_x p_x S(\rho_{x\,B_1B_2})}_{} + S\left(\sum_x p_x \rho_{x\,B_2}\right)$$

Lemma to be proved $$\leq S\Big(\underbrace{\sum_x p_x \rho_{x\,B_1}}_{=\ \text{③}\ \mathrm{tr}_2 |\phi\rangle\langle\psi|}\Big) - S\Big(\underbrace{\sum_x p_x \rho_{x\,B_1B_2}}_{\text{①}}\Big) + S\Big(\underbrace{\sum_x p_x \rho_{x\,B_2}}_{\text{②}}\Big)$$

③ $\mathrm{tr}_2 |\phi\rangle\langle\psi|$ but also $\mathrm{tr}_2\, \rho$

① this is $I \otimes N^{\otimes}(\rho)$ for $\rho = \sum_x p_x\, I\otimes A_x |\phi\rangle\langle\psi| I \otimes A_x^{\dagger}$

② this is $N^{\otimes n}(\mathrm{tr}_{B_1} \rho)$

$\therefore$ Classical capacity $\leq \sup_n \frac{1}{n} \max_{\rho}\ S(\mathrm{tr}_2 \rho) + S(N^{\otimes n}(\mathrm{tr}_1 \rho)) - S(I \otimes N^{\otimes}(\rho))$

(replacing max p_x, ρ_x)

$$= \sup_n \frac{1}{n} \max_\rho S(R:B^{\otimes n})_{I \otimes N^{\otimes}(\rho)}$$

Finally, by additivity, replace $N^{\otimes n}$ by N

Also, can max over pure ρ (a mixed ρ can be purified & including purification is reverse of discarding $\therefore$ QMI nondecreasing).

$$\therefore C_E(N) \le \max_{|\psi\rangle_{RA}} S(R:B)_{I \otimes N(|\psi\rangle\langle\psi|_{RA})}.$$

(4) Direct coding (immediate after proving the "father" next class).

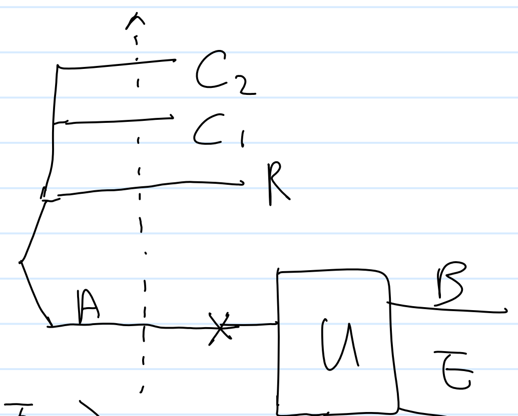
Lemma:

Let ρ_0, ρ_1 be density matrices, $0 \le p_0 \le 1$, $p_1 = 1-p_0$, $\rho = p_0\rho_0 + p_1\rho_1$

Then $S(\rho) - S(I\otimes N(\Phi_\rho)) \ge \sum_{i=0}^{1} p_i \left[S(\rho_i) - S(I\otimes N(\Phi_{\rho_i})) \right]$

purifies ρ purifies ρ_i

Pf



$\sqrt{p_0}\,|00\rangle_{C_2C_1}|\Phi_{\rho_0}\rangle_{RA}$
$+\sqrt{p_1}\,|11\rangle_{C_2C_1}|\Phi_{\rho_1}\rangle_{RA}$

isometric extension for N

Consider the pure state on C_2C_1RBE (after the channel acts).

