PAPER • OPEN ACCESS

Versatile relative entropy bounds for quantum networks

New Journal of Physics
The open access journal at the forefront of physics

Deutsche Physikalische Gesellschaft DPG
IOP Institute of Physics

Published in partnership with: Deutsche Physikalische Gesellschaft and the Institute of Physics

OPEN ACCESS

RECEIVED
18 July 2017

REVISED
5 December 2017

ACCEPTED FOR PUBLICATION
7 December 2017

PUBLISHED
24 January 2018

PAPER

Versatile relative entropy bounds for quantum networks

Luca Rigovacca[1,2], **Go Kato**[3,4], **Stefan Bäuml**[1,4], **M S Kim**[2], **W J Munro**[1,4,5] **and Koji Azuma**[1,4]

[1] NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi 243-0198, Japan
[2] Blackett Laboratory, Imperial College London, London SW7 2AZ, United Kingdom
[3] NTT Communication Science Laboratories, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi 243-0198, Japan
[4] NTT Research Center for Theoretical Quantum Physics, NTT Corporation, 3-1 Morinosato-Wakamiya, Atsugi 243-0198, Japan
[5] National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan

E-mail: luca.rigovacca@gmail.com

Keywords: quantum communication, quantum networks, quantum information

Abstract

We provide a versatile upper bound on the number of maximally entangled qubits, or private bits, shared by two parties via a generic adaptive communication protocol over a quantum network when the use of classical communication is not restricted. Although our result follows the idea of Azuma *et al* (2016 *Nat. Commun.* **7** 13523) of splitting the network into two parts, our approach relaxes their strong restriction, consisting of the use of a single entanglement measure in the quantification of the maximum amount of entanglement generated by the channels. In particular, in our bound the measure can be chosen on a channel-by-channel basis, in order to make it as tight as possible. This enables us to apply the relative entropy of entanglement, which often gives a state-of-the-art upper bound, on every Choi-simulable channel in the network, even when the other channels do not satisfy this property. We also develop tools to compute, or bound, the max-relative entropy of entanglement for channels that are invariant under phase rotations. In particular, we present an analytical formula for the max-relative entropy of entanglement of the qubit amplitude damping channel.

1. Introduction

Whenever two parties, say Alice and Bob, want to communicate by using a quantum channel, its noise unavoidably limits their communication efficiency [1]. In the limit of many channel uses, their asymptotic optimal performance can be quantified by the channel capacity, which represents the supremum of the number of qubits/bits that can be faithfully transmitted per channel use. Obtaining an exact expression for this quantity is typically far from trivial. Indeed, in addition to the difficulty of studying the asymptotic behaviour of the channel, the value of the capacity also depends on the task Alice and Bob want to perform, as well as on the free resources available to them [1]. Two representative tasks, which will be considered in our paper, involve the generation and distribution of a string of shared private bits (pbits) [2, 3] or of maximally entangled states (ebits) [4]. These are known to be fundamental resources for more complex protocols, such as secure classsical communication [5, 6], quantum teleportation [7], and quantum state merging [8]. An example of free resource involves the possibility of exchanging classical information over a public classical channel, such as a telephone line or over the internet. Depending on the restrictions on this, the capacity is said to be assisted by zero, forward, backward, or two-way classical communication [1]. In this paper we will focus on the last option, that is, no restriction will be imposed on the use of classical communication.

Although the capacity of a quantum channel is by definition an abstract and theoretical quantity, it is also practically useful in that it can be compared with the performance of known transmission schemes. This comparison could then give an indication on the extent of improvements that could be expected in the future. From this perspective, similar conclusions could be obtained even by studying upper bounds on the channel capacity itself, if they are close enough to its value. For example, with this approach Takeoka *et al* [9] provided strong evidences for the need of quantum repeaters for long-distance quantum key distribution (QKD) [10–12]. This reason, together with the fundamental appeal of characterising the ultimate transmission rate achievable by

a channel, led to recent intensive research for computable and simple upper bounds on channel capacities, preferably determined by a single use of the channel [9, 13–20].

The results in this direction have been obtained by considering the maximum entanglement that could be shared through a *single* use of a channel $\mathcal{N}_{A\to B}$, which takes as input a quantum state on Alice's side and yields an output on Bob's one. Indeed, for any entanglement measure E across the bipartition A:B, we can define the entanglement of the channel as

$$E(\mathcal{N}) \equiv \max_{\rho_{AA'}} E(\mathcal{N}_{A'\to B}[\rho_{AA'}]), \tag{1}$$

along the lines of [13–15, 17]. For some choices of $\mathcal{N}_{A\to B}$ and E, this can be used to upper bound the private capacity $K(\mathcal{N})$, assisted by two-way classical communication. Hence, $E(\mathcal{N})$ also acts as an upper bound on the two-way quantum capacity $Q(\mathcal{N})$ of the channel, because $Q(\mathcal{N}) \leqslant K(\mathcal{N})$ (since an ebit can be considered a special case of pbit [2, 3]). By generically labelling with $C(\mathcal{N})$ one of these two capacities, these upper bounds can be compactly written as

$$C(\mathcal{N}) \leqslant E(\mathcal{N}). \tag{2}$$

A result of this form has been proven in [9, 13] for *any* quantum channel by employing a particular entanglement measure, the squashed entanglement E_{sq} [21]. However, due to the difficulty of computing $E_{\mathrm{sq}}(\mathcal{N})$ exactly [14, 16, 22], one often needs to resort to upper bounds on it, thus loosening the bound for the capacity. The relative entropy of entanglement E_{R} is also known to provide an upper bound on the capacity of Choi-simulable quantum channels [14, 17], i.e., channels that can be simulated by performing LOCCs on their Choi–Jamiołkowski states. Quantum channels with this property are also called Choi-stretchable channels [14]. Remarkably, this upper bound often has no gap with respect to the best known lower bound on the capacity, and when this happens a single-letter formula for the capacity has been found. However, a drawback of the upper bound based on the relative entropy of entanglement is that at the moment it is not known whether equation (2), with $E = E_{\mathrm{R}}$, is valid when applied on a generic, non Choi-simulable, quantum channel. Another option is to use in equation (2) the max-relative entropy of entanglement $E_{\max}$ [15]. The resulting bound is formally proven only for quantum channels acting on finite dimensional systems, but it is thought to hold in general (see [15] for a short discussion). The set of pairs $(E, \mathcal{N})$ for which equation (2) is known to hold is the subject of ongoing research, and its extension represents an interesting and challenging problem.

In the future, it is reasonable to expect that all the parties involved in a communication task will be located at different nodes of a quantum network. In this vision, multiple users will be interconnected by a network of quantum channels, which can be utilised with the aim of transmitting or sharing quantum information. This scenario represents the evolution of today's internet in a quantum regime, and is therefore known as 'quantum internet' [23–26]. Experimental demonstrations of QKD over metropolitan networks are currently under way [27–31]. Similarly to the single-channel scenario, it is of fundamental and practical importance to seek upper bounds on the rate at which ebits (or pbits) can be shared by two parties by using the channels of the network. This issue has been addressed in [32] and [24], where the authors obtained network versions of equation (2), by respectively using E_{R} or E_{sq} as measures of entanglement. The possibility of dealing with quantum broadcast channels [33] has also been considered in [34–39]. When multiple channels are involved, a typical approach consists in splitting the whole network into two parts, and then in using the maximum amount of entanglement generated by the channels connecting them in order to bound the number of ebits (pbits) produced by a communication protocol. Thanks to the broad applicability of the single-channel bound given in equation (2) for $E = E_{\mathrm{sq}}$, the result of [24] holds for arbitrary quantum networks. However, a non-vanishing gap with the optimal number of ebits (or pbits) generated by the network could exist, in analogy with the single-channel case where the upper bounds on the capacity based on the squashed entanglement are typically not tight. It is thus natural to wonder whether different entanglement measures could improve this sort of network bound, and to what extent the choice of entanglement measure could be tailored to the characteristics of the channels in the network.

In this paper, we start by emphasising how a common strategy is adopted in all the known proofs of the bounds with the form given in equation (2). This allows us to formally identify two sufficient properties that, if satisfied by a given pair $(E, \mathcal{N})$, lead to a new instance of equation (2). We then show that those two properties also allow us to generalise the result of [24] on quantum networks to different entanglement measures: E_{R} when the channels in the network are Choi-simulable, or $E_{\max}$. The first case is particularly interesting, because equation (2) is often known to be tighter when stated in terms of E_{R}, rather than in terms of E_{sq}. The same advantage is therefore expected to be inherited by the corresponding upper bounds on the performance of quantum networks. However, notice that the E_{R}-based bound cannot be applied to arbitrary quantum networks. For example, even if a quantum network is composed almost entirely by Choi-simulable channels that are well bounded by their relative entropy entanglement, the presence of a single channel that is not Choi-simulable forces the use of a weaker entanglement measure (such as E_{sq}) for the whole network. This suggests

that a better bound could be obtained if there was the possibility of changing entanglement measures on a channel-by-channel basis. Our second and most important result goes exactly in this direction. We exploit an intermediate step in the discussion by Christandl and collaborators in [15] in order to bound the performance of a quantum network by means of either E_R or E_{max}. In particular, as E_{max} is always larger than E_R, we use the relative entropy of entanglement on the Choi-simulable channels of the network, and the max-relative entropy of entanglement on the others. The resulting bound allows us to maintain the precision guaranteed by the relative entropy of entanglement, without the need to restrict its applicability to Choi-simulable networks. After having presented this general result, we will provide examples of networks where our bound yields an advantage over its counterpart based on the squashed entanglement. In order to do this, we will also evaluate the max-relative entropy of entanglement for the most common qubit channels, by exploiting their symmetry under phase rotations and a recent semidefinite programming (SDP) formulation of E_{max} [40]. In particular, for the qubit amplitude damping channel we are able to analytically solve the SDP optimisation, thus finding the exact expression for its max-relative entropy of entanglement. This quantity upper bounds the private and quantum capacities of the channel assisted by unlimited classical communication, but is less tight than the best known upper bound based on the squashed entanglement [14].

The remainder of this paper is organised as follows. In section 2 we introduce our notation and some preliminary notions that will be used in the following. In section 3 we formally identify sufficient properties that, if satisfied by a pair $(E, \mathcal{N})$, lead to an upper bound on the capacity of the channel as in equation (2). Furthermore, along the lines of [24], we show how the same properties are also sufficient to obtain an upper bound on the number of ebits (or pbits) generated through a quantum network. Our main result is presented in section 4, where we derive a similar versatile upper bound, in which different entanglement measures are applied to the channels of the network depending on their Choi-simulability. Analytical or numerical evaluations of the max-relative entropy of entanglement for the most common qubit channels can be found in section 5, while examples of networks where our bound performs better than the one based on the squashed entanglement are presented in section 6. A final discussion on our results can be found in section 7, together with our conclusions. Technical details are left for the appendices.

2. Preliminaries

In this section we introduce the basic concepts necessary to understand the remainder of the paper, and we describe the notation we will use. In particular, we start by looking at the definitions and properties of the relative and max-relative entropy. Then, we introduce the notion of private states and of Choi-simulable channels. We also formally describe the structure of a quantum network and of the most general adaptive protocol, assisted by free classical communication, that could be employed to share ebits (or pbits). At the end of the section, we discuss the figure of merit we use to quantify the performance of a given communication strategy, and we comment on its relation to the usual single-channel capacity.

2.1. Relative and max-relative entropies

Given two quantum states ρ and σ, with supports satisfying $\mathrm{Supp}(\rho) \subseteq \mathrm{Supp}(\sigma)$, their relative entropy [41] and max-relative entropy [42] are respectively defined as

$$S(\rho\|\sigma) = \mathrm{Tr}[\rho(\log_2\rho - \log_2\sigma)], \tag{3}$$

$$D_{max}(\rho\|\sigma) = \inf\{x \in \mathbb{R} | 2^x\sigma - \rho \geqslant 0\}, \tag{4}$$

while their values are set to ∞ if the condition on the supports is not satisfied. The relative and max-relative entropy of two states are related by

$$S(\rho\|\sigma) \leqslant D_{max}(\rho\|\sigma), \tag{5}$$

they are also non-negative, equal to zero if and only if $\rho = \sigma$, and invariant under joint unitary operations, that is:

$$S(U\rho U^\dagger\|U\sigma U^\dagger) = S(\rho\|\sigma), \qquad D_{max}(U\rho U^\dagger\|U\sigma U^\dagger) = D_{max}(\rho\|\sigma), \tag{6}$$

for any unitary U. Moreover, the relative entropy is jointly convex in its arguments [43], whereas the max-relative entropy is jointly quasi-convex:

$$S\left(\sum_i p_i\rho_i\Big\|\sum_i p_i\sigma_i\right) \leqslant \sum_i p_i S(\rho_i\|\sigma_i), \tag{7}$$

$$D_{\max}\left(\sum_i p_i\rho_i\Big\|\sum_i p_i\sigma_i\right) \leqslant \max_i D_{\max}(\rho_i\|\sigma_i), \tag{8}$$

where $\{\rho_i\}_i$ and $\{\sigma_i\}_i$ are quantum states, and $p_i \geqslant 0$ with $\sum_i p_i = 1$.

The relative and max-relative entropies can be used to define entanglement measures respectively known as relative entropy of entanglement [44] and max-relative entropy of entanglement [42]. For a given bipartite state ρ_{AB}, their values are obtained by optimising over all separable states as follows:

$$E_{\mathrm{R}}^{A:B}(\rho_{AB}) = \min_{\sigma_{AB}\in\mathrm{SEP}} S(\rho_{AB}\|\sigma_{AB}), \tag{9}$$

$$E_{\max}^{A:B}(\rho_{AB}) = \min_{\sigma_{AB}\in\mathrm{SEP}} D_{\max}(\rho_{AB}\|\sigma_{AB}). \tag{10}$$

In the following we do not explicitly write the bipartition $A{:}B$ in the symbols E_{R} and $E_{\max}$, unless needed to avoid confusion. If the local quantum systems of Alice (or Bob) are divided into smaller subsystems, these will be labelled for example as A, A', A'' (or B, B', B''). In this case, the default evaluation of an entanglement measure has to be considered across the bipartition $AA'A''{:}BB'B''$. As any good entanglement measure, E_{R} and $E_{\max}$ are, on average, monotonically non-increasing under local operations and classical communication (LOCC). For an entanglement measure E, this property can be explicitly written as

$$\sum_k p_k E(\rho_{AB}^{(k)}) \leqslant E(\rho_{AB}), \tag{11}$$

where k represents the measurement outcome of the LOCC operation applied on ρ_{AB}, p_k is the probability of obtaining it, and $\rho_{AB}^{(k)}$ is the output state of the system post-selected on that result. Moreover, the ordering relation in equation (5) can also be straightforwardly extended to the entanglement measures E_{R} and $E_{\max}$, as well as to the entanglement of a channel $\mathcal{N}$ (see equation (1)):

$$E_{\mathrm{R}}(\rho_{AB}) \leqslant E_{\max}(\rho_{AB}), \qquad E_{\mathrm{R}}(\mathcal{N}) \leqslant E_{\max}(\mathcal{N}). \tag{12}$$

Further details on $E_{\max}$ can be found in [45].

