nature physics

LETTERS

PUBLISHED ONLINE: 15 MARCH 2009 | DOI: 10.1038/NPHYS1224

Superadditivity of communication capacity using entangled inputs

M. B. Hastings*

The design of error-correcting codes used in modern communications relies on information theory to quantify the capacity of a noisy channel to send information[1]. This capacity can be expressed using the mutual information between input and output for a single use of the channel; although correlations between subsequent input bits are used to correct errors, they cannot increase the capacity. For quantum channels, it has been an open question whether entangled input states can increase the capacity to send classical information[2]. The additivity conjecture[3,4] states that entanglement does not help, making practical computations of the capacity possible. Although additivity is widely believed to be true, there is no proof. Here, we show that additivity is false, by constructing a random counter-example. Our results show that the most basic question of classical capacity of a quantum channel remains open, with further work needed to determine in which other situations entanglement can boost capacity.

In the classical setting, Shannon presented a formal definition of a noisy channel $\mathcal{E}$ as a probabilistic map from input states to output states. In the quantum setting, the channel becomes a linear, completely positive, trace-preserving map from density matrices to density matrices, modelling noise in the system due to interaction with an environment. Such a channel can be used to send either quantum or classical information. In the first case, a marked violation of operational additivity was recently shown, in that there exist two channels, both having zero capacity to send quantum information no matter how many times it is used, which can be used in tandem to send quantum information[5].

Here, we address the classical capacity of a quantum channel. To specify how information is encoded in the channel, we must pick a set of states ρ_i which we use as input signals with probabilities p_i. Then the Holevo formula[2] for the capacity is:

$$\chi = H\left(\sum_i p_i \mathcal{E}(\rho_i)\right) - \sum_i p_i H\left(\mathcal{E}(\rho_i)\right)$$

where $H(\rho) = -\mathrm{Tr}(\rho \ln(\rho))$ is the von Neumann entropy. The maximum capacity of a channel is the maximum over all input ensembles:

$$\chi_{\max}(\mathcal{E}) = \max_{\{p_i\},\{\rho_i\}} \chi(\mathcal{E}, \{p_i\}, \{\rho_i\})$$

Suppose we have two different channels, $\mathcal{E}_1$ and $\mathcal{E}_2$. To compute this capacity, it seems necessary to consider entangled input states between the two channels. Similarly, when using the same channel multiple times, it may be useful to use input states that are entangled across multiple uses of the same channel. The additivity conjecture

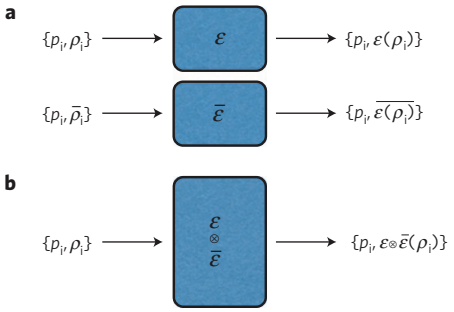

Figure 1 | Communicating classical information over a quantum channel. **a**, A set of states ρ_i are used with probabilities p_i as signal states on the channel $\mathcal{E}$. The inputs are unentangled between channels $\mathcal{E}$ and $\bar{\mathcal{E}}$. The capacity of $\mathcal{E}$ is equal to that of $\bar{\mathcal{E}}$. **b**, A set of entangled input states ρ_i are used on the channel $\mathcal{E} \otimes \bar{\mathcal{E}}$. The question addressed is whether entangling can increase capacity.

(see Fig. 1) is the conjecture that this does not help and that instead

$$\chi_{\max}(\mathcal{E}_1 \otimes \mathcal{E}_2) = \chi_{\max}(\mathcal{E}_1) + \chi_{\max}(\mathcal{E}_2)$$

The additivity conjecture makes it possible to compute the classical capacity of a quantum channel. Furthermore, Shor[4] showed that several different additivity conjectures in quantum information theory are all equivalent. These are the additivity conjecture for the Holevo capacity, the additivity conjecture for entanglement of formation[6], strong superadditivity of entanglement of formation[7] and the additivity conjecture for minimum output entropy[3]. Here, we show that all of these conjectures are false, by constructing a counter-example to the last of these conjectures. Given a channel $\mathcal{E}$, define the minimum output entropy $H^{\min}$ by

$$H^{\min}(\mathcal{E}) = \min_{|\psi\rangle} H(\mathcal{E}(|\psi\rangle\langle\psi|))$$

The minimum output entropy conjecture is that for all channels $\mathcal{E}_1$ and $\mathcal{E}_2$, we have

$$H^{\min}(\mathcal{E}_1 \otimes \mathcal{E}_2) = H^{\min}(\mathcal{E}_1) + H^{\min}(\mathcal{E}_2)$$

A counter-example to this conjecture would be an entangled input state that has a lower output entropy, and hence is more resistant to noise, than any unentangled state (see Fig. 2).

Our counter-example to the additivity of minimum output entropy is based on a random construction, similar to those Winter and Hayden used to show violation of the maximal p-norm multiplicativity conjecture for all $p > 1$ (refs 8–10). For $p = 1$, this violation would imply violation of the minimum output entropy

Center for Nonlinear Studies and Theoretical Division, Los Alamos National Laboratory, Los Alamos, New Mexico 87545, USA. *e-mail: hastings@lanl.gov.

conjecture; however, the counter-example found in ref. 9 requires a matrix size that diverges as $p \to 1$. We use different system and environment sizes (note that $D \ll N$ in our construction below) and make a different analysis of the probability of different output entropies. Other violations are known for p close to 0 (ref. 11).

We define a pair of channels $\mathcal{E}$ and $\overline{\mathcal{E}}$, which are complex conjugates of each other. Each channel acts by randomly choosing a unitary from a small set of unitaries U_i $(i = 1 \ldots D)$ and applying that to ρ. This models a situation in which the unitary evolution of the system is determined by an unknown state of the environment. We define

$$\mathcal{E}(\rho) = \sum_{i=1}^{D} P_i U_i^{\dagger} \rho U_i$$

$$\overline{\mathcal{E}}(\rho) = \sum_{i=1}^{D} P_i \overline{U}_i^{\dagger} \rho \overline{U}_i$$

where the U_i are N-by-N unitary matrices, chosen at random from the Haar measure, and the probabilities P_i are chosen randomly as described in Supplementary Information. The P_i are all roughly equal. We pick

$$1 \ll D \ll N$$

In Supplementary Information we prove the following theorem:

For sufficiently large D and for sufficiently large N, there is a non-zero probability that a random choice of U_i from the Haar measure and of P_i (as described in Supplementary Information) will give a channel $\mathcal{E}$ such that

$$H^{\min}(\mathcal{E} \otimes \overline{\mathcal{E}}) < H^{\min}(\mathcal{E}) + H^{\min}(\overline{\mathcal{E}})$$

$$= 2H^{\min}(\mathcal{E})$$

The size of N depends on D.

For any pure-state input, the output entropy of $\mathcal{E}$ is at most $\ln(D)$ and that of $\mathcal{E} \otimes \overline{\mathcal{E}}$ is at most $2\ln(D)$. To prove the above theorem, we first construct an entangled state with a lower output entropy for the channel $\mathcal{E} \otimes \overline{\mathcal{E}}$. The entangled state we use is the maximally entangled state

$$|\Psi_{ME}\rangle = (1/\sqrt{N}) \sum_{\alpha=1}^{N} |\alpha\rangle \otimes |\alpha\rangle$$

As shown in Lemma 1 in Supplementary Information, the output entropy for this state is bounded by

$$H\left(\mathcal{E} \otimes \overline{\mathcal{E}}(|\Psi_{ME}\rangle\langle\Psi_{ME}|)\right) \leq 2\ln(D) - \ln(D)/D \qquad (1)$$

We then use the random properties of the channel to show that no product state input can obtain such a low output entropy. Lemmas 2–5 in Supplementary Information show that, with non-zero probability, the entropy $H^{\min}(\mathcal{E})$ is at least $\ln(D) - \delta S^{\max}$, for

$$\delta S^{\max} = c_1/D + p_1(D)\mathcal{O}(\sqrt{\ln(N)/N})$$

where c_1 is a constant and $p_1(D) = \mathrm{poly}(D)$. Thus, because for large enough D and for large enough N we have $2\delta S^{\max} < \ln(D)/D$, the theorem follows.

The output entropy can be understood differently: for a given pure-state input, can we determine from the output which of the unitaries $U_i^{\dagger}$ was applied? Recall that

$$U^{\dagger} \otimes \overline{U}^{\dagger} |\Psi_{ME}\rangle = |\Psi_{ME}\rangle \qquad (2)$$

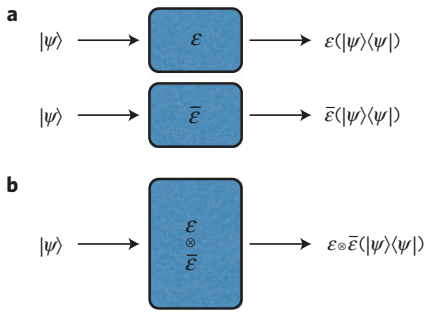

Figure 2 | Minimum output entropy of a quantum channel. a, A pure state $|\psi\rangle$ is input to the channel $\mathcal{E}$. Although $|\psi\rangle$ is a pure state, the output may be a mixed state. We attempt to minimize the output entropy over all pure input states. **b**, An entangled input state $|\psi\rangle$ is input to the channel $\mathcal{E} \otimes \overline{\mathcal{E}}$. The question addressed is whether this entangled input state can have a lower output entropy for channel $\mathcal{E} \otimes \overline{\mathcal{E}}$ than the sum of the minimum output entropies for the two channels.

for any unitary U. This means that, for the maximally entangled state, if a unitary $U_i^{\dagger}$ was applied to one subsystem, and $\overline{U}_i^{\dagger}$ was applied to the other subsystem, we cannot determine which unitary i was applied by looking at the output. This is the key idea behind equation (1).

Note that the minimum output entropy of $\mathcal{E}$ must be less than $\ln(D)$ by an amount at least of order $1/D$. Suppose U_1 and U_2 are the two unitaries with the largest l_i. Choose a state $|\psi\rangle$ that is an eigenvector of $U_1 U_2^{\dagger}$. For this state, we cannot distinguish between the states $U_1^{\dagger}|\psi\rangle$ and $U_2|\psi\rangle$, and so

$$H^{\min}(\mathcal{E}) \leq \ln(D) - (2/D)\ln(2)$$

Our randomized analysis bounds how much further the output entropy of the channel $\mathcal{E}$ can be lowered for a random choice of U_i.

Our work raises the question of how strong a violation of additivity is possible. The relative violation we have found is numerically small, but it may be possible to increase this, and to find new situations in which entangled inputs can be used to increase channel capacity, or novel situations in which entanglement can be used to protect against decoherence in practical devices. The map $\mathcal{E}$ is similar to that used[12] to construct random quantum expanders[13,14], raising the possibility that deterministic expander constructions can provide stronger violations of additivity.

Although we have used two different channels, it is also possible to find a single channel $\mathcal{E}$ such that $H^{\min}(\mathcal{E} \otimes \mathcal{E}) < 2H^{\min}(\mathcal{E})$, by choosing U_i from the orthogonal group. Alternatively, we can add an extra classical input used to 'switch' between $\mathcal{E}$ and $\overline{\mathcal{E}}$ (P. Hayden, private communication).

The equivalence of the different additivity conjectures[4] means that the violation of any one of the conjectures has profound impacts. The violation of additivity of the Holevo capacity means that the problem of channel capacity remains open, because if a channel is used many times, we must do an intractable optimization over all entangled inputs to find the maximum capacity. However, we conjecture that additivity holds for all channels of the form

$$\mathcal{E} = \mathcal{F} \otimes \overline{\mathcal{F}}$$

Our intuition for this conjecture is that we believe that multi-party entanglement (between the inputs to three or more channels) is not useful, because it is very unlikely for all channels to apply the same unitary; note that the state Ψ_{ME} has a low minimum output entropy precisely because it is left unchanged as in equation (2) if both channels apply corresponding unitaries. This two-letter additivity conjecture would enable us to restrict our attention to considering

input states with a bipartite entanglement structure, possibly opening the way to computing the capacity for arbitrary channels.

Received 7 October 2008; accepted 12 February 2009; published online 15 March 2009

References

1. Shannon, C. E. A mathematical theory of communication. *Bell Syst. Tech. J.* **27**, 379–423 (1948).
2. Holevo, A. S. Bounds for the quantity of information transmitted by a quantum communication channel. *Probl. Info. Transm. (USS)* **9**, 177–183 (1973).
3. King, C. & Ruskai, M. B. Minimal entropy of states emerging from noisy quantum channels. *IEEE Trans. Inf. Theory* **47**, 192–209 (2001).
4. Shor, P. W. Equivalence of additivity question in quantum information theory. *Comm. Math. Phys.* **246**, 453–472 (2004).
5. Smith, G. & Yard, J. Quantum communication with zero-capacity channels. *Science* **321**, 1812–1815 (2008).
6. Bennett, C. H., DiVincenzo, D. P., Smolin, J. A. & Wootters, W. K. Mixed-state entanglement and quantum error correction. *Phys. Rev. A* **54**, 3824–3851 (1996).
7. Benatti, F. & Narnhofer, H. Additivity of the entanglement of formation. *Phys. Rev. A* **63**, 042306 (2001).
8. Winter, A. The maximum output p-norm of quantum channels is not multiplicative for any $p > 2$. Preprint at <http://arxiv.org/abs/0707.0402> (2007).
9. Hayden, P. The maximal p-norm multiplicativity conjecture is false. Preprint at <http://arxiv.org/abs/0707.3291> (2007).
10. Hayden, P. & Winter, A. Counterexamples to the maximal p-norm multiplicativity conjecture for all $p > 1$. *Commun. Math. Phys.* **284**, 263–280 (2008).
11. Cubitt, T., Harrow, A. W., Leung, D., Montanero, A. & Winter, A. Counterexamples to additivity of minimum output p-Renyi entropy for p close to 0. *Commun. Math. Phys.* **284**, 281–290 (2008).
12. Hastings, M. B. Random unitaries give quantum expanders. *Phys. Rev. A* **76**, 032315.
13. Ben-Aroya, A. & Ta-Shma, A. Quantum expanders and the quantum entropy difference problem. Preprint at <http://arxiv.org/abs/quant-ph/0702129> (2007).
14. Hastings, M. B. Entropy and entanglement in quantum ground states. *Phys. Rev. B* **76**, 035114 (2007).

Acknowledgements

I thank J. Yard, P. Hayden and A. Harrow. This work was supported by US DOE Contract No. DE-AC52-06NA25396.

Additional information

Supplementary Information accompanies this paper on www.nature.com/naturephysics. Reprints and permissions information is available online at http://npg.nature.com/reprintsandpermissions.