

ARTICLE

Received 18 Oct 2014 | Accepted 23 Feb 2015 | Published 31 Mar 2015

DOI: 10.1038/ncomms7739

Unbounded number of channel uses may be required to detect quantum capacity

Toby Cubitt¹, David Elkouss², William Matthews^{1,3}, Maris Ozols¹, David Pérez-García² & Sergii Strelchuk¹

Transmitting data reliably over noisy communication channels is one of the most important applications of information theory, and is well understood for channels modelled by classical physics. However, when quantum effects are involved, we do not know how to compute channel capacities. This is because the formula for the quantum capacity involves maximizing the coherent information over an unbounded number of channel uses. In fact, entanglement across channel uses can even increase the coherent information from zero to non-zero. Here we study the number of channel uses necessary to detect positive coherent information. In all previous known examples, two channel uses already sufficed. It might be that only a finite number of channel uses is always sufficient. We show that this is not the case: for any number of uses, there are channels for which the coherent information is zero, but which nonetheless have capacity.

¹Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, UK. ²Departamento de Análisis Matemático and Instituto de Matemática Interdisciplinar, Universidad Complutense de Madrid, 28040 Madrid, Spain. ³Statistical Laboratory, University of Cambridge, Wilberforce Road, Cambridge CB3 0WB, UK. Correspondence and requests for materials should be addressed to D.E. (email: delkouss@ucm.es).

In the classical case, not only can we exactly characterize the maximum rate of communication over any channel—its capacity—we also have practical error-correcting codes that attain this theoretical limit. It is instructive to review why the capacity of classical channels is a solved problem. Even though optimal communication over a discrete, memoryless classical channel involves encoding the information across many uses of the channel, Shannon showed that a channel's capacity is given by optimizing an entropic quantity (the mutual information) over a single use of the channel. This follows immediately from the fact that mutual information is additive.

It is for this reason that additivity questions for quantum channel capacities took on such importance, and why the major recent breakthroughs proving that additivity is violated^{1,2} had such an impact. A regularized expression for the quantum capacity has been known for some time^{3–5}—the optimization of an entropic quantity (the coherent information I_{coh}) in the limit of arbitrarily many uses of the channel:

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

$$Q(\mathcal{N}) := \lim_{n \rightarrow \infty} Q^{(n)}(\mathcal{N}). \quad (2)$$

Here

$$I_{\text{coh}}(\mathcal{N}^{A \rightarrow B}, \rho^A) := S(\mathcal{N}(\rho^A)) - S(\mathcal{N}(\rho^{\text{AR}})) \quad (3)$$

where $\mathcal{N}^{A \rightarrow B}$ is a channel from A to B, ρ^{AR} is a purification of ρ^A , and S denotes the von Neumann entropy. However, the regularization renders computing the quantum capacity infeasible; it involves an optimization over an infinite parameter space.

Were the coherent information additive, so that $Q^{(n)}(\mathcal{N}) = Q^{(1)}(\mathcal{N})$, the regularization could be removed and the quantum capacity could be computed by a single optimization, similarly to classical channels. However, this is not the case. The first explicit examples of superadditivity were given by Di Vincenzo *et al.*⁶, and extended by Smith *et al.*⁷. For these examples (where \mathcal{N} is a particular depolarizing channel) it was shown (numerically) that $0 \leq Q^{(1)}(\mathcal{N}) < Q^{(n)}(\mathcal{N})$ for small values of $n \leq 33$.

While the classical capacity of quantum channels also involves a regularized formula², we at least know precisely in which cases it is zero: simply for those channels whose output is completely independent of the input. The set of channels with zero quantum capacity is much richer. Indeed, the complete characterization of such channels is unknown. To date, we know of only two kinds of channels with zero quantum capacity: antidegradable channels^{8,9} and entanglement-binding channels¹⁰. The former has the property that the environment can reproduce the output, thus $Q = 0$ by the no-cloning theorem¹¹. The latter can only distribute PPT entanglement, which cannot be distilled by local operations and classical communication¹², again implying $Q = 0$.

