

Lemma: \( Q(N) = \sup_K \left( \frac{1}{n} \max_{\rho \in \mathcal{B}(I)} I_{c}(K; B^o) \right) \)

HSS: \( C(N) = \sup_K \left( \frac{1}{n} \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \right) \)

BSST: \( C(N) = \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \)

Shannon: \( C(N) = \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \)

\( \frac{1}{n} \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \)

Additivity:

Recall that, in the proof of additivity of mutual information for separable channels:

\( I_{\text{separable}}(X; Y) \leq I_{\text{separable}}(X; Y) \)

Claim: \( f(N) = f(N) + f(N) \)

Proof: \( \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \)

\( \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \)

\( \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \)

\( \max_{\rho \in \mathcal{B}(I)} S(K; B^o) \)

General protocol for entanglement-assisted classical comm
(3) Converse:
- PROVE SUFFICIENCY OF CONSIDERING UNITARY ENCODING ONLY
- PROVE UNIVERSE FOR UNITARY ENCODING

For Bob, the most general protocol is same as one in which Alice is sent to Bob via X (the completely randomizing map).

By additivity, \( C(N \otimes R) = C(N) + C(X) \).

We can always analyze \( N \otimes R \) instead & focus on unitary encodings.

\[
X(\{p_x, p_{xy}, p_{yx}, p_{yx}\}) = S(\sum_x p_x (x_{1x} 0_{2x})) - \sum_x p_x S(\{x_{1x}\})
\]

\[
\frac{\sum_x}{n} \leq \frac{1}{n} \max N \{\sum_x p_x S(\{x_{1x}\}) - \sum_x p_x S(\{x_{1x}\})\}
\]

Similarly, we have:
\[
S(\sum_x p_x S(x_{1x})) - \sum_x p_x S(\{x_{1x}\})
\]

Finally, by additivity, replace \( N^{\otimes n} \) by \( N \).

Also, can now zero part of \( G \) mixed \( G \) cannot be prepared & induce unitary function is zero by the argument above (most non-constructively).

\[
\sum_x p_x S(x_{1x}) \leq \max \sum_x S(x_{1x}) \quad \text{then} \quad \sum_x p_x S(x_{1x})
\]

(4) Direct coding (immediate after proving the "factor" results)

**LEMMA:**
- \( \sum_x p_x S(x_{1x}) \leq \max \sum_x S(x_{1x}) \quad \text{then} \quad \sum_x p_x S(x_{1x}) = \sum_x p_x S(x_{1x}) \)
- \( \sum_x p_x S(x_{1x}) \leq \max \sum_x S(x_{1x}) \quad \text{then} \quad \sum_x p_x S(x_{1x}) = \sum_x p_x S(x_{1x}) \)

\[
\text{ENR} \otimes S(G,C) \leq S(G,C) = S(G,C) + \frac{1}{n} \sum_{i=0}^{n-1} p_{i} S(p_{i})
\]

\[
s(C) = \frac{1}{n} \sum_{i=0}^{n-1} p_{i} S(p_{i})
\]

\[
\text{LHS} - \text{RHS} = \sum_{i=0}^{n-1} p_{i} S(p_{i}) = S(C,G) - S(C,G)
\]

\[
\text{RHS} - \text{LHS} = S(C,G) - S(C,G)
\]

\[
\text{Satisfied for } C, C, G, B.
\]
3 If $N$ is an arbitrary classical channel, $C(N) = C(E(N)) (\text{due to } \mathbb{E})$

From 1, we tempting to suspect $C(E(N)) = C(N)$ for entanglement breaking channels or $C(E(N))/C(N) \leq 2/\ln N$.

Both be proved by:

4 If $N$ is an entanglement breaking channel with rate $\frac{\rho}{2}$, 

$$\text{due to } \mathbb{E} = \mathbb{E}n$$

The error can be suffered by using classical error correcting codes when $\rho \rightarrow 0$, and any large rate of classical chan $\rightarrow 1$.

Say, we send a codeword $x = (x_1, x_2, \ldots, x_n)$.

To send $x$,

\[ x \rightarrow y \rightarrow [P(x) \rightarrow 0] \]

If $L = C$, extra bits needed for detection can be produced by exist $\mathbb{E}$ channel uses

2 Approx bit messages sent via $d + $ exist $\mathbb{E}$ channel uses, as $n \to \infty$, rate $= \log_2 \frac{n}{2}$ same as original code.