We stress that in the remainder of this paper any generic entanglement measure E satisfies equation (11), and becomes zero when evaluated on any separable state.

2.2. Target states: maximally entangled or private states

The typical goal of two parties, say Alice and Bob, in a quantum communication protocol is to share one or multiple copies of a d-dimensional maximally entangled state

$$\psi_{AB}(d) = \sum_{i,j=1}^{d} \frac{1}{d}|ii\rangle\langle jj|_{AB}, \tag{13}$$

where $\{|i\rangle_{A(B)}\}_i$ forms a local orthonormal basis. Any single copy of these states corresponds to $\log_2 d$ ebits, which Alice and Bob can use to perform one of many possible tasks. For example, they can transmit any d-dimensional state via the teleportation protocol, or they can perform a projective measurement on it in order to share a string of $\log_2 d$ bits of private randomness. The maximally entangled state, however, is not the only quantum state from which a private key can be obtained by performing local measurements. It has been shown that this is possible whenever Alice and Bob are able to distil via LOCC a so-called 'private state' [2, 3], which has the following form:

$$\gamma_{ABA'B'}(d) = U^{(\mathrm{twist})}_{ABA'B'}(\psi_{AB}(d)\otimes\sigma_{A'B'})U^{(\mathrm{twist})\dagger}_{ABA'B'}. \tag{14}$$

The state $\sigma_{A'B'}$ is arbitrary and the controlled unitary

$$U^{(\mathrm{twist})}_{ABA'B'} = \sum_{i,j=1}^{d} |i\rangle\langle i|_A \otimes |j\rangle\langle j|_B \otimes U^{(ij)}_{A'B'} \tag{15}$$

is known as 'twisting unitary', with each $U^{(ij)}_{A'B'}$ a unitary operator. The local subsystems A and B are called 'key systems', whereas A' and B' are known as 'shield systems'. The role of the latter is to prevent an eavesdropper from getting access to the key component, and they could have any dimension.

2.3. Choi-simulable channels

The idea of using quantum teleportation in order to simplify the structure of a computation for communication task has been used several times in the past [46–51, 51, 52]. Recently, a similar idea has been used in [14] and in [17, 32] in order to obtain upper bounds on the capacities of quantum channels $\mathcal{N}$ such that their action on a quantum state $\tilde{\rho}_{A'}$ can be written as

$$\mathcal{N}_{A'\to B'}(\tilde{\rho}_{A'}) = \Lambda_{A'A'':B'}(\tilde{\rho}_{A'} \otimes \pi_{A''B'}(\mathcal{N})). \tag{16}$$

Here $\Lambda_{A'A'':B'}$ is a trace-preserving LOCC operation and $\pi_{A''B'}(\mathcal{N}) = \mathcal{N}_{\tilde{A}\to B'}(\psi_{A''\tilde{A}})$ represents the Choi–Jamiołkowski state associated with the quantum channel $\mathcal{N}$, with $\psi_{A''\tilde{A}}$ a maximally entangled state. We will say that channels satisfying equation (16) are Choi-simulable, as they can be simulated by applying LOCCs to their Choi–Jamiołkowski state. This property can also go under the name of 'Choi-stretchability' [14, 32]. The importance of equation (16) lies in the fact that it gives the possibility of reducing the effect of a quantum channel to the presence of an initially shared Choi state, up to some LOCC transformation. Equation (16) makes the description of the quantum communication much simpler, because the LOCC $\Lambda_{A'A'':B'}$ can be included among those freely performed by the parties. In the following, if a channel $\mathcal{N}$ is Choi-simulable we will write $\mathcal{N} \in \mathcal{S}$.

Remarkably, the relative entropy of entanglement of a Choi-simulable channel $\mathcal{N}$, as defined in equation (1), provides an upper bound on its capacity assisted by two-way classical communication [14, 17]. Moreover, $E_R(\mathcal{N})$ exactly coincides with the capacity $C(\mathcal{N})$ on a particular subset of Choi-simulable channels, whose capacities $C(\mathcal{N})$ can thus be written as single-letter formulas [14]. Channels for which this happens can also be called 'distillable' [14, 32]. Among these, we can enumerate the erasure and dephasing channels in finite dimensional systems, as well as the bosonic lossy channel. Interestingly, for many Choi-simulable channels (such as Pauli channels) $E_R(\mathcal{N})$ turns out [14] to be a tighter upper bound on $C(\mathcal{N})$ than other known upper bounds based on the squashed entanglement [9, 13]. However, one should keep in mind that this is not always the case, as can be seen by considering a channel having an antisymmetric Choi state. Indeed, the squashed entanglement of this state, and thus of the associated quantum channel, can be arbitrarily small compared to its relative entropy of entanglement [53, 54].

We now explicitly derive a property that the relative entropy of entanglement satisfies when applied on the output of a Choi-simulable channel. Although it is obvious from the discussion in [14], it is beneficial to go through its proof in detail, because it will play a central role in the remainder of this paper. In particular, we prove that if $\tilde{\rho}_{AB'B}$ is obtained as output of a Choi-simulable channel $\mathcal{N} \in \mathcal{S}$ as

$$\tilde{\rho}_{AB'B} = \mathcal{N}_{A'\to B'}(\rho_{AA'B}), \tag{17}$$

the following chain of inequalities holds:

$$\begin{aligned} E_R(\tilde{\rho}_{AB'B}) &\leqslant E_R(\rho_{AA'B} \otimes \pi_{A''B'}(\mathcal{N})) \\ &\leqslant E_R(\pi_{A''B'}(\mathcal{N})) + E_R(\rho_{AA'B}) \\ &= E_R(\mathcal{N}_{A'\to B'}) + E_R(\rho_{AA'B}). \end{aligned} \tag{18}$$

The first inequality comes from equation (16) and from the monotonicity of E_R under LOCC, while the second one follows from its sub-additivity under tensor products. The final equality can be proven by showing inequalities in both directions. Indeed, the inequality '$\leqslant$' is obtained by noticing that a maximisation over all input states would be needed in order to obtain the relative entropy of entanglement of a channel (see equation (2)). The converse direction, instead, is once again a consequence of equation (16) and of the monotonicity of E_R under LOCC [14]:

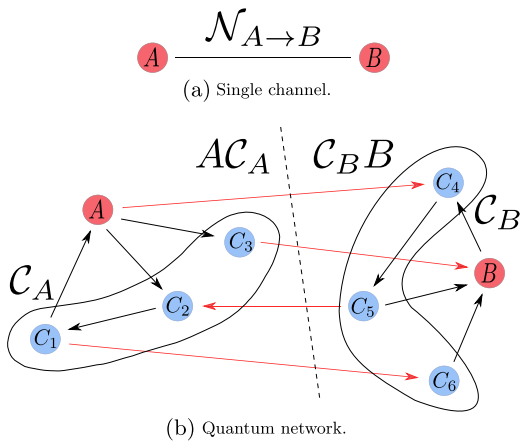
$$E_R(\mathcal{N}_{A'\to B'}[\rho_{AA'}]) = E_R(\Lambda_{A'A'':B}[\rho_{AA'} \otimes \pi_{A''B'}(\mathcal{N})]) \leqslant E_R(\pi_{A''B}(\mathcal{N})), \tag{19}$$

which holds for any $\rho_{AA'}$ and thus also for its maximum value $E_R(\mathcal{N}_{A'\to B'})$. Hence, equation (18) shows that the amount of entanglement which can be found in output of a Choi-simulable channel, as measured by E_R, can be upper bounded by the amount already present in input plus the maximum amount that can be created by the channel itself. Up to date, it is not known whether the same conclusion could be obtained also for any quantum channel.

2.4. Quantum networks as graphs

The simplest setup that allows Alice and Bob to exchange quantum information is shown in figure 1(a), where a quantum channel $\mathcal{N}_{A\to B}$ connects Alice's laboratory with Bob's. More generally, we can think of them as being two local users having access to a quantum network, as in figure 1(b). A quantum network is composed of several nodes, connected by many quantum channels potentially different from each other. We can formally describe this structure by a directed graph $G = (V, L)$, where $V = \{V_0,\ldots,V_{M+1}\}$ is the set of nodes and L is the set of directed edges, or links, between the nodes. For any edge $l = (V_i, V_j) \in L$, there is a quantum channel $\mathcal{N}^{(l)}$ from node V_i to node V_j. Without loss of generality, we can assume that nodes $A = V_0$ and $B = V_{M+1}$ are respectively controlled by Alice and Bob, whereas the remaining nodes $\{C_i\}_{i=1}^{M}$, with $C_i = V_i$, are not.

In the following we will often make use of the notion of 'bipartition' of a quantum network. This is defined by dividing the nodes $\{C_i\}_i$ into two disjoint sets: $\mathcal{C}_A \subset \{C_i\}_i$ and $\mathcal{C}_B = \{C_i\}_i \setminus \mathcal{C}_A$. Once a bipartition has been chosen, the set of edges connecting the nodes in $\{A\} \cup \mathcal{C}_A$ with those in $\mathcal{C}_B \cup \{B\}$, or vice versa, will be labelled as $L_{\mathcal{C}_A} \subset L$. Moreover, in order to keep our notation simple, in the remainder of this paper we will refer to the subsets of nodes $\{A\} \cup \mathcal{C}_A$ and $\mathcal{C}_B \cup \{B\}$ by writing respectively $A\mathcal{C}_A$ and $\mathcal{C}_B B$.



(a) Single channel.

(b) Quantum network.

Figure 1. (a) Single-channel communication scenario, where A and B are connected through the channel $\mathcal{N}_{A\to B}$. (b) An example of quantum network, with $M = 6$ additional nodes. Every arrow corresponds to a quantum channel. The bipartition $\mathcal{C}_A = \{C_1, C_2, C_3\}, \mathcal{C}_B = \{C_4, C_5, C_6\}$ is shown as an example, and the channels $\mathcal{N}^{(l)}$ with $l \in L_{\mathcal{C}_A}$, which connect the two partitions, are coloured in red.

2.5. Adaptive strategy over quantum networks

We assume that full quantum control over the local systems is available on each node of the network, and that all parties can freely exchange classical information at any stage of the protocol in order to coordinate their strategy. Moreover, we also assume that every node in the network will collaborate with Alice and Bob in order to allow them to achieve their goal. At the beginning of the most general adaptive communication protocol, the parties initialise their systems in a separable state $\rho^{(1)}_{ABC_1\ldots C_M}$. Then, they iteratively exchange (part of) their systems via the quantum channels, and perform LOCCs on the obtained states, which may involve measurements. For this reason, every choice made by the parties at a certain stage of the protocol may depend on all previously obtained LOCC outcomes. In the remainder of this section we formally describe any protocol of this kind, similarly to what has been done in [24, 32, 36]. For the sake of simplicity, we will drop the subscript $ABC_1 \ldots C_M$ from states spread over the whole network.

Between any two channel uses several LOCC may be performed, but we can group them into a single 'round of LOCCs' yielding an overall multi-index outcome k. In this way, a single 'round of the protocol' will be composed by the application of a channel followed by a round of LOCCs. Let us group within the vector $\boldsymbol{k}_i = (k_0, k_1, \ldots, k_{i-1}, k_i)$ the sequence of LOCC outcomes obtained in the first i rounds, with $k_0 \equiv 1$ added for convenience. In this way, the ith round of the protocol receives as input $\rho^{\boldsymbol{k}_{i-1}}$ and transforms it into $\rho^{\boldsymbol{k}_i}$ via the following two steps.

- Depending on the previous LOCC outcomes, grouped within $\boldsymbol{k}_{i-1}$, the parties may use the channel $\mathcal{N}^{(l_{\boldsymbol{k}_{i-1}})}$ to transmit a quantum state along the edge $l_{\boldsymbol{k}_{i-1}} \in L$ of the graph G characterising the network. The global state at the end of this step is labelled by $\tilde{\rho}^{\boldsymbol{k}_{i-1}}$;
- A round of LOCCs $\Lambda^{(\boldsymbol{k}_{i-1})}$ is performed on $\tilde{\rho}^{\boldsymbol{k}_{i-1}}$, with output k_i obtained with probability $p(k_i|\boldsymbol{k}_{i-1})$. The output quantum state $\rho^{\boldsymbol{k}_i}$ will be used as input for the following round of the protocol.

When the protocol stops, say after n rounds, the final state $\rho^{\boldsymbol{k}_n}_{AB} = \mathrm{Tr}_{C_1,\ldots,C_M}[\rho^{\boldsymbol{k}_n}]$ shared by Alice and Bob has to be ϵ-close in trace distance to an ideal target state $\phi_{AB}(d_{\boldsymbol{k}_n})$, i.e., such that for any sequence of outcomes $\boldsymbol{k}_n$ one has

$$\|\rho^{\boldsymbol{k}_n}_{AB} - \phi_{AB}(d_{\boldsymbol{k}_n})\|_1 = \epsilon, \tag{20}$$

where $\|O\|_1 \equiv \mathrm{Tr}[\sqrt{O^\dagger O}]$. The target state $\phi_{AB}(d_{\boldsymbol{k}_n})$ can either be a maximally entangled state $\psi_{AB}(d_{\boldsymbol{k}_n})$ (see equation (13)) or a private state $\gamma_{AB}(d_{\boldsymbol{k}_n})$ (see equation (14)), depending on the task of Alice and Bob.

All the details of the adaptive strategy leading to equation (20) are determined by the protocol $\mathcal{P}_{\epsilon,n}$ that the parties are following. These details include the error threshold ϵ, the maximum number of rounds n, the target states $\phi_{AB}(d_{\boldsymbol{k}_n})$, and the set of rules that, at any round of the protocol, map the vectors of previous outcomes $\{\boldsymbol{k}_i\}_{i=0}^{n-1}$ to the channel and LOCC operations used in the following. In the remainder of this paper we will often have to average some function $F(\boldsymbol{k}_n)$ over all possible LOCC outcomes $\{\boldsymbol{k}_n\}$. It is thus convenient to introduce the shorthand notation

$$\langle F\rangle_{\mathcal{P}_{\epsilon,n}} \equiv \sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) F(\boldsymbol{k}_n), \tag{21}$$

where $p(\boldsymbol{k}_n)$ is the probability of obtaining this particular sequence of LOCC outcomes according to the protocol $\mathcal{P}_{\epsilon,n}$.

We point out that the number of channels used in the protocol will generally be smaller than n. This is because in any round the parties *may* decide to use a channel of the network, but are not forced to do so. However, without loss of generality we can assume that a channel is used in any round of the protocol up to a certain point, after which the parties can only perform LOCCs and the communication protocol is effectively aborted. Indeed, if this were not the case, we could recover this situation simply by merging all the LOCCs performed between two channel uses into a single round of LOCCs. Notice that depending on the LOCC outcomes already obtained, the parties can decide to effectively abort the communication after different numbers of channel uses. In particular, for any edge $l \in L$ and vector $\boldsymbol{k}_n$, we can define as $m^{(l)}(\boldsymbol{k}_n)$ the total number of times channel $\mathcal{N}^{(l)}$ has been used in that particular realisation of outcomes. Formally, this can be written as

$$m^{(l)}(\boldsymbol{k}_n) = \sum_{i=0}^{n-1} \delta_{l,l_{\boldsymbol{k}_i}}, \tag{22}$$

where the symbol δ represents the Kronecker delta, while the total number of channel uses is

$$m(\boldsymbol{k}_n) = \sum_{l\in L} m^{(l)}(\boldsymbol{k}_n). \tag{23}$$

A value of $m(\boldsymbol{k}_n)$ strictly smaller than n means that the protocol has been effectively interrupted after $m(\boldsymbol{k}_n)$ rounds.

