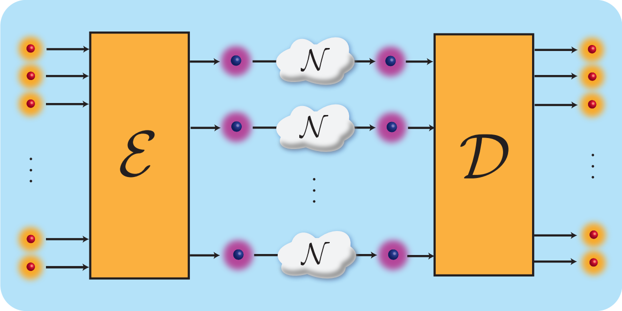
Quantum Communication With Zero-Capacity Channels

Graeme Smith (IBM Watson)
Jon Yard (LANL)

arXiv:0807.4935
Science 321, 1812-1815 (2008)

QIP 2009

Goal: Quantum Communication Over a Quantum Channel

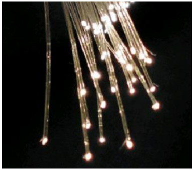


$$\mathcal{Q}(\mathcal{N}) = \max\left(\frac{\#\text{qubits sent}}{\#\text{channel uses}}\right)$$

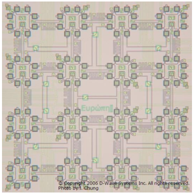
Quantum Capacity:
the rate, in qubits per channel use, at which A can send high fidelity quantum information to B, given $\mathcal{N}^{\otimes n}$.

Goal: Quantum Communication Over a Quantum Channel

Why?



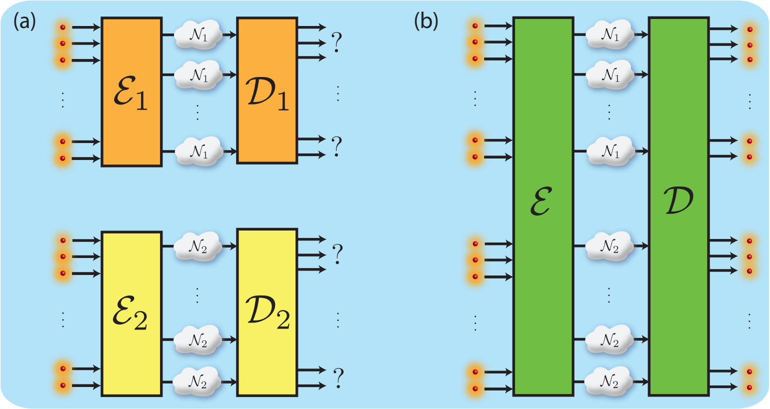
- You may have a noisy quantum channel



- You may be interested in error correction

- You may be interested in packing problems

Main Result

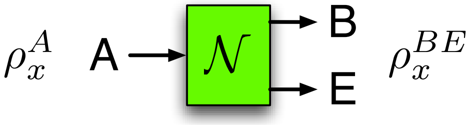


There are channels $\mathcal{N}_1$ and $\mathcal{N}_2$ such that:
$\mathcal{Q}(\mathcal{N}_1) = 0$ and $\mathcal{Q}(\mathcal{N}_2) = 0$, but $\mathcal{Q}(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$.

Outline

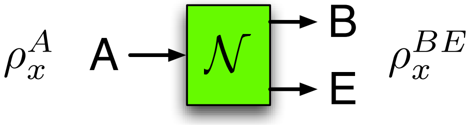
- Quantum and Private Capacities
- Channels with Zero Quantum Capacity
- Superactivation of Quantum Capacity
- Application: superadditivity of coherent information
- Open Questions and Conclusions

Capacities: Quantum



- Coherent information: $\mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\phi_A}(S(B) - S(E))$
- $\mathcal{Q}(\mathcal{N}) \geq \mathcal{Q}^{(1)}(\mathcal{N})$ [Lloyd, Shor, Devetak]
- $\mathcal{Q}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n})$
- $\mathcal{Q}(\mathcal{N}) \neq \mathcal{Q}^{(1)}(\mathcal{N})$ [DiVincenzo, Shor, Smolin]

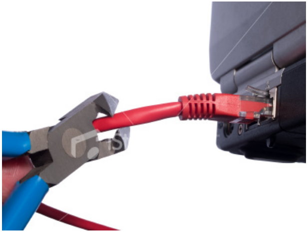
Capacities: Private



- Private Capacity: max rate of private classical communication
- Private Information: $\mathcal{P}^{(1)}(\mathcal{N}) = \max_{p_x,\phi_x}\left(I(X;B) - I(X;E)\right)$
- $\mathcal{P}^{(1)}$ is achievable [Devetak].
- $\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n})$
- $\mathcal{P}(\mathcal{N}) \neq \mathcal{P}^{(1)}(\mathcal{N})$ [Smith, Renes, Smolin]

Zero Capacity Channels—The Puppy Question

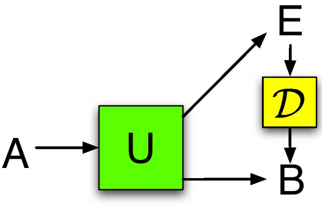
Classical Capacity



- $\mathcal{C} = 0 \leftrightarrow p(y|x)$ independent of x
- Quantum channel: $\mathcal{N}(\rho) = \mathcal{N}(\sigma)\ \forall \rho, \sigma$

Quantum Capacity

- $\mathcal{Q} = 0$ 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:



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

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):

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

$\mathcal{N}$ Horodecki $\Leftrightarrow \forall \phi_{AA'}$
$\rho_{AB} = I \otimes \mathcal{N}(\phi_{AA'})$ is PPT

$$\mathcal{Q}_2(\mathcal{N}) = 0 \Rightarrow Q(\mathcal{N}) = 0$$

A Lousy Two (qu)bit Channel

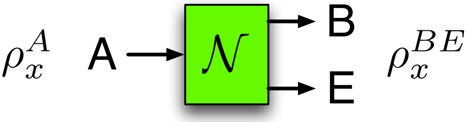
Recall there are states with perfectly secure key that are not maximally entangled: "twisted maximally entangled states".

The idea is this:

- ρ_1 is a twisted EPR pair ("key").
- ρ_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 ρ is PPT. This happens for $p \neq 1/2$, and we have $\mathcal{P}(\mathcal{N}) = 1 - H(p)$.

[Horodecki, Pankowski, Horodecki, Horodecki]

Counterexample to additivity of $\mathcal{Q}$

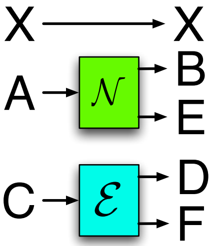


Theorem. Let $\mathcal{N}$ be any channel and $\mathcal{E}$ be a 50%-erasure channel. Then

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

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

Proof



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

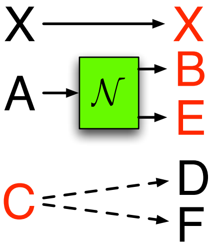
$$\text{so } \rho^{XA} = \sum_x p(x) |x\rangle\langle x|^X \otimes \rho_x^A$$

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

Proof

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

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

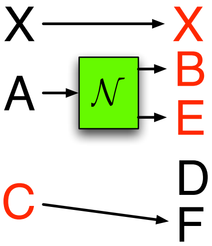


$$Q^{(1)} \geq H(BD) - H(EF)$$

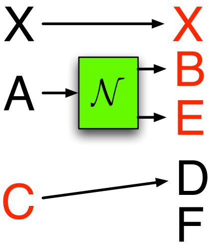
write as entropies on state $|\rho\rangle^{XBEC}$ before erasure $\mathcal{E}$

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

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



$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}\big(H(B) - H(EC)\big)
\end{aligned}
$$



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

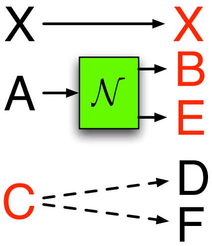
so $\rho^{XA} = \sum_x p(x)|x\rangle\langle x|^X \otimes \rho_x^A$

$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}\big(H(B) - H(EC)\big) + \tfrac{1}{2}\big(H(BC) - H(E)\big)
\end{aligned}
$$

Proof

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

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

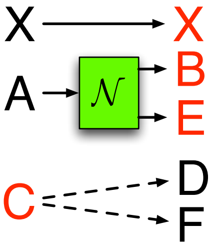


$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}\big(H(B) - H(EC)\big) + \tfrac{1}{2}\big(H(BC) - H(E)\big) \\
&= \tfrac{1}{2}\big(H(B) - H(XB)\big) + \tfrac{1}{2}\big(H(XE) - H(E)\big) \quad \left(\text{on } |\rho\rangle^{XBEC}\right)
\end{aligned}
$$

Proof

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

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



$$
\begin{aligned}
Q^{(1)} &\geq H(BD) - H(EF) \\
&\quad \text{write as entropies on state } |\rho\rangle^{XBEC} \text{ before erasure } \mathcal{E} \\
&= \tfrac{1}{2}\big(H(B) - H(EC)\big) + \tfrac{1}{2}\big(H(BC) - H(E)\big) \\
&= \tfrac{1}{2}\big(H(B) - H(XB)\big) + \tfrac{1}{2}\big(H(XE) - H(E)\big) \quad \left(\text{on } |\rho\rangle^{XBEC}\right) \\
&= \tfrac{1}{2} I(X;B) - \tfrac{1}{2} I(X;E) = \tfrac{1}{2}\mathcal{P}^{(1)}(\mathcal{N})
\end{aligned}
$$

Application: Big gap between $\mathcal{Q}^{(1)}$ and $\mathcal{Q}$

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

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

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

A_j^i are Kraus operators of $\mathcal{N}_i$.

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

$\mathcal{Q}^{(1)}(\mathcal{T}) = 0$, but $\mathcal{Q}(\mathcal{T}) \geq \frac{1}{2}\mathcal{Q}^{(1)}(\mathcal{T} \otimes \mathcal{T}) \geq 0.005n$.
Next talk: $\mathcal{Q}^{(1)} \leq \epsilon$ with $\mathcal{Q} \geq \frac{1}{8}\log D$

Application: Quantum capacity is not convex

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

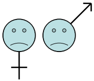
$$|\phi\rangle_{ABTB'S} = \frac{1}{\sqrt{2}} \sum_x |x\rangle_A |x\rangle_B |x\rangle_T \left|\phi^+\right\rangle_{B'S}$$

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

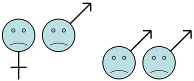
$$2p(1-p)I^{\mathrm{coh}}(\mathcal{E} \otimes \mathcal{N}_H, \phi) + p^2 I^{\mathrm{coh}}(\mathcal{N}_H \otimes \mathcal{N}_H, \phi)$$

For $p \ll 1$ the 1st term dominates.

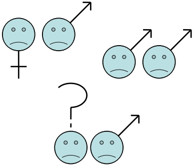
Open Question: How Many Sexes?



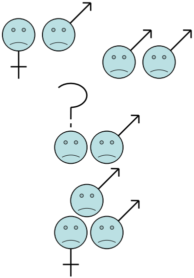
Open Question: How Many Sexes?



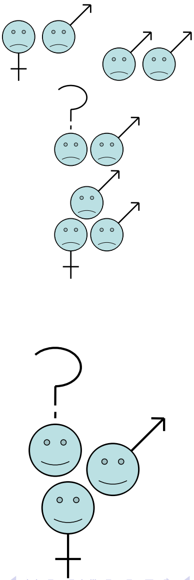
Open Question: How Many Sexes?



Open Question: How Many Sexes?



Open Question: How Many Sexes?



Summary

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

From Slashdot:

Alrighty (Score:2)

by gcnaddict (841664) <gcnaddict@ g m a il.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.

Open Questions

Questions:

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