LHS ①: ρ = state on A prior to U

$S(\rho) = S(C_2C_1R)$ $\because$ C_2C_1RA pure

LHS ②: $S(I\otimes N(\Phi_\rho)) = S(C_2C_1RB)$

Same for all purifications so use C_1C_2R as described

$$\text{RHS } ①: S(C_1R) = S(C_1) + \sum_{i=0}^{1} p_i S\left(\mathrm{tr}_A(\Phi_{\rho_i})\right)$$

$$= S(C_1) + \sum_{i=0}^{1} p_i S(\rho_i)$$

$\because$ R purifies ρ_i

$$\therefore \sum_{i=1}^{1} p_i S(\rho_i) = S(C_1R) - S(C_1)$$

$$\text{RHS } ②: S(C_1RB) = S(C_1) + \sum_{i=0}^{1} p_i S(I \otimes N(\Phi_{\rho_i}))$$

$$\therefore \sum_{i=1}^{1} p_i S\left(I \otimes N(\Phi_{\rho_i})\right) = S(C_1RB) - S(C_1)$$

$$\text{LHS} - \text{RHS of claim} = \left[S(C_2C_1R) - S(C_2C_1RB)\right]$$

$$- \left[\left(S(C_1R) - S(C_1)\right) - \left(S(C_1RB) - S(C_1)\right)\right]$$

$$= S(C_2C_1R) - S(C_2C_1RB) - S(C_1R) + S(C_1RB)$$

≥ 0 SSA on C_2, C_1R, B,

egs (for using $C_E(N) = \max_{|\psi\rangle_{RA}} S(R:B)_{I\otimes N(|\psi\rangle\langle\psi|)}$)

① If $N = I$, $|\psi\rangle_{RA} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ is optimal.

We recover superdense coding

② If N = erasure channel w/ error prob p:

$$I\otimes N(|\psi\rangle\langle\psi|_{RA}) = (1-p)\,|\psi\rangle\langle\psi|_{RB} + p\,\mathrm{tr}_B(|\psi\rangle\langle\psi|) \otimes |2\rangle\langle 2|$$

$$S(R:B) = S(R) + S(B) - S(RB)$$

$$= S(\mathrm{tr}_B(|\psi\rangle\langle\psi|)) + H(p) + (1-p)\,S(\mathrm{tr}_R(|\psi\rangle\langle\psi|))$$

$$- [H(p) + p\,S(\mathrm{tr}_B(|\psi\rangle\langle\psi|))]$$

$$= 2(1-p)\,S(\mathrm{tr}_B(|\psi\rangle\langle\psi|))$$

Again, $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ optimal, $C_E(N) = 2(1-p)$.

(3) If N is an arbitrary classical channel, $C(N) = C_E(N)$ (save for A3)

From (1)–(3), tempting to suspect $C_E(N) = C(N)$ for entanglement breaking channels or $C_E(N)/C(N) \leq 2 \;\forall N$.

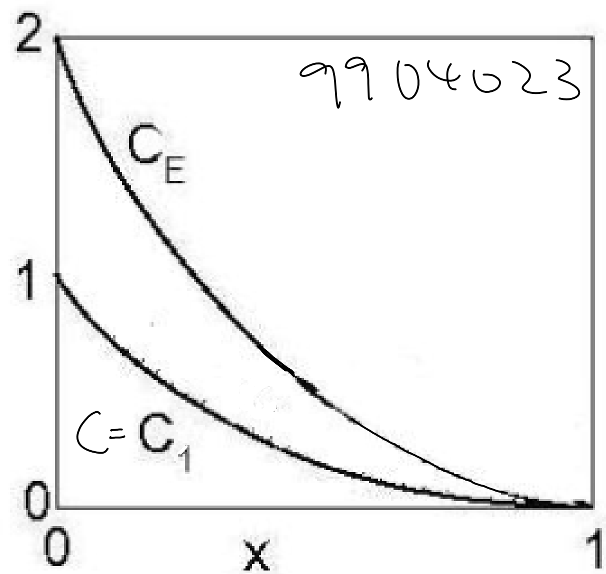
Both refuted by:

(4) If N depolarizing channel with prob error q,

as $q \to 1$

both $C(N), C_E(N) \to 0$

but $C_E/C \to \infty$!