2.6. Quantifying the performance of a communication protocol

The quality of a point-to-point adaptive communication protocol $\mathcal{P}_{\epsilon,n}$ can be quantified by its ability to produce a large number of shared ebits (or pbits) between Alice and Bob. For any realisation $\boldsymbol{k}_n$ of LOCC outcomes, this corresponds to the logarithm of the dimension $d_{\boldsymbol{k}_n}$ that characterises the target state $\phi_{AB}(d_{\boldsymbol{k}_n})$, ϵ-close to the final state $\rho_{AB}^{\boldsymbol{k}_n}$ produced by the protocol. Therefore, a good figure of merit for $\mathcal{P}_{\epsilon,n}$ can be obtained by averaging this quantity over all LOCC outcomes. In our notation, this can be written as $\langle \log_2 d\rangle_{\mathcal{P}_{\epsilon,n}}$.

This approach is particularly suitable to characterise the performance of protocols that use the channels of the network a finite number of times, because it directly provides the length of ebits (pbits) that Alice and Bob can expect to share at the end of the communication. However, the quantity $\langle \log_2 d\rangle_{\mathcal{P}_{\epsilon,n}}$ becomes unbounded when the asymptotic limit of infinitely many channel uses is considered. In a single-channel scenario, this issue has been traditionally addressed by considering the communication rate, i.e., the number of bits produced per channel use. We should point out that in this case one does not typically consider the possibility of interrupting the protocol depending on previous LOCC outcomes. This is because otherwise with non-zero probability the asymptotic regime of infinitely many channel uses would not be reached. For this reason only protocols which use the quantum channel after *every* round of LOCC are normally considered when assessing its asymptotic performance. In this paper, a protocol of this kind will be labelled as $\tilde{\mathcal{P}}_{\epsilon,N}$, where ϵ represents the error threshold and N is the fixed number of channel uses. With this notation, the quantum (or private) capacity of a quantum channel $\mathcal{N}$ assisted by two-way classical communication can be obtained as the limit

$$C(\mathcal{N}) = \lim_{\epsilon\to 0}\lim_{N\to\infty}\sup_{\tilde{\mathcal{P}}_{\epsilon,N}} \frac{\langle \log_2 d\rangle_{\tilde{\mathcal{P}}_{\epsilon,N}}}{N}. \tag{24}$$

For a generic quantum network the situation is more involved, and in the literature one can find multiple ways of assessing its communication performance in the asymptotic limit. For example, one can fix the frequency with which each channel is used, and divide $\langle \log_2 d\rangle_{\mathcal{P}_{\epsilon,n}}$ by the total number of channel uses [55]. Other options, proposed in [32], consist in using each 'path' connecting Alice and Bob with a certain probability, or in using each channel of the network exactly once. Then, the number of produced ebits (pbits) is respectively divided by the number of paths used, or by the total number of times the network has been accessed. Although the details of characterising the considered figure of merit can change on a case-by-case basis, one typically has to optimise $\langle \log_2 d\rangle_{\mathcal{P}_{\epsilon,n}}$ over a chosen class of protocols, and divide it by a quantity that counts how many times a basic operation has been repeated.

Similar to [24, 55], in the following we are able to provide an upper bound on $\langle \log_2 d\rangle_{\mathcal{P}_{\epsilon,n}}$ for a generic adaptive protocol running on a quantum network with graph G. This bound only depends on the maximum amount of entanglement that could be generated by the quantum channels composing the network, and on the number of times each channel has been used. From the previous discussion, it should be clear that our bound can be easily converted to a bound on a broad class of figures of merit, which could be chosen to quantify the

performance of the network. For example, in the case of a single channel, our bound can be connected to an upper bound on the capacity by means of equation (24).

3. Entanglement-based upper bounds

As mentioned in the introduction, recently several authors provided bounds on the number of ebits (pbits) shared by two parties at the end of a point-to-point communication protocol assisted by two-way classical communication. Some studies deal with the capacity of a single quantum channel [9, 13–15, 17], whereas others consider quantum networks with arbitrary topology [24, 32, 55]. However, they all share some common features. Here we identify these, and show how they can lead to known, new, or yet to be discovered communication bounds.

We start by considering a single channel $\mathcal{N}$ and a generic entanglement measure E, and we formally summarise in theorem 1 some important properties that have been used in the past in order to obtain upper bounds on the channel capacity. One advantage of this abstract formulation is that it can ease the process of identifying all the entanglement measures which can be used to bound the capacity of a given channel. By comparing all these bounds, it would then be possible to select the one with the minimum value, which represents the best known upper bound on the capacity $C(\mathcal{N})$. A second advantage of our abstract approach lies in the possibility of easily extending previous results on quantum networks to other entanglement measures, not explicitly studied in the original papers. This is because the same properties responsible for the upper bound on the capacity of a single channel are also the main ingredients used in [24] to derive an upper bound for the number of shared ebits (pbits) produced by a quantum network. In this way, we are able to show that the same bound of [24], originally expressed in terms of the squashed entanglement, is also valid for other entanglement measures: $E_{\max}$ and E_{R}, although the applicability of the latter is restricted to networks composed by Choi-simulable channels. This original contribution will be summarised as theorem 2.

Having multiple upper bounds on the communication performance of a quantum network, based on different entanglement measures, there is the possibility of combining them together in order to obtain a bound as tight as possible. An obvious option consists in evaluating each upper bound separately, and then selecting the one which yields the minimum value. However, it is possible to do better than this, and in section 4 we show how the bounds based on $E_{\max}$ and E_{R} can be joined together to form a single tighter bound.

3.1. General framework

We start by discussing the case of a single channel $\mathcal{N}$, and then we move to the more general situation of a quantum network with arbitrary topology. The proofs for the theorems presented here can be found at the end of the section.

All measures of entanglement E known to yield a bound on the number of ebits (pbits) generated by a communication protocol satisfy the following property:

P1. If a target state $\phi_{AB}(d)$ is ϵ-close to a quantum state ρ_{AB}, i.e., if $\|\rho_{AB} - \phi_{AB}(d)\|_1 = \epsilon$, then there exist two real functions f_E and g_E, with $\lim_{\epsilon\to 0} g_E(\epsilon) = 1$ and $\lim_{\epsilon\to 0} f_E(\epsilon) = 0$, such that

$$E(\rho_{AB}) \geqslant g_E(\epsilon)\log_2 d - f_E(\epsilon). \tag{25}$$

For a maximally entangled target state, this property can be easily proven for every *asymptotically continuous* [56] measure E. On the contrary, more effort is usually required to prove it for private target states. The reason for this is that the quantity d appearing on the right-hand side of equation (25) needs to be the dimension of the key systems, rather than the dimension of the whole key-shield systems. Nonetheless, property P1 has been proven for E_{sq} [57] and E_{R} [3, 14, 17]. It can also be easily proven for $E_{\max}$, by slightly varying the proof of lemma IV.2 in [15] in order to obtain equation (25) with

$$g_{E_{\max}} = 1, \qquad \text{and} \qquad f_{E_{\max}} = -2\log_2(1 - \epsilon/2). \tag{26}$$

Another important property of a pair concerns the relation between the amount of entanglement in the input and output states of the channel $\mathcal{N}$, as measured by the entanglement measure E. A pair $(E, \mathcal{N})$ is said to satisfy property P2 if for all states $\rho_{AA'B}$ one has

P2. $\tilde{\rho}_{AB'B} = \mathcal{N}_{A'\to B'}(\rho_{AA'B}) \implies E(\tilde{\rho}_{AB'B}) \leqslant E(\mathcal{N}) + E(\rho_{AA'B})$,

where $E(\mathcal{N})$ is the maximum entanglement shared through a single use of the channel (see equation (1)). This is known to hold for any quantum channel when $E = E_{\mathrm{sq}}$ [9, 13], and for any Choi-simulable channel when

$E = E_R$ (see equation (18)). Moreover, property P2 has been recently shown for the max-relative entropy of entanglement for any channel acting on finite-dimensional system, but it is conjectured to hold even without this assumption [15].

In order to ease the connection with quantum networks, we provide a bound on $\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}}$ also in the single-channel scenario, from which the usual bound on the capacity can be recovered as a corollary by using the definition in equation (24). Furthermore, we can also provide conditions sufficient to prove the strong converse property of an upper bound on the channel capacity. In particular, corollary 1 can be used together with equation (26) in order to show that $E_{\max}$ provides a strong converse bound on the capacity of a single channel, as originally proven in [15].

Theorem 1. *If E and $\mathcal{N}$ satisfy properties P1 and P2, the average number of ebits (pbits) generated by an adaptive protocol $\mathcal{P}_{\epsilon,n}$ assisted by two-way classical communication can be upper bounded as*

$$\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}} \leqslant \frac{1}{g_E(\epsilon)} [f_E(\epsilon) + \langle m \rangle_{\mathcal{P}_{\epsilon,n}} E(\mathcal{N})], \tag{27}$$

where $\langle m \rangle_{\mathcal{P}_{\epsilon,n}}$ is the average number of times the channel has been used.

Corollary 1. *If E and $\mathcal{N}$ satisfy properties P1 and P2, the capacity of $\mathcal{N}$ assisted by two-way classical communication can be upper bounded as*

$$C(\mathcal{N}) \leqslant E(\mathcal{N}). \tag{28}$$

Furthermore, if $g_E(\epsilon) = 1$ and $f_E(\epsilon) = c \log_2 \frac{1}{1-\epsilon/2}$, for $c > 0$, this is a strong converse bound.

Proof of corollary 1. By definition of capacity (see equation (24)), only protocols using the channel a fixed number of times should be considered. Equation (28) is thus a straightforward consequence of $\langle m \rangle_{\tilde{\mathcal{P}}_{\epsilon,N}} = N$, $\lim_{\epsilon \to 0} g_E(\epsilon) = 1$, and $\lim_{\epsilon \to 0} f_E(\epsilon) = 0$. In order to see the strong converse property, we need to express equation (27) in terms of the error $\frac{1}{2}\|\rho_{AB} - \phi_{AB}(d)\|_1 = \epsilon/2 \in [0, 1]$. Namely

$$\epsilon/2 \geqslant 1 - 2^{-\frac{1}{c}[\langle \log_2 d \rangle_{\tilde{\mathcal{P}}_{\epsilon,N}} - NE(\mathcal{N})]}, \tag{29}$$

which tends to 1 exponentially fast in the number N of channel uses as the rate $\frac{1}{N}\langle \log_2 d \rangle_{\tilde{\mathcal{P}}_{\epsilon,N}}$ exceeds $E(\mathcal{N})$. □

As can be expected, a bipartite situation A:B is easier to study than a scenario in which Alice and Bob need to cooperate with other nodes $\{C_i\}_{i=1}^N$ in the network in order to achieve their communication task. Building on this intuition, the authors of [24, 32] derived upper bounds on network capacities by considering a bipartition AC_A:BC_B, and by extending the regions controlled by Alice and Bob so as to include in them also the remaining nodes on their side. Intuitively, an upper bound can be obtained in this manner because the achievable communication rate between the 'extended' parties has to be larger than the one achievable by the real A and B. In this framework, any given bipartition $\{\mathcal{C}_A, \mathcal{C}_B\}$ of the network leads to a different upper bound, in which only the channels corresponding to the edges in $L_{\mathcal{C}_A}$ contribute. Although the proof that led to the result in [24] is based on a particular choice of entanglement measure, we can see how the same reasoning applies to any entanglement measure satisfying properties P1 and P2 for any channel connecting the two network partitions. This is the result of the next theorem.

Theorem 2. *Consider a quantum network with an associated directed graph G. For a given bipartition $\{\mathcal{C}_A, \mathcal{C}_B\}$ of the network nodes $\{C_i\}_i$, let $L_{\mathcal{C}_A} \subset L$ be the set of edges in G that connect a node in AC_A with one in $\mathcal{C}_B B$. The average number of ebits (or pbits) that Alice and Bob share at the end of a given adaptive protocol $\mathcal{P}_{\epsilon,n}$, assisted by unlimited classical communication, can be upper bounded as*

$$\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}} \leqslant \frac{1}{g_E(\epsilon)} [f_E(\epsilon) + \mathcal{E}_E(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A)], \tag{30}$$

where

$$\mathcal{E}_E(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A) \equiv \sum_{l \in L_{\mathcal{C}_A}} \langle m^{(l)} \rangle_{\mathcal{P}_{\epsilon,n}} E(\mathcal{N}^{(l)}), \tag{31}$$

for any entanglement measure E satisfying hypotheses P1 and P2 for any channel $\mathcal{N}^{(l)}$ with $l \in L_{\mathcal{C}_A}$.

At this point we can make a few comments on this bound. In virtue of theorem 1, we point out that the entanglement of the channel $\mathcal{N}^{(l)}$ has to be larger than the single-channel capacity $C(\mathcal{N})$. Therefore, the gap between the two sides of equation (30) is reduced if a certain measure of entanglement can better approximate the capacity of the channels in $L_{\mathcal{C}_A}$. Furthermore, among the known entanglement measures satisfying P1 and P2

for any channel $\mathcal{N}^{(l)}$ with $l \in L_{\mathcal{C}_A}$, the best choice is to choose the one minimising $\mathcal{E}_E(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A)$. If we label by $E|_{\mathcal{C}_A}$ the set of entanglement measures satisfying properties P1 and P2 for the channels connecting the two partitions, the following bound can be obtained:

$$\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}} \leqslant \min_{\mathcal{C}_A} \min_{E|_{\mathcal{C}_A}} \frac{1}{g_E(\epsilon)} [f_E(\epsilon) + \mathcal{E}_E(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A)], \tag{32}$$

where we also optimised over all possible choices for $\mathcal{C}_A$.

3.2. Proofs for theorems 1 and 2

Any single channel can be interpreted as a simple quantum network, hence we first show how theorem 1 can be derived from theorem 2, and then we prove the latter. The ideas that will be used for these proofs are basically the same as those used in [9, 13–15, 17, 24, 32, 55].

