$\forall n\ \exists \mathcal{N}\ Q^{(n)}(\mathcal{N}) = 0, Q(\mathcal{N}) > 0;$

or

Unbounded number of channel uses are required to see quantum capacity

Toby Cubitt, David Elkouss, William Matthews,
Maris Ozols, David Pérez-García and Sergii Strelchuk *

Full version of paper: arXiv:1408.5115

Abstract

The only general formula known for the quantum capacity Q of a channel is the large n limit of $Q^{(n)}$ – the maximal coherent information per channel use for n uses of the channel. We show that for any n there are channels for which $Q^{(n)}$ is zero, but which still have positive quantum capacity. Therefore, in general, one may have to consider the coherent information for an arbitrarily large number of channel uses just to establish that the channel has non-zero capacity, $Q > 0$.

To solve practical problems of information transmission we need to characterise the utility of the available resources. In the classical world, we have powerful tools available for this: We can compute the *classical capacity* of any discrete, memoryless classical channel by an optimisation which only involves a single use of the channel. This figure completely characterises the asymptotic rate of reliable communication which is possible in the limit of many uses of the channel. When we turn to quantum channels, we find that their capacities for transmitting classical or quantum information cannot be characterized by a single use of the channel: the best expressions we have are the $n \to \infty$ ("regularised") limits of a sequence of optimisation problems involving n uses of the channel. For the quantum capacity, the expression is

$$Q(\mathcal{N}) := \lim_{n\to\infty} Q^{(n)}(\mathcal{N}), \quad Q^{(n)}(\mathcal{N}) := \frac{1}{n} \max_{\rho^{(n)}} I_{\text{coh}}(\mathcal{N}^{\otimes n}, \rho^{(n)}),$$

where $Q^{(n)}(\mathcal{N})$ is the coherent information maximized over a joint input $\rho^{(n)}$ for n uses of the channel $\mathcal{N}$. This regularisation renders computing the quantum capacity unfeasible because it involves optimization over a Hilbert space of unbounded dimension. The need for regularisation is a direct consequence of the fact that strict *superadditivity* $Q^{(n+1)}(\mathcal{N}) > Q^{(n)}(\mathcal{N})$ is possible. The first explicit examples of this superadditivity of $Q^{(1)}$ were given by Di Vincenzo et al. in [1], and this work was extended by Smith et al. [3]. For these examples (where $\mathcal{N}$ is a particular depolarising channel) it was shown that, for certain values of n, $0 \leq Q^{(1)}(\mathcal{N}) < Q^{(n)}(\mathcal{N})$.

While the classical capacity of quantum channels does require a regularised expression, we at least know precisely in which cases it is *zero*: Simply for those channels whose output is not correlated with the input. For the *quantum* capacity the set of zero-capacity channels is much richer and we do not have a complete characterization. To date, we know of only two

*Toby Cubitt, Maris Ozols, Will Matthews and Sergii Strelchuk are with Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, U.K.. David Elkouss and David Pérez-García are with Departamento de Análisis Matemático and Instituto de Matemática Interdisciplinar, Universidad Complutense de Madrid, 28040 Madrid, Spain.

effective criteria for zero quantum capacity: *Antidegradable* channels, from whose environment one can can reproduce the output, have $Q = 0$ by the no-cloning theorem. *PPT-binding* channels can only distribute PPT entanglement, which cannot be distilled by local operations and classical communication and, these too have $Q = 0$. Remarkably, it is possible to take two quantum channels, $\mathcal{N}_1$ antidegradable and $\mathcal{N}_2$ PPT-binding, so that $Q(\mathcal{N}_1) = Q(\mathcal{N}_2) = 0$, which when used together can transmit quantum information reliably i.e. $Q(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$. This phenomenon, called "superactivation", was discovered by Smith and Yard [4]. They used their examples to construct a single channel $\mathcal{N}$ exhibiting an extreme form of superadditivity of $Q^{(1)}$, where $0 = Q^{(1)}(\mathcal{N}) < Q^{(2)}(\mathcal{N})$. In their construction, having two uses of $\mathcal{N}$ effectively enables one use of $\mathcal{N}_1$ and one of $\mathcal{N}_2$.

These recent additivity violation results demonstrated how much we still don't understand about communication over quantum channels, and have raised many basic questions about the structure of quantum Shannon theory. Just how badly behaved can superadditivity be? One might hope that, in general, at least in order to determine whether a channel has *any* non-zero quantum capacity or not, one only needs to look at a finite number of uses of a channel. Indeed, since the Smith and Yard construction relies on combining the only two known types of zero-capacity channel, one might even dare to hope that two copies is enough for this.

Our main result is that for any n, one can construct a channel $\mathcal{N}$ such that $Q^{(n)}(\mathcal{N}) = 0$ but $Q(\mathcal{N}) > 0$. So one may have to look through an arbitrary number of uses of the channel just to decide whether the channel has any quantum capacity at all! In fact, this is also the first proof that there can be a gap between $Q^{(n)}(\mathcal{N})$ and the quantum capacity for arbitrarily large n.

The first indication that such a result may be true comes from the work of Watrous [5] where it was shown that an arbitrary large number of copies of a bipartite quantum state might be required for entanglement distillation facilitated by two-way classical communication. Our result can be regarded as the counterpart of [5] for the quantum capacity. However, the proof ideas and techniques of [5] require two-way communication, thus they are not applicable in the usual capacity setting. Our result is instead based on the construction of Smith and Yard, and the intuition provided by Oppenheim's commentary thereon [2], but we have to extend these ideas quite carefully to obtain the desired channel properties for any value of n.

A natural question which we leave open is whether a stronger form of the result holds, which gives a constant upper bound on the channel dimension. It is even conceivable that the presence of quantum capacity is undecidable, which would imply the stronger form of result mentioned. We will now give an overview of our channel construction and proof.

Channel construction.
The *erasure channel with erasure probability* p is $\mathcal{E}_p^{\mathsf{A}\to\mathsf{FB}} := (1-p)|0\rangle\langle 0|^{\mathsf{F}} \otimes \mathcal{I}^{\mathsf{A}\to\mathsf{B}} + p|1\rangle\langle 1|^{\mathsf{F}} \otimes \mathbf{1}^{\mathsf{B}}/(\dim(\mathsf{B}))$, where $\mathcal{I}^{\mathsf{A}\to\mathsf{B}}$ is the identity channel from A to B, and F is the erasure flag.

The channel $\Gamma^{\mathbf{A}\to\mathbf{B}}$ belongs to the class of PPT entanglement-binding channels whose Choi state is an approximate *pbit* (*private bit*) [6]. The system $\mathbf{A}$ consists of subsystems aA and $\mathbf{B}$ of subsystems bB. If Alice (holding aA) and Bob (holding bB) share the Choi state for Γ then they cannot distill any entanglement (since the state is PPT), while if Bob obtains Alice's "shield" A they can distill by one-way classical communication from Alice to Bob. We show that Γ can be constructed with $\mathsf{A} = \mathsf{A}_1 \ldots \mathsf{A}_N$ and $\mathsf{B} = \mathsf{B}_1 \ldots \mathsf{B}_N$ consisting of N parts, such that even if Bob only receives part A_i of Alice's shield for any i, they obtain approximately one ebit of one-way distillable entanglement. Let $\tilde{\Gamma}_\kappa^{\mathbf{A}\to\mathbf{FB}} := \mathcal{E}_\kappa^{\mathbf{B}\to\mathbf{FB}} \circ \Gamma^{\mathbf{A}\to\mathbf{B}}$ be a noisy version of the channel Γ. Our construction uses channels of the form

$$\mathcal{M}^{\mathsf{SA}\to\mathsf{SFB}} := \mathcal{P}_0^{\mathsf{S}\to\mathsf{S}} \otimes \tilde{\Gamma}_\kappa^{\mathbf{A}\to\mathbf{FB}} + \mathcal{P}_1^{\mathsf{S}\to\mathsf{S}} \otimes \mathcal{E}_p^{\mathbf{A}\to\mathbf{FB}}. \tag{1}$$

Here $\mathcal{P}_i^{\mathsf{S}\to\mathsf{S}}$ projects onto the i-th computational basis vector of the qubit system S which thereby acts as a classical switch allowing Alice to choose whether the channel acts as $\mathcal{E}_p$ or $\tilde{\Gamma}_\kappa$ on the main input $\mathbf{A}$. S is retained in the output which lets Bob learn which choice was made.

Theorem 1. *For any positive integer n, if $\kappa \in (0, 1/2)$ and $p \in ((1+\kappa^n)^{-1/n}, 1)$ then there exists a channel Γ such that $Q^{(n)}(\mathcal{M}) = 0$ and $Q(\mathcal{M}) > 0$.*

Proof ingredients.
The proof of Theorem 1 is divided in two parts. We first prove that, given n and κ, for any Γ with zero capacity there is a range of p that makes the coherent information of $\mathcal{M}^{\otimes n}$ zero. In the second part we prove that there exists Γ with zero capacity such that $\mathcal{M}$ has positive capacity.

For the first part we can simplify the analysis of $\mathcal{M}^{\otimes n}$ by showing that it is optimal to make a definite choice (i.e. a computational basis state input) for each of the n switch registers. For each possible setting of the n switches, the coherent information is a convex combination of the coherent information for three cases, weighted by their probabilities: (a) every channel erases, (b) all of the $\mathcal{E}_p$ erase but not all $\tilde{\Gamma}$ erase, (c) at least one of the $\mathcal{E}_p$ does not erase (and therefore acts as the identity channel). The coherent information for cases (b) and (c) can be upper bounded respectively by zero and $H(\mathsf{R})$, where R is a system that purifies the input. For (a) it is bounded above by $-H(\mathsf{R})$. Weighting by the probabilities, we find that the total coherent information is bounded by $\big(1-(1+\kappa^n)p^n\big)H(\mathsf{R})$. This allows us to conclude that for any n and κ we can find p such that the coherent information of n uses of the channel is zero.

To prove the second part of Theorem 1, we show that for fixed κ, p we can find a Γ with a shield of N parts (as described in Section 2) such that the coherent information of $N+1$ uses of the channel $\mathcal{M}$ is positive for some $N+1 > n$. We number the channel uses $0, \ldots, N$ and label the systems involved in the i-th use of the channel with superscript i. Consider the following input. The switch registers are set to choose $\tilde{\Gamma}_\kappa$ for use 0 and $\mathcal{E}_p$ for the remaining uses $1, \ldots, N$. We maximally entangle subsystem A_i^0 of $\mathbf{A}^0$ (which is acted on by $\tilde{\Gamma}_\kappa$) with subsystem A_1^i of $\mathbf{A}^i$ (acted on by an erasure channel). We also maximally entangle subsystem a^0 of $\mathbf{A}^0$ with a purifying reference system a which is retained by Alice. The remaining input subsystems are set to an arbitrary pure state. The resulting coherent information is a convex combination of cases where (a) $\tilde{\Gamma}_\kappa$ erases, (b) $\tilde{\Gamma}_\kappa$ does not erase but all the $\mathcal{E}_p$ erase, and (c) $\tilde{\Gamma}_\kappa$ and at least one $\mathcal{E}_p$ do not erase. Case (a) contributes coherent information -1 weighted by its probability κ. Case (b) contributes approximately zero coherent information (due to a standard property of pbits). In case (c), after channel use 0, Alice and Bob share the Choi state of Γ on systems $\mathsf{a}\mathsf{b}^0\mathsf{A}_1^1\mathsf{B}_1^0 \ldots \mathsf{A}_1^N\mathsf{B}_N^0$, and after the N uses of $\mathcal{E}_p$ at least one of $\mathsf{A}_1^1 \ldots \mathsf{A}_1^N$ (the j-th one in the figure) reaches Bob unerased. They then share a state with approximately one ebit of one-way distillable entanglement (coherent information $+1$). This contribution is weighted by the probability $(1-\kappa)(1-p^N)$. We show that for $p \in (0,1)$, $\kappa \in (0, 1/2)$, we can find a Γ with large enough N for which the overall coherent information is positive, proving that $Q(\mathcal{M}) > 0$.

References

[1] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, "Quantum-channel capacity of very noisy channels," *Phys. Rev. A*, vol. 57, no. 2, pp. 830–839, Feb 1998.

[2] J. Oppenheim, "For Quantum Information, Two Wrongs Can Make a Right," Science 321, 1783 (2008).

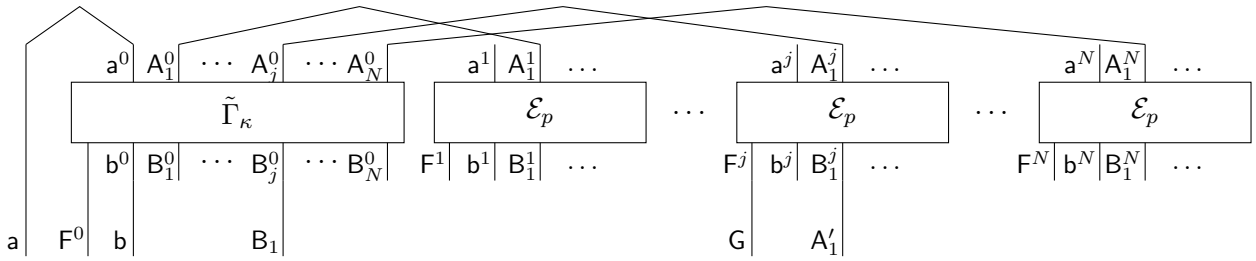

Figure 1: Illustration of the input that demonstrates positive coherent information for $N+1$ channel uses. If one or more of the erasure channels do not erase we select j from among these, and otherwise pick it at random. We show that, for a suitable PPT-binding channel Γ, the coherent information between the reference a and the systems $\mathsf{F}^0\mathsf{b}\mathsf{B}_1\mathsf{G}\mathsf{A}_1'$ is positive.

[3] G. Smith and J. A. Smolin, "Degenerate quantum codes for Pauli channels," *Phys. Rev. Lett.*, vol. 98, no. 3, p. 030501, Jan 2007.

[4] G. Smith and J. Yard, "Quantum communication with zero-capacity channels," *Science*, vol. 321, no. 5897, pp. 1812–1815, 2008.

[5] J. Watrous, "Many copies may be required for entanglement distillation," *Phys. Rev. Lett.*, vol. 93, no. 1, p. 010502, Jul 2004.

[6] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, "General paradigm for distilling classical key from quantum states," *IEEE Trans. Inf. Theory*, vol. 55, no. 4, pp. 1898–1929, April 2009.