Remarks on C_E:

① $C_E(N) = 0 \iff N$ trivial $\quad (N(\rho)$ indep of $\rho)$

② The most general protocol can use ebits instead of arbitrary entangled state $|\phi\rangle$ by the following argument:

Say, we use a special $|\phi\rangle$ in some (M, n) code with error δ_n.

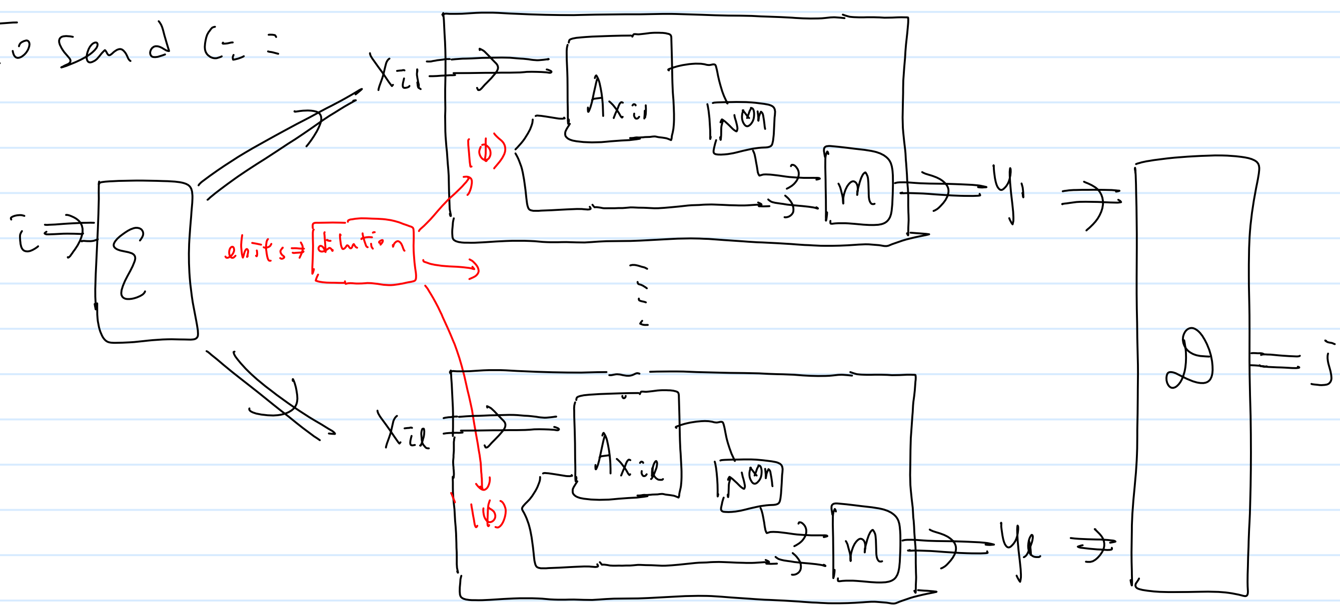
We can make l copies of $|\phi\rangle$ using $\approx S(\mathrm{tr}_1 |\phi\rangle\langle\phi|)$ ebits and $O(\sqrt{l})$ cbits, w/ error $\varepsilon_l' \to 0$ as $l \to \infty$, run the (M, n) code l times in parallel. Each code block is a giant classical channel with prob of error ε_n.

The error due to $\mathcal{E}_l'$ & $\mathcal{E}_n$ can be suppressed by using classical error correcting code. When $\epsilon_n \to 0$, n, l are large, rate of classical code $\to 1$.

Say, code words of classical code: $c_1 = x_{11} x_{12} \cdots x_{1l}$

$\vdots$ $\quad c_2 = x_{21} x_{22} \cdots x_{2l}$

To send c_i:



$[\Pr(i \neq j) \to 0]$

If $l \sim \sqrt{n}$, extra cbits needed for dilution can be produced by const $\times \sqrt{n}$ channel uses

ii Approx lM messages send via $ln + \text{const} \sqrt{n}$ channel uses, As $n \to \infty$, rate $\approx \frac{\log M}{n}$ same as original code.

