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

LSD: $Q(N) = \sup_n \frac{1}{n} \max_{|14\rangle_{RA^n}} I(\mathcal{R}:B^{\otimes n})$

HSW: $C(N) = \sup_n \frac{1}{n} \max_{\{p_x | x \subseteq X \otimes 14 \times 4, 14^{\otimes n} \}} S(\mathcal{R}:B^{\otimes n})$

$I \otimes N^{\otimes n} / \rho_{in}$
Consider "assisted" capacities instead, when some extra unlimited non-local resource is available for free.

\[ C_E(N), Q_N(E), Q \rightarrow (N), Q \leftarrow (N), Q \leftrightarrow (N), C \rightarrow (N) \]

- Free entanglement
- Free forward
- Backward
- Two-way classical communication

Assisting resources shouldn't trivialize the task:

- Entanglement is static - it's independent of the message
- Classical communication by itself has no quantum capacity
- Backward comm by itself cannot forward data.

Motivations - upper bounds for unassisted capacities
- Operationally interesting (e.g., $Q_2(N)$)
- Pieces of a bigger simpler theory
- Inspires unexpected results (like superation of $Q$)
LSO: \( Q(N) = \sup_n \frac{1}{n} \max_{|\psi\rangle_{RA}^n} I_{\psi^n} (R \otimes B^n) \)

HSW: \( C(N) = \sup_n \frac{1}{n} \max_{|\psi\rangle_{RA}^n} S(R \otimes B^n) \)

\[ \prod_{x \in \{1,\ldots,n\}} (|x\rangle \otimes |x\rangle)_{RA} \]

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

Bennett
Shor
Smolin
Thapliyal
0106052
BSS
Cerf & Adami 9609024
Childs, L. 0506029

Shannon: \( C(N) = \max_{|\psi\rangle_{RA}^n} S(R \otimes B^n) \)

\[ \prod_{x \in \{1,\ldots,n\}} (|x\rangle \otimes |x\rangle)_{RA} \]
Additivity:

Recall lec 11, p18-19, in the proof of additivity of coherent info for degradable channels:

\[ S(B_1B_2|E_1E_2) \leq S(B_1|E_1) + S(B_2|E_2) \quad \text{(due to mono QMI)} \]

Let \( f(N) = \max_{(4)} S(R:B) \quad \text{subject to } N(14 \times 41) \)

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

Pf: \( \text{LHS} = \max_{(4)} S(R:B,B_2) \quad \text{subject to } N_1 \otimes N_2 (14 \times 41) \)

\[ = \max_{(4)} S(R) + S(B_1B_2) - S(RB_1B_2) \]

\[ = \max_{(4)} S(B_1B_2|E_1E_2) + S(B_1B_2) - S(E_1E_2) \]
\( \max_{14 \, R_1, R_2} S(B_1, B_2 \in E_1, E_2) + S(B_1, B_2) \)

\( \leq \max_{14 \, R_1, R_2} S(B_1 \in E_1) + S(B_2 \in E_2) + S(B_1) + S(B_2) \)

\( = \max_{14 \, R_1, R_2} S(R_1 \in B_1) + S(R_2 \in B_2) \)

\( \leq f(N_1) + f(N_2) \)
2) General protocol for entanglement assisted classical comm

But $Ax$ is TCP, WLOG, can use isometric version & $A3$ not rectified

$|\Phi\rangle$

arbitrary initial entangled state between Alice & Bob.

$P_x = (N^{\otimes n} A_x \otimes I)(|\Psi\rangle\langle\Psi|)$

(without $A2, A3, A1, B1$, above reduces to an unassisted protocol)

WB: Lack of feedback from Bob to Alice gives the simple structure of the protocol.
3) Converse:
(a) Prove sufficiency of considering unitary encoding only.
(b) Prove converse for unitary encoding.

Pt. (a) For Bob, the most general protocol is same as one in which A2 is sent to him via R (the completely randomizing map).