Proof of theorem 1. For a single-channel scenario, the only possible bipartition $A\mathcal{C}_A{:}\mathcal{C}_B B$ of the network is the trivial one $A{:}B$. Moreover, at every round of the adaptive strategy the only channel Alice and Bob can use is $\mathcal{N}_{A\to B}$, which is associated with the only edge l_0 of the graph. Therefore, for all $\boldsymbol{k}_n$

$$m^{(l_0)}(\boldsymbol{k}_n) = m(\boldsymbol{k}_n), \tag{33}$$

and the thesis of theorem 2 simplifies to:

$$\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}} \leqslant \frac{1}{g_E(\epsilon)} [f_E(\epsilon) + \langle m \rangle_{\mathcal{P}_{\epsilon,n}} E(\mathcal{N})]. \tag{34}$$

□

Proof of theorem 2. In this proof we will make use of the notation introduced in section 2.5 to describe a generic adaptive protocol $\mathcal{P}_{\epsilon,n}$. Property P1, together with equation (20), implies:

$$\log_2 d_{\boldsymbol{k}_n} \leqslant \frac{1}{g_E(\epsilon)} (f_E(\epsilon) + E^{A:B}(\rho_{AB}^{\boldsymbol{k}_n})). \tag{35}$$

By exploiting the monotonicity of E under partial trace, and by averaging over all possible outcomes, we can write for any bipartition $\{\mathcal{C}_A, \mathcal{C}_B\}$ of the set of nodes $\{C_i\}_i$:

$$\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}} = \sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) \log_2 d_{\boldsymbol{k}_n} \leqslant \frac{1}{g_E(\epsilon)} \left[f_E(\epsilon) + \sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_n}) \right], \tag{36}$$

where $\rho^{\boldsymbol{k}_n}$ is the final state of the protocol, spread across the whole network. The second term written between square brackets on the right-hand side can be expanded into two terms as

$$\sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_n}) \leqslant \sum_{\boldsymbol{k}_{n-1}} p(\boldsymbol{k}_{n-1}) E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_{n-1}}) + \sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) \sum_{l \in L_{\mathcal{C}_A}} \delta_{l,l_{\boldsymbol{k}_{n-1}}} E[\mathcal{N}^{(l)}]. \tag{37}$$

The former is self-similar, but evaluated on the previous round of the protocol, while the latter characterises the ability of the last channel used to create entanglement across the bipartition $A\mathcal{C}_A{:}\mathcal{C}_B B$. In particular, the second term does not always appear, because the channel $\mathcal{N}^{(l_{\boldsymbol{k}_{n-1}})}$ might not connect $A\mathcal{C}_A$ with $\mathcal{C}_B B$, or the parties may have decided not to use a channel at all. This last case could be represented, for example, by any value of $l_{\boldsymbol{k}_{n-1}}$ not in the set L of graph edges. In order to prove equation (37), we can first expand the left-hand side as

$$\sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_n}) = \sum_{\boldsymbol{k}_{n-1}} p(\boldsymbol{k}_{n-1}) \left[\sum_{k_n} p(k_n|\boldsymbol{k}_{n-1}) E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_n}) \right], \tag{38}$$

and then use the following chain of inequalities:

$$\sum_{k_n} p(k_n|\boldsymbol{k}_{n-1}) E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_n}) \overset{\text{(i)}}{\leqslant} E^{A\mathcal{C}_A:\mathcal{C}_B B}(\tilde{\rho}^{\boldsymbol{k}_{n-1}}) \overset{\text{(ii)}}{\leqslant} E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_{n-1}}) + \sum_{l \in L_{\mathcal{C}_A}} \delta_{l,l_{\boldsymbol{k}_{n-1}}} E[\mathcal{N}^{(l)}], \tag{39}$$

where (i) is due to the monotonicity of E under LOCC operations, while (ii) directly follows from property P2. After combining equations (38) and (39), we can recover equation (37) simply by noticing that the average over $\boldsymbol{k}_{n-1}$ on the rightmost term of equation (39) can be freely changed into an average over $\boldsymbol{k}_n$. The same procedure can be iteratively applied for every round of the protocol, so that at the end we are left with

$$\sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{\boldsymbol{k}_n}) \leqslant E^{A\mathcal{C}_A:\mathcal{C}_B B}(\rho^{(1)}) + \sum_{j=0}^{n-1} \sum_{\boldsymbol{k}_n} p(\boldsymbol{k}_n) \sum_{l \in L_{\mathcal{C}_A}} \delta_{l,l_{k_j}} E[\mathcal{N}^{(l)}]$$
$$= \sum_{l \in L_{\mathcal{C}_A}} \langle m^{(l)} \rangle E[\mathcal{N}^{(l)}], \tag{40}$$

where the last equality is due to the separability of the initial state $\rho^{(1)}$ and to the definition of $\langle m^{(l)} \rangle$ given in equation (22). At this point, the thesis of theorem 2 follows directly from the inequality given in equation (36). □

4. Versatile upper bound for quantum networks

As we have seen, an entanglement measure E can lead to an upper bound on the capacity of a channel if it satisfies a continuity inequality (property P1), and a recursive relation connecting the entanglement of the state before and after the channel application (property P2). In the previous section we discussed the possibility of changing entanglement measures across different bipartitions. However, in doing so we have to guarantee that, for each bipartition $\mathcal{C}_A$, the chosen measure satisfies property P2 for *every* channel $\mathcal{N}^{(l)}$ with $l \in L_{\mathcal{C}_A}$. This constraint leads to weaker upper bounds than what would be obtained if we could change entanglement measure on a channel-by-channel basis. For example, consider a situation where all the channels in a given bipartition are Choi-simulable, with only one exception: the presence of this single unsimulable channel prevents us from using E_{R} in the bound of theorem 2. Instead, we are forced to use some broadly applicable entanglement measure (as E_{sq} or $E_{\max}$) on every channel of the bipartition, thus loosening the bound.

In this section we overcome this issue, by exploiting a recent result on sandwiched Rényi entropies [15]. In particular, we construct an upper bound on $\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}}$ that allows us to switch between E_{R} and $E_{\max}$, depending on the Choi-simulability of each channel. To begin with, in the following we describe the recent result obtained in [15], which is the cornerstone of our method. Then, we prove our main result.

4.1. Versatile property P2 for the relative and max-relative entropy of entanglement

For any quantum channel $\mathcal{N}_{A'\to B'}$, and any real parameter $1 \leqslant \alpha < \infty$, if

$$\tilde{\rho}_{AB'B} = \mathcal{N}_{A'\to B'}(\rho_{AA'B}), \tag{41}$$

one has [15]

$$E_\alpha(\tilde{\rho}_{AB'B}) \leqslant E_{\max}(\mathcal{N}_{A'\to B'}) + E_\alpha(\rho_{AA'B}). \tag{42}$$

The quantity E_α is defined in terms of the sandwiched Rényi relative entropy $\tilde{D}_\alpha$ [58, 59]:

$$E_\alpha(\rho_{AB}) = \min_{\sigma_{AB} \in \mathrm{SEP}} \tilde{D}_\alpha(\rho_{AB} \| \sigma_{AB})$$
$$= \min_{\sigma_{AB} \in \mathrm{SEP}} \frac{1}{\alpha - 1} \log_2 \mathrm{Tr}\left[\left(\sigma_{AB}^{\frac{1-\alpha}{2\alpha}} \rho_{AB} \sigma_{AB}^{\frac{1-\alpha}{2\alpha}} \right)^\alpha \right], \tag{43}$$

where σ_{AB} is optimised over all separable states. As E_α tends respectively to E_{R} and $E_{\max}$ in the limits of $\alpha \to 1$ and $\alpha \to \infty$, by setting $\alpha = 1$ in equation (44) we obtain

$$E_{\mathrm{R}}(\tilde{\rho}_{AB'B}) \leqslant E_{\max}(\mathcal{N}_{A'\to B'}) + E_{\mathrm{R}}(\rho_{AA'B}). \tag{44}$$

This inequality closely resembles property P2 for E_{R}, which was obtained in equation (18) for Choi-simulable channels. However, thanks to the introduction of $E_{\max}$ on the right hand side, equation (44) now holds even for non Choi-simulable channels. By combining equation (18) with equation (44), we can obtain a versatile property P2 for the relative entropy of entanglement, in which the right-hand side changes according to the Choi-simulability of $\mathcal{N}_{A'\to B'}$:

$$E_{\mathrm{R}}(\tilde{\rho}_{AB'B}) \leqslant E_{\mathrm{R}}(\rho_{AA'B}) + \begin{cases} E_{\mathrm{R}}(\mathcal{N}), & \text{if } \mathcal{N} \in \mathcal{S}, \\ E_{\max}(\mathcal{N}), & \text{otherwise}, \end{cases} \tag{45}$$

where $\mathcal{S}$ is the set of Choi-simulable channels. Note that this is the best choice, as $E_R \leqslant E_{\max}$ for all states (see equation (12)).

4.2. Versatile upper bound for quantum networks

We have now all the tools to obtain a versatile upper bound on the length of ebit (or pbits) shared by Alice and Bob at the end of a generic adaptive protocol $\mathcal{P}_{\epsilon,n}$, assisted by unlimited classical communication, over a quantum network.

Theorem 3. *Consider a quantum network with an associated directed graph G. For a given bipartition* $\{\mathcal{C}_A, \mathcal{C}_B\}$ *of the network nodes* $\{C_i\}_i$*, let* $L_{\mathcal{C}_A} \subset L$ *be the set of edges in G that connect a node in* AC_A *with one in* $\mathcal{C}_B B$*. The average number of ebits (or pbits) that Alice and Bob share at the end of a given adaptive communication protocol* $\mathcal{P}_{\epsilon,n}$*, assisted by unlimited classical communication, can be upper bounded as*

$$\langle \log_2 d \rangle_{\mathcal{P}_{\epsilon,n}} \leqslant \frac{1}{g_{E_R}(\epsilon)} [f_{E_R}(\epsilon) + \mathcal{E}'(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A)], \tag{46}$$

where

$$\mathcal{E}'(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A) \equiv \sum_{\substack{l \in L_{\mathcal{C}_A}: \\ \mathcal{N}^{(l)} \in \mathcal{S}}} \langle m^{(l)} \rangle_{\mathcal{P}_{\epsilon,n}} E_R(\mathcal{N}^{(l)}) + \sum_{\substack{l \in L_{\mathcal{C}_A}: \\ \mathcal{N}^{(l)} \notin \mathcal{S}}} \langle m^{(l)} \rangle_{\mathcal{P}_{\epsilon,n}} E_{\max}(\mathcal{N}^{(l)}), \tag{47}$$

with $f_{E_R}(\epsilon) = -2[\epsilon \log_2 \epsilon + (1-\epsilon)\log_2(1-\epsilon)]$ *and* $g_{E_R}(\epsilon) = 1 - 8\epsilon$.

Proof of theorem 3. The proof follows closely the one provided for theorem 2, with $E = E_R$. The only difference lies in equation (39), where we use the inequality in equation (45) instead of the original property P2. Therefore, equation (39) has to be substituted with

$$E_R^{AC_A:C_BB}(\tilde{\rho}^{\boldsymbol{k}_{n-1}}) \leqslant E_R^{AC_A:C_BB}(\rho^{\boldsymbol{k}_{n-1}}) + \sum_{\substack{l \in L_{\mathcal{C}_A}: \\ \mathcal{N}^{(l)} \in \mathcal{S}}} \delta_{l,l_{\boldsymbol{k}_{n-1}}} E_R(\mathcal{N}^{(l)}) + \sum_{\substack{l \in L_{\mathcal{C}_A}: \\ \mathcal{N}^{(l)} \notin \mathcal{S}}} \delta_{l,l_{\boldsymbol{k}_{n-1}}} E_{\max}(\mathcal{N}^{(l)}), \tag{48}$$

where we split the sum over the Choi-simulable and non-Choi-simulable channels connecting the nodes on different sides of the network partition. The remainder of the proof then follows the same steps used in the proof of theorem 2. We also explicitly provide the expressions for the functions $f_{E_R}(\epsilon)$ and $g_{E_R}(\epsilon)$ appearing in property 1 (see e.g. [14]). □

Thanks to this result, we have managed to merge the upper bounds based on the quantities $\mathcal{E}_{E_R}$ and $\mathcal{E}_{E_{\max}}$ into a single bound, which retains the advantages given by the two entanglement measures, i.e., tightness and broad applicability. Therefore, in assessing the communication performance of an adaptive protocol $\mathcal{P}_{\epsilon,n}$ over a quantum network, for any given bipartition $AC_A{:}C_BB$ one just needs to compare $\mathcal{E}'$ with the bound $\mathcal{E}_{E_{sq}}$ based on the squashed entanglement [24]. This is because the dependence on f_E and g_E vanishes for small errors ϵ. In particular, the advantage of using $\mathcal{E}'$ over $\mathcal{E}_{E_{sq}}$ for the bipartition $AC_A{:}C_BB$ can be quantified by the parameter

$$\mu_{\mathcal{C}_A}(\mathcal{P}_{\epsilon,n}) = \frac{\mathcal{E}_{E_{sq}}(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A) - \mathcal{E}'(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A)}{\mathcal{E}_{E_{sq}}(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A) + \mathcal{E}'(\mathcal{P}_{\epsilon,n}, \mathcal{C}_A)}, \tag{49}$$

which is defined in the range $[-1, +1]$ and is positive when the versatile bound $\mathcal{E}'$ is tighter than $\mathcal{E}_{E_{sq}}$. The sign of $\mu_{\mathcal{C}_A}(\mathcal{P}_{\epsilon,n})$ will ultimately depend on the details of the bipartition and on the average number of times each channel is used. However, we can expect $\mathcal{E}'$ to be tighter than $\mathcal{E}_{E_{sq}}$ on bipartitions mostly connected by Choi-simulable channels, because the most common of these channels satisfy $E_R(\mathcal{N}) < E_{sq}(\mathcal{N})$. In contrast, when there is a considerable amount of channels that are not Choi-simulable, the sign of $\mu_{\mathcal{C}_A}(\mathcal{P}_{\epsilon,n})$ will strongly depend on the sign of $E_{sq}(\mathcal{N}) - E_{\max}(\mathcal{N})$: every non Choi-simulable channel $\mathcal{N}$ for which this difference is positive will enhance the usefulness of $\mathcal{E}'$ over $\mathcal{E}_{E_{sq}}$.

We should stress that $\mathcal{E}'$, $\mathcal{E}_{E_{sq}}$, and thus $\mu_{\mathcal{C}_A}(\mathcal{P}_{\epsilon,n})$ might not be easily evaluated, because the exact values of $E_{sq}(\mathcal{N})$ and $E_{\max}(\mathcal{N})$ are not known for many channels. When evaluating communication bounds, in practice it is common to consider the smallest known upper bounds $\tilde{E}_{sq}(\mathcal{N})$ and $\tilde{E}_{\max}(\mathcal{N})$ on those unknown quantities, rather than their exact values. When these approximations are introduced in equations (31) and (47) we are left with slightly different quantities $\tilde{\mathcal{E}}'$ and $\tilde{\mathcal{E}}_{E_{sq}}$, which if used instead of $\mathcal{E}'$ and $\mathcal{E}_{E_{sq}}$ in equation (49) lead to a modified parameter $\tilde{\mu}_{\mathcal{C}_A}(\mathcal{P}_{\epsilon,n})$. Then, we can say that currently our versatile upper bound yields a better result than the network bound based on squashed entanglement when $\tilde{\mu}_{\mathcal{C}_A}(\mathcal{P}_{\epsilon,n}) > 0$.

Before discussing examples of networks where the bound provided by theorem 3 becomes tighter than its counterpart based on the squashed entanglement, we first need to evaluate $E_{\max}(\mathcal{N})$ for some channels of interest. In particular, in the next section we will consider typical qubit quantum channels.

5. Max-relative entropy of entanglement of qubit channels

In this section we develop a method to obtain lower and upper bounds on the max-relative entropy of entanglement of channels invariant under phase rotations, and to evaluate $E_{\max}$ itself for Choi-simulable channels with the same symmetry. After that, we discuss the possibility of using SDP in order to evaluate the max-relative entropy of entanglement of qubit channels, by using a formulation recently introduced in [40]. Interestingly, by combining these tools we are able to analytically obtain the max-relative entropy of

entanglement of the qubit amplitude damping channel $\mathcal{N}^{(\mathrm{ad})}$. As this channel is not Choi-simulable its capacity is still unknown, although several upper bounds on it have been recently derived [14, 16]. At the end of this section we also numerically evaluate the max-relative entropy of entanglement of other common Choi-simulable qubit channels: dephasing, erasure and depolarising channels. Although the relative entropy of entanglement could be used to bound the capacities of these channels, the purpose of this analysis is to see how far off the upper bound based on max-relative entropy of entanglement is, compared with other bounds known in the literature.

In general, the calculation of the max-relative entropy of entanglement of a channel involves a max–min optimisation (see equations (4) and (10)):

$$E_{\max}(\mathcal{N}) = \max_{\rho_{AA'}} \min_{\sigma_{AB}\in \mathrm{SEP}} \inf_{x} \{x \in \mathbb{R} | 2^{x}\sigma_{AB} - \mathcal{N}_{A'\to B}[\rho_{AA'}] \geqslant 0\}. \tag{50}$$

In fact, the maximisation over $\rho_{AA'}$ can be restricted to bipartite pure states with the dimension of A equal to that of A'. This can be shown by purifying $\rho_{AA'}$ and by applying the Schmidt decomposition and the date processing inequality for the sandwiched Rényi relative entropy [60]. Nonetheless, typically the optimisation leading to $E_{\max}(\mathcal{N})$ is still not trivial to perform. However, the max-relative entropy of entanglement of a channel can always be bounded from both sides as stated in the following proposition, whose proof can be found in appendix A. The upper bound is a re-elaborated version of the upper bound on the max-relative entropy of entanglement of a channel studied in [15]. In order to explicitly perform the required optimisations, it is useful to exploit as much as possible the symmetries of the considered channel $\mathcal{N}$. In particular, in appendix B we develop tools applicable to qubit channels invariant under phase rotations.

Proposition 1. *Let $\pi_{\mathcal{N}} = \mathbb{1}_A \otimes \mathcal{N}_{A'\to B}[\psi_{AA'}]$ be the Choi–Jamiołkowski state associated with the quantum channel $\mathcal{N}$ with input dimension d, where $\psi_{AA'}$ is a maximally entangled state. Then, we have*

$$\min_{\sigma_{AB}\in \mathrm{SEP}} D_{\max}(\pi_{\mathcal{N}}\|\sigma_{AB}) \leqslant E_{\max}(\mathcal{N}) \leqslant \min_{\substack{\sigma_{AB}\in \mathrm{SEP} \\ \mathrm{Tr}_B[\sigma_{AB}]=\mathbb{1}_A/d}} D_{\max}(\pi_{\mathcal{N}}\|\sigma_{AB}). \tag{51}$$

Moreover, if $\mathcal{N}$ is Choi-simulable, the lower bound is equal to $E_{\max}(\mathcal{N})$ itself.

An alternative expression for the max-relative entropy of a channel has been recently proposed in [40], and can be written as

$$E_{\max}(\mathcal{N}) = \log_2 \Sigma(\mathcal{N}), \tag{52}$$

where

$$\Sigma(\mathcal{N}) = \min_{Y_{AB}\in \overrightarrow{\mathrm{SEP}}} \{\| \mathrm{Tr}_B[Y_{AB}]\|_\infty : Y_{AB} - d\, \pi_{\mathcal{N}} \geqslant 0\}. \tag{53}$$

Here d is the input dimension of the channel $\mathcal{N}$, and $\overrightarrow{\mathrm{SEP}}$ denotes the cone of (unnormalised) separable operators, i.e., the set of all operators X_{AB} that can be decomposed as $X_{AB} = \sum_{i=1}^{L} P_A^i \otimes Q_B^i$ for some positive integer L and positive semidefinite operators P_A^i and Q_B^i. Note that for qubit channels we can replace $\overrightarrow{\mathrm{SEP}}$ by the cone of all positive semidefinite operators that are PPT, thus making the evaluation of equation (53) efficiently computable via SDP.

5.1. Amplitude damping channel

We begin by studying the most important example among channels that are not Choi-simulable: the qubit amplitude damping channel $\mathcal{N}_\lambda^{(\mathrm{ad})}$, which can be written as

$$\mathcal{N}_\lambda^{(\mathrm{ad})}(\rho) = \sum_{i=1}^{2} M_i(\mathcal{N}_\lambda^{(\mathrm{ad})})\rho M_i^\dagger(\mathcal{N}_\lambda^{(\mathrm{ad})}), \tag{54}$$

in terms of the Kraus operators:

$$M_1(\mathcal{N}_\lambda^{(\mathrm{ad})}) = |0\rangle\langle 0| + \sqrt{1-\lambda}|1\rangle\langle 1|, \qquad M_2(\mathcal{N}_\lambda^{(\mathrm{ad})}) = \sqrt{\lambda}|0\rangle\langle 1|. \tag{55}$$

Note that $\mathcal{N}_\lambda^{(\mathrm{ad})}$ reduces to the identity channel when $\lambda = 0$. In particular, we analytically calculate the lower and upper bounds on $E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})})$ found in proposition 1:

$$F(\lambda) \leqslant E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \leqslant \tilde{E}_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}), \tag{56}$$

where

$$F(\lambda) \equiv \begin{cases} \log_2\left[\frac{1}{2}(1+\sqrt{1-\lambda})^2\right], & \text{if } \lambda \leqslant \frac{\sqrt{5}-1}{2}, \\ \log_2\left(\frac{1+\lambda}{2\lambda}\right), & \text{if } \lambda \geqslant \frac{\sqrt{5}-1}{2}, \end{cases} \qquad \text{and} \qquad \tilde{E}_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \equiv \log_2(2-\lambda). \tag{57}$$

The proofs for these inequalities can be found respectively in appendices C and D.

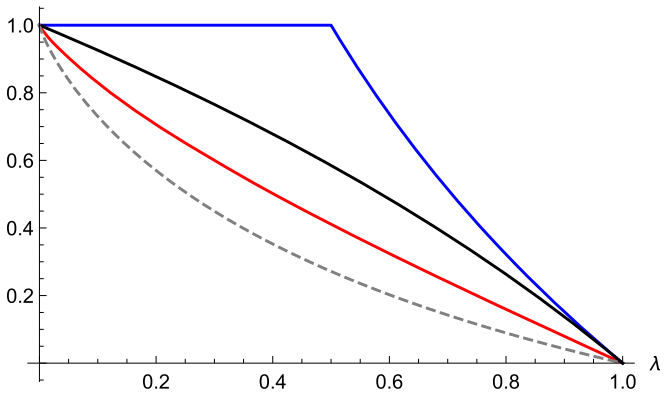


Figure 2. Grey dashed line: best known lower bound on the capacity $C(\mathcal{N}^{(\mathrm{ad})})$, corresponding to the reverse coherent information [61] of the channel (see [14]). The remaining solid lines are all upper bounds on the capacity $C(\mathcal{N}^{(\mathrm{ad})})$. In particular, the top blue line is the bound based on the relative entropy of entanglement discussed in [14], the bottom red line is the best known bound based on the squashed entanglement [14], and the black line in the middle is $E_{\max}(\mathcal{N}^{(\mathrm{ad})})$.

We stress that $\tilde{E}_{\max}(\mathcal{N}_{\lambda}^{(\mathrm{ad})})$ is also an upper bound on the capacity $C(\mathcal{N}_{\lambda}^{(\mathrm{ad})})$, whereas $F(\lambda)$ does not have any known relation with the capacity. Interestingly, the numerical evaluation of $E_{\max}(\mathcal{N}^{(\lambda)})$ via the SDP procedure in equation (53) coincides with the upper bound in equation (56) up to numerical errors. This suggests that for all $\lambda \in [0,\ 1]$ the max-relative entropy of entanglement of the amplitude damping channel exactly coincides with its upper bound found through proposition 1. Indeed, this is analytically proven in appendix E, and we can write it here as a proposition.

Proposition 2. *The max-relative entropy of entanglement of a qubit amplitude damping channel* $\mathcal{N}_{\lambda}^{(\mathrm{ad})}$ *is*

$$E_{\max}(\mathcal{N}_{\lambda}^{(\mathrm{ad})}) = \log_2(2 - \lambda). \tag{58}$$

The plot in figure 2 shows how $E_{\max}(\mathcal{N}_{\lambda}^{(\mathrm{ad})})$, plotted as a black curve, can be compared with other bounds on $C(\mathcal{N}_{\lambda}^{(\mathrm{ad})})$ known in the literature. In particular, it is much smaller than the upper bound on the capacity obtained in [14], represented by the top blue solid curve in figure 2. The latter was obtained by decomposing the amplitude damping channel as $\mathcal{N}_{\lambda}^{(\mathrm{ad})} = \mathcal{N}_1 \circ \mathcal{L} \circ \mathcal{N}_2$, where $\mathcal{L} \in \mathcal{S}$ but $\mathcal{N}_1$ and $\mathcal{N}_2$ are not, and by considering the bound $C(\mathcal{N}_{\lambda}^{(\mathrm{ad})}) \leqslant E_{\mathrm{R}}(\mathcal{L})$. However, the upper bound on the capacity based on the squashed entanglement [14] is smaller than our result obtained through $E_{\max}$. For completeness, we also plotted the best known lower bound on $C(\mathcal{N}_{\lambda}^{(\mathrm{ad})})$, which narrows the region where the capacity value could be [14, 16]. From this analysis, we can conclude that at the moment the best known upper bound on the capacity of the amplitude damping channel remains based on its squashed entanglement.

5.2. Other Choi-simulable channels

Here we numerically evaluate the max-relative entropy of entanglement of some common qubit channels: dephasing, erasure, and depolarising channels. Note that the capacities of the first two channels are given by single-letter formulas, and are thus known exactly. In our numerical simulations we perform the SDP optimisation in equation (53), which yields the same results obtained by numerically evaluating the lower bound in proposition 1.

The dephasing channel $\mathcal{N}_{\lambda}^{(\mathrm{deph})}$ and depolarising channel $\mathcal{N}_{\lambda}^{(\mathrm{depo})}$ can be respectively written in terms of a set of 2 and 5 Kraus operators:

$$M_1(\mathcal{N}_{\lambda}^{(\mathrm{deph})}) = \sqrt{1 - \frac{\lambda}{2}}\,\mathbb{1}, \qquad M_2(\mathcal{N}_{\lambda}^{(\mathrm{deph})}) = \sqrt{\frac{\lambda}{2}}\,\sigma_z, \tag{59}$$

$$M_0(\mathcal{N}_{\lambda}^{(\mathrm{depo})}) = \sqrt{1 - \lambda}\,\mathbb{1}, \qquad M_{ij}(\mathcal{N}_{\lambda}^{(\mathrm{depo})}) = \sqrt{\frac{\lambda}{2}}\,|i\rangle\langle j|, \tag{60}$$

with $i,\ j = 0,\ 1$. The erasure channel $\mathcal{N}^{(\mathrm{er})}$, on the other hand, is characterised by the Kraus operators

$$M_2(\mathcal{N}_{\lambda}^{(\mathrm{er})}) = \sqrt{1 - \lambda}\,\mathbb{1}, \qquad M_i(\mathcal{N}_{\lambda}^{(\mathrm{er})}) = \sqrt{\lambda}\,|e\rangle\langle i|, \tag{61}$$

where $i = 0, 1$, and $|e\rangle$ is an error state orthogonal to both $|0\rangle$ and $|1\rangle$. All these channels reduce to the identity channel when $\lambda = 0$.

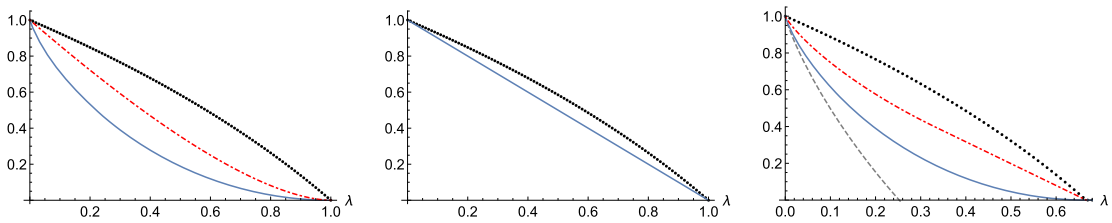


Figure 3. Bounds on the capacity of three Choi-simulable qubit channels. In each plot, the solid blue line represents $E_{\mathrm{R}}(\mathcal{E}_\lambda)$, and coincides with the capacity $C(\mathcal{E}_\lambda)$ for the dephasing and erasure channel. For the depolarising channel, the capacity $C(\mathcal{E}_\lambda^{(\mathrm{depo})})$ lies between the blue solid line and the grey dashed line, which respectively represent its best known upper and lower bounds (see, e.g., [14]). The depolarising channel has zero capacity for $\lambda > 2/3$, where it becomes entanglement breaking, so that region has not been plotted. Red dotted–dashed lines: smallest known upper bound on the squashed entanglement of the channels [13, 16]. In the specific case of the erasure channel, one has $E_{\mathrm{sq}}(\mathcal{E}_\lambda^{(\mathrm{er})}) = E_{\mathrm{R}}(\mathcal{E}_\lambda^{(\mathrm{er})})$ [14, 16]. Black dots: numerical evaluations of $E_{\max}(\mathcal{N}_\lambda)$, obtained via the SDP optimisation in equation (53).

We point out that exact values for the max-relative entropy of entanglement of these channels are not needed when evaluating the versatile network bound of theorem 3. This is because they are all Choi-simulable, and the entanglement generated by them can be quantified by means of E_{R}. Nonetheless, we numerically evaluated $E_{\max}(\mathcal{N})$ for these channels in order to see whether the obtained values could be smaller than their counterparts based on the squashed entanglement. The results can be seen in figure 3. In all these cases E_{R} yields the tighter upper bound on the capacity, followed by the squashed entanglement, while $E_{\max}$ provides the loosest bound.

6. Examples

As we already mentioned in section 4.2, in order to assess whether theorem 3 leads to a tighter bound than the version of theorem 2 based on the squashed entanglement, for any considered bipartition of the network one should study the sign of the parameter $\tilde{\mu}_{\mathcal{C}_A}$. This can be found as in equation (49), but substituting $E_{\mathrm{sq}}(\mathcal{N})$ with its best known upper bound available in the literature. In what follows we provide two examples where $\tilde{\mu}_{\mathcal{C}_A} > 0$.

At first, we should stress that there are quantum channels with $E_{\mathrm{sq}}(\mathcal{N})$ much larger than $E_{\max}(\mathcal{N})$. An example are the 'flower channels' [62, 63] for which the gap between these two quantities can increase with the dimension of the input system [15]. This is due to the fact that the squashed entanglement is 'lockable', which means that by tracing out a subsystem of dimension d its value can change by an amount more than logarithmic in d. On the contrary, $E_{\max}$ is not lockable, and it does not suffer from this drawback. Therefore, $\mathcal{E}'$ would be much tighter than $\mathcal{E}_{E_{\mathrm{sq}}}$ when evaluated on bipartitions mostly composed by flower channels, or composed by flower channels and Choi-simulable channels with E_{R} smaller than E_{sq}, as the qubit channels studied in section 5.2. However, it could be argued that this example is rather artificial, and it is not likely to appear in any realistic communication scenario. For this reason, we also consider a more practical example where the two components of a bipartition $AC_A{:}C_BB$ are connected by k dephasing channels $\mathcal{N}_x^{(\mathrm{deph})}$ and 1 amplitude damping channel $\mathcal{N}_\lambda^{(\mathrm{ad})}$, as shown in figure 4.

If we assume that all channels are used the same average number of times, we can express $\tilde{\mu}_{\mathcal{C}_A}$ as a function of k and of the parameters $x,\ \lambda \in [0,\ 1]$. In particular, we can write

$$\tilde{\mu}_{\mathcal{C}_A} = \frac{k[\tilde{E}_{\mathrm{sq}}(\mathcal{N}_x^{(\mathrm{deph})}) - E_{\mathrm{R}}(\mathcal{N}_x^{(\mathrm{deph})})] + [\tilde{E}_{\mathrm{sq}}(\mathcal{N}_\lambda^{(\mathrm{ad})}) - E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})})]}{k[\tilde{E}_{\mathrm{sq}}(\mathcal{N}_x^{(\mathrm{deph})}) + E_{\mathrm{R}}(\mathcal{N}_x^{(\mathrm{deph})})] + [\tilde{E}_{\mathrm{sq}}(\mathcal{N}_\lambda^{(\mathrm{ad})}) + E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})})]}, \tag{62}$$

where $\tilde{E}_{\mathrm{sq}}(\mathcal{N}_x^{(\mathrm{deph})})$ and $\tilde{E}_{\mathrm{sq}}(\mathcal{N}_\lambda^{(\mathrm{ad})})$ are respectively the best known upper bounds on $E_{\mathrm{sq}}(\mathcal{N}_x^{(\mathrm{deph})})$ [13] and $E_{\mathrm{sq}}(\mathcal{N}_\lambda^{(\mathrm{ad})})$ [14], which have been plotted as red dotted–dashed curves in figures 3(a) and 2:

$$\tilde{E}_{\mathrm{sq}}(\mathcal{N}_x^{(\mathrm{deph})}) = h\left(\sqrt{\frac{x}{2}\left(1 - \frac{x}{2}\right)} + \frac{1}{2}\right), \tag{63}$$

$$\tilde{E}_{\mathrm{sq}}(\mathcal{N}_\lambda^{(\mathrm{ad})}) = h\left(\frac{1}{2} - \frac{\lambda}{4}\right) - h\left(1 - \frac{\lambda}{4}\right), \tag{64}$$

where $h(y) \equiv -y\log_2 y - (1-y)\log_2(1-y)$. Moreover, the quantity $E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})})$ has been shown to coincide with the upper bound obtained in proposition 1, whereas the quantity $E_{\mathrm{R}}(\mathcal{N}_x^{(\mathrm{deph})})$ is known to be equal to $1 - h(x/2)$ [14]. The results obtained for $\tilde{\mu}_{\mathcal{C}_A}$ are plotted in figure 5 for $k = 1,\ 5,\ 10$ and 50. As expected, we can see that the region of parameters $(x,\ \lambda)$ with $\tilde{\mu}_{\mathcal{C}_A} > 0$, i.e., in which our versatile bound is advantageous,

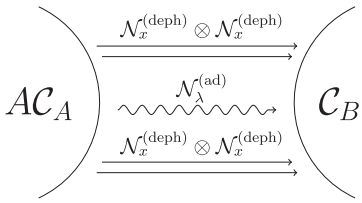
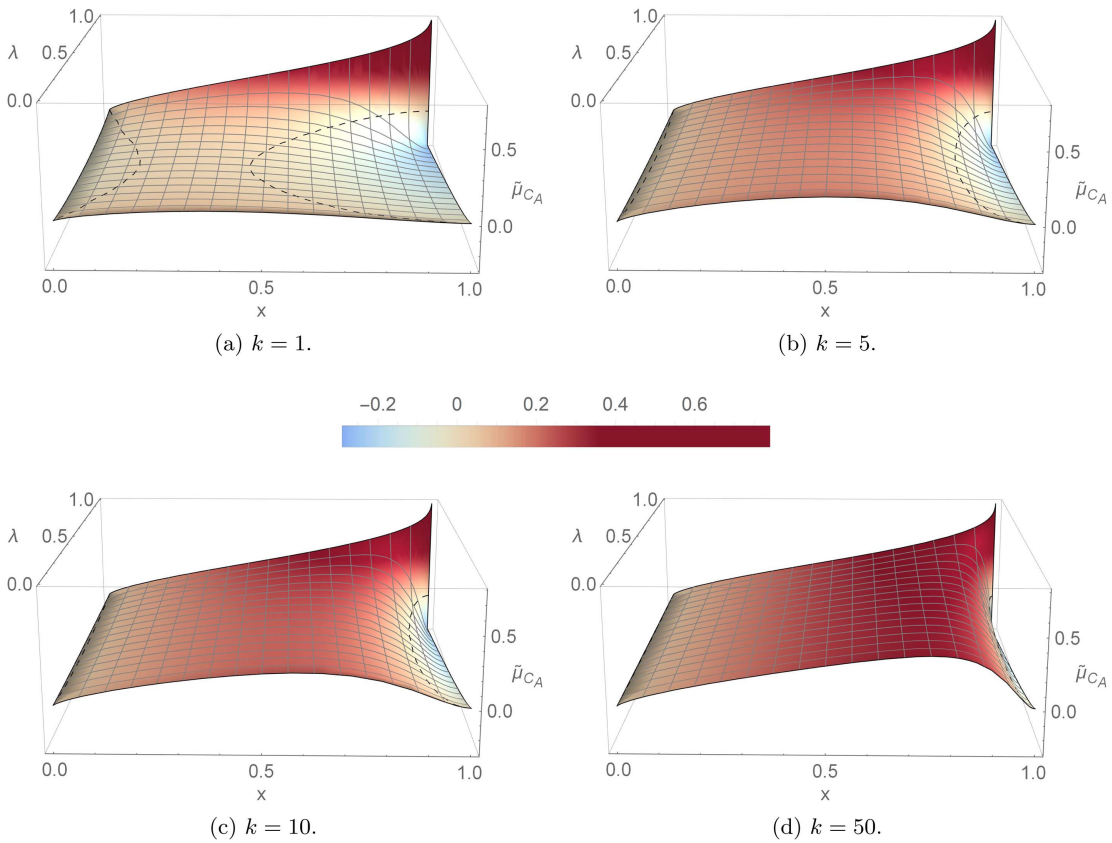


Figure 4. Example of bipartition $AC_A{:}C_BB$ connected by $k = 4$ dephasing channels (straight lines) and 1 amplitude damping channel (wiggling line). Once a bipartition of the network has been selected, it is not necessary to keep track of the precise nodes connected by the channels in order to apply theorem 3.



(a) $k = 1$. (b) $k = 5$. (c) $k = 10$. (d) $k = 50$.

Figure 5. Relative advantage of the versatile upper bound $\mathcal{E}'$ over the upper bound $\mathcal{E}_{E_{\mathrm{sq}}}$ based on the squashed entanglement, as measured by the parameter $\tilde{\mu}_{\mathcal{C}_A}$, for a bipartition of the network whose components are connected by k dephasing channels $\mathcal{N}_x^{(\mathrm{deph})}$ and 1 amplitude damping channel $\mathcal{N}_\lambda^{(\mathrm{ad})}$. The set of points characterised by $\tilde{\mu}_{\mathcal{C}_A} = 0$ is highlighted on the plots by dashed black curves. Our versatile bound is tighter than the best known upper bound based on the squashed entanglement on the regions where $\tilde{\mu}_{\mathcal{C}_A} > 0$.

becomes larger with k. However, even for $k = 1$ there is a broad set of parameters for which our versatile bound is tighter than the bound based on the squashed entanglement. In particular, this is the case when $\lambda \simeq 1$, because the negative contribution in $\tilde{\mu}_{\mathcal{C}_A}$ from $E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \geqslant \tilde{E}_{\mathrm{sq}}(\mathcal{N}_\lambda^{(\mathrm{ad})})$ is close to zero. On the contrary, the bound based on the squashed entanglement is preferable when $x \simeq 1$, because $E_{\mathrm{sq}}(\mathcal{N}_x^{(\mathrm{deph})})$ is close to zero and $E_{\mathrm{R}}(\mathcal{N}_x^{(\mathrm{deph})})$ cannot be significantly smaller. The peak that can be observed in $\tilde{\mu}_{\mathcal{C}_A}$ for $x,\ \lambda \to 1$ is due to the fact that the upper bounds on the number of ebits (pbits) produced by the network go to zero, and small differences of one bound with respect to the other become significant.

7. Discussion and conclusions

In this paper, we investigated the possibility of using multiple entanglement measures in order to upper bound the number of ebits (or pbits) shared by two parties at the end of a communication protocol over a quantum network, with no limit on their classical communication. In particular, we exploited the special relation between

the relative entropy and the max-relative entropy of entanglement, summarised by equation (44), in order to jointly use them in a single bound, which retains the advantages of both measures. For instance, it is possible to take advantage from the presence of Choi-simulable channels in the network, without requiring this property beforehand. From a theoretical perspective, our versatile bound performs much better than the previously known bound, which was based on the squashed entanglement, on networks composed by flower channels and Choi-simulable channels with E_{R} smaller than E_{sq}. For more physically relevant quantum networks, in general one should check on a case-by-case basis which upper bound yields the tightest result. However, we can expect the versatile bound introduced in theorem 3 to be the best choice when the number of Choi-simulable channels is larger than the number of channels not satisfying this property, at least as long as E_{R} provides tighter bounds than E_{sq} on the Choi-simulable components of the network. This intuition was confirmed for a network composed by k dephasing channels and one amplitude damping channel, where already for $k = 5$ our versatile bound performed better on a broad range of parameters.

We should also reiterate that, according to the authors of [15], equation (42) has been rigorously proven only for channels acting on finite dimensional systems. As theorem 3 heavily relies upon that inequality, one should pay special attention when applying theorem 3 to infinite dimensional channels, as long as the proof of equation (42) will not be suitably extended. Notice, however, that at least some bosonic channels (e.g., photon losses) are Choi-simulable: in these cases we can safely upper bound the entanglement of their output state via equation (18) [14] and theorem 3 still holds.

The advantage provided by our method would be further increased if more entanglement measures could be included within the same framework. An obvious candidate would be the squashed entanglement, because it typically provides tighter upper bounds on the capacity of a quantum channel than $E_{\max}$, while being at the same time broadly applicable. This research line could go together with the search for other entanglement measures that can provide upper bounds on channel capacities. From this point of view, we feel that the schematic framework provided by theorems 1 and 2 could act as a guideline for future investigations. It would also be interesting to look into the possibility of extending this 'versatile' approach to a multi-user scenario, where the network is composed by broadcast quantum channels [34–39].

As a final remark, notice that the idea behind our result can be applied more generally in order to bound the rate at which a parallel composition of quantum channels can generate ebits (or pbits), when assisted by unlimited classical communication. Furthermore, although this paper has been developed from the perspective of quantum communication, it is worth stressing that the problem of quantifying the amount of bipartite, or multipartite, entanglement shared among the nodes of a network is also relevant from the perspective of quantum computation. In this paradigm, the quantum channels can be interpreted as noisy physical operations, and the nodes could represent, for example, the components of a cluster state. As the possibility of performing measurement-based universal quantum computation strongly depends on the entanglement of the initial resource state [64], the ideas developed in this paper could also help in assessing the quality of entangled resources [65], by considering $\mathcal{P}_{\epsilon,n}$ as the sequence of operations generating them.

Acknowledgments

The authors thank Alexander Müller-Hermes for discussions. We are also indebted with an anonymous referee for bringing to our attention the SDP formulation of the max-relative entropy of entanglement of qubit channels, as well as the sufficient conditions for the strong converse property mentioned in corollary 1. LR expresses his gratitude to the Theoretical Quantum Physics Research Group of NTT BRL for the warm hospitality received during his visit, and acknowledges financial support from the People Programme (Marie Curie Actions) of the European Unions Seventh Framework Programme (FP7/2007-2013) under REA Grant Agreement 317232. KA and GK thank support from the ImPACT Program of Council for Science, Technology and Innovation (Cabinet Office, Government of Japan). MSK acknowledges the UK EPSRC grant (EP/K034480/1), Samsung GRO programme and the Royal Society. WJM acknowledges support from the John Templeton Foundation (JTF #60478). The opinions expressed in this publication are those of the author(s) and do not necessarily reflect the views of the John Templeton Foundation.

Appendix A. Proof of proposition 1

The lower bound is simply obtained by using the maximally entangled state $\psi_{AA'}$ as input in equation (50), without optimising over all $\rho_{AA'}$. Furthermore, its equality with $E_{\max}(\mathcal{N})$ itself in the case of Choi-simulable channels can be obtained as in the last step of equation (18). Indeed, that argument holds for any entanglement measure and not only for E_{R}.

The upper bound, on the other hand, is a re-elaborated version of the upper bound on the max-relative entropy of a channel studied in [15]. In order to obtain their result, the authors introduce a generic entanglement breaking (EB) channel $\mathcal{T}_{A'\to B}$, and use the following chain of inequalities:

$$\begin{aligned} E_{\max}(\mathcal{N}) &\leqslant \max_{\rho_{AA'}} \min_{\mathcal{T}_{A'\to B}\in \mathrm{EB}} \inf_x \{x\in\mathbb{R} | (2^x \mathcal{T}_{A'\to B} - \mathcal{N}_{A'\to B})[\rho_{AA'}] \geqslant 0\} \\ &\leqslant \min_{\mathcal{T}\in\mathrm{EB}} \inf_x \{x\in\mathbb{R} | 2^x \pi_{\mathcal{T}} - \pi_{\mathcal{N}} \geqslant 0\} = \min_{\mathcal{T}\in\mathrm{EB}} D_{\max}(\pi_{\mathcal{N}} \| \pi_{\mathcal{T}}). \end{aligned} \tag{A1}$$

The first inequality is obtained by optimising over a smaller set of separable states, in which σ_{AB} is obtained as output of entanglement-breaking channels acting on the same input state $\rho_{AA'}$. The second inequality is then obtained by noticing that $(2^x\mathcal{T}_{A'\to B} - \mathcal{N}_{A'\to B})[\rho_{AA'}] \geqslant 0$ for any input $\rho_{AA'}$ if the operator $(2^x\mathcal{T}_{A'\to B} - \mathcal{N}_{A'\to B})$ is completely positive, and that this last condition is implied by the positivity of its Choi–Jamiołkowski state. In order to obtain the upper bound of proposition 1, we just need to show that the set of states $\pi_{\mathcal{T}}$ appearing in equation (A1) corresponds to the set of separable density matrices σ_{AB} such that $\mathrm{Tr}_B[\sigma_{AB}] = \mathbb{1}_A/d$. One inclusion is trivial, while the other follows from the fact that, for any such σ_{AB}, we can find a corresponding completely positive and trace preserving (CPTP) map $\tau^{(\sigma_{AB})} \in \mathrm{EB}$ via the teleportation protocol:

$$\mathcal{T}^{(\sigma_{AB})}_{A'\to B}(\tau_{A'}) = d^2\, \mathrm{Tr}_{A'A}[\psi_{A'A}(\tau_{A'}\otimes\sigma_{AB})], \tag{A2}$$

where $\psi_{A'A}$ is a maximally entangled state. Indeed, this map is CPTP because from equation (A2) we obtain a possible set of Kraus operators given by:

$$N^{(h,k)}_{A'\to B} = d\ {}_{A'A}\langle\psi|\ \sqrt{\sigma_{AB}}\ |k\rangle_A |h\rangle_B, \tag{A3}$$

with $\sum_{h,k=1}^{d}(N^{(h,k)}_{A'\to B})^\dagger N^{(h,k)}_{A'\to B} = \mathbb{1}_{A'}$, and a straightforward calculation shows that $\pi_{\mathcal{T}^{(\sigma_{AB})}} = \sigma_{AB}$, thus proving that $\mathcal{T}^{(\sigma_{AB})} \in \mathrm{EB}$ because of the separability of σ_{AB}.

Appendix B. Bounding the max-relative entropy of entanglement of qubit channels invariant under phase rotations

Most of the typical qubit channels are invariant under rotations around the axis associated with the Pauli matrix $\sigma_z = \mathrm{Diag}(+1, -1)$, and it is thus interesting to study the consequences of this fact for the evaluation of the upper and lower bounds identified in proposition 1. Let $\mathcal{N}$ be a quantum channel acting on a qubit, such that

$$\mathcal{N}(\mathrm{e}^{\mathrm{i}\theta\sigma_z}\rho\mathrm{e}^{-\mathrm{i}\theta\sigma_z}) = \mathrm{e}^{\mathrm{i}\theta\sigma_z}\mathcal{N}(\rho)\mathrm{e}^{-\mathrm{i}\theta\sigma_z}, \tag{B1}$$

for all angles θ and input states ρ. As the maximally entangled state $\psi_{AA'}$ is left invariant by the unitary operation

$$U_\theta = \mathrm{e}^{+\mathrm{i}\frac{\theta}{2}\sigma_z^{(A)}} \otimes \mathrm{e}^{-\mathrm{i}\frac{\theta}{2}\sigma_z^{(B)}}, \tag{B2}$$

we can conclude that its Choi state $\pi_{\mathcal{N}}$ is also invariant under U_θ, for any $\theta \in [0, 2\pi]$. This immediately implies that the average of $\pi_{\mathcal{N}}$ over all possible θ rotations coincides with $\pi_{\mathcal{N}}$ itself:

$$\pi_{\mathcal{N}} = \int \frac{\mathrm{d}\theta}{2\pi} U_\theta \pi_{\mathcal{N}} U_\theta^\dagger. \tag{B3}$$

This allows us to prove the following lemma, whose proof can be found at the end of this appendix.

Lemma 1. *Let $\pi_{\mathcal{N}}$ be a bipartite state invariant under the separable unitary evolution U_θ defined in equation (B2), and σ^*_{AB} be the state which minimises $D_{\max}(\pi_{\mathcal{N}}\|\sigma_{AB})$ among all separable states σ_{AB}. If $\overline{\sigma^*}_{AB}$ is the averaged version of σ^*_{AB},*

$$\overline{\sigma^*}_{AB} \equiv \int \frac{\mathrm{d}\theta}{2\pi} U_\theta \sigma^*_{AB} U_\theta^\dagger, \tag{B4}$$

then $\overline{\sigma^*}_{AB}$ is separable and

$$D_{\max}(\pi_{\mathcal{N}}\|\sigma^*_{AB}) = D_{\max}(\pi_{\mathcal{N}}\|\overline{\sigma^*}_{AB}). \tag{B5}$$

Similarly, if σ^*_{AB} is the state which minimises $D_{\max}(\pi_{\mathcal{N}}\|\sigma_{AB})$ over all separable states σ_{AB} with $\mathrm{Tr}_B[\sigma_{AB}] = \mathbb{1}_A/2$, the same conclusion holds with $\mathrm{Tr}_B[\overline{\sigma^*}_{AB}] = \mathbb{1}_A/2$.

As a corollary of lemma 1, we can restrict the minimisation over all separable states σ_{AB} in equation (51) to be only over the states which are left unaltered by being averaged over all possible θ rotations. The density matrix associated with these states in the basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$ has the form

$$\sigma_{AB} = \frac{1}{2}\begin{pmatrix} \alpha & & & \xi e^{i\phi} \\ & \gamma & & \\ & & \delta & \\ \xi e^{-i\phi} & & & \beta \end{pmatrix}, \tag{B6}$$

with α, β, γ, δ, $\xi \geqslant 0$, $\alpha + \beta + \gamma + \delta = 2$, $\phi \in [0, 2\pi]$ and $0 \leqslant \xi \leqslant \min\{\sqrt{\alpha\beta}, \sqrt{\gamma\delta}\}$. Note that the last inequality comes from the PPT criterion, which works for two-qubit states as a necessary and sufficient condition for separability [66]. When evaluating the upper bound in proposition 1, we simply need to add the additional constraints $\gamma = 1 - \alpha$ and $\delta = 1 - \beta$, in order to assure $\mathrm{Tr}_B[\sigma_{AB}] = \mathbb{1}_A/2$.

Proof of lemma 1. The max-relative entropy $D_{\max}(\rho\|\sigma)$ is invariant under joint unitary operations applied on both ρ and σ, and is jointly quasi-convex. Both these properties have been previously introduced in section 2.1, respectively in equation (6) and equation (8). Together with equation (B3), these facts lead to

$$\begin{aligned} D_{\max}(\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \| \overline{\sigma^*}_{AB}) &= D_{\max}\left(\int \frac{\mathrm{d}\theta}{2\pi} U_\theta \pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} U_\theta^\dagger \Big\| \int \frac{\mathrm{d}\theta}{2\pi} U_\theta \sigma^*_{AB} U_\theta^\dagger\right) \\ &\leqslant \max_\theta D_{\max}(U_\theta \pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} U_\theta^\dagger \| U_\theta \sigma^*_{AB} U_\theta^\dagger) = D_{\max}(\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \| \sigma^*_{AB}). \end{aligned} \tag{B7}$$

The converse inequality follows because $\overline{\sigma^*}_{AB}$ is separable, due to the structure of U_θ (see equation (B2)), and because σ^*_{AB} minimises $D_{\max}(\pi_{\mathcal{N}}\|\sigma_{AB})$ over all separable states. The final remark can be easily proven by noticing that $\mathrm{Tr}_B[\overline{\sigma^*}_{AB}] = \mathbb{1}_A/2$ if $\mathrm{Tr}_B[\sigma^*_{AB}] = \mathbb{1}_A/2$. □

Appendix C. Proof for the upper bound in equation (56)

In order to prove the desired result, we need to explicitly perform the optimisation appearing in the upper bound of proposition 1, i.e.

$$\tilde{E}_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \equiv \min_{\substack{\sigma_{AB}\in \mathrm{SEP} \\ \mathrm{Tr}_B[\sigma_{AB}] = \mathbb{1}_A/2}} D_{\max}(\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \| \sigma_{AB}) = \min_{\sigma_{AB}} \inf\{x \in \mathbb{R} | 2^x \sigma_{AB} - \pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \geqslant 0\}, \tag{C1}$$

where thanks to lemma 1 on the rightmost term we can consider only states σ_{AB} with the form given in equation (B6), with $\gamma = 1 - \alpha$ and $\delta = 1 - \beta$. Let us introduce the parameter $y = 2^x$. By explicitly computing the Choi–Jamiołkowski state $\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}}$, the condition $y\sigma_{AB} - \pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \geqslant 0$ can be rewritten as the system of inequalities:

$$\begin{cases} y(1 - \beta) \geqslant \lambda, \\ y\tilde{\sigma} - \tilde{\pi}_\lambda \geqslant 0, \end{cases} \tag{C2}$$

where $\tilde{\sigma}$ and $\tilde{\pi}$ are 2×2 matrices

$$\tilde{\sigma} = \begin{pmatrix} \alpha & \xi e^{i\phi} \\ \xi e^{-i\phi} & \beta \end{pmatrix}, \qquad \tilde{\pi}_\lambda = \begin{pmatrix} 1 & \sqrt{1-\lambda} \\ \sqrt{1-\lambda} & 1 - \lambda \end{pmatrix}. \tag{C3}$$

We now define $y_1(\lambda, \sigma_{AB})$ and $y_2(\lambda, \sigma_{AB})$ as the smallest values of y that satisfy respectively the first and the second inequalities appearing in equation (C2), and we rewrite the minimisation leading to the upper bound on $E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})})$ as

$$\tilde{E}_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \equiv \min_{\sigma_{AB}} \inf\{x \in \mathbb{R} | 2^x \sigma_{AB} - \pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \geqslant 0\} = \log_2 \min_{\sigma_{AB}} \max\{y_1(\lambda, \sigma_{AB}), y_2(\lambda, \sigma_{AB})\}. \tag{C4}$$

We can easily show that this quantity is smaller than or equal to $\log_2(2 - \lambda)$ by providing a matrix σ_{AB} of the desired form such that $\max\{y_1(\lambda, \sigma_{AB}), y_2(\lambda, \sigma_{AB})\} = 2 - \lambda$. This can be achieved with the choices:

$$\alpha = \frac{1}{2 - \lambda}, \qquad \beta = 1 - \alpha, \qquad \xi = \sqrt{\alpha\beta}, \qquad \phi = 0, \tag{C5}$$

which yield $y_1 = \lambda(2 - \lambda)$ and $y_2 = 2 - \lambda$, as can be verified by directly substituting these values into equation (C2). The converse inequality, i.e. $\tilde{E}_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \geqslant \log_2(2 - \lambda)$, requires some additional work. Thanks to the monotonicity of the logarithm and the trivial relation $\max\{y_1, y_2\} \geqslant y_2$, we can bound $\tilde{E}_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})})$ from below as

$$\tilde{E}_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \geqslant \log_2 \min_{\sigma_{AB}} y_2(\lambda, \sigma_{AB}). \tag{C6}$$

Hence, we are left with the task of showing that $\min_{\sigma_{AB}} y_2(\lambda, \sigma_{AB}) \geqslant 2 - \lambda$, where the optimisation has to be effectively performed over the parameters α, β, ξ, ϕ satisfying the conditions detailed after equation (B6), with $\gamma = 1 - \alpha$ and $\delta = 1 - \beta$.

The condition $y\tilde{\sigma} - \tilde{\pi}_\lambda \geqslant 0$ involves 2×2 matrices, and can be rewritten using Pauli matrices $\vec{\sigma} = \{\sigma_x, \sigma_y, \sigma_z\}$ as

$$y(\alpha + \beta)(\mathbb{1} + \vec{v} \cdot \vec{\sigma}) - (2 - \lambda)(\mathbb{1} + \hat{n} \cdot \vec{\sigma}) \geqslant 0, \tag{C7}$$

where

$$\vec{v} = \frac{1}{\alpha + \beta}\begin{pmatrix} 2\xi \cos\phi \\ -2\xi \sin\phi \\ \alpha - \beta \end{pmatrix}, \qquad \hat{n} = \frac{1}{2 - \lambda}\begin{pmatrix} 2\sqrt{1 - \lambda} \\ 0 \\ \lambda \end{pmatrix}. \tag{C8}$$

This in turn reduces to

$$y \geqslant \frac{2 - \lambda}{\alpha + \beta}\,\frac{2(1 - \nu \cos\psi)}{1 - \nu^2} \equiv y_2(\lambda, \sigma_{AB}), \tag{C9}$$

where $\nu = |\vec{v}| \leqslant 1$ and ψ is the angle between $\vec{v}$ and $\hat{n}$. Note that the second fraction appearing in equation (C9) is always larger than 1, therefore, when $\alpha + \beta \leqslant 1$ the condition $y_2(\lambda, \sigma_{AB}) \geqslant 2 - \lambda$ holds. On the other hand, if $1 \leqslant \alpha + \beta \leqslant 2$, we can use the parametrisation:

$$2\xi = \eta(2 - \alpha - \beta)\sin\zeta, \qquad \alpha - \beta = \eta(2 - \alpha - \beta)\cos\zeta, \tag{C10}$$

with $\eta \in [0, 1]$ and $\zeta \in [0, \pi]$. This allows us to conclude because of the following chain of inequalities:

$$\begin{aligned} y_2(\lambda, \sigma_{AB}) &= 2(2 - \lambda)\frac{(\alpha + \beta) - \eta(2 - \alpha - \beta)[\cos(\theta - \zeta) - \sin\theta \sin\zeta(1 - \cos\phi)]}{(\alpha + \beta)^2 - \eta^2(2 - \alpha - \beta)^2} \\ &\geqslant 2(2 - \lambda)\frac{(\alpha + \beta) - \eta(2 - \alpha - \beta)}{(\alpha + \beta)^2 - \eta^2(2 - \alpha - \beta)^2} \\ &= (2 - \lambda)\frac{2}{2\eta + (1 - \eta)(\alpha + \beta)} \geqslant (2 - \lambda), \end{aligned} \tag{C11}$$

where $\theta = \arctan(2\sqrt{1 - \lambda}/\lambda)$ is the angle describing the direction of $\hat{n}$.

Appendix D. Proof for the lower bound in equation (56)

The goal of this appendix is to provide a proof for the following lower bound on $E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})})$:

$$E_{\max}(\mathcal{N}_\lambda^{(\mathrm{ad})}) \geqslant \min_{\sigma_{AB} \in \mathrm{SEP}} \tilde{D}_{\max}(\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \| \sigma_{AB}) = \begin{cases} \log_2\left(\frac{1}{2}(1 + \sqrt{1 - \lambda})^2\right), & \text{if } \lambda \leqslant \frac{\sqrt{5} - 1}{2}, \\ \log_2\left(\frac{1 + \lambda}{2\lambda}\right), & \text{if } \lambda \geqslant \frac{\sqrt{5} - 1}{2}. \end{cases} \tag{D1}$$

Thanks to lemma 1, we can reduce the optimisation over all separable states σ_{AB} that are left unaltered under all possible θ rotations, which can be parametrised as in equation (B6). The condition $y\sigma_{AB} - \pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \geqslant 0$ can be explicitly rewritten as

$$\begin{cases} y \geqslant \frac{\lambda}{\delta}, \\ y \geqslant \frac{\alpha(1 - \lambda) + \beta - 2\sqrt{1 - \lambda}\xi\cos\phi}{\alpha\beta - \xi^2}, \end{cases} \tag{D2}$$

so that

$$\tilde{D}_{\max}(\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}} \| \sigma_{AB}) = \log_2 \max\left\{\frac{\alpha(1 - \lambda) + \beta - 2\xi\cos\phi\sqrt{1 - \lambda}}{\alpha\beta - \xi^2}, \frac{\lambda}{\delta}\right\}. \tag{D3}$$

In what follows, for any fixed λ we will minimise this quantity over the parameters α, β, γ, δ, ξ, ϕ, satisfying the constraints detailed after equation (B6).

