Quantum Capacity Can Be Greater Than Private Information for Arbitrarily Many Uses

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**
delkouss@ucm.es

2 **QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands**
D.ElkoussCoronas@tudelft.nl

3 **Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, U.K.**
ss870@cam.ac.uk

Abstract

The quantum capacity of a quantum channel is always smaller than the capacity of the channel for private communication. However, both quantities are given by the infinite regularization of respectively the coherent and the private information. Here, we construct a family of channels for which the private and coherent information can remain strictly superadditive for unbounded number of uses. 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. It turns out that even though the quantum capacity is upper bounded by the private capacity, the non-regularized quantities can be interleaved. From an operational point of view, the private capacity can be used for gauging the practical value of quantum channels for secure communication and, consequently, for key distribution. We thus show that in order to evaluate the interest a channel for this task it is necessary to optimize the private information over an unlimited number of uses of the channel.

1998 ACM Subject Classification H.1.1 Systems and Information Theory, E.4 Coding and information theory.

Keywords and phrases Quantum channels, capacity, private information

Digital Object Identifier 10.4230/LIPIcs.TQC.2015.64

1 Introduction

How well is it possible to characterize the resources available to transmit information? In classical information theory, this proves to be fully within our computational abilities: given a description of a channel, answering the question about its capacity to convey information to the receiver is straightforward. However, our world is inherently quantum and when one turns to the channels which transmit quantum information – the amount of resources required to compute their capacities is unknown at best. To compute a number of different types of capacity of the quantum channel, defined as regularized quantities [15, 10, 18, 20, 5, 16, 2, 8], it is necessary to perform an unbounded optimization over the number of the copies of the 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 $\mathcal{N}_c^{A\to E}(\rho) = \mathrm{tr}_B V\rho V^*$. In the following, we will omit the register superscripts when it does not add to clarity.

The quantum and classical capacity of a channel [15, 10, 18, 20, 5] are given by:

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

$$\mathcal{C}(\mathcal{N}) = \lim_{n\to\infty} \frac{1}{n}\mathcal{C}^{(1)}(\mathcal{N}^{\otimes n}) \tag{2}$$

where

$$\mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\rho^A} H(B) - H(E), \tag{3}$$

$$\mathcal{C}^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B). \tag{4}$$

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 $\mathcal{R}$ the set of classical-quantum states of the form $\rho^{XA} = \sum_x p_x|x\rangle\langle x|^X \otimes \rho_x^A$. Where X is an auxiliary classical register, H is the von Neumann entropy and $I(X;B)$ is the quantum mutual information.

From the above expressions it follows that one has to optimize over an *infinite* number of copies of the channel in order to compute its capacity. Do we have to resort to the regularized expression in order to compute the capacity of a quantum channel? It has recently been shown that at least in the case of the quantum capacity this is unavoidable [6, 22] even when we attempt to answer the question whether the channel has any capacity at all [4]. For the classical capacity, which is known to be superadditive for two uses of the channel [9], there is some evidence that ultimately the regularization might not be required [17, 24].

Arguably, the biggest practical success of quantum information theory to date is the possibility of quantum key distribution (QKD). 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[1]. 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 [3, 13, 11, 19], some of the fundamental questions about the capacity to transmit secure correlations remain unanswered.

The private capacity $\mathcal{P}$ of a channel is used to describe the ability of the channel to send secure messages to the receiver [5, 1]. It has a clear operational interpretation as the maximum rate at which the sender, Alice, can send private *classical* communication to the receiver, Bob. It is defined as follows:

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

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

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\rho\in\mathcal{R}} I(X;B) - I(X;E). \tag{6}$$

One can view private capacity as the optimal rate of reliable communication keeping Eve in a product state with Alice and Bob.

[1] In order to characterize the channel and to implement a specific QKD protocol one might need a public authentic classical channel or a small preshared secret.

This capacity characterizes the optimal rates of QKD. A better understanding of this quantity would allow to evaluate precisely the usefulness of communications channels for practical QKD links. For instance, the private capacity of Gaussian channels [25] remains open. Beyond the pure loss channel [27] only lower bounds on the private information of a single use are known.

Despite the significance of the private information, we still understand very little about its behaviour when the communication channel is used many times. Authors in [21, 12] provide evidence that $\mathcal{P}^{(1)}(\mathcal{N})$ is superadditive for two channel uses, although the magnitude of this effect is quantitatively very small. Recently, it has been shown 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 [23]. This example shows that the private capacity is a superadditive quantity (this was also proved in [14] using a different construction).

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 quantum channel $\mathcal{N}_n$ such that for $n > k \geq 1$:*

$$\frac{1}{k}\mathcal{P}^{(1)}(\mathcal{N}_n^{\otimes k}) < \frac{1}{k+1}\mathcal{Q}^{(1)}(\mathcal{N}_n^{\otimes k+1}). \tag{7}$$

This proves that entangled inputs increase the private information of a quantum channel and this effect persists for an *arbitrary* number of channel uses. As a bonus, we obtain a qualitatively different proof for the unbounded superadditivity of the coherent information [4].

The following relation holds for any channel [26]:

$$\mathcal{Q}^{(1)}(\mathcal{N}_n) \leq \mathcal{P}^{(1)}(\mathcal{N}_n) \leq \mathcal{C}^{(1)}(\mathcal{N}_n). \tag{8}$$

This means, that even though the coherent information is upper bounded by the private information and the quantum capacity is upper bounded by the private capacity, Theorem 1 implies that the non-regularized quantities can be interleaved.

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

2 Main construction

We first introduce *switch channels*:

$$\mathcal{N}^{SA\to SB}(\rho^{SA}) = \sum_i P_i^{S\to S} \otimes \mathcal{N}_i^{A\to B}(\rho^{SA}). \tag{9}$$

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 $\mathcal{P}^{(1)}(\mathcal{N})$ when $\mathcal{N}$ is of the form (9) can be simplified; it suffices to restrict inputs to a special form. The equivalent result for the quantum capacity was proved in [7].

▶ **Lemma 2.** *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*

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{1\leq s<n} \mathcal{P}^{(1)}(\mathcal{N}_s), \tag{10}$$

and $\mathcal{P}^{(1)}(\mathcal{N})$ can be achieved by some $\rho \in \mathcal{T}$.

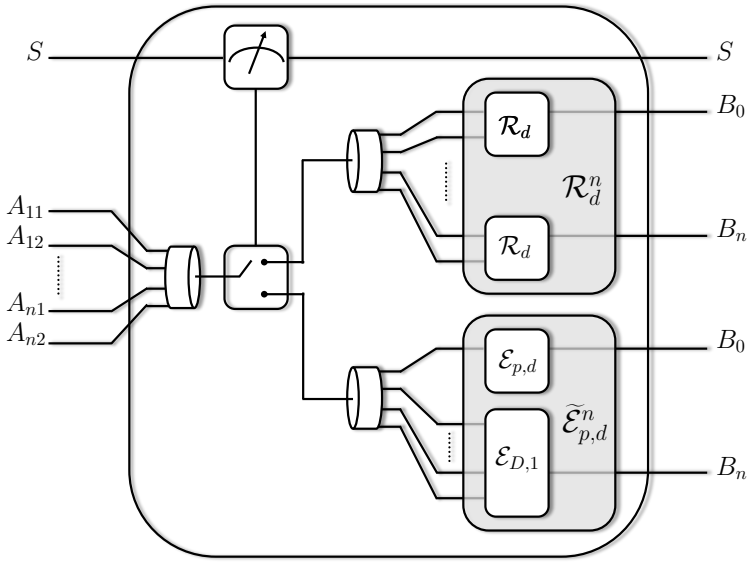

Figure 1 The channel has two input registers the control register S and the data register A. The control register is measured in the computational basis and depending on the output either the erasure channel $\widetilde{\mathcal{E}}_{p,d}^n$ or n copies of the d-dimensional rocket channel are applied.

Proof. The channel complementary to a switch channel is also a switch channel with component channels $\{\mathcal{N}_i^c\}_{i=1}^n$ complementary to $\{\mathcal{N}_i\}_{i=1}^n$ [4]. We denote the output systems of the complementary channel by S and E. Let $\rho \in \mathcal{R}$ be the input state that maximizes $\mathcal{P}^{(1)}(\mathcal{N})$, then $\mathcal{N}$ takes ρ to $\sum_{x,s} p_x p_{s|x} |x\rangle\langle x| \otimes |s\rangle\langle s| \otimes \mathcal{N}_s(\rho_{s|x})$ and $\mathcal{N}^c$ takes ρ to $\sum_{x,s} p_x p_{s|x} |x\rangle\langle x| \otimes |s\rangle\langle s| \otimes \mathcal{N}_s^c(\rho_{s|x})$. The following chain of inequalities holds:

$$
\begin{aligned}
& I(X;BS) - I(X;ES) && (11)\\
&\quad = \sum_s p_s \Big(I(X;B|S=s) - I(X;E|S=s) \Big) && (12)\\
&\quad \leq \max_s \Big(I(X;B|S=s) - I(X;E|S=s) \Big) && (13)\\
&\quad \leq \max_s \mathcal{P}^{(1)}(\mathcal{N}_s). && (14)
\end{aligned}
$$

The first equality follows because S is a classical system. The first inequality follows by choosing the value of s which maximizes the difference between the mutual informations. The second one since the difference between the between the mutual informations to the receiver and the environment is upper bounded by the private information of the channel $\mathcal{N}_s$. This upper bound is achievable by an input state of the form $\sigma^{XSA} = \sum_x p_x |x\rangle\langle x| \otimes |s\rangle\langle s| \otimes \rho_x$ where $\mathrm{tr}_S(\sigma^{XSA})$ is the state that achieves the private information of channel $\mathcal{N}_s$. Finally note that $\sigma^{XSA} \in \mathcal{T}$. ◀

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

$$\mathcal{E}_{p,d}^{A\to B}(\rho_A) = (1-p)\rho_B + p|e\rangle\langle e|_B \qquad (15)$$

where $|e\rangle\langle e|$ is the erasure flag and d the dimension of the input register A. For $p \leq 1/2$ 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 $\mathcal{C}(\mathcal{E}_{p,d}) = (1-p)\log d$.

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

▶ **Lemma 3.** *For all quantum channels* $\mathcal{N}$

$$\mathcal{C}^{(1)}\left(\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n}\right)=\mathcal{C}^{(1)}(\mathcal{N})+n\mathcal{C}^{(1)}(\mathcal{E}_{p,d}). \tag{16}$$

Proof. The inequality $\mathcal{C}^{(1)}\left(\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n}\right)\geq\mathcal{C}^{(1)}(\mathcal{N})+n\mathcal{C}^{(1)}(\mathcal{E}_{p,d})$ is trivial. In order to prove the other direction consider the following chain of inequalities:

$$\begin{aligned}
\mathcal{C}^{(1)}(\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n}) &= \mathcal{C}^{(1)}(\mathcal{M}\otimes\mathcal{E}_{p,d}) && (17)\\
&= \max_{\rho} I(X;B_1B_2) && (18)\\
&= \max_{\rho}(1-p)I(X;B_1A_2)+pI(X;B_1) && (19)\\
&\leq (1-p)\mathcal{C}^{(1)}(\mathcal{M}\otimes I)+p\mathcal{C}^{(1)}(\mathcal{M}) && (20)\\
&= \mathcal{C}^{(1)}(\mathcal{M})+(1-p)\log d && (21)\\
&= \mathcal{C}^{(1)}(\mathcal{N})+n(1-p)\log d. && (22)
\end{aligned}$$

The first equality follows by identifying $\mathcal{M}$ with $\mathcal{N}\otimes\mathcal{E}_{p,d}^{\otimes n-1}$. We let A_1, A_2 and B_1, B_2 be the input and output of $\mathcal{M}$ and $\mathcal{E}_{p,d}$ respectively. The second equality is just the definition of the classical information (see Eq. 2). The third equality breaks the mutual information depending on the erasure channel transmitting or erasing. The inequality follows by maximizing each of the two mutual informations individually. The fourth inequality follows by taking into account that the classical information of the identity is additive and the last one by applying the same argument recursively for $n-1$ times. ◀

Intuitively, Lemma 3 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 expression for the classical capacity to obtain a trivial bound for the private information. It turns out that this trivial bound is tight and is saturated by the channel construction that we introduce below.

The second channel that we use alongside $\mathcal{E}_{p,d}$ is a d-dimensional 'rocket' channel, $\mathcal{R}_d$ [23]. 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 channel, hence it has a very low classical capacity: $\mathcal{C}(\mathcal{R}_d)\leq 2$.

Our switch channel construction has the following form:

$$\mathcal{N}_{n,p,d}=P_0\otimes\mathcal{R}_d^n+P_1\otimes\widetilde{\mathcal{E}}_{p,d}^n \tag{23}$$

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

2.1 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 $\widetilde{\mathcal{E}}_{p,d}^n$. Thus, the upper bound for $\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k})$ for $k\geq 1$

reads:

$$\begin{aligned}\mathcal{P}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes k}) &= \max_{0\leq i\leq k} \mathcal{P}^{(1)}(\mathcal{E}_{p,d}^{\otimes i}\otimes(\mathcal{R}_d^n)^{\otimes k-i}) \\ &\leq \max\begin{cases} \mathcal{C}^{(1)}((\mathcal{R}_d^n)^{\otimes k}) \\ \max\limits_{1\leq i\leq k-1} \mathcal{C}^{(1)}(\mathcal{E}_{p,d}^{\otimes i}\otimes(\mathcal{R}_d^n)^{\otimes k-i}), \\ \mathcal{P}^{(1)}(\mathcal{E}_{p,d}^{\otimes k}) \end{cases} \\ &\leq \max\begin{cases} 2kn, \\ (2n+(k-1)(1-p)\log d)\,. \\ (1-2p)\,k\log d \end{cases} \end{aligned} \tag{24}$$

2.2 Superadditivity of $\mathcal{P}^{(1)}$

First, we present the input state such that for $j > i$ uses and for some range of parameters allows to conclude that the private information for j uses is higher than the upper bound (24) for i uses. This state has the form:

$$\rho = \bigotimes_{k=1}^{j-1}\left(\Phi^+_{\widetilde{A}_k A_{k1}^{[1]}}\otimes\Phi^+_{A_{k2}^{[1]}A_{11}^{[k+1]}}\otimes\sigma_A\right) \tag{25}$$

where $\Phi^+_{AB} = 1/d\sum_{i,j=1}^d |ii\rangle\langle jj|$. For the first use Alice chooses the rocket channel and for the remaining $j-1$ uses of the channel she selects $\mathcal{E}_{p,d}^n$. We denote with superscript $[k]$ the k-th use of the channel and the subscript ij indicates the input register as pictured in Fig. 1. The state can be read operationally as follows: Alice keeps the $\widetilde{A}_{km}$ registers and sends $A_{k1}^{[1]}$ through the first input of k-th $\mathcal{R}_d$ channel, $A_{k2}^{[1]}$ through the second (which will be subsequently discarded by the channel) and $A_{11}^{[k]}$ through $\mathcal{E}_{p,d}$. The remaining inputs do not play any role, so Alice can send any pure state σ_A through $\mathcal{E}_{D,1}$ and $\mathcal{R}_d^{[k]}$ for $k > j$. It is easy to verify that:

$$\mathcal{Q}^{(1)}(\mathcal{N}_{n,p,d}^{\otimes j},\rho) = \frac{(j-1)(1-p)}{j}\log d. \tag{26}$$

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

Proof.

Fix $d = 2^{4n^2/(1-2p)}$ and $p = \frac{11}{24}$. Then the regularized upper bounds (24) for $\mathcal{P}^{(1)}$ after k uses of the channel have the form:

$$U_k^1 = \frac{2n}{k}, \tag{27}$$

$$U_k^2 = \frac{2n(13(k-1)n+1)}{k} \tag{28}$$

and

$$U_k^3 = 4n^2; \tag{29}$$

the lower bound (26) after $k+1$ uses of the channel has the form:

$$L_{k+1} = \frac{26kn^2}{k+1}. \tag{30}$$

Consider the differences $D_k^i = -U_k^i + L_{k+1}$ for $i = 1, 2, 3$. Then, a simple substitution shows that:

$$D_k^1 = \frac{26kn^2}{k+1} - \frac{2n}{k}, \tag{31}$$

$$D_k^2 = -\frac{2n(k-13n+1)}{k(k+1)} \tag{32}$$

and

$$D_k^3 = \frac{2(11k-2)n^2}{k+1}. \tag{33}$$

All of the differences are positive for $n > k \geq 1$. ◀

The results of the theorem indicate that in order to compute the *exact* private capacity of a channel $\mathcal{N}$ it is necessary to compute $\mathcal{P}^{(1)}(\mathcal{N}^{\otimes n})$ for an arbitrary number of uses n. In addition, we found an example whereby for each n and $1 \leq k < n$ having access to one additional copy of the channel up to n provides the parties with the largest possible gain in the capacity, proportional to the output dimension of the channel. Note, that for the channel $\mathcal{N}_{n,p,d}$ strict superadditivity of both private and coherent information holds for all number of uses of the channel up to n. This is markedly different from all previously known channel constructions which exhibit various superadditivity effects for quantum channel capacities. Such constructions exhibited superadditivity for some fixed number of uses of the channel t versus $t + c$ for some c. Our construction above shows that the private and coherent information of the *same* channel can be strictly superadditive for an arbitrary number of channel uses.

3 Discussion

In this paper 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.

The private capacity of a quantum channel characterizes its ability to convey classical information securely. We proved that in order to compute the private capacity it is necessary to consider regularized expressions (5).

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.

Acknowledgements. We thank David Perez García and Māris Ozols for many useful discussions and feedback. SS acknowledges the support of Sidney Sussex College and European Union under project QALGO (Grant Agreement No. 600700). DE acknowledges 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). 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 #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.

References

1 Ning Cai, Andreas Winter, and Raymond W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40(4):318–336, 2004.

2 Filippo Caruso, Vittorio Giovannetti, Cosmo Lupo, and Stefano Mancini. Quantum channels and memory effects. *Reviews of Modern Physics*, 86(4):1203–1259, December 2014.

3 L. C. Comandar, B. Fröhlich, M. Lucamarini, K. A. Patel, A. W. Sharpe, J. F. Dynes, Z. L. Yuan, R. V. Penty, and A. J. Shields. Room temperature single-photon detectors for high bit rate quantum key distribution. *Applied Physics Letters*, 104(2):021101, 2014.

4 Toby Cubitt, David Elkouss, William Matthews, Maris Ozols, David Pérez-García, and Sergii Strelchuk. Unbounded number of channel uses may be required to detect quantum capacity. *Nat Commun*, 6, 03 2015.

5 I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *Information Theory, IEEE Transactions on*, 51(1):44–55, Jan 2005.

6 David P. DiVincenzo, Peter W. Shor, and John A. Smolin. Quantum-channel capacity of very noisy channels. *Phys. Rev. A*, 57(2):830–839, Feb 1998.

7 Motohisa Fukuda and Michael M. Wolf. Simplifying additivity problems using direct sum constructions. *Journal of mathematical physics*, 48(7):072101, 2007.

8 Saikat Guha, Patrick Hayden, Hari Krovi, Seth Lloyd, Cosmo Lupo, Jeffrey H. Shapiro, Masahiro Takeoka, and Mark M. Wilde. Quantum enigma machines and the locking capacity of a quantum channel. *Physical Review X*, 4(1):011016, 2014.

9 Matthew B. Hastings. Superadditivity of communication capacity using entangled inputs. *Nature Physics*, 5(4):255–257, Apr 2009.

10 A. S. Holevo. The capacity of the quantum channel with general signal states. *IEEE Transactions on Information Theory*, 44(1):269–273, January 1998.

11 Paul Jouguet, Sébastien Kunz-Jacques, Anthony Leverrier, Philippe Grangier, and Eleni Diamanti. Experimental demonstration of long-distance continuous-variable quantum key distribution. *Nature Photonics*, 7(5):378–381, 2013.

12 Oliver Kern and Joseph M. Renes. Improved one-way rates for bb84 and 6-state protocols. *Quantum Information & Computation*, 8(8):756–772, 2008.

13 Boris Korzh, Charles Ci Wen Lim, Raphael Houlmann, Nicolas Gisin, Ming Jun Li, Daniel Nolan, Bruno Sanguinetti, Rob Thew, and Hugo Zbinden. Provably secure and practical quantum key distribution over 307 km of optical fibre. *Nature Photonics*, 2015.

14 Ke Li, Andreas Winter, XuBo Zou, and GuangCan Guo. Private capacity of quantum channels is not additive. *Phys. Rev. Lett.*, 103(12):120501, Sep 2009.

15 Seth Lloyd. Capacity of the noisy quantum channel. *Phys. Rev. A*, 55(3):1613–1622, Mar 1997.

16 Rex A. C. Medeiros and Francisco M. De Assis. Quantum zero-error capacity. *International Journal of Quantum Information*, 3(01):135–139, 2005.

17 Ashley Montanaro. Weak multiplicativity for random quantum channels. *Communications in Mathematical Physics*, 319(2):535–555, 2013.

18 Benjamin Schumacher and Michael D. Westmoreland. Optimal signal ensembles. *Physical Review A*, 63(2):022308, January 2001.

19 Kaoru Shimizu, Toshimori Honjo, Mikio Fujiwara, Toshiyuki Ito, Kiyoshi Tamaki, Shigehito Miki, Taro Yamashita, Hirotaka Terai, Zhen Wang, and Masahide Sasaki. Performance of long-distance quantum key distribution over 90-km optical links installed in a field environment of tokyo metropolitan area. *Journal of Lightwave Technology*, 32(1):141–151, 2014.

20 Peter W. Shor. The quantum channel capacity and coherent information, 2002. Lecture Notes, MSRI Workshop on Quantum Computation.

21 Graeme Smith, Joseph M. Renes, and John A. Smolin. Structured codes improve the bennett-brassard-84 quantum key rate. *Phys. Rev. Lett.*, 100(17):170502, 2008.

22 Graeme Smith and John A. Smolin. Degenerate quantum codes for pauli channels. *Phys. Rev. Lett.*, 98(3):030501, Jan 2007.

23 Graeme Smith and John A. Smolin. Extensive nonadditivity of privacy. *Phys. Rev. Lett.*, 103(12):120503, Sep 2009.

24 Graeme Smith and John A. Smolin. An exactly solvable model for quantum communications. *Nature*, 504:263–267, 2013.

25 Christian Weedbrook, Stefano Pirandola, Raúl García-Patrón, Nicolas J. Cerf, Timothy C. Ralph, Jeffrey H. Shapiro, and Seth Lloyd. Gaussian quantum information. *Rev. Mod. Phys.*, 84:621–669, May 2012.

26 M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2013.

27 Michael M. Wolf, David Pérez-García, and Geza Giedke. Quantum capacities of bosonic channels. *Phys. Rev. Lett.*, 98:130501, Mar 2007.