This method is called "double blocking" (& error reduction is needed in the end).

③ $2Q_E = C_E$

Pf ($\geq$): if $n(C_E - \delta_n)$ cbits can be communicated with error $\varepsilon_n \to 0$ as $n \to \infty$, use these cbits to teleport $\frac{n}{2}(C_E - \delta_n)$ qubits (also with prob error $\leq \varepsilon_n$)

$\therefore Q_E \geq \frac{C_E}{2}$.

Pf ($\leq$): if $n(Q_E - \delta_n)$ qbits comm w/ error $\varepsilon_n \to 0$

use these qbits to (super) dense-code $2n(Q_E - \delta_n)$ cbits

$\therefore C_E \geq 2Q_E$

④ Reverse Shannon theorem:

ⓐ Consider classical channels.

Think of direct coding as simulating $n\,C(N)$ uses of the identity channel I_2 by using N n times.

Turns out simulating n uses of N takes about $n\,C(N)$ uses of identity channel — the "reverse Shannon theorem" (assuming shared randomness free).

Why such a perverted idea? Then n_1 uses of N_1 simulates n_2 uses of N_2 for $\frac{n_1}{n_2} \approx \frac{C(N_2)}{C(N_1)}$ — $C(N)$ the only relevant parameter.

conceptually, only 1 parameter to describe a channel in the asymptotic setting w/ free ent

(b) quantum channels

- if ebits are free, then n uses of N simulates nC_E cbits.
- turns out if ARBITRARY entangled states are free (not just ebits) then nC_E cbits also simulates n uses of N — the "quantum reverse Shannon Thm"

0912.5537 Bennett Devetak Harrow Shor Winter (starting 2000)

Alt proof: 0912.3805 Berta, Christandl, Renner

(2 guest lectures by Will Matthews in July).

Now consider $Q_{\leftrightarrow}(N)$ (q. capacity assisted by 2-way free classical communication (CC)).

Claim $Q_{\leftrightarrow}(N) = E_{\leftrightarrow}(N)$ (ent capacity of N given 2-way CC).

Pf idea "$\geq$": If Alice & Bob can create $n E_{\leftrightarrow}(N)$ ebits w/ error $\leq \varepsilon_n$ by using N n times & 2-way CC

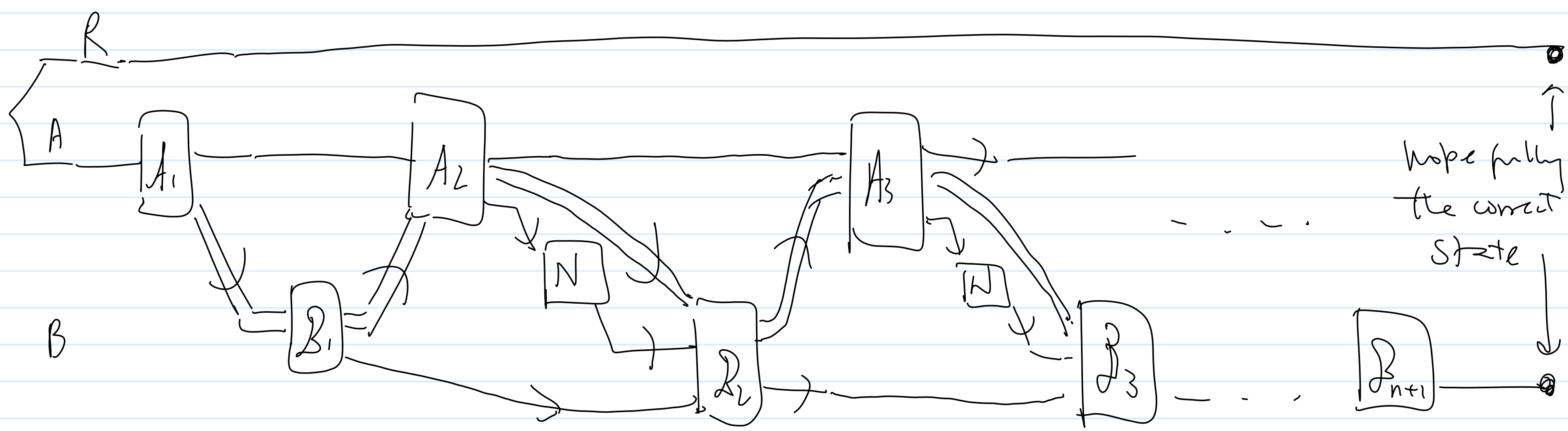
trace distance

Then Alice can teleport $n E_{\leftrightarrow}(N)$ ebits with $2n E_{\leftrightarrow}(N)$ extra cbits w/ same error.

Pf idea "$\leq$" : If $n\, Q_{\leftrightarrow}(N)$ qubits can be comm from Alice to Bob w/ error (including references) $\leq \varepsilon_n$

she can transmit halves of $n\, Q_{\leftrightarrow}(N)$ ebits w/ same error bound.

General protocol for $Q_{\leftrightarrow}$:



General protocol for $E_{\leftrightarrow}$:

Same as above but Alice also holds R & only max ent state is seeked at the output.

eg. If N = erasure channel w/ prob error p

then $Q_{\leftrightarrow}(N) = 1-p$

$$\left(\begin{array}{l} \text{cf } Q(N) = 1-2p \\ \quad\; C(N) = 1-p \\ \quad\; C_E(N) = 2(1-p) \end{array} \right)$$

How?

① Alice sends n halves of n ebits, using $N^{\otimes n}$.

② Bob tells Alice which of the n transmissions are erased.

③ They discard the erased ebits

④ They use the ebits + forward cc to teleport $\approx n(1-p)$ qubits.

Unfortunately, neither $Q_{\leftrightarrow}$ nor $\bar{E}_{\leftrightarrow}$ are known for most channels.

If we aren't impressed with our regularized capacity expressions $Q(N)$ or $C(N)$ we don't even have any expression for $Q_{\leftrightarrow}(N)$.

What about $Q_{\leftarrow}(N)$?

Worse ... no expression & no link to $\bar{E}_{\leftarrow}$

eg. N = erasure channel w/ prob erasure p.

We can lower bound $Q_{\leftarrow}(N)$ by $\frac{1-p}{3}$ by protocol: Same as that for $Q_{\leftrightarrow}$ but since there's no free forward cc, use N to send classical data for teleportation.

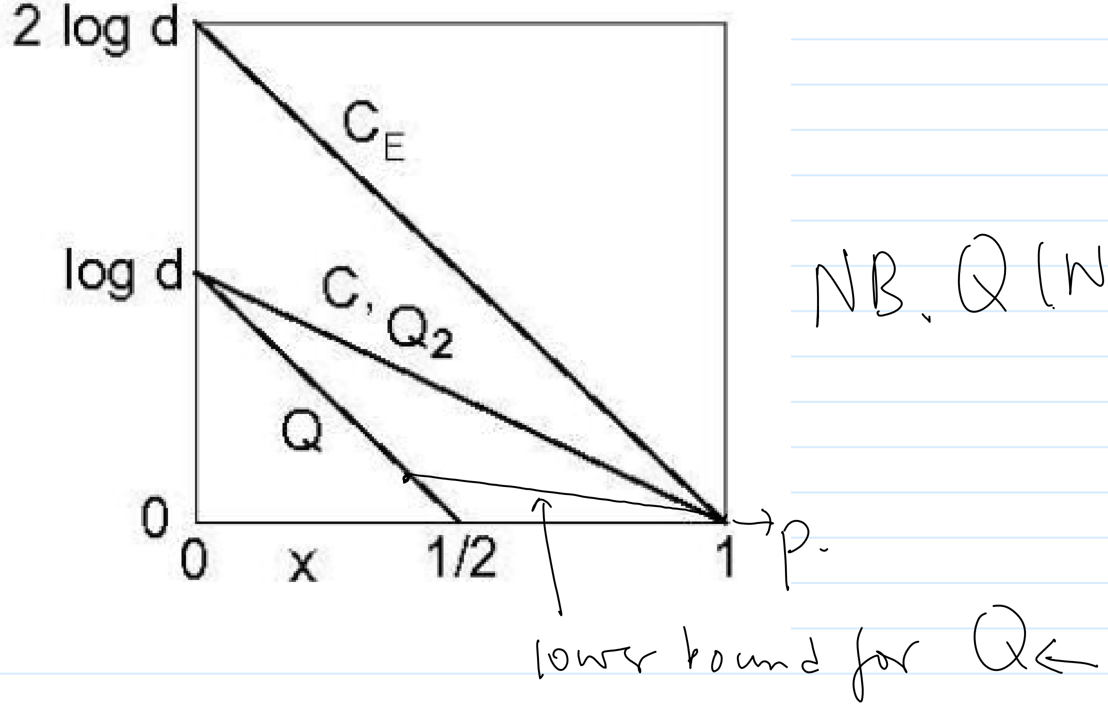
Say n uses $\longrightarrow$ $\approx n(1-p)$ ebits