This method is called “decode before” (or error reduction is needed in both end).

3 $D = C_1$

If $\mathbb{E} > 0$, alternate bits can be communicated with error $\mathbb{E} \rightarrow 0$ as $n \to \infty$, use these $\mathbb{E}$ bits to teleport $\frac{1}{2} (E - \mathbb{E}d_n)$ qudits into with $\frac{1}{2}$ error $\mathbb{E}$.

4 $\mathbb{E} > 0$, $\frac{1}{2} (E - \mathbb{E}d_n)$ qudits commi with error $\mathbb{E}$ into $E$.

Use these qudits to $(\text{make})$ base code $2n (Q_1 - \mathbb{E}d_n)$ bits
4. Reverse Shannon theorem:
   a) Length classical channels.

   Think of transmitting as simulating $nC(n)$ uses of the identity channel $I_n$ by using $N$ $n$ times.

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

   Why such a perverse idea? Then $n$ uses of $N$ simulates $N^n$ uses of $N_x$ for $n \approx C(n)$ — $C(n)$ the only relevant parameter.

Now consider $Q_{es}(N)$ (a capacity assisted by every per classical communication $cc$).

Claim $Q_{es}(N) = E_g(N)$ (w/capacity of $N$ given $2^{nQE(N)}$).

If idea "$\geq$": If Alice & Bob can create $nE_{es}(N)$

then $n$ errors $\leq E_n$ by using $N$ $n$ times & $2^{nQE(N)}$.

Then Alice can take first $nE_{es}(N)$

errors with $2^{nQE(N)}$ extra bits by same proof.

General protocol for $E_{es}$:

General protocol for $E_{es}$:

Some other but Alice also adds $R$ & only one at a time is picked at the output.

eq. If $N$: erasure channel w/ prob error $p$

then $Q_{es}(N) = 1-p$ (or $E_{es}(N) = 1-2p$)

$C(n) = 1-p$

$C(n) = 3(1-p)

How?

1. Alice sends $n$ blocks of $n$ bits using $N^{10n}$.
2. Bob tells Alice which of the $n$ transmissions are erased.
3. They discard the erased bits.
4. They use the bits forward $CC$ to $E_{es}(N)$ parity.

Unfortunately, neither $Q_{es}$ nor $E_{es}$ are known for most channels.

If we aren't interested in $E_{es}$ regularized capacity expressions $Q_{es}(K)$ or $C(n)$ we don't have any expression for $Q_{es}(K)$.

What about $Q_{es}(N)$?

Worse... no expression & no link to $E_{es}$.
Eq. N: erasure channel is just erasure p.

We can lower bound \( Q_e(N) \) by \( \frac{1}{3} \) by protocol: Same as that for \( Q_e \) but since there's no free forward cc, we need to send classical data for teleportation.

Say \( n \) uses \( \rightarrow \) \( n(1-p) \) errors \( \rightarrow \) \( n(1-p) \) qubits

2n uses \( \rightarrow \) \( 2n(1-p) \) errors \( \rightarrow \) \( 4np \) qubits

Rate: \( \frac{2(1-p)}{3n} = \frac{1}{3} \).

\[ Q_e(N) \geq \frac{1}{3} Q_e(N) \]

It turns out whether \( 3N \) s.t. \( Q_e(N) \leq \frac{1}{3} Q_e(N) \)

was not easy to determine.

0.710 ± 0.043 (L. c.m. 95%), again for the erasure channel.

\[ Q_e \text{ same here in the dark region} \]

\[ Q_e \text{ below here for } Q_e \]

What about \( Q_N \) ?

Claim: \( N \): \( Q_e(N) = Q(N) \) (so free forward cc does not increase \( Q(N) \))

If:

\[ NB. Q_e(N) \leq Q(N) \leq Q_{Ee}(N) \]

\[ \text{lower bound for } Q_e \]

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

How can this be?

Can prove the same universe with feedback

- see Cover & Thomas (1st edition Sec. 12)

- classical feedback also doesn't increase \( C_N(N) \) ? What

- quantum feedback (free a channel from Bob to Alice)

- increase \( C \) to \( C_{Ee} \) and \( Q \) to \( Q_{EE} \) but no further.

( G. Bowen)