By additivity, $C_e(N \otimes R) = C_e(N) + C_e(R)$

We can always analyze NO_R instead & focus on unitary encodings.
b) The most general protocol with uses gives a Q-box:

\[ (I \otimes N^w A_x) (|\psi X \phi_1\rangle) = p_x \]

By the HSW theorem, the classical capacity

\[ = \sup_{n} \| \sum_{A_x, p_x} \max_{X \in \{p_x, p_x^\perp\}} U X \cdot (p_x)_{B_1} = 1 \]

Facts useful later:

\[ U_{A_x}, p_{X B_1} = tr A_x, |\psi X \phi_1\rangle, \quad \text{unitarity of } A_x \]

\[ S(p_{X B_1}) = S(tr A_x, |\psi X \phi_1\rangle) / S(tr B_2, |\psi X \phi_2\rangle) \]
\[ X(\{p_x, p_{x \oplus b_2}\}) = S(\sum_x p_x p_{x \oplus b_2}) - \sum_x p_x S(p_{x \oplus b_2}) \]

\[ \leq S(\sum_x p_x p_{x \oplus b_1}) + S(\sum_x p_x p_{x \oplus b_2}) - \sum_x p_x S(p_{x \oplus b_2}) \]

\[ \text{Fact} = \sum_x p_x S(p_{x \oplus b_1}) - \sum_x p_x S(p_{x \oplus b_2}) + S(\sum_x p_x p_{x \oplus b_2}) \]

\[ \text{Lemma to be proved} \leq S(\sum_x p_x p_{x \oplus b_1}) - S(\sum_x p_x p_{x \oplus b_2}) + S(\sum_x p_x p_{x \oplus b_2}) \]

3. \( \text{tr}_2 |\rho \psi | \psi \rangle \) 1. this is \( \text{ION}^\oplus(p) \) for

but also \( \text{tr}_2 \rho \)

\[ \rho = \sum_x \rho A_x |\psi \rangle \langle \psi | \rho A_x^\dagger \]

"Classical capacity \( \leq \sum_x p_x \max_{p_x} \max_{\text{tr}_2 p} \left[ S(\text{tr}_2 p) + S(\text{ION}^\oplus(\text{tr}_2, p)) - S(\text{ION}^\oplus(p)) \right] \) (replacing \( \max p_x, p_{x \oplus b} \))"
\[
\sup_n \frac{1}{n} \max \sum_{i=1}^{n} S(R_i^n) I(\Theta^{N^n}(I)) 
\]

Finally, by additivity I replace \(N^n\) by \(N\).

Also, any pure \(P\) (a mixed \(P\) can be purified \& including purification is reversible if \(s\) wording is non decreasing).

\[
\text{CE}(N) \leq \max_{(\mu)} S(R^B(I^*(\mu))) I(\Theta^{N}(1^*(\mu)|\mu)) 
\]

4) Direct coding (immediate after leaving the "hatch" next day)
Lemma:

Let $\rho_0, \rho_1$ be density matrices, $0 \leq \rho_0 \leq 1$, $\rho_1 = 1 - \rho_0$, $\rho = \rho_0 \rho_0 + \rho_1 \rho_1$.

Then $S(\rho) - S(\text{ION}(\rho_1)) \geq \sum_{i=0}^{n} \hat{p}_i \left[ S(\rho_{i}) - S(\text{ION}(\rho_{i})) \right]$

\[ \text{purifies } \rho \]
\[ \text{purifies } \rho_i \]

Proof:

Consider the pure state on $\mathbb{C}^2 \mathbb{C}_1 \mathbb{R} \mathbb{B} G$

(after the channel acts).

LHS (1): $\rho$ = state on $A$ near to $U$.

$L(\rho) = S(\mathbb{C}_2 \mathbb{C}_1 \mathbb{R})$ : \( \mathbb{C}_2 \mathbb{C}_1 \mathbb{R} \) pure

LHS (2) = $S(\text{ION}(\rho_1)) = S(\mathbb{C}_2 \mathbb{C}_1 \mathbb{R} \mathbb{B})$

Same for all purifications.

So use $\mathbb{C}_2 \mathbb{C}_1 \mathbb{R}$ as desired.
\[
\text{RHS } \odot: S(C_1 R) = S(C_1) + \sum_{i=0}^{1} p_i S(\text{tr}_e(\overline{p}_i)) \\
= S(C_1) + \sum_{i=0}^{1} p_i S(p_i) \\
\text{if } R \text{ minorizes } p_i \\
\Rightarrow \frac{1}{2} \sum_{i=0}^{1} p_i S(p_i) = S(C_1 R) - S(C_1) \\
\text{RHS } \odot: S(C_1 RB) = S(C_1) + \sum_{i=0}^{1} p_i S(\text{tr}_e(\overline{p}_i)) \\
= \frac{1}{2} \sum_{i=0}^{1} p_i S(\text{tr}_e(\overline{p}_i)) = S(C_1 RB) - S(C_1) \\
\text{LHS - RHS of claim: } \left[ S(C_2 C_1 R) - S(C_2 C_1 RB) \right] \\
- \left[ (S(C_1 R) - S(C_1)) - (S(C_1 RB) - S(C_1)) \right] \\
= S(C_2 C_1 R) - S(C_2 C_1 RB) - S(C_1 R) + S(C_1 KB) \\
\geq 0 \text{ SSA on } C_2, C_1 R, B.
\( \mathcal{E}_S \) (for using \( \mathcal{E}(N) = \max_{(y)_{RA}} S(R:B) \), \( \mathcal{E}_N(14 \times 41) \))

1. If \( N = 2 \), \( (y)_{RA} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \) is optimal.
   
   We recover super dense coding.

2. If \( N \) is erasure channel \( \mathcal{W} \) error prob \( p \):

   \[ I(\mathcal{E}_N(14 \times 41)_{RA}) = (-p) \ 14 \times 41_{RB} + p \ \text{tr}_B \ (12 \times 21) \otimes 12 \times 21 \]

   \[ S(R:B) = S(R) + S(B) - S(RB) \]

   \[ = S(\text{tr}_B \ (14 \times 41)) + H(p) + (1-p) S(\text{tr}_R \ (14 \times 41)) \]

   \[ - [H(p) + p \ S(\text{tr}_B \ (14 \times 41))] \]

   \[ = 2 \ (-p) \ S(\text{tr}_B \ (14 \times 41)) \]

   Again, \( (y) = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \) optimal, \( \mathcal{E}(N) = 2 \ (-p) \).
3. If $N$ is an arbitrary classical channel, $C(N) = C_e(N) \quad \text{(save for)}$

From 1-3, tempting to suspect $C_e(N) = C(N)$ for entanglement breaking channels or $C_e(N)/C(N) \leq 2$ U.N.

Both rephrased by:

4. If $N$ dephasing channel with probability $\frac{1}{2}$,

as $\frac{1}{2} \to 1$

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 ($N(p)$ independent)

2. The most general protocol can use ebits instead of arbitrary entangled state $(\Phi)$ by the following argument:

Say, we use a special $(\Phi)$ in some $(M,n)$ code with error $\delta n$.

We can make $l$ copies of $(\Phi)$ using $\sim S(\text{tr}, 1\Phi\otimes\Phi^{l})$ ebits and $O(\sqrt{l})$ qubits, with error $\delta l \rightarrow 0$ as $l \rightarrow \infty$, run the $(M,n)$ code $l$ times in parallel. Each code block is a giant classical channel with prob of error $\delta n$. 
The error can be suppressed by using classical error correcting code. When $m \rightarrow 0$, $n, d$ are large, rate of classical code $\rightarrow 1$.

Say, code words of classical code: $C_i = X_{i1} X_{i2} \ldots X_{iE}$

\[ C_2 = X_{21} X_{22} \ldots X_{2E} \]
If \( e \sim \sqrt{n} \), extra bits needed for dilution can be produced by \( \text{const} \times \sqrt{n} \) channel uses.

Approx \( \log M \) messages sent via \( d \log n + \text{const} \sqrt{n} \) channel uses, \( A \sim n \to \infty \), rate \( \mathbf{r} = \frac{\log M}{n} \)

Same as original code.

This method is called "double blocking" (no error reduction is needed in the end).
\( 2Q_{E} = C_{E} \)

**Proof (\( \geq \))**: If \( n(C_{E} - d_{n}) \) qubits can be communicated with error \( E_{n} \to 0 \) as \( n \to \infty \); use these qubits to teleport \( \frac{n}{2}(C_{E} - d_{n}) \) qubits (also with prob error \( \leq E_{n} \))

\[ \therefore Q_{E} \geq \frac{C_{E}}{2} \]

**Proof (\( \leq \))**: If \( n(Q_{E} - d_{n}) \) qubits comm w/ error \( E_{n} \to 0 \), use these qubits to (super)dense-code \( 2n(Q_{E} - d_{n}) \) cbits

\[ \therefore C_{E} \geq 2Q_{E} \]
4. Reverse Shannon theorem:

(a) 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 heretical 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.
quantum channels

- if ebits are free, then $n$ uses of $N$ simulates $nC_e$ ebits.

- turns out if ARBITRARY entangled states are free (not just ebits) then $nC_e$ ebits also simulates $n$ uses of $N$ — the "quantum reverse Shannon Theorem"

0912.5537 Bennett Devetak Haraor Shor Winter (starting 2000)

Alt proof: 0912.3805 Barton, Christandl, Renner
(2 guest lectures by Will Matthews in July)
Now consider $Q_{\leftarrow} (N)$ (q. capacity assisted by 2-way pre classical communication (CC)).

Claim $Q_{\leftarrow} (N) = \mathbb{E}_{\rightarrow} (N)$ (ent. capacity of $N$ given $2$-way CC).

Proof "\(\geq\)" : If Alice & Bob can create $n \mathbb{E}_{\rightarrow} (N)$ inphase $\ell$ ebits w/ error $\leq \mathbb{E}_n$ by using $N$ n times & 2-way CC, then Alice can teleport $n \mathbb{E}_{\rightarrow} (N)$ ebits with $2n \mathbb{E}_{\rightarrow} (N)$ extra ebits w/ same error.
If idea "≤" : If \( n Q = (n) \) qubits can be comm from Alice to Bob w/ error (including references) \( ≤ 3n \) she can transmit halves of \( n Q = (n) \) qubits w/ same error bound.

General protocol for \( Q = (n) \):

```
A1 -> A2 -> A3
B1 -> B2 -> B3
```

A1, A2, A3, B1, B2, B3, N, N1, N2, N3.
General protocol for Eve:
Same as above but Alice also holds R and only max is fed to the output.

Eq. If $N$ = erasure channel w/ prob error $p$

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

($Q(N) = 1 - 2p$

$C(N) = 1 - p$

$E(N) = 2(1 - p)$)

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 to forward $cc$ to teleport $\leq n(1 - p)$ qubits.
Unfortunately, neither $Q_{\omega}$ nor $\bar{E}_{\omega}$ 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 $Q_{\omega}(N)$.

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

Worse ... no expression & no link to $\bar{E}_{\omega}$.
\[ \text{Eq. } N = \text{ erasure channel w/ prob erasure } p. \]

We can lower bound \( Q_e(N) \) by \( \frac{1-p}{3} \) by protocol:

Same as that for \( Q_e \) but since there's no free forward cc, use \( N \) to send classical data for teleportation.

Say \( n \) uses \( \Rightarrow \approx n \left( 1 - p \right) \) ebits

\[ 2n \text{ uses } \Rightarrow \approx 2n \left( 1 - p \right) \text{ ebits} \]

\[
\text{Rate: } \frac{n(1-p)}{3n} = \frac{1-p}{3}.
\]
Capacities for erasure channel as of 9904023

\[ 2 \log d \]

\[ \log d \]

\[ 0 \]

\[ x \]

\[ 1/2 \]

\[ 1 \]

\[ Q \]

\[ C_e, Q_2 \]

\[ C, Q \]

NB. \( Q(N) \leq Q_2(N) \leq Q_e(N) \)

Lower bound for \( Q \)
i. for some channels \( Q \leq (N) \neq Q (N) \)

It turns out whether \( \exists N \) s.t. \( Q \leq (N) \leq Q (N) \) was not easy to determine.

In 0710.5943 (L. Lim. Shor), again for the ensure

\[ Q \leq \text{some where in the dark region} \]

\[ Q \leq \text{old lower bound for } Q \leq \]
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 Sec 8.12)

Classical feedback also doesn't increase $C_2(N)$? Winter for a quantum channel $N$

Quantum feedback (free a channel from Bob to Alice) increase $C$ to $C_3$, $Q$ to $Q_2$ but no further. (G. Bowen)
What about $Q_D$?

Claim: $\forall N \ Q \Rightarrow (N) = Q(N)$ (so free forward CC does not increase $Q(N)$)

pf: