# Superadditivity of Private Information for Any Number of Uses of the Channel

David Elkouss[1,2] and Sergii Strelchuk[3]
[1]Departamento de Análisis Matemático and Instituto de Matemática Interdisciplinar, Universidad Complutense de Madrid, 28040 Madrid, Spain
[2]QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, Netherlands
[3]Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, United Kingdom

(Received 4 February 2015; revised manuscript received 16 May 2015; published 20 July 2015)

The quantum capacity of a quantum channel is always smaller than the capacity of the channel for private communication. Both quantities are given by the infinite regularization of the coherent and the private information, respectively, which makes their evaluation very difficult. Here, we construct a family of channels for which the private and coherent information can remain strictly superadditive for unbounded number of uses, thus demonstrating that the regularization is necessary. We prove this by showing that the coherent information is strictly larger than the private information of a smaller number of uses of the channel. This implies that even though the quantum capacity is upper bounded by the private capacity, the nonregularized quantities can be interleaved.

DOI: 10.1103/PhysRevLett.115.040501 PACS numbers: 03.67.Hk, 03.67.Dd

Efficient information transmission is the cornerstone of all information processing tasks in our interconnected world. In the most basic scenario, two parties, linked by a fixed communication channel wish to exchange messages with each other. What is the maximum rate at which they can reliably transmit information?

Classical information theory gives an exhaustive answer to this question [1]. There exists an efficient convex optimization algorithm which takes the description of a channel and calculates its capacity to convey information. This is the consequence of a particularly simple analytic expression for the classical capacity of a channel. Our world is inherently quantum and when we turn to the channels that transmit quantum information we are able to perform many novel information processing tasks which are impossible in the classical theory, such as establishing entanglement between sender and receiver. Presently, when confronted with the above question for the quantum channels, there is no known efficient algorithm that takes the description of an arbitrary channel and calculates its capacity. Different types of capacity of the quantum channel are defined as regularized quantities [2–9], which implies that in order to compute them it is necessary to perform an unbounded optimization over the number of the copies of the channel. In practice it means that to estimate the capacity for $n$ uses of the channel the dimension of the state space which one has to optimize over may increase exponentially in $n$.

Arguably, the biggest practical success of quantum information theory to date is the possibility of quantum key distribution (QKD) [10–12]. QKD allows two distant parties to agree on a secret key independent of any eavesdropper. The required assumptions are access to a quantum channel with positive private capacity and the validity of quantum physics. However, in practice one does not know the quantum channel exactly, and to characterize it one uses a public authentic classical channel. On the other hand, key distribution is a primitive that can only be implemented with classical resources if one is willing to constrain the power of the eavesdropper. Even though there exist practical QKD schemes which enable secure communication over large distances with high key rates [13–16], some of the fundamental questions about the capacity to transmit secure correlations remain unanswered.

There are essentially two quantities that describe the ability of the channel to send secure messages to the receiver, and consequently, generate secret keys. The first one is called private capacity $\mathcal{P}$ [6,17]. It can be viewed as the optimal rate at which the sender, Alice, can send *classical* communication to the receiver, Bob, while keeping Eve in a product state with Alice and Bob. For a quantum channel, which is a completely positive trace-preserving map $\mathcal{N}$, it is given by

$$\mathcal{P}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n}), \tag{1}$$

The private capacity is given by the regularization of $\mathcal{P}^{(1)}(\mathcal{N})$, the private information of the channel

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B) - I(X;E), \tag{2}$$

where the maximum is taken over the set of classical-quantum states $\mathcal{R}$ of the form $\rho^{XA} = \sum_x p_x |x\rangle\langle x|^X \otimes \rho_x^A$, with $X$ being an auxiliary classical register, and $I(X;B)$ the quantum mutual information [18].

 

This capacity also characterizes the optimal rates for key distribution [6,17]. A better understanding of this quantity would allow us to evaluate precisely the usefulness of communications channels for practical QKD links.

In the case of private capacity, the eavesdropper, Eve, is given a purification of the channel output which means that she is as powerful as is allowed by quantum mechanics. However, this setting may be too restrictive for practical applications given the current state of the art in quantum information processing. A natural relaxation of this strong security requirement is to assume that Eve obtains information about the key by performing a measurement on her state. This security requirement is reflected in the second quantity, locking capacity $\mathcal{L}$. By $\mathcal{L}$ we denote all the recently introduced locking capacities [9] of a quantum channel. They are defined by the optimal rate of reliable classical communication requiring Eve to have vanishing accessible information about the message. This difference in the security criterion has striking consequences. For instance, it implies that some channels that have no private capacity have close to maximum locking capacity [19], and for some relevant classes of channels locked communication can be performed at almost the classical capacity rate [20]. The following upper bound is known for the locking capacities:

$$\mathcal{L}(\mathcal{N}) \leq \mathcal{L}_u(\mathcal{N}) = \sup_n \frac{1}{n}\mathcal{L}_u^{(1)}(\mathcal{N}^{\otimes n}), \tag{3}$$

where $\mathcal{L}_u^{(1)}$, which we will call the locking information, is given by

$$\mathcal{L}_u^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B) - I_{\mathrm{acc}}(X;E). \tag{4}$$

The *accessible information* $I_{\mathrm{acc}}(X;E) = \max_\Gamma I(X;Y)$, where $\Gamma$ is the set of all POVMs on $E$.

Two other important types of capacity of a quantum channel are the quantum [2,5,6] and classical capacity [3,4] given by

$$\mathcal{Q}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n}), \tag{5}$$

$$\mathcal{C}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{C}^{(1)}(\mathcal{N}^{\otimes n}), \tag{6}$$

where

$$\mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho^A} H(B) - H(E), \tag{7}$$

$$\mathcal{C}^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B). \tag{8}$$

The optimization of the quantum capacity is performed over all valid states on the input register $A$ while the optimization of the classical capacity is performed over the set $\mathcal{R}$ as in Eq. (1), and $H$ is the von Neumann entropy.

The form of the expression for the capacities in Eqs. (1), (3), (5), and (6) contains the optimization over an *infinite* number of copies of the channel. This is not at all computationally feasible. Do we have to resort to the infinite regularization, or, perhaps, we can stop the regularization after a constant number of uses? It has recently been shown that at least in the case of the quantum capacity the calculation cannot involve a fixed number of channel uses even when we attempt to answer the question whether the channel has any capacity at all [21]. For the classical capacity, which is known to be superadditive for two uses of the channel [22], there is some evidence that ultimately the regularization might not be required [23,24].

Despite the significance of the private and locking information, we still understand very little about its behavior when the communication channel is used many times. Authors in Refs. [25,26] provide evidence that $\mathcal{P}^{(1)}(\mathcal{N})$ is superadditive for a small finite number of channel uses, although the magnitude of this effect is quantitatively very small. Recently, the existence of two quantum channels $\mathcal{N}_1, \mathcal{N}_2$ with $\mathcal{C}(\mathcal{N}_1) \leq 2, \mathcal{P}(\mathcal{N}_2) = 0$ for which $\mathcal{P}(\mathcal{N}_1 \otimes \mathcal{N}_2) \geq 1/2 \log d$, where $d$ is the dimension of the output of the joint channel, has been shown [27]. This example shows that the private capacity is a superadditive quantity (this was also proved in Ref. [28] using a different construction).

Even less is known about the locking capacity. It follows trivially that $\mathcal{L}_u^{(1)}$ is sandwiched between the classical information and the private information [9]:

$$\mathcal{Q}^{(1)}(\mathcal{N}) \leq \mathcal{P}^{(1)}(\mathcal{N}) \leq \mathcal{L}_u^{(1)}(\mathcal{N}) \leq \mathcal{C}^{(1)}(\mathcal{N}). \tag{9}$$

Here we show that private information can be strictly superadditive for an arbitrarily large number of uses of the channel. More precisely, we prove the following theorem:

*Theorem 1.*—For any $n$ there exists a triple $(n, p, d)$ and a quantum channel $\mathcal{N}_{n,p,d}$ such that for $n > k \geq 1$

$$\frac{1}{k}\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k}) < \frac{1}{k+1}\mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k+1}). \tag{10}$$

This proves that entangled inputs increase the private information of a quantum channel and this effect persists for an *arbitrary* number of channel uses. Furthermore, since $\mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}) \leq \mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}) < \mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes 2})/2 \leq \mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes 2})/2 < \ldots < \mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes n})/n \leq \mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes n})/n$ follows from Theorem 1, it turns out that even though the quantum capacity is upper bounded by the private capacity, the nonregularized quantities can be interleaved. As a bonus, we obtain a qualitatively different proof for the unbounded superadditivity of the coherent information [21]. The construction of the latter exhibits a jump from

zero coherent information to positive coherent information between $n_0$ and $n_1$ uses, with $n_0 \ll n_1$; here, we obtain a jump in the coherent information (also in the private information) between consecutive uses for each of the first $n$ uses of the channel for any fixed $n > 1$.

We now introduce the key components of our construction which are required to prove Theorem 1.

*Main construction: Switch channel.*—The action of a channel $\mathcal{N}^{A\to B}$ can be defined via an isometry $V^{A\to BE}$: $\mathcal{N}^{A\to B}(\rho) = \mathrm{tr}_E V\rho V^*$, and its complementary channel is $\mathcal{N}_c^{A\to E}(\rho) = \mathrm{tr}_B V\rho V^*$. Register superscripts are omitted when they do not add to clarity.

We first introduce *switch channels*:

$$\mathcal{N}^{SA\to SB}(\rho^{SA}) = \sum_i P_i^{S\to S} \otimes \mathcal{N}_i^{A\to B}(\rho^{SA}). \tag{11}$$

A switch channel consists of two input registers $S$ and $A$ of dimensions $d$ and $n$, respectively. Register $S$ is measured in the standard basis and conditioned on the measurement outcome $i$; a *component* channel $\mathcal{N}_i$ is applied to the second register. The computation of $\mathcal{P}^{(1)}(\mathcal{N})$ and $\mathcal{L}_u^{(1)}(\mathcal{N})$ when $\mathcal{N}$ is of the form (11) can be simplified; it suffices to restrict inputs to a special form. The equivalent result for the quantum capacity was proved in Ref. [29].

*Lemma 1.*—Consider a switch channel $\mathcal{N}^{SA\to SB}$ and let $\mathcal{T} = \{\rho : \rho = \sum_x p_x |x\rangle\langle x|^X \otimes |s\rangle\langle s|^S \otimes \rho_x^A\}$. Then (1) $\mathcal{P}^{(1)}(\mathcal{N}) = \max_{1\le s<n} \mathcal{P}^{(1)}(\mathcal{N}_s)$, (2) $\mathcal{L}_u^{(1)}(\mathcal{N}) = \max_{1\le s<n} \mathcal{L}_u^{(1)}(\mathcal{N}_s)$. Both $\mathcal{P}^{(1)}(\mathcal{N})$ and $\mathcal{L}_u^{(1)}(\mathcal{N})$ can be achieved by some $\rho \in \mathcal{T}$.

The proof of Lemma 1 is located in the Supplemental Material [30].

There are two types of channels which we will use in place of $\mathcal{N}_i$. The first channel is the erasure channel:

$$\mathcal{E}_{p,d}^{A\to B}(\rho_A) = (1-p)\rho_B + p|e\rangle\langle e|_B, \tag{12}$$

where $|e\rangle\langle e|$ is the erasure flag and $d$ the dimension of the input register $A$. For $p \le 1/2$ the erasure channel is degradable and $\mathcal{Q}(\mathcal{E}_{p,d}) = \mathcal{P}(\mathcal{E}_{p,d}) = \max\{0, (1-2p)\log d\}$, and $\mathcal{C}(\mathcal{E}_{p,d}) = (1-p)\log d$ [31].

For any quantum channel $\mathcal{N}$ used alongside $\mathcal{E}_{p,d}$ the classical information is additive:

*Lemma 2.*—For all quantum channels $\mathcal{N}$

$$\mathcal{C}^{(1)}(\mathcal{N} \otimes \mathcal{E}_{p,d}^{\otimes n}) = \mathcal{C}^{(1)}(\mathcal{N}) + n\mathcal{C}^{(1)}(\mathcal{E}_{p,d}). \tag{13}$$

The proof of Lemma 2 is located in the Supplemental Material [30].

Intuitively, Lemma 2 states that the erasure channel cannot convey more information than an identity channel of dimension $d^{1-p}$, even in the presence of other channels. Furthermore, we can use the classical capacity to obtain a trivial bound for the locking and private information.

The second channel that we use alongside $\mathcal{E}_{p,d}$ is a $d$-dimensional "rocket" channel, $\mathcal{R}_d$ [27]. It consists of two $d$-dimensional input registers $A_1$ and $A_2$ and a $d$-dimensional output register $B$. $A_1$ and $A_2$ are first subject to a random unitary and then jointly decoupled with a controlled dephasing gate. Then, the contents of $A_1$ becomes the output of the channel and the contents of $A_2$ is traced out. Bob also receives the classical description of the unitaries which acted on $A_1$ and $A_2$. Since dephasing occurs after the input registers have been scrambled by a random unitary, it is very hard for Alice to code for such a channel; hence, it has a very low classical capacity: $\mathcal{C}(\mathcal{R}_d) \le 2$.

Our switch channel construction has the following form:

$$\mathcal{N}_{n,p,d} = P_0 \otimes \mathcal{R}_d^n + P_1 \otimes \tilde{\mathcal{E}}_{p,d}^n. \tag{14}$$

That is, it allows Alice to choose between $\mathcal{R}_d^n = \mathcal{R}_d^{\otimes n}$ and $\tilde{\mathcal{E}}_{p,d}^n = \mathcal{E}_{p,d} \otimes \mathcal{E}_{1,d^{2n-1}}$, a $d$-dimensional erasure channel padded with a full erasure channel to match the input dimension of $\mathcal{R}_d^n$.

*Upper bound.*—To upper bound the private information of $\mathcal{N}_{n,p,d}$ we only need to optimize over all the possible different choices of $\mathcal{R}_d^n$ and $\tilde{\mathcal{E}}_{p,d}^n$. Thus, the upper bound for $\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k})$ for $k \ge 1$ reads

$$\begin{aligned}\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k}) &= \max_{0\le i\le k} \mathcal{P}^{(1)}(\mathcal{E}_{p,d}^{\otimes i} \otimes (\mathcal{R}_d^n)^{\otimes k-i}) \\ &\le \max\begin{cases} \mathcal{C}^{(1)}((\mathcal{R}_d^n)^{\otimes k}) \\ \max\limits_{1\le i\le k-1} \mathcal{C}^{(1)}(\mathcal{E}_{p,d}^{\otimes i} \otimes (\mathcal{R}_d^n)^{\otimes k-i}), \\ \mathcal{P}^{(1)}(\mathcal{E}_{p,d}^{\otimes k}) \end{cases} \\ &\le \max\begin{cases} 2kn, \\ (2n + (k-1)(1-p)\log d). \\ (1-2p)k\log d \end{cases}\end{aligned} \tag{15}$$

*Superadditivity of $\mathcal{P}^{(1)}$.*—We denote $A_{xy}^{[k]}$ with superscript $[k]$ to indicate the $k$th use of the channel and the subscript $xy$ to indicate the input register as pictured in Fig. 1.

Consider the following protocol for conveying quantum information over $j+1 > 1$ uses: Alice chooses the rocket channel for the first use and $\mathcal{E}_{p,d}^n$ for the remaining $j$ uses. She prepares a maximally entangled state in the registers $R_z A_{z1}^{[1]}$ and $A_{z2}^{[1]} A_{11}^{[z+1]}$ for $z \in [1, j]$ (see Fig. 2). After the first use of $\mathcal{N}_{n,p,d}$ the registers $A_{11}^{[1]}, A_{21}^{[1]}, \ldots, A_{j1}^{[1]}$ get completely dephased by $\mathcal{R}_d^n$. Without the auxiliary registers $A_{11}^{[2]}, A_{11}^{[3]}, \ldots, A_{11}^{[j+1]}$ Bob is unable to undo the dephasing and thus establish maximally entangled states between the registers $R_1, R_2, \ldots, R_j$ and $B_1, B_2, \ldots, B_j$, respectively. So Alice transmits the former registers using the erasure channel. The input registers $A_{ki}^{[1]}$ of the rocket channel for $k \ge j$, $i = \{1, 2\}$ and the registers that pad the dimension of the erasure channel do not play any role in the

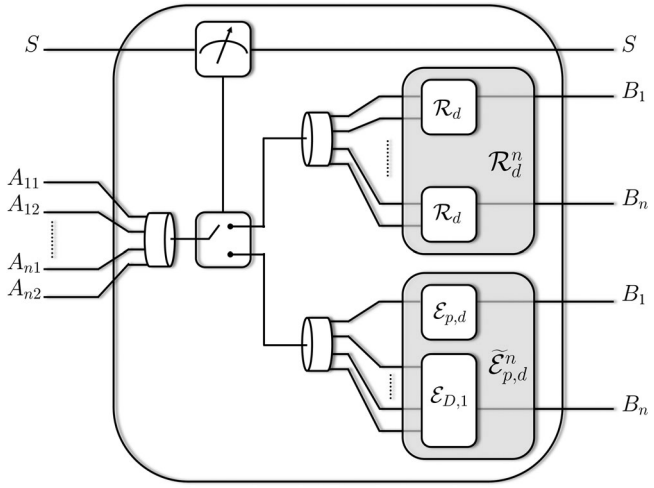


FIG. 1. The channel has two input registers: the control register $S$ and the data register $A = A_{11}A_{12}A_{21}\ldots A_{n2}$. The control register is measured in the computational basis and depending on the output either the erasure channel $\tilde{\mathcal{E}}_{p,d}^n$ or $n$ copies of the $d$-dimensional rocket channel are applied. For each $A_{xy}$, $xy$ enumerates the input register. In particular, when $\mathcal{R}_d^n$ acts on $A$, $x$ denotes the input to the $x$th instance of $\mathcal{R}_d$. For each $\mathcal{R}_d$, while $y$ specifies one of the two inputs to $\mathcal{R}_d$.

protocol, so Alice can send any pure state through each of them. The input state without the padding subsystems has the form

$$\rho = \bigotimes_{z=1}^{j} \left( \Phi^+_{R_z A_{z1}^{[1]}} \otimes \Phi^+_{A_{z2}^{[1]} A_{11}^{[z+1]}} \right), \tag{16}$$

where $\Phi^+_{AB} = 1/d \sum_{i,j=1}^{d} |ii\rangle\langle jj|_{AB}$.

We now analyze the coherent information established by this protocol between Alice and Bob. For every use of the rocket channel, if the auxiliary register gets erased the coherent information is zero—the state is completely dephased in a random basis. If the auxiliary register is transmitted to Bob, he can reverse the action of the channel and obtain a maximally entangled state [27]. This occurs with probability $1 - p$, in which case the coherent information is $\log d$. Since this process is repeated $j$ times, the regularized coherent information is

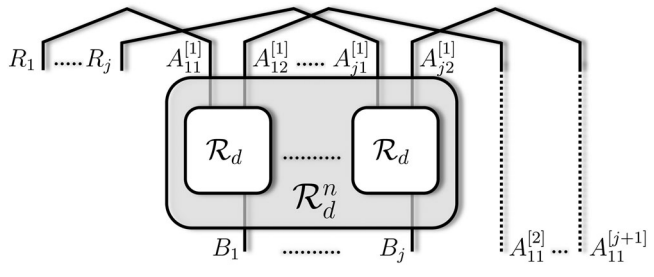


FIG. 2. The first part of the protocol consists in sending a state maximally entangled between the different inputs of the rocket channel and an external reference.

$$\mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes j+1}, \rho) = \frac{j}{j+1}(1-p)\log d. \tag{17}$$

This immediately gives a lower bound for the locking and private information. Now, we are ready to prove Theorem 1.

*Proof.*—Fix $d = 2^{4n^2/(1-2p)}$ and $p = (11/24)$. Then the regularized upper bounds (15) for $\mathcal{P}^{(1)}$ after $k$ uses of the channel have the form $U_k^1 = (2n/k)$, $U_k^2 = \{2n[13(k-1)n+1]/k\}$ and $U_k^3 = 4n^2$; the lower bound (17) after $k+1$ uses of the channel has the form $L_{k+1} = [26kn^2/(k+1)]$.

Consider the differences $D_k^i = -U_k^i + L_{k+1}$ for $i = 1, 2, 3$. Then, a simple substitution shows that $D_k^1 = [26kn^2/(k+1)] - (2n/k)$, $D_k^2 = -[2n(k-13n+1)/k(k+1)]$, $D_k^3 = [2(11k-2)n^2/(k+1)]$. All of the differences are positive for $n > k \geq 1$. □

*Superadditivity of* $\mathcal{L}_u^{(1)}$.—We now study the conditions necessary to obtain a similar result for the locking information of our channel construction. First, we need to establish several bounds about the locking capacity of the channels which are used in it. The locking information of the erasure channel is currently unknown. An upper bound is obtained in the following lemma:

*Lemma 3.*—Let $p \leq 1/2$, the locking information of $\mathcal{E}_{p,d}$ is upper bounded by

$$\mathcal{L}_u^{(1)}(\mathcal{E}_{p,d}) \leq (1-p)\log d - p\gamma_d \log e, \tag{18}$$

where $\gamma_d := \ln d - \sum_{t=2}^{d} t^{-1}$, and $\lim_{d\to\infty}\gamma_d = \gamma$ is Euler's constant.

The proof of Lemma 3 is located in the Supplemental Material [30].

Some algebra shows that the upper bound given by Lemma 3 combined with the lower bound given by Eq. (17) does not yield superadditivity. Our upper bound is very loose and might be improved: we show that if Eve applies the trivial strategy and performs a random measurement on her state, then she would be able to extract the amount of information which is equal to subentropy [32]. The maximum value of the latter is constant and is independent of the dimension. It is natural to conjecture that Eve could extract an amount of information which is proportional to the dimension of her system by applying some other strategy. The smallest bound on Eve's accessible information as a function of the dimension of her output which leads to superadditivity of the locking information in our construction is given below:

*Conjecture 1.*—[Sharper upper bound for $\mathcal{L}_u^{(1)}$]

$$\mathcal{L}_u^{(1)}(\mathcal{E}_{p,d}) \leq (1-p)\log d - p\epsilon \log d, \tag{19}$$

where $\epsilon > [(1-p)/p(n-1)]$.

The proof of the conjecture together with the techniques used in the proof of Theorem 1 would allow us to prove superadditivity.

*Discussion*.—In this Letter we have constructed a family of channels for which the private and coherent information can remain strictly superadditive any number of uses of the channel. We are able to prove this result by showing that the private information of $k$ uses of the channel is smaller than the coherent information of $k+1$ uses. That is, both quantities can be interleaved use after use for the first $n$ uses of the channel. This shows that even though the quantum capacity is upper bounded by the infinite regularization of the private information, the quantum capacity can be larger than a finite regularization of the private information.

Similarly, we expect weak locking information to be superadditive. For this to be true with our channel construction a tighter bound on the accessible information to the environment would be necessary.

The results shown here raise questions about the properties that a channel has to verify such that its different capacities can be computed exactly using only finitely many (preferably only a few) copies of the channel.

We thank David Perez García and Māris Ozols for many useful discussions and feedback. We also thank the referees for the detailed comments. S. S. acknowledges the support of Sidney Sussex College and the European Union under project QALGO (Grant Agreement No. 600700). D. E. acknowledges financial support from the European CHIST-ERA project CQC (funded partially by MINECO Grant No. PRI-PIMCHI-2011-1071) and from Comunidad de Madrid (Grant QUITEMAD + −CM, Ref. S2013/ICE-2801). This work has been partially supported by STW, QuTech and by the project HyQuNet (Grant No. TEC2012-35673), funded by Ministerio de Economía y Competitividad (MINECO), Spain. This work was made possible through the support of Grant No. 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.

[1] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, edited by D. L. Schilling (Wiley, New York, 2001).
[2] S. Lloyd, Phys. Rev. A **55**, 1613 (1997).
[3] A. Holevo, IEEE Trans. Inf. Theory **44**, 269 (1998).
[4] B. Schumacher and M. D. Westmoreland, Phys. Rev. A **63**, 022308 (2001).
[5] P. Shor, *Proceedings of MSRI Workshop on Quantum Computation* (2002).
[6] I. Devetak, IEEE Trans. Inf. Theory **51**, 44 (2005).
[7] R. A. Medeiros and F. M. De Assis, Int. J. Quantum. Inform. **03**, 135 (2005).
[8] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, Rev. Mod. Phys. **86**, 1203 (2014).
[9] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, Phys. Rev. X **4**, 011016 (2014).
[10] C. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing* (IEEE, Bellingham, WA, 1984), p. 175.
[11] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[12] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[13] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photonics **7**, 378 (2013).
[14] K. Shimizu, T. Honjo, M. Fujiwara, T. Ito, K. Tamaki, S. Miki, T. Yamashita, H. Terai, Z. Wang, and M. Sasaki, J. Lightwave Technol. **32**, 141 (2014).
[15] L. Comandar, B. Fröhlich, M. Lucamarini, K. Patel, A. Sharpe, J. Dynes, Z. Yuan, R. Penty, and A. Shields, Appl. Phys. Lett. **104**, 021101 (2014).
[16] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163(2015).
[17] N. Cai, A. Winter, and R. W. Yeung, Probl. Inf. Transm. **40**, 318 (2004).
[18] M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, England, 2013).
[19] A. Winter, arXiv:1403.6361.
[20] C. Lupo and S. Lloyd, Phys. Rev. Lett. **113**, 160502 (2014).
[21] T. Cubitt, D. Elkouss, W. Matthews, M. Ozols, D. Pérez-García, and S. Strelchuk, Nat. Commun. **6**, 6739 (2015).
[22] M. B. Hastings, Nat. Phys. **5**, 255 (2009).
[23] A. Montanaro, Commun. Math. Phys. **319**, 535 (2013).
[24] G. Smith and J. A. Smolin, Nature (London) **504**, 263 (2013).
[25] G. Smith, J. M. Renes, and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008).
[26] O. Kern and J. M. Renes, Quantum Inf. Comput. **8**, 0756 (2008).
[27] G. Smith and J. A. Smolin, Phys. Rev. Lett. **103**, 120503 (2009).
[28] K. Li, A. Winter, X. B. Zou, and G. C. Guo, Phys. Rev. Lett. **103**, 120501 (2009).
[29] M. Fukuda and M. M. Wolf, J. Math. Phys. (N.Y.) **48**, 072101 (2007).
[30] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.115.040501 for the proof of Lemma 2 of the main text.
[31] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).
[32] R. Jozsa, D. Robb, and W. K. Wootters, Phys. Rev. A **49**, 668 (1994).