Non-convexity of private capacity and classical environment-assisted capacity of a quantum channel

David Elkouss[1] and Sergii Strelchuk[2]

[1] *QuTech, Delft University of Technology, Lorentzweg 1, 2628 CJ Delft, The Netherlands*
[2] *Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge CB3 0WA, U.K.*

The capacity of classical channels is convex. This is not the case for the quantum capacity of a channel: the capacity of a mixture of different quantum channels exceeds the mixture of the individual capacities and thus is non-convex. Here we show that this effect goes beyond the quantum capacity and holds for the private and classical environment-assisted capacities of quantum channels.

Introduction

Classical information theory was laid down by Shannon in the nineteen forties to characterize the ultimate rate at which one could hope to transmit classical information over a classical communication channel: the channel capacity. Surprisingly in retrospective, not only it achieved its purpose but the capacity of classical channels turned out to comply with all the properties that one could expect for such a quantity: it can be efficiently computed [1, 2] and it gauges the usefulness of the channel in the presence of any additional contextual channel. It is a natural consequence of additivity and convexity of the capacity in the set of channels.

With quantum channels complemented by various auxiliary resources, a whole new range of communication tasks became feasible. Notably, they allow for the transmission of quantum and private classical communication – tasks beyond the reach of classical channels. For most of these tasks, the tools used to prove the capacity theorems in the classical case can be generalized. However, computability, additivity, and convexity — the three convenient properties of the classical capacity of classical channels — do not necessarily translate to the quantum case. In Table I we summarize what is known about these properties for a set of relevant quantum channel capacities.

With the exception of the entanglement-assisted capacity [3, 4], there is no known algorithm to compute any of these capacities. It is due to their characterization which in most cases is given by a regularized formula [5–15]. Moreover, even non-regularized quantities are notoriously hard to compute. For instance, the Holevo information is known to be NP-complete [16].

A capacity is non-additive as a function of a channel if for a given pair of channels the sum of their individual capacities is strictly smaller than the capacity of another channel which is constructed by using both channels in parallel. Hence, a non-additive capacity is contextual: the usefulness of a channel for communication depends on what other channels are available. The private and quantum capacities are known to be non-additive [17–19]. This observation motivated authors in [15] to define a new quantity – the potential capacity – which characterizes the usefulness of a channel used in parallel with the best possible contextual channel.

Another important property of the capacities of quantum channels is convexity. The capacity $\mathcal{T}$ of a quantum channel $\mathcal{N}$ is non-convex if there exists a pair of channels $\mathcal{N}_1$ and $\mathcal{N}_2$ and $p \in (0,1)$ such that:

$$p\mathcal{T}(\mathcal{N}_1) + (1-p)\mathcal{T}(\mathcal{N}_2) < \mathcal{T}(p\mathcal{N}_1 + (1-p)\mathcal{N}_2). \quad (1)$$

In a same vein, non-convexity also implies that capacity is contextual. For a channel $\mathcal{N}$, a contextual channel $\mathcal{M}$ and a mixing parameter $p \in (0,1)$ we can define a non-convexity functional:

$$\mathcal{G}_{p,\mathcal{M}}(\mathcal{N}) = 1/p\,[\mathcal{T}(p\mathcal{N} + (1-p)\mathcal{M}) - (1-p)\mathcal{T}(\mathcal{M})] \quad (2)$$

analogous to the one defined in [15] for non-additivity. This functional induces a (new) potential capacity given by the maximization of $\mathcal{G}_{p,\mathcal{M}}(\mathcal{N})$ over all contextual channels $\mathcal{M}$ and $p \in (0,1]$. If $\mathcal{T}$ is non-convex, then there exists a channel $\mathcal{N}$ such that its potential capacity is strictly larger than $\mathcal{T}(\mathcal{N})$ or, equivalently, there exists a triple $p, \mathcal{N}, \mathcal{M}$ for which $\mathcal{G}_{p,\mathcal{M}}(\mathcal{N}) > \mathcal{T}(\mathcal{N})$.

Non-convexity is a surprising property in connection to two communication scenarios in which Alice, the sender, has access to two channels that are used with probabilities p and $1-p$. In the first one, Alice uses both channels independently. In the second one, Alice encodes jointly over the two channels but has no control over which of the channels is applied; instead, a black box applies them at random with the same probabilities p and $1-p$. The two scenarios are depicted in Fig. 1.

In contrast to the classical capacity of classical channels, it was shown that the capacity of quantum channels for transmitting quantum information, i.e. the quantum

	Computability	Additivity	Convexity
$\mathcal{Q}$	?	No [17]	No [17]
$\mathcal{P}$	?	No [18, 19]	No
$\mathcal{C}$	?	?	?
$\mathcal{C}_e$	Yes [4]	Yes [3]	Yes [3, 4]
$\mathcal{C}_H$	?	No [14]	No

TABLE I. Main properties of quantum channel capacities: convexity, additivity, and computability. We consider quantum capacity $\mathcal{Q}$, private capacity $\mathcal{P}$ and unassisted, entanglement-assisted and environment-assisted classical capacities, $\mathcal{C}$, $\mathcal{C}_e$ and $\mathcal{C}_H$ respectively.

capacity, is non-convex [17]. The question that we address in the following is whether non-convexity is limited to the transmission of quantum information or can be observed beyond the task of entanglement transmission. We show that the private capacity and the classical environment-assisted capacities of a quantum channel are non-convex.

Communication tasks

The action of a quantum channel can always be defined by an isometry V that takes the input system A' to the output B together with an auxiliary system called the environment E: $\mathcal{N}^{A'\to B}(\rho^{A'}) = \mathrm{tr}_E V^{A'\to BE}\rho^{A'}(V^{A'\to BE})^\dagger$. This isometry allows to define the action of the complementary channel: $\hat{\mathcal{N}}^{A'\to E}(\rho^{A'}) = \mathrm{tr}_B V^{A'\to BE}\rho^{A'}(V^{A'\to BE})^\dagger$. We denote the systems involved by a superscript, which we omit when they are clear from the context.

Let ρ^A be a quantum state, we denote by $H(A) = -\mathrm{tr}\rho\log\rho$ the von Neumann entropy. Let ρ^{AB} be a bipartite quantum state, we denote by $I(A;B) = H(A) + H(B) - H(AB)$ the mutual information between the systems A and B.

We are interested in the following communication tasks and the associated channel capacities.

The first task is the transmission of quantum information. The quantum capacity characterizes the ability of a quantum channel for this task in the absence of additional resources [5, 8, 10]

$$\mathcal{Q}(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes n}), \tag{3}$$

where $\mathcal{Q}^{(1)}(\mathcal{N}) = \max_{\phi^{AA'}}\mathcal{Q}^{(1)}(\mathcal{N},\phi^{AA'})$ is the coherent information of a quantum channel. The maximum is taken over all input states purified with a reference system A. The quantity $\mathcal{Q}^{(1)}(\mathcal{N},\phi^{AA'}) = H(B) - H(AB)$, where $H(B), H(AB)$ are the von Neumann entropies of $\rho^B = \mathcal{N}(\mathrm{tr}_{A'}\phi^{AA'})$, $\rho^{AB} = \mathsf{id}^A \otimes \mathcal{N}^{A'\to B}(\phi^{AA'})$ and id denotes the identity channel.

For some channels, the coherent information is additive and thus exactly characterizes their capacity. In these cases, it is possible to compute the capacity exactly [20]. However, there are examples when this is not the case [21, 22]: coherent information is superadditive. Not only the coherent information is superadditive, but also, the quantum capacity itself is superadditive [17, 23] – there exist pairs of channels such that their joint capacity is strictly larger than the sum of their capacities.

The second task is the transmission of private classical information. The capacity of a channel for this task without additional resources is called the private capacity [9, 10]. We define the private information to be

$$\mathcal{P}^{(1)}(\mathcal{N}) = \max_{\sum_x p_x|x\rangle\langle x|^X\otimes\rho^{A'}} I(X;B) - I(X;E), \tag{4}$$

where $I(X;B)$ and $I(X;E)$ are evaluated on the states $\mathsf{id}^X \otimes \mathcal{N}^{A'\to B}(\sum_x p_x|x\rangle\langle x|^X \otimes \rho^{A'})$ and $\mathsf{id}\otimes\hat{\mathcal{N}}^{A'\to E}(\sum_x p_x|x\rangle\langle x|^X\otimes\rho^{A'})$. The private capacity is given by the regularization of the private information

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

Both private information [24–26] and the private capacity [18, 19, 27] were found to be superadditive.

The third task is the transmission of classical information. The classical capacity [6, 7] characterizes the capacity of a quantum channel for transmitting classical information without additional resources. To characterize the classical capacity we first define the Holevo information

$$\mathcal{C}^{(1)}(\mathcal{N}) = \max_{\sum_x p_x|x\rangle\langle x|^X\otimes\rho^{A'}} I(X;B). \tag{6}$$

The classical capacity is given by the regularization of the Holevo information

$$\mathcal{C}(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\mathcal{C}^{(1)}(\mathcal{N}^{\otimes n}). \tag{7}$$

Holevo information is superadditive [28] but it is a challenging open question whether or not the classical capacity verifies any of the three properties of convexity, additivity, and computability.

In some scenarios, sender and receiver may share additional resources which they can leverage to increase their communication rates. The capacities of a channel for a communication task assisted by additional resources turn out to have completely different properties than their unassisted counterparts. One such example is shared entanglement. The entanglement-assisted classical capacity of a quantum channel $\mathcal{C}_e(\mathcal{N})$ is both convex and additive and can be computed efficiently [4].

Alternatively, one may consider the environment of the channel as a friendly helper that 'assists' the sender during information transmission [29]. This third party can input states independently of the sender or even interact with the sender by exchanging messages. This gives rise to a host of environment-assisted classical capacities depending on whether we have active or passive environment assistance [13] or whether the sender and environment are allowed to share entanglement or interact by means of local operations and classical communication. In our work, we focus on the weakest variant of assistance for classical communication when the helper is in the product state with the sender [14]. The corresponding capacity is given by

$$\mathcal{C}_H(\mathcal{N}) = \lim_{n\to\infty}\frac{1}{n}\max_\eta \mathcal{C}^{(1)}(\mathcal{N}_\eta^{\otimes n}), \tag{8}$$

where $\mathcal{N}_\eta^{\otimes n}(\rho) = \mathrm{tr}_F W^{\otimes n}(\rho\otimes\eta)(W^{\otimes n})^\dagger$. $W^{AE\to BF}$ is an isometric extension of the channel such that: $\mathcal{N}^{A\to B}(\rho^A) = \mathrm{tr}_F W\rho^A\otimes|0\rangle\langle 0|^E W^\dagger$ and η is a state of the system E over n uses of the channel.

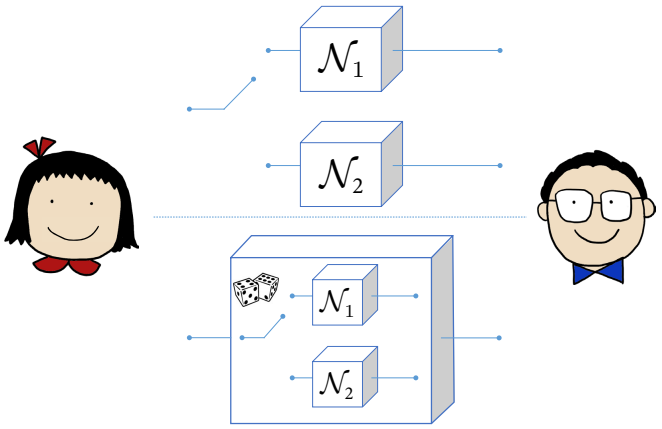

FIG. 1. Operational interpretation of non-convexity. Above, Alice has full control over which channel is applied in the transmission, but she has to apply each channel with some probability. Below, a black box chooses the channel for Alice (with the same probabilities). Non-convexity implies that Alice might communicate at a strictly higher rate in the scenario below.

Private capacity

We first show that private capacity is non-convex. Let us first define two families of channels. The first is the d-dimensional erasure channel $\mathcal{E}_{d,p}$. Its action is defined as follows:

$$\mathcal{E}_{d,p}(\rho) = (1-p)\rho + p|e\rangle\langle e|. \tag{9}$$

That is, $\mathcal{E}_{d,p}$ takes the input to the output with probability $1-p$ and with probability p it outputs an erasure flag. The private capacity of the erasure channel is known to be [20]:

$$\mathcal{P}\left(\mathcal{E}_{d,p}\right) = \max\{0, (1-2p)\log d\}. \tag{10}$$

The second is the 'rocket channel' R_d. It was introduced by Smith and Smolin in [19]. It takes two d-dimensional inputs that we label C and D. The channel chooses two unitaries U and V at random [30] and applies them to C and D respectively, followed by the application of a joint dephasing operation P. The map is given by $P = \sum_{ij} \omega^{ij}|i\rangle\langle i|\otimes|j\rangle\langle j|$ with ω being a primitive d-th root of unity. Finally, the first system is traced out and the second system together with a classical description of U and V is sent to the receiver. Given U and V the action of the channel can be written as

$$R_d^{UV}(\rho) = \mathrm{tr}_C\left(PUV\rho^{CD}\left(PUV\right)^*\right)\otimes|U\rangle\langle U|\otimes|V\rangle\langle V|\,, \tag{11}$$

where $PUV = P\cdot(U\otimes V)$. The total action of the channel is the average

$$R_d(\rho) = \mathbb{E}_{UV} R_d^{UV}(\rho). \tag{12}$$

Rocket channels have small classical capacity for $d \geq 9$ [19]:

$$0 < \mathcal{C}(R_d) \leq 2. \tag{13}$$

Now let us consider a convex combination of a flagged erasure channel and a flagged rocket channel:

$$\mathcal{N}_{q,d,p} = q\mathcal{N}^1_{d,p} + (1-q)\mathcal{N}^2_d. \tag{14}$$

where $\mathcal{N}^1_{d,p} = \mathcal{E}_{d^2,p}\otimes|0\rangle\langle 0|$ and $\mathcal{N}^2_d = R_d\otimes|1\rangle\langle 1|$.

In the following we prove that for some ranges of d, p and q

$$\mathcal{P}(\mathcal{N}_{q,d,p}) > q\mathcal{P}(\mathcal{N}^1_{d,p}) + (1-q)\mathcal{P}(\mathcal{N}^2_d). \tag{15}$$

The right-hand side of (15) is bounded from above by

$$q\cdot\max\{0,(1-2p)2\log d\} + 2(1-q). \tag{16}$$

We can bound $\mathcal{P}(\mathcal{N}_{q,d,p})$ from below by $\mathcal{Q}(\mathcal{N}_{q,d,p})$. Hence, we can argue that any achievable rate for quantum communication (itself a lower bound on the quantum capacity) is a lower bound on the private capacity. Let $\rho^{A^1A^2C_1D_1C_2D_2}$ be some input for two uses of channel $\mathcal{N}_{q,d,p}$. Then:

$$\mathcal{P}(\mathcal{N}_{q,d,p}) \geq \mathcal{Q}(\mathcal{N}_{q,d,p}) \geq \frac{1}{2}\mathcal{Q}^{(1)}\left(\mathcal{N}^{\otimes 2}_{q,d,p},\rho\right). \tag{17}$$

Now, let the input be:

$$\rho^{A^1A^2C_1D_1C_2D_2} = \Phi^{A^1D_1}\otimes\Phi^{C_1C_2}\otimes\Phi^{A^2D_2}, \tag{18}$$

where Φ^{AB} represents a maximally entangled state between systems A and B. We use a subscript if the register corresponds to a concrete channel use and a superscript to number the subsystem: C^1_2 stands for the first subsystem of the register C in the second use of the channel and A^2 the second subsystem of an auxiliary register A.

The coherent information achieved by (18) is:

$$\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes 2}_{q,d,p},\rho) = 2q((1-q)(2-3p)+q(1-2p))\log d. \tag{19}$$

See the Supplemental material for details. Consequently, the private capacity of $\mathcal{N}_{q,d,p}$ is bounded from below by:

$$\begin{aligned}\mathcal{P}(\mathcal{N}_{q,d,p}) &\geq \frac{1}{2}\mathcal{Q}^{(1)}(\mathcal{N}^{\otimes 2}_{q,d,p},\rho) &(20)\\ &\geq q\left((1-q)(2-3p)+q(1-2p)\right)\log d. &(21)\end{aligned}$$

It remains to compare the achievable bound in (21) with the converse bound in (16). For any triple (q,d,p) such that (21) is strictly greater than (16) the private capacity is non-convex. Figure 2 depicts the achievable region for which we exhibit non-convexity.

Classical environment-assisted capacity

We now turn to non-convexity of classical capacity with the weakest environment assistance. We start with providing two channels and a special entangled input state which we use to demonstrate this effect. Consider a flagged combination of the two channels used in [14] to show superadditivity of $\mathcal{C}_H$.

The first channel is defined by a controlled unitary $V^{AE\to FB} = \sum_{x,z}|xz\rangle^F\langle xz|^A\otimes\left(W(x,z)\right)^{E\to B}$ where

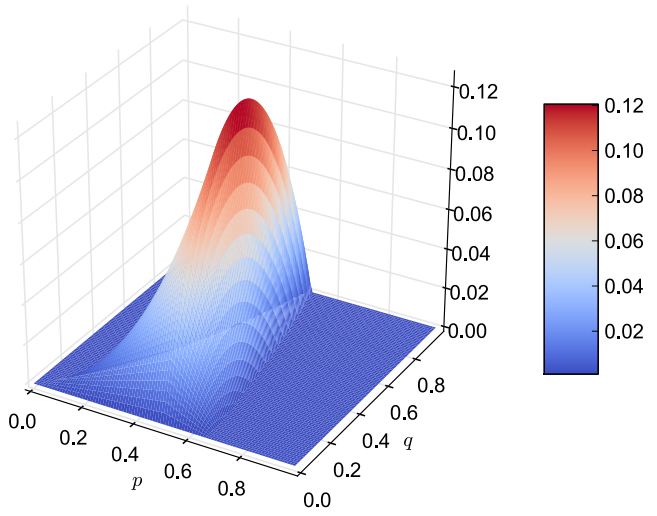

FIG. 2. The figure shows the difference between (21) and (16) normalized by $\log d$ when d goes to infinity. A value larger than zero implies non-convexity of $\mathcal{P}$.

$W(x,z) = X(x)Z(z)$, $X(x)|j\rangle = |(x+j) \mod d\rangle$, $Z(z)|j\rangle = \omega^{zj}|j\rangle$ and ω is again the primitive d-th root of unity.

The second channel is a SWAP channel: $\text{SWAP}(|\phi\rangle^A \otimes |\psi\rangle^E) = |\psi\rangle^B \otimes |\phi\rangle^F$.

Thus, our channels will have the form $\mathcal{N}_1 = |0\rangle\langle 0| \otimes V^{AE\to BF}$ and $\mathcal{N}_2 = |1\rangle\langle 1| \otimes \text{SWAP}^{AE\to BF}$. Fix $|A| = |F| = d^2, |E| = d, |B| = d$. In the following we prove that for some range of p:

$$\mathcal{C}_H\left(p\mathcal{N}_1 + (1-p)\mathcal{N}_2\right) > p\mathcal{C}_H(\mathcal{N}_1) + (1-p)\mathcal{C}_H(\mathcal{N}_2). \quad (22)$$

It follows from [14] that $C_H(\mathcal{N}_1) = \log d$ and $\mathcal{C}_H(\mathcal{N}_2) = 0$. Hence, the right-hand side of (22) is bounded from above by

$$p\mathcal{C}_H(\mathcal{N}_1) + (1-p)\mathcal{C}_H(\mathcal{N}_2) \leq p \log d\ . \quad (23)$$

In order to bound from below the left-hand side of (22), consider two uses of the channel $\mathcal{M} = p\mathcal{N}_1 + (1-p)\mathcal{N}_2$. Let the state of the environment be the maximally entangled state between E_1 and E_2: $\Phi^{E_1E_2}$ and the input state to the channel:

$$\rho^{XA_1A_2} = \frac{1}{d^2}\sum_{i,j=0}^{d-1} |ij\rangle\langle ij|^X \otimes |ij\rangle\langle ij|^{A_1} \otimes |ij\rangle\langle ij|^{A_2} \quad (24)$$

Then,

$$\mathcal{C}_H(\mathcal{M}^{\otimes 2}) \geq I(X:B_1B_2)_{\mathcal{M}^{\otimes 2}(\rho)}, \quad (25)$$

and since $\mathcal{M}$ is flagged, we can also divide the mutual information into the sum of the mutual information associated with each channel action. Let us compute the corresponding output states:

$$\mathcal{N}_1^{\otimes 2}(\rho) = \frac{1}{d^2}\sum_{i,j=0}^{d-1} |ij\rangle\langle ij|^X \otimes Z(j) \otimes Z(j)(\Phi^{B_1B_2}) \quad (26)$$

$$\mathcal{N}_1 \otimes \mathcal{N}_2(\rho) = \frac{1}{d^2}\sum_{i,j=0}^{d-1} |ij\rangle\langle ij|^X \otimes \mathsf{id} \otimes W(i,j)\left(\Phi^{B_1B_2}\right) \quad (27)$$

$$\mathcal{N}_2^{\otimes 2}(\rho) = \frac{1}{d^2}\sum_{i,j=0}^{d-1} |ij\rangle\langle ij|^X \otimes \Phi^{B_1B_2} \quad (28)$$

Note that $\mathcal{N}_2 \otimes \mathcal{N}_1(\rho)$ is just $\mathcal{N}_1 \otimes \mathcal{N}_2(\rho)$ with B_1 and B_2 swapped. The state obtained from the action of $\mathcal{N}_1^{\otimes 2}(\rho)$ follows from the observation that $W(x,z) \otimes W(x,z)\Phi = \mathsf{id} \otimes W(x,z)^T W(x,z)\Phi = Z(j) \otimes Z(j)\Phi$.

It is easy to verify that $I(X;B_1B_2)$ vanishes when $\mathcal{N}_2 \otimes \mathcal{N}_2$ is applied and takes the value $2\log d$ when either $\mathcal{N}_2 \otimes \mathcal{N}_1$ or $\mathcal{N}_1 \otimes \mathcal{N}_2$ is applied. In the case of $\mathcal{N}_1 \otimes \mathcal{N}_1$ we can bound the mutual information by:

$$I(X;B_1B_2)_\rho = \begin{cases} \log d \text{ if } d \text{ is odd} \\ \log\ d/2 \text{ if } d \text{ is even} \end{cases} \quad (29)$$

Let us justify (29). The input state is a clasical-quantum state of the form: $\sum_{ij} |ij\rangle\langle ij|^X \otimes \rho_{ij}^{A_1A_2}$. We can write explicitly the input states as:

$$\rho_{ij}^{A_1A_2} = |ij\rangle\langle ij|^{A_1} \otimes |ij\rangle\langle ij|^{A_2}\ . \quad (30)$$

If we apply the channel to an input state, we can conclude from (26) that the output does only depend on j and it simplifies to:

$$\Phi_j^{B_1B_2} := W(i,j) \otimes W(i,j)\Phi \quad (31)$$

$$= \frac{1}{\sqrt{2}} Z(j) \otimes Z(j) \sum_{i=0}^{d-1} |ii\rangle \quad (32)$$

$$= \sum_{i=0}^{d-1} \omega^{2ji}|ii\rangle\ . \quad (33)$$

Let $0 \leq a, b \leq d-1$ and $a \neq b$, we can check the orthogonality between two output states:

$$\langle\Phi_a|\Phi_b\rangle = \frac{1}{d}\sum_{i,j=0}^{d-1} \omega^{-2ai}\omega^{2bj}\langle ii|jj\rangle \quad (34)$$

$$= \frac{1}{d}\sum_{j=0}^{d-1} (\omega^{2(b-a)})^j. \quad (35)$$

(35) is a geometric series. Then, if $\omega^{2(b-a)} - 1 \neq 0$:

$$\langle\Phi_a|\Phi_b\rangle = \frac{(\omega^{2(b-a)})^d - 1}{(\omega^{2(b-a)}) - 1} = 0\ . \quad (36)$$

That is, Φ_a and Φ_b are orthogonal except if $\omega^{2(b-a)} = 1$ and then $\Phi_a = \Phi_b$. This is the case if d divides $2(b-a)$ which can only occur for $2(b-a) = d$. Hence if d is even there are $d/2$ orthogonal states and if d is odd there are d orthogonal states. We conclude that $I(X; B_1B_2)$ equals $\log d$ if d is odd and $\log d/2$ if d is even as claimed.

Adding all the contributions we obtain for odd d:

$$\begin{aligned} \mathcal{C}_H(\mathcal{M}) &\geq \frac{1}{2}\left(2p(1-p)2\log d + p^2 \log d\right) \\ &= \left(2p - \frac{3}{2}p^2\right)\log d. \end{aligned} \tag{37}$$

Finally, comparing the achievable bound in (37) with the converse bound in (23) one observes that for odd $d > 1$ and $0 < p < 2/3$ the classical capacity with passive environment-assisted capacity is non-convex.

Discussion

Computability, additivity, and convexity are three fundamental properties of capacity which allow to characterize the usefulness of a quantum channel for a concrete communication task.

Here, we focused our attention on non-convexity. Prior to our work, non-convexity had only been proven for the quantum capacity. We exhibit non-convexity of communication tasks involving classical information via quantum channels. Hence, our results show that non-convexity is a generic feature of communications over quantum channels that is not merely restricted to the transmission of quantum information. Furthermore, non-convexity is not an effect which concerns only a zero-measure set of quantum channels: by perturbing the channels in our construction one finds that the result still holds. However, it remains open how typical is non-convexity (and non-additivity) if one chooses two channels at random.

Both our non-convexity proofs and that of the quantum capacity build on top of non-additivity proofs. It is unclear if this is an artifact of the constructions or they hint to a deeper relation between both properties. Moreover, the non-convexity functional that we introduce here gives rise to a potential capacity analogous to the one induced by non-additivity. It is tempting to conjecture that the the two potential capacities, and more broadly, non-convexity and non-additivity, are closely related. Hence, a better understanding of this relation might shed some light into how much do the different capacities really gauge the usefulness of quantum channels for communication tasks.

Acknowledgments: We thank Kenneth Goodenough, Frédéric Grosshans, Jonas Helsen and Stephanie Wehner for useful discussions and feedback. SS acknowledges the support of Sidney Sussex College and European Union under project QALGO (Grant Agreement No. 600700). DE has been partially supported by STW, the NWO Vidi grant "Large quantum networks from small quantum devices" and by the project HyQuNet (Grant No. TEC2012-35673), funded by Ministerio de Economía y Competitividad (MINECO), Spain.

[1] S. Arimoto, Information Theory, IEEE Transactions on **18**, 14 (1972).
[2] R. E. Blahut, Information Theory, IEEE Transactions on **18**, 460 (1972).
[3] C. Adami and N. J. Cerf, Physical Review A **56**, 3470 (1997).
[4] C. H. Bennett, P. W. Shor, J. Smolin, A. V. Thapliyal, *et al.*, Information Theory, IEEE Transactions on **48**, 2637 (2002).
[5] S. Lloyd, Phys. Rev. A **55**, 1613 (1997), quant-ph/9604015.
[6] B. Schumacher and M. D. Westmoreland, Physical Review A **56**, 131 (1997).
[7] A. Holevo, IEEE Transactions on Information Theory **44**, 269 (1998).
[8] P. Shor (Lecture Notes, MSRI Workshop on Quantum Computation, 2002).
[9] N. Cai, A. Winter, and R. W. Yeung, Problems of Information Transmission **40**, 318 (2004).
[10] I. Devetak, Information Theory, IEEE Transactions on **51**, 44 (2005), quant-ph/0304127.
[11] R. A. Medeiros and F. M. De Assis, International Journal of Quantum Information **3**, 135 (2005).
[12] S. Guha, P. Hayden, H. Krovi, S. Lloyd, C. Lupo, J. H. Shapiro, M. Takeoka, and M. M. Wilde, Physical Review X **4**, 011016 (2014).
[13] S. Karumanchi, S. Mancini, A. Winter, and D. Yang, IEEE Transactions on Information Theory **62**, 1733 (2016).
[14] S. Karumanchi, S. Mancini, A. Winter, and D. Yang, arXiv:1602.02036 [quant-ph] (2016), arXiv: 1602.02036.
[15] A. Winter and D. Yang, IEEE Transactions on Information Theory **62**, 1415 (2016).
[16] S. Beigi and P. W. Shor, arXiv preprint arXiv:0709.2090 (2007).
[17] G. Smith and J. Yard, Science **321**, 1812 (2008), 0807.4935.
[18] K. Li, A. Winter, X. B. Zou, and G. C. Guo, Phys. Rev. Lett. **103**, 120501 (2009).
[19] G. Smith and J. A. Smolin, Phys. Rev. Lett. **103**, 120503 (2009).
[20] M. Wilde, *Quantum Information Theory* (Cambridge University Press, 2013).
[21] D. P. DiVincenzo, P. W. Shor, and J. A. Smolin, Phys. Rev. A **57**, 830 (1998), quant-ph/9706061.
[22] T. Cubitt, D. Elkouss, W. Matthews, M. Ozols, D. Pérez-García, and S. Strelchuk, Nat Commun **6** (2015).
[23] F. G. S. L. Brandão, J. Oppenheim, and S. Strelchuk, Phys. Rev. Lett. **108**, 040501 (2012), 1107.4385.
[24] G. Smith, J. M. Renes, and J. A. Smolin, Phys. Rev. Lett. **100**, 170502 (2008).
[25] O. Kern and J. M. Renes, Quantum Information & Com-

putation **8**, 756 (2008).
[26] D. Elkouss and S. Strelchuk, Phys. Rev. Lett. **115**, 040501 (2015).
[27] G. Smith and J. A. Smolin, Phys. Rev. Lett. **102**, 010501 (2009).
[28] M. B. Hastings, Nature Physics **5**, 255 (2009), 0809.3972.
[29] A. Winter, arXiv preprint quant-ph/0507045 (2005).
[30] The unitaries U and V are chosen uniformly at random from a unitary 2-design. Choosing the Clifford group or any other finite unitary 2 design has the advantage that the output of the channel is finite dimensional.

Supplemental Material

Non-convexity of private capacity and classical environment-assisted capacity of a quantum channel

Supplemental Material

Appendix A: Justification of (19).

Now we analyze the coherent information achieved by the input

$$\rho^{A^1A^2C_1D_1C_2D_2} = \Phi^{A^1D_1} \otimes \Phi^{C_1C_2} \otimes \Phi^{A^2D_2}. \tag{A1}$$

After sending ρ through two copies of the channel $\mathcal{N}_{q,d,p}^{\otimes 2}$, the resulting state is:

$$\begin{aligned}\mathcal{N}_{q,d,p}^{\otimes 2}(\rho) = q^2(\mathcal{E}_{d^2,p} \otimes \mathcal{E}_{d^2,p})(\rho) \otimes |0\rangle\langle 0| \otimes |0\rangle\langle 0| \\ + q(1-q)(\mathcal{E}_{d^2,p} \otimes R_d)(\rho) \otimes |0\rangle\langle 0| \otimes |1\rangle\langle 1| \\ + (1-q)q(R_d \otimes \mathcal{E}_{d^2,p})(\rho) \otimes |1\rangle\langle 1| \otimes |0\rangle\langle 0| \\ + (1-q)^2(R_d \otimes R_d)(\rho) \otimes |1\rangle\langle 1| \otimes |1\rangle\langle 1|. \end{aligned} \tag{A2}$$

Since the channel is a flagged combination of $\mathcal{E}$ and R, the coherent information is just the weighted sum of four terms

$$\begin{aligned}\mathcal{Q}^{(1)}(\mathcal{N}_{q,d,p}^{\otimes 2}, \rho) = q^2\mathcal{Q}^{(1)}(\mathcal{E}_{d^2,p} \otimes \mathcal{E}_{d^2,p}, \rho) \\ + q(1-q)\mathcal{Q}^{(1)}(R_d \otimes \mathcal{E}_{d^2,p}, \rho) \\ + q(1-q)\mathcal{Q}^{(1)}(\mathcal{E}_{d^2,p} \otimes R_d, \rho) \\ + (1-q)^2\mathcal{Q}^{(1)}(R_d \otimes R_d, \rho). \end{aligned} \tag{A3}$$

By symmetry of the input state, one has

$$\mathcal{Q}^{(1)}(\mathcal{E}_{d^2,p} \otimes R_d, \rho) = \mathcal{Q}^{(1)}(R_d \otimes \mathcal{E}_{d^2,p}, \rho). \tag{A4}$$

Let us compute each of the three terms. First, we consider two erasure channels. The resulting state is

$$\begin{aligned}\left(\mathsf{id}^{A^1A^2} \otimes \mathcal{E}_{d^2,p}^{C_1D_1 \to B_1^1B_1^2} \otimes \mathcal{E}_{d^2,p}^{C_2D_2 \to B_2^1B_2^2}\right)(\rho) = (1-p)^2\Phi^{A^1B_1^1} \otimes \Phi^{B_1^2B_2^2} \otimes \Phi^{A^2B_2^1} \\ + p(1-p)\Phi^{A^1B_1^1} \otimes \pi^{B_1^2} \otimes \pi^{A^2} \otimes |e\rangle\langle e|^{B_2^1B_2^2} \\ + p(1-p)\Phi^{A^2B_2^2} \otimes \pi^{B_2^1} \otimes \pi^{A^1} \otimes |e\rangle\langle e|^{B_1^1B_1^2} \\ + p^2\pi^{A^1A^2} \otimes |e\rangle\langle e|^{B_1^1B_1^2} \otimes |e\rangle\langle e|^{B_2^1B_2^2}, \end{aligned} \tag{A5}$$

where π stands for the maximally mixed state. The four states of this mixture can be differentiated by checking the erasure flag. This implies that the coherent information can also be divided into the sum of the coherent information of each term.

$$\mathcal{Q}^{(1)}(\mathcal{E}_{d^2,p} \otimes \mathcal{E}_{d^2,p}, \rho) = (1-p)^2 2\log d + 2p(1-p)0 + p^2(-2\log d) \tag{A6}$$

$$= (1-2p)2\log d. \tag{A7}$$

The resulting state in the case of one erasure channel and one rocket channel is

$$(R_d \otimes \mathcal{E}_{d^2,p})(\rho) = (1-p)(R_d \otimes \mathsf{id})(\rho) + p(R_d \otimes \mathcal{E}_{d^2,1})(\rho) \tag{A8}$$

which yields

$$\mathcal{Q}^{(1)}(R_d \otimes \mathcal{E}_{d^2,p}, \rho) = (2-3p)\log d. \tag{A9}$$

Finally, the use of two rocket channels yields

$$\mathcal{Q}^{(1)}(R_d \otimes R_d, \rho) \geq 0. \tag{A10}$$

For justification of (A9) and (A10) see Appendix B.

We plug (A6), (A9), and (A10) back into (A3)

$$\mathcal{Q}^{(1)}(\mathcal{N}_{q,d,p}^{\otimes 2}, \rho) = 2q((1-q)(2-3p) + q(1-2p))\log d \tag{A11}$$

Appendix B: Justification of (A9) and (A10).

The arguments follow from [1]. Let us analyze the action of one rocket channel and one erasure. This action can be decomposed into the action of the identity channel with probability $(1-p)$ and an erasure with probability p as stated in (A8). Let us compute the resulting state in both situations. For $\rho^{A^1A^2C_1D_1C_2D_2} = \Phi^{A^1D_1} \otimes \Phi^{C_1C_2} \otimes \Phi^{A^2D_2}$ we get:

$$(R_d \otimes \mathsf{id})(\rho) = R_d^{C_1D_1 \to B_1} \left(\Phi^{A^1D_1} \otimes \Phi^{C_1B_2^1}\right) \otimes \Phi^{A^2B_2^2} \tag{B1}$$

The key idea here is that the register C_1 is maximally entangled with the register B_2^1, which is available to the receiver. Hence, the receiver can undo each unitary applied to C_1 by applying the inverse of the transpose of the corresponding unitary. More precisely, for each choice of U and V from the channel:

$$\left((V^\dagger)^{B_1} \circ P^{B_1B_2^1} \circ ((U^T)^\dagger)^{B_2^2} \circ R_d^{UV}\right) \left(\Phi^{A^1D_1} \otimes \Phi^{C_1B_2^1}\right) = \Phi^{A^1D_1} \otimes \pi^{B_2^1} \tag{B2}$$

In the case of rocket channel and erasure we obtain:

$$(R_d \otimes \mathcal{E}_{d^2,1})(\rho) = R_d^{C_1D_1 \to B_1} \left(\Phi^{A^1D_1} \otimes \pi^{C_1}\right) \otimes \pi^{A^2} \otimes |e\rangle\langle e|^{B_2^1B_2^2} \tag{B3}$$

Let us denote by $\Phi_U^{AB} = (\mathsf{id} \otimes U)\,\Phi^{AB}\left(\mathsf{id} \otimes U^\dagger\right)$, then: $\Phi_{U^T}^{AB} = (U \otimes \mathsf{id})\,\Phi^{AB}\left(U^\dagger \otimes \mathsf{id}\right)$. If we focus our attention on the action of the rocket channel for some concrete U and V:

$$\begin{aligned} R_d^{UV}\left(\Phi^{A^1D_1} \otimes \pi^{C_1}\right) &= \mathrm{tr}_{C_1}\left(\sum_{ijkl} \omega^{ij-kl} |ij\rangle\langle ij|^{D_1C_1} (\Phi_V \otimes \pi) |kl\rangle\langle kl|^{D_1C_1}\right) \\ &= \sum_{ijl} \omega^{i(j-l)} |j\rangle\langle j|^{D_1} \Phi_V |l\rangle\langle l|^{D_1} \\ &= \sum_{j} |j\rangle\langle j|^{D_1} \Phi_V |j\rangle\langle j|^{D_1} \\ &= \sum_{j} \left(V^T \otimes |j\rangle\langle j|^{D_1}\right) \Phi \left(\left(V^T\right)^\dagger \otimes |j\rangle\langle j|^{D_1}\right) \\ &= U^T \otimes \bar{D}\,(\Phi) \end{aligned} \tag{B4}$$

where $\bar{D}$ denotes the completely dephasing channel in the computational basis. We can conclude that $\mathcal{Q}^{(1)}(R_d \otimes \mathsf{id}, \rho) = 2\log d$, $\mathcal{Q}^{(1)}(R_d \otimes \mathcal{E}_{d^2,1}, \rho) = -\log d$ and $\mathcal{Q}^{(1)}(R_d \otimes \mathcal{E}_{d^2,p}, \rho) = (2-3p)\log d$.

Now, let us analyze the action of two rocket channels. From the data processing inequality for coherent information we have that $\mathcal{Q}^{(1)}(R_d \otimes R_d, \rho) \geq \mathcal{Q}^{(1)}(\bar{D} \circ R_d \otimes \bar{D} \circ R_d, \rho)$. Now we will show that,

$$\left[\mathsf{id}^{A^1} \otimes \bar{D} \circ R_d^{UV}\right] \otimes \left[\mathsf{id}^{A^2} \otimes \bar{D} \circ R_d^{WX}\right] \left(\Phi^{A^1D_1} \otimes \Phi^{C_1C_2} \otimes \Phi^{A^2D_2}\right) \tag{B5}$$

$$= \left[\left(V^T\right)^{A^1} \otimes \bar{D}\right] \otimes \left[\left(X^T\right)^{A^2} \otimes \bar{D}\right] \left(\Phi^{A^1D_1} \otimes \Phi^{A^2D_2}\right), \tag{B6}$$

where the action of R_d^{UV} and R_d^{WX} is described in (B4). Then, since coherent information is invariant under the application of local unitaries:

$$\mathcal{Q}^{(1)}(R_d^{UV} \otimes R_d^{WX}, \rho) \geq \mathcal{Q}^{(1)}(\bar{D} \otimes \bar{D}, \Phi^{A^1D_1} \otimes \Phi^{A^2D_2}) = 0\ . \tag{B7}$$

We can write explicitly the form of the output after acting on the input state with $R_d^{UV} \otimes R_d^{WX}$:

$$\sigma^{A^1A^2D_1D_2} = \tag{B8}$$

$$= \sum_{\substack{ijkl \\ abcd}} \omega^{ij-kl+ab-cd} \left(\mathsf{id} \otimes |j\rangle\langle j| \Phi_V^{A^1D_1} \mathsf{id} \otimes |l\rangle\langle l|\right) \otimes \left(\mathsf{id} \otimes |b\rangle\langle b| \Phi_X^{A^2D_2} \mathsf{id} \otimes |d\rangle\langle d|\right) \mathrm{tr}\left(|i\rangle\langle i| \otimes |a\rangle\langle a| \Phi_{U^TW} |k\rangle\langle k| \otimes |c\rangle\langle c|\right) \tag{B9}$$

$$= \sum_{\substack{ijl \\ abd}} \omega^{i(j-l)+a(b-d)} \left(\mathsf{id} \otimes |j\rangle\langle j| \Phi_V^{A^1D_1} \mathsf{id} \otimes |l\rangle\langle l|\right) \otimes \left(\mathsf{id} \otimes |b\rangle\langle b| \Phi_X^{A^2D_2} \mathsf{id} \otimes |d\rangle\langle d|\right) \langle ia| \Phi_{U^TW} |ia\rangle. \tag{B10}$$

If we apply a dephasing channel at the output we obtain the following:

$$\bar{D} \otimes \bar{D} \left(\sigma^{A^1 A^2 D_1 D_2} \right) = \sum_{xy} \mathsf{id}^{A^1 A^2} \otimes |xy\rangle\langle xy|^{D_1 D_2} \sigma^{A^1 A^2 D_1 D_2} \mathsf{id}^{A^1 A^2} \otimes |xy\rangle\langle xy|^{D_1 D_2} \tag{B11}$$

$$= \sum_{iajb} \left(\mathsf{id} \otimes |j\rangle\langle j| \Phi_V^{A^1 D_1} \mathsf{id} \otimes |j\rangle\langle j| \right) \otimes \left(\mathsf{id} \otimes |b\rangle\langle b| \Phi_X^{A^2 D_2} \mathsf{id} \otimes |b\rangle\langle b| \right) \langle ia| \Phi_{U^T W} |ia\rangle \tag{B12}$$

$$= \sum_{jb} \left(\mathsf{id} \otimes |j\rangle\langle j| \Phi_V^{A^1 D_1} \mathsf{id} \otimes |j\rangle\langle j| \right) \otimes \left(\mathsf{id} \otimes |b\rangle\langle b| \Phi_X^{A^2 D_2} \mathsf{id} \otimes |b\rangle\langle b| \right) \tag{B13}$$

$$= \left(V^T \right)^{A^1} \otimes \bar{D} \otimes \left(X^T \right)^{A^2} \otimes \bar{D} \left(\Phi^{A^1 D_1} \otimes \Phi^{A^2 D_2} \right). \tag{B14}$$

---

[1] G. Smith and J. A. Smolin, Phys. Rev. Lett. **103**, 120503 (2009).