Supporting Online Material for

Quantum Communication with Zero-Capacity Channels

Graeme Smith* and Jon Yard

*To whom correspondence should be addressed. E-mail: gsbsmith@gmail.com

Published 21 August 2008 on Science Express
DOI: 10.1126/science.1162242

This PDF file includes:

- SOM Text
- References
Quantum Communication with Zero-Capacity Channels

(Supporting Online Material)

Graeme Smith and Jon Yard

In this supporting material, we assume a basic knowledge of quantum information theory at the level of (1). We denote the dimension of a Hilbert space \( A \) as \( |A| \) while abbreviating tensor products as \( AB = A \otimes B \) and the restriction of a density matrix \( \rho^{AB} \) to the subsystem \( A \) as \( \rho^{A} \). By an ensemble of states \( \{p_x, \rho_x^A\} \), we mean that the density matrix \( \rho_x^A \) on \( A \) occurs with probability \( p_x \). We freely associate such ensembles with the joint state \( \sum_x p_x |x\rangle\langle x| \otimes \rho_x^A \), where \( \{|x\rangle\}_{X} \) denotes an orthonormal basis for \( X \). For a channel with input \( A \), output \( B \) and environment \( E \), we abbreviate \( I_e(\mathcal{N}, \rho^A) = H(B) - H(E) \) so that \( Q^{(1)}(\mathcal{N}) = \max_{\rho^A} I_e(\mathcal{N}, \rho^A) \).

Superactivation with finite dimensional channels

Our key tool in this work was the relationship \( \frac{1}{2} q(\mathcal{N}) \leq Q(\mathcal{N} \otimes \mathcal{A}) = Q_{\mathcal{A}}(\mathcal{N}) \), which is valid for any quantum channel \( \mathcal{N} \). A disadvantage of this result is that the input and output systems of the channel \( \mathcal{A} \) are infinite. Guided by that result, we now give a weaker, more manageable bound in which a 50%-erasure channel \( \mathcal{A}_e \) with finite-dimensional input and output systems plays the role of \( \mathcal{A} \).

Consider a channel \( \mathcal{N} \) with input \( A \), output \( B \) and environment \( E \). By Eq. 2 in the main text, observe that every ensemble \( \{p_x, \rho_x^A\} \) yields the lower bound

\[
I(X; B) - I(X; E) \leq \mathcal{P}^{(1)}(\mathcal{N})
\]

where the mutual informations are evaluated on the state

\[
\rho^{XBE} = \sum_x p_x |x\rangle\langle x| \otimes \rho_x^{BE}
\]
and $\rho_{BE}^x$ is the joint state of the output and environment when $\rho_A^x$ is sent through the channel. Furthermore, if the input to $\mathcal{N}$ is finite, this bound is achievable using a finite ensemble (2).

Currently, every known private Horodecki channel $\mathcal{N}_H$ also satisfies $\mathcal{P}^{(1)}(\mathcal{N}_H) > 0$. Therefore, for such a channel, there is a finite ensemble for which $I(X; B) - I(X; E) > 0$. With this in mind, we will demonstrate the following:

**Theorem**: Given an ensemble $\{p_x, \rho_A^x\}$ and a channel $\mathcal{N}$ with input $A$, output $B$ and environment $E$, let $\mathcal{A}_e$ be a 50%-erasure channel with input space $C$ of dimension equal to the sum of the ranks of the states $\rho_A^x$. Then there is a state $\rho^{AC}$ such that

$$I_e(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) = \frac{1}{2}(I(X, B) - I(X; E)).$$

The next section describes a private Horodecki channel $\mathcal{N}^{(4)}_H$ with a four-dimensional input and an ensemble with two rank-two states such that $I(X; B) - I(X; E) > 0.02$. Therefore, there is an erasure channel $\mathcal{A}_e^{(4)}$ with a four-dimensional input $C$ and a state $\rho^{AC}$ such that $\mathcal{Q}(\mathcal{N}_H \otimes \mathcal{A}_e) \geq I_e(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) > 0.01$.

Our strategy of proof is as follows. When the states in the ensemble are pure, i.e. $\rho_A^x = |\rho_x\rangle\langle\rho_x|^A$, we have the identity (2)

$$I_e(\mathcal{N}, \rho^A) = I(X; B) - I(X; E)$$

where $\rho^A = \sum_x p_x |\rho_x\rangle\langle\rho_x|$. Consequently, the coherent information is obtained by restricting the maximization for the private information to pure state ensembles. Since we begin with a mixed state ensemble, we consider a related ensemble of purified states and send the purifying system through a 50%-erasure channel.
**Proof of Theorem:** Define purifications $|\rho_x^{x} AC\rangle$ of the states $\rho_x^A$ such that the supports of the $\rho_x^C$ are disjoint. Then the pure state

$$|\rho^{XAC}\rangle = \sum_x \sqrt{p_x} |x^X\rangle |\rho_x^{AC}\rangle$$

is a purification of the state $\sum_x p_x |x^X\rangle \otimes \rho_x^A$ associated to the ensemble. We will evaluate the coherent information resulting from sending $A$ through $\mathcal{N}$ and $C$ through $\mathcal{A}_e$. Denoting the output of $\mathcal{A}_e$ by $D$ and the environment of $\mathcal{A}_e$ by $F$, we obtain the following chain of inequalities:

$$I_c(\mathcal{N} \otimes \mathcal{A}_e, \rho^{AC}) = H(BD) - H(EF)$$

**(S1)**

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

**(S2)**

$$= \frac{1}{2} (H(B) - H(XB)) + \frac{1}{2} (H(XE) - H(E))$$

**(S3)**

$$= \frac{1}{2} (I(X;B) - I(X;E)).$$

**(S4)**

In Eq. S1, the entropies are evaluated on the state obtained by sending the $AC$ parts of $|\rho^{XAC}\rangle$ through the respective channels. Eq. S2 holds because with equal probability, $\mathcal{N}_e$ either delivers $C$ to its output $D$ or to its environment $F$, so this difference of entropies can be rewritten in terms of quantities evaluated on the state on $XBE\mathcal{C}$ obtained by sending only the $A$ part of $|\rho^{XAC}\rangle$ through $\mathcal{N}$. Eq. S3 is true because bipartitions of any pure state have the same entropy and Eq. S4 uses the definition of mutual information after adding $H(X)$ to the first term and subtracting it from the second. 

\[\square\]
A four-dimensional private Horodecki channel

For convenience we give an explicit description of the four-dimensional private Horodecki channel $\mathcal{N}^{(4)}_H$ from (3). The action of any channel $\mathcal{N}$ can be written in Kraus form as

$$\mathcal{N}(\rho) = \sum_{k} N_k \rho N_k^\dagger,$$

where the Kraus matrices $N_k$ satisfy $\sum_k N_k^{\dagger} N_k = I$. We denote the input of $\mathcal{N}^{(4)}_H$ as a tensor product of two qubits $A = A_1 A_2$ and denote the output as $B$. This channel is specified by the following six Kraus matrices:

$$\sqrt{\frac{q}{2}} I \otimes |0\rangle \langle 0|, \sqrt{\frac{q}{2}} Z \otimes |1\rangle \langle 1|, \sqrt{\frac{q}{4}} I \otimes Y, \sqrt{\frac{q}{4}} I \otimes X, \sqrt{1 - q} X \otimes M_0, \sqrt{1 - q} Y \otimes M_1.$$

Here, $q = \frac{\sqrt{2}}{1+\sqrt{2}}$, while $X, Y$ and $Z$ are the usual Pauli matrices and

$$M_0 = \begin{pmatrix} \frac{1}{2} \sqrt{2 + \sqrt{2}} & 0 \\ 0 & \frac{1}{2} \sqrt{2 - \sqrt{2}} \end{pmatrix}, \quad M_1 = \begin{pmatrix} \frac{1}{2} \sqrt{2 - \sqrt{2}} & 0 \\ 0 & \frac{1}{2} \sqrt{2 + \sqrt{2}} \end{pmatrix}.$$

A lower bound of 0.02 on the private capacity $\mathcal{P}(\mathcal{N}^{(4)}_H)$ is obtained via the ensemble consisting of two equiprobable states $\rho^A = |x\rangle \langle x| \otimes \frac{1}{2} I^{A_2}$ because the state $\rho^{XBE}$ resulting from putting $A$ into the channel $\mathcal{N}^{(4)}_H$ satisfies (3)

$$I(X; B) - I(X; E) \geq 1 - q \log_2 q - (1 - q) \log_2 (1 - q) > 0.02.$$
Nonconvexity of quantum capacity

We now use the results of the first section to show that $Q$ is not convex. Fix a private Horodecki channel $\mathcal{N}_H$ and a 50%-erasure channel $\mathcal{A}_e$ such that the input $A$ to $\mathcal{N}_H$ and the input $C$ to $\mathcal{A}_e$ have the same dimension, and such that there is a state $\rho^{AC}$ which is symmetric under interchanging $A$ and $C$ satisfying $I_c(\mathcal{N}_H \otimes \mathcal{A}_e, \rho^{AC}) > 0$. In particular, the channel $\mathcal{N}_H^{(4)}$ from the previous section and a four-dimensional erasure channel $\mathcal{A}_e^{(4)}$ satisfy these criteria with respect to the state

$$\rho^{AC} = \frac{1}{2}(|0\rangle\langle 0|_{A_1} \otimes |0\rangle\langle 0|_{C_1} + |1\rangle\langle 1|_{A_1} \otimes |1\rangle\langle 1|_{C_1}) \otimes |\phi_+\rangle\langle \phi_+|_{A_2 C_2}$$

where $|\phi_+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, $A = A_1 A_2$ and $C = C_1 C_2$. Identifying $A \simeq C$, we define the channel

$$\mathcal{M}_p = p\mathcal{N}_H \otimes |0\rangle\langle 0| + (1-p)\mathcal{A}_e \otimes |1\rangle\langle 1|$$

where $0 \leq p \leq 1$. With probability $p$, this channel applies $\mathcal{N}_H$ to the input and otherwise applies $\mathcal{A}_e$, while telling the receiver which channel was applied. Although $\mathcal{M}_p$ is a convex combination of the zero-capacity channels $\mathcal{N}_H \otimes |0\rangle\langle 0|$ and $\mathcal{A}_e \otimes |1\rangle\langle 1|$, we will show that for small enough values of $p$, their convex combination $\mathcal{M}_p$ has a positive capacity. On any input state $\rho$, we have

$$I_c(\mathcal{M}_p \otimes \mathcal{M}_p, \rho) = p^2 I_c(\mathcal{N}_H \otimes \mathcal{N}_H, \rho) + p(1-p)I_c(\mathcal{N}_H \otimes \mathcal{A}_e, \rho)$$

$$+ p(1-p)I_c(\mathcal{A}_e \otimes \mathcal{N}_H, \rho) + (1-p)^2 I_c(\mathcal{A}_e \otimes \mathcal{A}_e, \rho).$$

Since $\mathcal{A}_e \otimes \mathcal{A}_e$ is a symmetric channel, the last term is always zero. Choosing the state $\rho = \rho^{AC}$, which was assumed to be symmetric, we find that

$$I_c(\mathcal{M}_p \otimes \mathcal{M}_p, \rho^{AC}) = 2p(1-p)I_c(\mathcal{N}_H \otimes \mathcal{A}_e, \rho^{AC}) + p^2 I_c(\mathcal{N}_H \otimes \mathcal{N}_H, \rho^{AC}).$$

For $0 < p < 1$, the first term is positive by assumption. The second term can never be greater than zero because $Q(\mathcal{N}_H) = 0$, although it is lower bounded by $-2p^2 c$, where
c = \log_2 |E|$. Here $c$ is finite because $|E|$ is finite when the input and output of $\mathcal{N}_H$ have finite dimension. Simple algebra reveals that $I_c(\mathcal{M}_p \otimes \mathcal{M}_p, \rho^{AC}) > 0$ for all $p$ satisfying

$$0 < p < \frac{I_c(\mathcal{N}_H \otimes \mathcal{A}_e, \rho^{AC})}{c + I_c(\mathcal{N}_H \otimes \mathcal{A}_e, \rho^{AC})}.$$  

For the four-dimensional example of the previous section, one has $c = \log_2 6$ so the corresponding convex combination has a positive capacity if $0 < p < 0.0041$. Stronger violations are expected to be found in larger examples.

**Arbitrarily large gap between $Q^{(1)}$ and $Q$**

Although it has long been known that $Q$ can be strictly greater than $Q^{(1)}$, there has been speculation that deviations of $Q$ from $Q^{(1)}$ may be fairly small. Thus, while the regularized nature of the capacity expression is unwieldy, we might hope that for practical purposes the quantum capacity is well approximated by $Q^{(1)}$ and analysis could proceed by considering the computable function $Q^{(1)}$. Our work shows that this is not true, as there exist channels $\mathcal{M}$ with $Q^{(1)}(\mathcal{M}) = 0$ for which the actual capacity can be arbitrarily large.

Let $\mathcal{N}_H$ be a private Horodecki channel and let $\mathcal{A}_e$ be a 50%-erasure channel with the same input dimension for which $Q^{(1)}(\mathcal{N}_H \otimes \mathcal{A}_e) > 0$. For example, the four-dimensional channels discussed above would work. Define $\mathcal{M}$ to be a channel with input $A = A_1 A_2$, where $A_1$ is a qubit and $A_2$ is the input space of $\mathcal{N}_H$ and $\mathcal{A}_e$. The channel measures the first qubit $A_1$ in the $\{|0\rangle, |1\rangle\}$ basis and, depending on the outcome, applies one of the channels $\mathcal{N}_H$ or $\mathcal{A}_e$ to $A_2$. The outcome of the measurement is revealed to the receiver. This channel can be seen to have $Q^{(1)}(\mathcal{M}) = 0$ because $Q^{(1)}(\mathcal{N}_H) = Q^{(1)}(\mathcal{A}_e) = 0$. However, the sender has control over which channel is applied to which input, so $Q^{(1)}(\mathcal{M} \otimes \mathcal{M}) \geq Q^{(1)}(\mathcal{N}_H \otimes \mathcal{A}_e) > 0$. By replacing $\mathcal{N}_H$ in the above discussion with $n$ instances of $\mathcal{N}_H$, and similarly for $\mathcal{A}_e$, this violation can be made arbitrarily large.
References and Notes