$2n$ uses $\longrightarrow$ $\approx 2n(1-p)$ cbits

$\Big\} \overset{\text{telep}}{\Longrightarrow} n(1-p)$ qbits

$$\text{Rate} = \frac{n(1-p)}{3n} = \frac{1-p}{3}.$$

Capacities for erasure channel as of 9904023

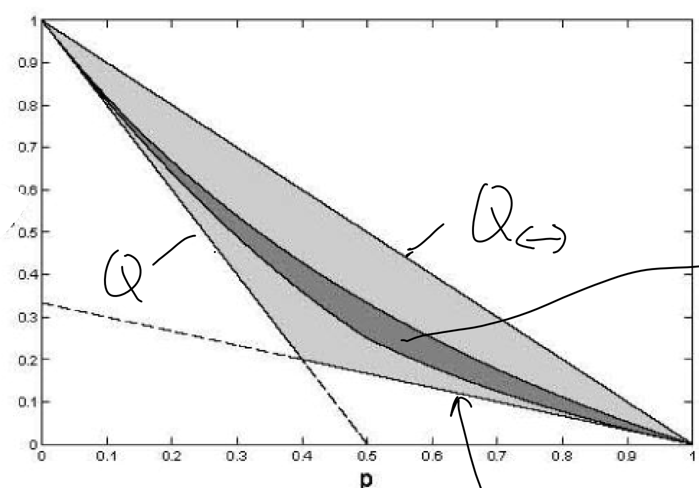


NB. $Q(N) \leq Q_{\leftarrow}(N) \leq Q_{\leftrightarrow}(N)$

$\therefore$ for some channels $Q_{\leftarrow}(N) \underset{\neq}{>} Q(N)$

It turns out whether $\exists N$ s.t. $Q_{\leftarrow}(N) \underset{\neq}{<} Q_{\leftrightarrow}(N)$
was not easy to determine.

In 0710.5943 (Li, Lim, Shor), again for the erasure channel:



$Q_{\leftarrow}$ somewhere in the dark region

old lower bd for $Q_{\leftarrow}$

- Note that for classical channels, free back comm does not increase the classical capacity.

How can this be?
Can prove the SAME converse with feedback

- see Cover & Thomas (if 1st edition Lec 8.12)

- Classical feedback also doesn't increase $C_E(N)$ for a quantum channel N } ? Winter or BSST

- Quantum feedback (free Q channel from Bob to Alice) increase C to C_E, Q to Q_E but no further.
(G. Bowen)

What about $Q_{\to}$?

Claim: $\forall N \quad Q_{\to}(N) = Q(N)$ (so free forward CC does not increase $Q(N)$).

Pf: