Quantum Communication With Zero-Capacity Channels

Graeme Smith (IBM Watson)
Jon Yard (LANL)

arXiv:0807.4935

QIP 2009
Quantum Communication Over a Quantum Channel

**Goal:**

Quantum Capacity:
the rate, in qubits per channel use, at which A can send high fidelity quantum information to B, given $\mathcal{N}^\otimes n$.

$$Q(\mathcal{N}) = \max \left( \frac{\text{#qubits sent}}{\text{#channel uses}} \right)$$
Goal: Quantum Communication Over a Quantum Channel

Why?

- You may have a noisy quantum channel
- You may be interested in error correction
- You may be interested in packing problems
There are channels $\mathcal{N}_1$ and $\mathcal{N}_2$ such that:
$Q(\mathcal{N}_1) = 0$ and $Q(\mathcal{N}_2) = 0$, but $Q(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$. 
Outline

- Quantum and Private Capacities
- Channels with Zero Quantum Capacity
- Superactivation of Quantum Capacity
- Application: superadditivity of coherent information
- Open Questions and Conclusions
Coherent information: $Q^{(1)}(\mathcal{N}) = \max_{\phi_A} (S(B) - S(E))$

- $Q(\mathcal{N}) \geq Q^{(1)}(\mathcal{N})$ [Lloyd, Shor, Devetak]
- $Q(\mathcal{N}) = \lim_{n \to \infty} \frac{1}{n} Q^{(1)}(\mathcal{N} \otimes^n)$
- $Q(\mathcal{N}) \neq Q^{(1)}(\mathcal{N})$ [DiVincenzo, Shor, Smolin]
Private Capacity: max rate of private classical communication

Private Information: $P^{(1)}(\mathcal{N}) = \max_{\rho_x,\phi_x} (I(X;B) - I(X;E))$

$P^{(1)}$ is achievable [Devetak].

$P(\mathcal{N}) = \lim_{n \to \infty} \frac{1}{n} P^{(1)}(\mathcal{N} \otimes n)$

$P(\mathcal{N}) \neq P^{(1)}(\mathcal{N})$ [Smith, Renes, Smolin]
Zero Capacity Channels—The Puppy Question

Classical Capacity

Quantum Capacity

- $Q = 0$ does not imply uncorrelated
- Two important convex subsets: Anti-degradable and Horodecki
- Not a convex set
- I would harm this puppy for a complete characterization:

$C = 0 \iff p(y|x)$ independent of $x$

Quantum channel:
$\mathcal{N}(\rho) = \mathcal{N}(\sigma) \forall \rho, \sigma$
Antidegradable Channels

- Environment can simulate output
- $Q = 0$ by no cloning
- stable under $\otimes$
- Example: 50% erasure channel.
  \[ \mathcal{E}(\rho) = \frac{1}{2} \rho + \frac{1}{2} |\text{erase}\rangle\langle\text{erase}| \]
Horodecki Channels

Partial Transpose:

\[(|i\rangle \langle j| \otimes |k\rangle \langle l|)_{\Gamma} = |i\rangle \langle j| \otimes |l\rangle \langle k|)\]

Positive Partial Transpose (PPT):

\[\rho_{AB} \geq 0, \quad \rho_{AB}^{\Gamma} \geq 0 \Rightarrow \text{not distillable (even via 2-way! ops)}\]

\[\mathcal{N} \text{ Horodecki } \iff \forall \phi_{AA'} \]

\[\rho_{AB} = I \otimes \mathcal{N}(\phi_{AA'}) \text{ is PPT}\]

\[Q_2(\mathcal{N}) = 0 \Rightarrow Q(\mathcal{N}) = 0\]
Recall there are states with perfectly secure key that are not maximally entangled: "twisted maximally entangled states".

The idea is this:

- \( \rho_1 \) is a twisted EPR pair ("key").
- \( \rho_2 \) is twisted EPR pair with \( X \) applied to Bob ("anti-key").
- Let \( \rho = (1 - p)\rho_1 + p\rho_2 \) be the Choi matrix of your channel.
- Tune \( p \) so that \( \rho \) is PPT. This happens for \( p \neq 1/2 \), and we have \( \mathcal{P}(\mathcal{N}) = 1 - H(p) \).

[Horodecki, Pankowski, Horodecki, Horodecki]
**Theorem.** Let $\mathcal{N}$ be any channel and $\mathcal{E}$ be a 50%-erasure channel. Then

$$Q^{(1)}(\mathcal{N} \otimes \mathcal{E}) \geq \frac{1}{2} P^{(1)}(\mathcal{N}).$$

**Corollary.** There are $\mathcal{N}$ and $\mathcal{E}$ with $Q(\mathcal{N}) = Q(\mathcal{E}) = 0$ but $Q(\mathcal{N} \otimes \mathcal{E}) > 0$. 
Proof

Let $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)} |x\rangle^X |\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x) |x\rangle\langle x|^X \otimes \rho_x^A$

$$Q^{(1)} \geq H(BD) - H(EF)$$
Proof

Let \(|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)} |x\rangle^X |\rho_x\rangle^{AC}\)

so \(\rho^{XA} = \sum_x p(x) |x\rangle\langle x|^X \otimes \rho_x^A\)

\(Q^{(1)} \geq H(BD) - H(EF)\)

write as entropies on state \(|\rho\rangle^{XBEC}\) before erasure \(\mathcal{E}\)
Proof

Let \( |\rho\rangle^{XAC} = \sum_x \sqrt{p(x)} |x\rangle^X |\rho_x\rangle^AC \)

so \( \rho^{XA} = \sum_x p(x) |x\rangle\langle x|^X \otimes \rho_x^A \)

\[
Q^{(1)} \geq H(BD) - H(EF)
\]
write as entropies on state \( |\rho\rangle^{XBE} \)

\[
= \frac{1}{2}(H(B) - H(EC))
\]
Proof

Let $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)} |x\rangle^X |\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x) |x\rangle\langle x|^X \otimes \rho_x^A$

$Q^{(1)} \geq H(BD) - H(EF)$

write as entropies on state $|\rho\rangle^{XBE}$ before erasure $\mathcal{E}$

$= \frac{1}{2} (H(B) - H(EC)) + \frac{1}{2} (H(BC) - H(E))$
Proof

Let $|\rho\rangle^{XAC} = \sum_x \sqrt{p(x)} |x\rangle^X |\rho_x\rangle^{AC}$

so $\rho^{XA} = \sum_x p(x) |x\rangle\langle x|^X \otimes \rho_x^A$

$Q^{(1)} \geq H(BD) - H(EF)$

write as entropies on state $|\rho\rangle^{XBE}$ before erasure $E$

$= \frac{1}{2} (H(B) - H(EC)) + \frac{1}{2} (H(BC) - H(E))$

$= \frac{1}{2} (H(B) - H(XB)) + \frac{1}{2} (H(XE) - H(E)) \quad \text{(on } |\rho\rangle^{XBE})$
Proof

Let \( |\rho\rangle^{XAC} = \sum_{x} \sqrt{p(x)} |x\rangle^{X} |\rho_{x}\rangle^{AC} \)

so \( \rho^{XA} = \sum_{x} p(x) |x\rangle\langle x|^{X} \otimes \rho_{x}^{A} \)

\[
Q^{(1)} \geq H(BD) - H(EF)
\]

write as entropies on state \( |\rho\rangle^{XBEC} \) before erasure \( \mathcal{E} \)

\[
= \frac{1}{2} (H(B) - H(EC)) + \frac{1}{2} (H(BC) - H(E))
\]

\[
= \frac{1}{2} (H(B) - H(XB)) + \frac{1}{2} (H(XE) - H(E)) \quad \text{(on } |\rho\rangle^{XBEC} \text{)}
\]

\[
= \frac{1}{2} I(X; B) - \frac{1}{2} I(X; E) = \frac{1}{2} \mathcal{P}^{(1)}(\mathcal{N})
\]
Application: Big gap between $Q^{(1)}$ and $Q$

We know that $Q^{(1)}(\mathcal{N}) \neq Q(\mathcal{N})$. Could $Q^{(1)}(\mathcal{N}) \approx Q(\mathcal{N})$?

Let $\mathcal{N}_0 = \mathcal{N}_H \otimes^n$ and $\mathcal{N}_1 = \mathcal{E} \otimes^n$ and $\mathcal{T}$ have Kraus operators

$$B_{i,j} = A^i_j \otimes |i\rangle\langle i|$$

$A^i_j$ are Kraus operators of $\mathcal{N}_i$.

Basically: an extra qubit input lets you pick which $\mathcal{N}_i$.

$Q^{(1)}(\mathcal{T}) = 0$, but $Q(\mathcal{T}) \geq \frac{1}{2} Q^{(1)}(\mathcal{T} \otimes \mathcal{T}) \geq 0.005n$.

Next talk: $Q^{(1)} \leq \epsilon$ with $Q \geq \frac{1}{8} \log D$
Convexity: \((1 - p)f(x) + pf(y) \geq f((1 - p)x + py)\)

For capacities: doesn’t help to forget which channel you have.

Let \(\mathcal{M} = (1 - p)\mathcal{E} \otimes |0\rangle\langle 0| + p\mathcal{N}_H \otimes |1\rangle\langle 1|\).
\(Q^{(1)}(\mathcal{M}) = 0\), but \(Q^{(1)}(\mathcal{M} \otimes \mathcal{M})\) is not.

\[
|\phi\rangle_{ABTB'}S = \frac{1}{\sqrt{2}} \sum_x |x\rangle_A |x\rangle_B |x\rangle_T |\phi^+\rangle_{B'S}
\]

Feed \(BB'\) into one \(\mathcal{M}\), \(TS\) into the other, and coh. inf. is:

\[
2p(1 - p)I^{coh}(\mathcal{E} \otimes \mathcal{N}_H, \phi) + p^2I^{coh}(\mathcal{N}_H \otimes \mathcal{N}_H, \phi)
\]

For \(p \ll 1\) the 1st term dominates.
Open Question: How Many Sexes?

Graeme Smith (IBM Watson) Jon Yard (LANL)

Quantum Communication With Zero-Capacity Channels
Open Question: How Many Sexes?

Graeme Smith (IBM Watson) Jon Yard (LANL)

Quantum Communication With Zero-Capacity Channels
Open Question: How Many Sexes?

Graeme Smith (IBM Watson) Jon Yard (LANL)

Quantum Communication With Zero-Capacity Channels
Summary

- There are $\mathcal{A}$ and $\mathcal{N}_H$ with zero capacity but $Q(\mathcal{N} \otimes \mathcal{A}) > 0$.
- Tool 1: $\mathcal{N}_H$ with $P^{(1)}(\mathcal{N}_H) > 0$ but $Q(\mathcal{N}_H) = 0$.
- Tool 2: $Q^{(1)}(\mathcal{N} \otimes \mathcal{E}) \geq \frac{1}{2} P^{(1)}(\mathcal{N})$
- $\mathcal{N}$ and $\mathcal{A}$ transmit different types of quantum information that can be combined to make noiseless sort.
- Applications: $Q$ not convex, not close to $Q^{(1)}$, not additive.

From Slashdot:

Alrighty (Score:2)

by gcnaddict (841664) <gcnaddict@g.m.a_i_l.com> on Tuesday August 05, @11:05PM (#24491753) Homepage

So it's basically a mindfuck, just like the rest of quantum theory.

I'm kinda surprised this wasn't tested before. You'd think all the mindfucks would be checked since it's basically maybe opposite day over in quantum-land.
Questions:

- Can we quantify these different types of information?
- Other examples besides PPT + sym.?
- Are there triples?
- What about the private capacity?