This has marked consequences. It is possible to take two channels with no quantum capacity whatsoever ($Q(\mathcal{N}_1) = Q(\mathcal{N}_2) = 0$), \mathcal{N}_1 antidegradable and \mathcal{N}_2 entanglement-binding, which, when used together, do have quantum capacity ($Q(\mathcal{N}_1 \otimes \mathcal{N}_2) > 0$). This 'superactivation' phenomenon was discovered recently by Smith and Yard¹ (and extended in ref. 13). They also show that a single-channel \mathcal{N} , which can be 'switched' between acting like \mathcal{N}_1 or \mathcal{N}_2 , exhibits an extreme form of superadditivity of the coherent information, where $0 = Q^{(1)}(\mathcal{N}) < Q^{(2)}(\mathcal{N})$. Even stronger superactivation phenomena have been shown in the context of zero-error communication^{14–18}.

These recent additivity violation results demonstrate how much we still do not understand about the behaviour of

information in quantum mechanical systems. On the one hand, it means that the known formula for the quantum capacity must be regularized, hence cannot be used to compute the capacity. On the other hand, since the coherent information is additive for unentangled input states, additivity violation also implies that entanglement can protect information from noise in a way that is not possible classically.

But just how badly can additivity be violated? One might hope that, at least in determining whether the quantum capacity is non-zero, one need only consider 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 channels, one might dare to hope that even two uses suffice. (Similarly, for the classical capacity of quantum channels the only known method for constructing examples of additivity violation^{2,19} cannot give a violation for more than two uses of a channel, and there is some evidence that this may be more than just a limitation of the proof techniques²⁰.) Were this the case, one could decide if a channel has quantum capacity by optimizing the coherent information over two uses of the channel, which is not substantially more difficult than the optimization over a single-channel use.

In this paper, we show that this is not the case: additivity violation is essentially as bad as it could possibly be. More precisely (see Fig. 1), we prove that for any n one can construct a channel \mathcal{N} for which the coherent information of n uses is zero ($Q^{(n)}(\mathcal{N}) = 0$), yet for a larger number of uses the coherent information is strictly positive, implying that the channel has non-zero quantum capacity ($Q(\mathcal{N}) > 0$). We also prove that there can be a gap between $Q^{(n)}(\mathcal{N})$ and the quantum capacity for an arbitrarily large number n of uses of the channel. Our result implies that, in general, one must consider an arbitrarily large number of uses of the channel just to determine whether the channel has any quantum capacity at all.

Results

A channel with zero coherent information but positive capacity.

Perhaps the earliest indication that deciding whether a channel has quantum capacity may be difficult comes from the work of Watrous²¹, who showed that an arbitrarily large number of copies of a bipartite quantum state can be required for entanglement distillation assisted by two-way classical communication. Our result can be regarded as the counterpart of²¹ for the quantum capacity (which is mathematically equivalent to entanglement distillation assisted by one-way communication). However, since the proof ideas and techniques of²¹ assume two-way communication, they do not apply in our setting. Our result is instead based on the ideas of Smith and Yard, in particular the intuition provided by Oppenheim's commentary thereon²².

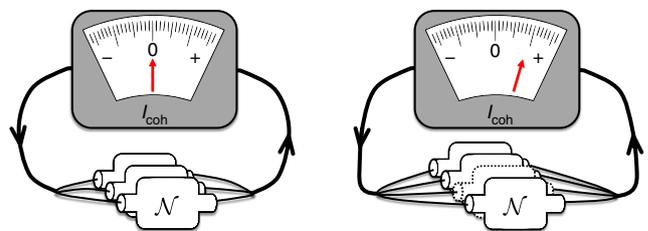


Figure 1 | Positive coherent information can be detected after unbounded uses. Checking the coherent information (I_{coh}) for $n = 3$ uses fails to reveal that channel \mathcal{N} has quantum capacity. However, the channel has capacity and this can be shown by checking some larger number of uses of the channel. We show that for any number of uses of the channel n there are channels with this behaviour.

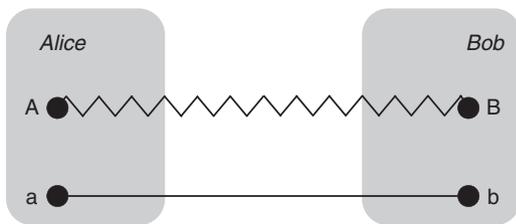


Figure 2 | Pbit representation. A pbit is a bipartite state with subsystems *ab* called the “key” and *AB* called the “shield”. One party, Alice, holds the subsystems *aA* and the other party, Bob, holds the subsystems *bB*

This intuition comes from a class of bipartite quantum states called pbits (private bits)²³, together with the standard equivalences between quantum capacity (sending entanglement over a channel) and distilling entanglement from the state obtained by sending one half of a maximally entangled state through the channel (its Choi–Jamiolkowski state). A pbit ρ_{aAbB} is a state shared between Alice (who holds *aA*) and Bob (who holds *bB*), where the *ab* part of the system is usually called the ‘key’, *AB* the ‘shield’ (see Fig. 2 for a graphical representation and refer to ‘Channel Construction’ in the Supplementary Note 1 for the mathematical details of the pbit construction). For concreteness let us consider a state ρ_{aAbB} of the following form:

$$\rho_{aAbB} = \frac{1}{2}(|\phi^+\rangle\langle\phi^+|_{ab} \otimes \sigma_{AB}^+ + |\phi^-\rangle\langle\phi^-|_{ab} \otimes \sigma_{AB}^-). \quad (4)$$

That is, they hold one of the two states $|\phi^\pm\rangle\langle\phi^\pm|_{ab} \otimes \sigma_{AB}^\pm$ with equal probability. Here $|\phi^\pm\rangle$ are Bell states and σ_{AB}^\pm are hiding states²⁴ encoding the identity of the Bell state. Hiding states are perfectly distinguishable globally, but cannot be distinguished locally using local operations and classical communication. If Alice and Bob knew which Bell state they held, they would have at least one ebit of shared entanglement. But this information, and hence the entanglement, is inaccessible to them unless one party is given the whole-shield *AB*.

Now imagine they have access to a quantum erasure channel $\mathcal{E}_{1/2}$ which with probability 1/2 transmits its input perfectly, but otherwise completely erases it. It is well known that such a channel cannot be used to transmit any entanglement²⁵. However, if they also share ρ_{aAbB} , Alice can use the erasure channel to send her part *A* of the shield to Bob. If the erasure channel transmits, Bob now holds the entire *AB* system and can now distinguish σ_{AB}^\pm . Thus, with probability 1/2, Alice and Bob can now extract the entanglement from ρ_{aAbB} .

Instead of supplying Alice and Bob with the state ρ_{aAbB} and an erasure channel, we supply them with a switched channel. This has an auxiliary classical input that controls whether the channel acts as $\mathcal{E}_{1/2}$ or Γ , where Γ is the channel with Choi–Jamiolkowski state ρ_{aAbB} . The above argument then implies that no quantum information can be sent over a single use of the channel, but it can be sent using two uses, by switching one to $\mathcal{E}_{1/2}$ and the other to Γ .

This is the intuition behind the Smith and Yard construction²². However, it is constructed out of two very particular types of quantum channels, so this idea does not seem to extend to more than two channel uses. Nonetheless, the intuition behind our result is based on a refinement of these ideas, which we now sketch.

Sketch of the general construction. We want to achieve two seemingly contradictory goals: Firstly, to prevent Alice from sending any quantum information to Bob over *n* of uses of the channel, and secondly to permit this when Alice has access to

some larger number of uses $N > n$. We can achieve the first goal by increasing the erasure probability of the erasure channel to something much closer to one, and also adding noise to the Γ channel; the noise then swamps any entanglement. The problem is that this seems to render the second goal impossible. If the channel is so noisy that it destroys all entanglement sent through it, then no amount of coding over multiple uses of the channel can transmit any quantum information.

However, note that the information that Alice needs to send to Bob in order to extract entanglement from the pbit ρ_{aAbB} is essentially classical. Bob just needs to know one classical bit of information to distinguish the two hiding states. This suggests that classical error correction might help Alice send this information to Bob, even when the channel is very noisy. The intuition behind our proof is that a simple classical repetition code suffices. Instead of the pbit ρ_{aAbB} , we use a pbit

$$\frac{1}{2}(|\phi^+\rangle\langle\phi^+|_{ab} \otimes \sigma_{A_1B_1}^+ \otimes \dots \otimes \sigma_{A_NB_N}^+ + |\phi^-\rangle\langle\phi^-|_{ab} \otimes \sigma_{A_1B_1}^- \otimes \dots \otimes \sigma_{A_NB_N}^-) \quad (5)$$

that contains *N* copies of the shield. For Bob to distinguish the hiding states, it suffices for a single copy to make it through the erasure channel. Alice now tries to send all of the copies of the shield through many uses of the erasure channel. However high the erasure probability, the probability that at least one will get through becomes arbitrarily close to one for sufficiently many attempts.

Making the above intuition rigorous is non-trivial: first, we must prove that the coherent information of *n* uses of the channel is strictly zero, for any input to the channel (not just the input states from the above intuition). To this end, we cannot directly use a pbit with *N*-copy shield of the form given above, as it would have distillable entanglement. We must instead adapt an approximate pbit construction from²³. However, we must then take this approximation into account in the proof that the channel does have capacity. This requires a delicate analysis of the various parameters of our channel to show that both of the desired properties can hold simultaneously, which requires a more technical argument described in the Methods section (with full technical details in the Supplementary Note 1).

Discussion

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. It would also be interesting to see if one can obtain a result analogous to ours for the private capacity of quantum channels.

Methods

Channel description. First, let us give a more precise description of our channel. The erasure channel with erasure probability *p* is

$$\mathcal{E}_p^{A \rightarrow FB} := (1-p)|0\rangle\langle 0|^F \otimes \mathcal{I}^{A \rightarrow B} + p|1\rangle\langle 1|^F \otimes \mathbb{1}^B / \dim(B), \quad (6)$$

where, $\mathcal{I}^{A \rightarrow B}$ is the identity channel from *A* to *B*, and *F* is the erasure flag. The channel $\Gamma^{aA \rightarrow bB}$ will belong to the class of PPT entanglement-binding channels whose Choi–Jamiolkowski state is an approximate pbit²³. We show that Γ can be constructed with $A := A_1 \dots A_N$ and $B := B_1 \dots B_N$ consisting of *N* parts, such that even if Bob only receives part *A_i* of Alice’s shield for any *i*, they obtain close to one ebit of one-way distillable entanglement. With the shorthand $\tilde{A} := aA$, and $\tilde{B} := bB$, let $\tilde{\Gamma}_\kappa$ be a noisy version of the channel Γ . More precisely, a composition of Γ with an erasure channel:

$$\tilde{\Gamma}_\kappa^{\tilde{A} \rightarrow \tilde{B}} := \mathcal{E}_\kappa^{\tilde{B} \rightarrow F} \circ \Gamma^{\tilde{A} \rightarrow \tilde{B}}. \quad (7)$$

Our construction uses channels of the form

$$\mathcal{M}^{\bar{S}\bar{A}\rightarrow\bar{S}\bar{F}\bar{B}} := \mathcal{P}_0^{\bar{S}\rightarrow\bar{S}} \otimes \tilde{\Gamma}_{\kappa}^{\bar{A}\rightarrow\bar{F}\bar{B}} + \mathcal{P}_1^{\bar{S}\rightarrow\bar{S}} \otimes \mathcal{E}_p^{\bar{A}\rightarrow\bar{F}\bar{B}}. \quad (8)$$

Here $\mathcal{P}_i^{\bar{S}\rightarrow\bar{S}}$ projects onto the i th computational basis vector of the qubit system \bar{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 \bar{A} . \bar{S} is retained in the output, which lets Bob learn which choice was made.

Proof outline. We now state and outline the proof of our main result—for any number of channel uses there exists a channel with positive capacity but zero coherent information. Formally, we prove the following:

Theorem. Let \mathcal{M} be the channel defined in equation (8). For any positive integer n , if $\kappa \in (0, 1/2)$ and $p \in [(1 + \kappa^n)^{-1/m}]$ then we can choose N and Γ such that:

1. $Q^{(n)}(\mathcal{M}) = 0$ and
2. $Q(\mathcal{M}) > 0$.

The proof 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 (that is, 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: every channel erases, all of the \mathcal{E}_p erase but not all $\tilde{\Gamma}$ erase and at least one of the \mathcal{E}_p does not erase (and therefore acts as the identity channel). The coherent information for second and third cases can be upper bounded, respectively, by zero and $H(R)$, where R is a system that purifies the input. For the first case it is bounded above by $-H(R)$. Weighting by the probabilities, we find that the total coherent information is upper bounded by $(1 - (1 + \kappa^n)p^n)H(R)$. For any n and κ we can therefore find p such that this upper bound is zero.

To prove the second part, we show that for fixed κ , p we can find a Γ with an N -copy shield 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 $0, \dots, N$ 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 select $\tilde{\Gamma}_{\kappa}$ for use 0 and \mathcal{E}_p for the remaining uses $1, \dots, N$. We maximally entangle subsystem A_i^0 of A^0 (which is acted on by $\tilde{\Gamma}_{\kappa}$) with subsystem A_i^1 of A^1 (acted on by an erasure channel). We also maximally entangle subsystem a^0 of A^0 with a purifying reference system, 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 $\tilde{\Gamma}_{\kappa}$ erases, $\tilde{\Gamma}_{\kappa}$ does not erase but all the \mathcal{E}_p erase, and $\tilde{\Gamma}_{\kappa}$ and at least one \mathcal{E}_p do not erase. The first case contributes coherent information -1 weighted by its probability κ . The second case contributes approximately zero coherent information (due to a standard property of pbits). In the third case, after channel use 0, Alice and Bob share the Choi–Jamiołkowski state of Γ on systems $ab^0A_1^1B_1^0 \dots A_N^1B_N^0$, and after the N uses of \mathcal{E}_p at least one of $A_1^1 \dots A_N^1$ reaches Bob unerased. They then share a state with close to 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 $Q(\mathcal{M}) > 0$. Further mathematical details are given in the Supplementary Note 1.

References

1. Smith, G. & Yard, J. Quantum communication with zero-capacity channels. *Science* **321**, 1812–1815 (2008).
2. Hastings, M. B. Superadditivity of communication capacity using entangled inputs. *Nat. Phys.* **5**, 255–257 (2009).
3. Lloyd, S. Capacity of the noisy quantum channel. *Phys. Rev. A* **55**, 1613–1622 (1997).
4. Shor, P. Lecture Notes, MSRI Workshop on Quantum Computation in *Proceedings of Quantum Error Correction* (Berkeley, CA, 2002).
5. Devetak, I. The private classical capacity and quantum capacity of a quantum channel. *IEEE Trans. Inf. Theory* **51**, 44–55 (2005).
6. DiVincenzo, D. P., Shor, P. W. & Smolin, J. A. Quantum-channel capacity of very noisy channels. *Phys. Rev. A* **57**, 830–839 (1998).

7. Smith, G. & Smolin, J. A. Degenerate quantum codes for pauli channels. *Phys. Rev. Lett.* **98**, 030501 (2007).
8. Bennett, C. H., DiVincenzo, D. P. & Smolin, J. A. Capacities of quantum erasure channels. *Phys. Rev. Lett.* **78**, 3217–3220 (1997).
9. Cubitt, T. S., Ruskai, M. B. & Smith, G. The structure of degradable quantum channels. *J. Math. Phys.* **49**, 102104 (2008).
10. Horodecki, P., Horodecki, M. & Horodecki, R. Binding entanglement channels. *J. Mod. Opt.* **47**, 347–354 (2000).
11. Wootters, W. K. & Zurek, W. H. A single quantum cannot be cloned. *Nature* **299**, 802–803 (1982).
12. Horodecki, M., Horodecki, P. & Horodecki, R. Mixed-state entanglement and distillation: is there a “bound” entanglement in nature? *Phys. Rev. Lett.* **80**, 5239–5242 (1998).
13. Brandao, F. G. S. L., Oppenheim, J. & Strelchuk, S. When does noise increase the quantum capacity? *Phys. Rev. Lett.* **108**, 040501 (2012).
14. Alon, N. The Shannon capacity of a union. *Combinatorica* **18**, 301–310 (1998).
15. Cubitt, T. S., Chen, J. & Harrow, A. W. Superactivation of the asymptotic zero-error classical capacity of a quantum channel. *IEEE Trans. Inf. Theory* **57**, 8114–8126 (2011).
16. Chen, J., Cubitt, T. S., Harrow, A. W. & Smith, G. Entanglement can completely defeat quantum noise. *Phys. Rev. Lett.* **107**, 250504 (2011).
17. Cubitt, T. S. & Smith, G. An extreme form of super-activation for quantum zero-error capacities. *IEEE Trans. Inf. Theory* **58**, 1953–1961 (2012).
18. Shirokov, M. E. On channels with positive quantum zero-error capacity having no n -shot capacity. Preprint at <http://arxiv.org/abs/1407.8524> (2014).
19. Hayden, P. & Winter, A. Counterexamples to the maximal p -norm multiplicativity conjecture for all $p > 1$. *Comm. Math. Phys.* **284**, 263–280 (2008).
20. Montanaro, A. Weak multiplicativity for random quantum channels. *Comm. Math. Phys.* **319**, 535–555 (2013).
21. Watrous, J. Many copies may be required for entanglement distillation. *Phys. Rev. Lett.* **93**, 010502 (2004).
22. Oppenheim, J. For Quantum Information, Two Wrongs Can Make a Right. *Science* **321**, 1783–1784 (2008).
23. Horodecki, K., Horodecki, M., Horodecki, P. & Oppenheim, J. General paradigm for distilling classical key from quantum states. *IEEE Trans. Inf. Theory* **55**, 1898–1929 (2009).
24. Egging, T. & Werner, R. F. Hiding classical data in multipartite quantum states. *Phys. Rev. Lett.* **89**, 097905 (2002).
25. Wilde, M. M. *Quantum Information Theory* (Cambridge Univ. Press, 2013).

Acknowledgements

D.E. and D.P. acknowledge financial support from the European CHIST-ERA project CQC (funded partially by MINECO grant PRI-PIMCHI-2011-1071) and from Comunidad de Madrid (grant QUITEMAD + -CM, ref. S2013/ICE-2801). T.S.C. is supported by the Royal Society. M.O. acknowledges financial support from European Union under project QALGO (Grant Agreement No. 600700). S.S. acknowledges the support of Sidney Sussex College. This work was made possible through the support of grant #48322 from the John Templeton Foundation. The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

Author contributions

D.E., D.P.G. and T.S.C. discussed and worked jointly on this result in Madrid; D.E., S.S., W.M., M.O. and T.S.C. discussed and worked jointly on this work in Cambridge; all authors helped to write the article.

Additional information

Supplementary Information accompanies this paper at <http://www.nature.com/naturecommunications>

Competing financial interests: The authors declare no competing financial interest.

Reprints and permission information is available online at <http://npg.nature.com/reprintsandpermissions/>

How to cite this article: Cubitt, T. *et al.* Unbounded number of channel uses may be required to detect quantum capacity. *Nat. Commun.* **6**:6739 doi: 10.1038/ncomms7739 (2015).