The minimisation in ϕ can be easily performed, with the optimal choice being $\phi = 0$. Moreover, for any fixed α, β, ξ, the maximum δ (and thus the minimum λ/δ) is given by

$$\delta_{\max} = \frac{1}{2}(2 - \alpha - \beta + \sqrt{(2 - \alpha - \beta)^2 - 4\xi^2}), \tag{D4}$$

that is, when $\delta > \gamma$ and $\gamma\delta$ equals the smallest allowed value ξ^2. Notice that this choice implies

$$2\xi = 2\sqrt{\gamma\delta} \leqslant \gamma + \delta = 2 - \alpha - \beta. \tag{D5}$$

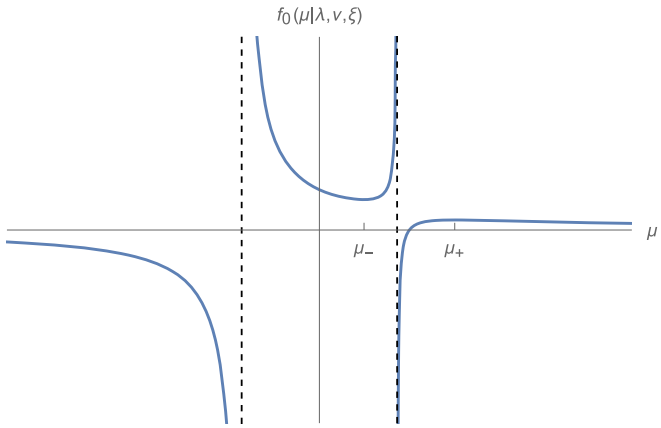


Figure 6. Typical plot of the function $f_0(\mu|\lambda,\,\nu,\,\xi)$ defined in equation (D8).

At this stage, the optimisation problem (without the logarithm) has been reduced to:

$$\min_{\alpha,\beta,\xi}\left\{\max\left[\frac{\alpha(1-\lambda)+\beta-2\xi\sqrt{1-\lambda}}{\alpha\beta-\xi^2},\,\frac{2\lambda}{2-\alpha-\beta+\sqrt{(2-\alpha-\beta)^2-4\xi^2}}\right]\,\middle|\,\begin{array}{c}\alpha,\,\beta,\,\xi\geqslant 0\ \wedge\ \xi^2\leqslant\alpha\beta\\ \wedge\,\alpha+\beta+2\xi\leqslant 2\end{array}\right\}. \tag{D6}$$

Now we introduce the parameters $\nu=(\alpha+\beta)/2$ and $\mu=(\alpha-\beta)/2$. As $\alpha>\delta$ always yields a smaller value than the converse choice, we can limit our study to $\mu\geqslant 0$ and rewrite the problem in the new parameters:

$$\min_{\nu,\mu,\xi}\left\{\max\left[\frac{\nu(2-\lambda)-\lambda\mu-2\xi\sqrt{1-\lambda}}{\nu^2-\xi^2-\mu^2},\,\frac{\lambda}{1-\nu+\sqrt{(1-\nu)^2-\xi^2}}\right]\,\middle|\,\begin{array}{c}0\leqslant\mu\leqslant\sqrt{\nu^2-\xi^2}\\ 0\leqslant\xi\leqslant\nu\ \wedge\ \nu+\xi\leqslant 1\end{array}\right\}. \tag{D7}$$

We can now minimise the first term over μ. The value μ_0 for which the function

$$f_0(\mu|\lambda,\,\nu,\,\xi)=\frac{\nu(2-\lambda)-\lambda\mu-2\xi\sqrt{1-\lambda}}{\nu^2-\xi^2-\mu^2} \tag{D8}$$

becomes zero is always bigger than $\sqrt{\nu^2-\xi^2}$ in the considered region. Together with the asymptotic scaling $f_0(\mu|\lambda,\,\nu,\,\xi)\sim\lambda/\mu$ for $|\mu|\gg 1$, this can be used to deduce the qualitative behaviour of $f_0(\mu|\lambda,\,\nu,\,\xi)$, which is shown in figure 6. Let $\mu_\pm(\lambda,\,\nu,\,\xi)$ be the zeros of $\partial_\mu f_0(\mu|\lambda,\,\nu,\,\xi)$, with $\mu_-\leqslant\mu_+$, where

$$\mu_\pm(\lambda,\,\nu,\,\xi)=\frac{1}{\lambda}[(2-\lambda)\nu-2\sqrt{1-\lambda}\xi]\pm\frac{1}{\lambda}|2\sqrt{1-\lambda}\nu-(2-\lambda)\xi|. \tag{D9}$$

As $f_0(\mu_-|\lambda,\,\nu,\,\xi)\geqslant f_0(\mu_+|\lambda,\,\nu,\,\xi)$, we can find the desired minimum of $f_0(\mu|\lambda,\,\nu,\,\xi)$ in $\mu\in[0,\,\sqrt{\nu^2-\xi^2}]$ as

$$\min_\mu f_0(\mu|\lambda,\,\nu,\,\xi)=\max\{f_0(\mu_-),\,f_0(\mu_+)\}=\max\left\{\frac{(1-\sqrt{1-\lambda})^2}{2(\nu-\xi)},\,\frac{(1+\sqrt{1-\lambda})^2}{2(\nu+\xi)}\right\}. \tag{D10}$$

It is worth substituting $\nu\to x(1+y)/2$ and $\xi\to x(1-y)/2$. In terms of the new variables, the problem after the optimisation in μ becomes

$$\min_{x,y}\left\{\max\left[\frac{(1-\sqrt{1-\lambda})^2}{2xy},\,\frac{(1+\sqrt{1-\lambda})^2}{2x},\,\frac{\lambda}{1-x\frac{(1+y)}{2}+\sqrt{(1-x)(1-xy)}}\right]\,\middle|\,\begin{array}{c}0\leqslant x\leqslant 1\\ 0\leqslant y\leqslant 1\end{array}\right\}, \tag{D11}$$

whose form is suitable to perform the minimisation in y. Let us label the three function appearing between square brackets in order as f_1, f_2 and f_3. Note that f_1 and f_3 are respectively monotonically decreasing and increasing with y, with only the first one diverging to infinity for $y\to 0$. If the two functions do not cross each other, i.e., if $x\leqslant x_{\rm th}\equiv(1-\sqrt{1-\lambda})/2$, the minimum over y is thus obtained by evaluating f_1 in $y=1$, otherwise we need to pick their intersection point. Explicitly, this can be written as

$$\min_y\{f_1,\,f_3\}=\begin{cases}\frac{(1-\sqrt{1-\lambda})^2}{2x}, & \text{if } 0\leqslant x\leqslant x_{\rm th},\\ f_4(x,\,\lambda), & \text{if } x_{\rm th}\leqslant x\leqslant 1,\end{cases} \tag{D12}$$

where

$$f_4(x,\,\lambda)=\frac{1}{2x^2}\left\{8+x\left[\left(\frac{1-\sqrt{1-\lambda}}{\sqrt{\lambda}}\right)^2-4\right]-4\sqrt{(1-x)\left[4+x\left(\frac{1-\sqrt{1-\lambda}}{\sqrt{\lambda}}\right)^2\right]}\right\}. \tag{D13}$$

Finally, we can optimise over x. If $x\leqslant x_{\rm th}$, we are left with:

$$\min_{x\leqslant x_{\rm th}}\max\left\{\frac{(1-\sqrt{1-\lambda})^2}{2x},\,\frac{(1+\sqrt{1-\lambda})^2}{2x}\right\}=\frac{(1+\sqrt{1-\lambda})^2}{2x_{\rm th}}=f_2(x_{\rm th},\,\lambda). \tag{D14}$$

On the other hand, when $x\geqslant x_{\rm th}$, we can apply the same reasoning used for the minimisation over y. In particular, f_2 and f_4 are respectively monotonically decreasing and increasing with x, $f_2(x_{\rm th})\geqslant f_4(x_{\rm th})$, and they have a crossing point only when $\lambda\geqslant(\sqrt{5}-1)/2$. If there is no crossing, the minimum over x is given by $f_2(x=1,\,\lambda)$, which is less than or equal to $f_2(x_{\rm th},\,\lambda)$ of equation (D14). If there is a crossing, instead, the minimum corresponds to the value of the functions at the intersection, which is $\frac{\lambda+1}{2\lambda}$. This concludes the proof.

Appendix E. Proof of proposition 2

Because of equation (52) we need to show the relation $\Sigma(\mathcal{N}_\lambda^{(\rm ad)})=2-\lambda$, where $\Sigma(\mathcal{N}_\lambda^{(\rm ad)})$ has been defined in equation (53). This is equivalent to showing that

$$\min_{Y_{AB}\in\overrightarrow{\rm SEP}}\{\|\,{\rm Tr}_B\,Y_{AB}\|_\infty\colon Y_{AB}-\pi_{\mathcal{N}_\lambda^{(\rm ad)}}\geqslant 0\}=1-\frac{1}{2}\lambda, \tag{E1}$$

where $\|W\|_\infty:=\max_{|\phi\rangle}\langle\phi|\,W|\phi\rangle$, and $\pi_{\mathcal{N}_\lambda^{(\rm ad)}}$ is the normalised Choi state of the amplitude damping channel, which in basis $\{|00\rangle,\,|01\rangle,\,|10\rangle,\,|11\rangle\}$ can be written as

$$\pi_{\mathcal{N}_\lambda^{(\rm ad)}}:=\frac{1}{2}\begin{pmatrix}1&0&0&\sqrt{1-\lambda}\\0&0&0&0\\0&0&\lambda&0\\\sqrt{1-\lambda}&0&0&1-\lambda\end{pmatrix}. \tag{E2}$$

Furthermore, as already observed in the main text, for qubit channels we can replace the cone of separable operators $\overrightarrow{\rm SEP}$ with that of PPT operators

$$\overrightarrow{\rm PPT}:=\{V\colon V\geqslant 0\wedge V^{\rm PT}\geqslant 0\}, \tag{E3}$$

where the superscript PT represents partial transposition on the second qubit.

For the proof we exploit once again the symmetry of the channel under phase rotations, and we define a subset of $\overrightarrow{\rm PPT}$ as

$$\begin{aligned}\overrightarrow{\rm PPT}'&:=\{V\colon V\in\overrightarrow{\rm PPT}\wedge U_\theta V U_\theta^\dagger=V\;\forall\theta\in\mathbb{R}\}\\&=\left\{V\colon V=\begin{pmatrix}\alpha&0&0&\xi e^{i\phi}\\0&\gamma&0&0\\0&0&\delta&0\\\xi e^{-i\phi}&0&0&\beta\end{pmatrix}\wedge\;\alpha,\,\beta,\,\gamma,\,\delta,\,\xi\geqslant 0\;\wedge\;\phi\in[0,\,2\pi]\;\wedge\;0\leqslant\xi\leqslant\min\{\sqrt{\alpha\beta},\,\sqrt{\gamma\delta}\}\right\},\end{aligned} \tag{E4}$$

where U_θ is the unitary rotation defined in equation (B2). We now obtain a long sequence of equalities, which will be commented in the following. In particular, one has

$$
\begin{aligned}
&\min_{Y_{AB}\in\overrightarrow{\mathrm{PPT}}}\{\|\mathrm{Tr}_B\, Y_{AB}\|_\infty\colon Y_{AB}-\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}}\ \geqslant\ 0\}\\
&\quad=\min_{Y_{AB}\in\overrightarrow{\mathrm{PPT}}'}\{\|\mathrm{Tr}_B\, Y_{AB}\|_\infty\colon Y_{AB}-\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}}\ \geqslant\ 0\}\\
&\quad=\min\{\|\mathrm{Tr}_B\, V\|_\infty\colon V-\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}}\ \geqslant\ 0\ \wedge\ V\in\overrightarrow{\mathrm{PPT}}'\}\\
&\quad=\min\left\{\max\{\alpha+\gamma,\,\delta+\beta\}\colon\begin{pmatrix}\alpha & \xi e^{i\phi}\\ \xi e^{-i\phi} & \beta\end{pmatrix}-\frac{1}{2}\begin{pmatrix}1 & \sqrt{1-\lambda}\\ \sqrt{1-\lambda} & 1-\lambda\end{pmatrix}\ \geqslant\ 0\right.\\
&\left.\wedge\,\delta-\frac{1}{2}\lambda\geqslant 0\ \wedge\ \alpha,\beta,\gamma,\delta\geqslant 0\ \wedge\ \phi\in[0,2\pi]\ \wedge\ 0\leqslant\xi\leqslant\min\{\sqrt{\alpha\beta},\sqrt{\gamma\delta}\}\right\}\\
&\quad=\min\left\{\max\{\alpha+\gamma,\,\delta+\beta\}\colon\alpha+\beta\geqslant 1-\frac{1}{2}\lambda\ \wedge\ \left(\alpha-\frac{1}{2}\right)\left[\beta-\frac{1}{2}(1-\lambda)\right]\geqslant\left|\,\xi e^{i\phi}-\frac{1}{2}\sqrt{1-\lambda}\,\right|^2\right.\\
&\left.\wedge\,\delta-\frac{1}{2}\lambda\geqslant 0\ \wedge\ \alpha,\beta,\gamma,\delta\geqslant 0\ \wedge\ \phi\in[0,2\pi]\ \wedge\ 0\leqslant\xi\leqslant\min\{\sqrt{\alpha\beta},\sqrt{\gamma\delta}\}\right\}\\
&\quad=\min\left\{\max\{\alpha+\gamma,\,\delta+\beta\}\colon\alpha+\beta\geqslant 1-\frac{1}{2}\lambda\ \wedge\ \left(\alpha-\frac{1}{2}\right)\left[\beta-\frac{1}{2}(1-\lambda)\right]\geqslant\left(\xi-\frac{1}{2}\sqrt{1-\lambda}\right)^2\right.\\
&\left.\wedge\,\delta-\frac{1}{2}\lambda\geqslant 0\ \wedge\ \alpha,\beta,\gamma,\delta\geqslant 0\ \wedge\ 0\leqslant\xi\leqslant\min\{\sqrt{\alpha\beta},\sqrt{\gamma\delta}\}\right\}\\
&\quad=\min\left\{\max\{\alpha+\gamma,\,\delta+\beta\}\colon\alpha+\beta\geqslant 1-\frac{1}{2}\lambda\ \wedge\ \delta-\frac{1}{2}\lambda\geqslant 0\ \wedge\ \alpha,\beta,\gamma,\delta\geqslant 0\right.\\
&\left.\wedge\left(\alpha-\frac{1}{2}\right)\left[\beta-\frac{1}{2}(1-\lambda)\right]\geqslant\left(\min\{\min\{\sqrt{\alpha\beta},\sqrt{\gamma\delta}\}-\frac{1}{2}\sqrt{1-\lambda},0\}\right)^2\right\}\\
&\quad=\min\left\{\max\{\alpha+\gamma,\,\delta+\beta\}\colon\delta-\frac{1}{2}\lambda\geqslant 0\ \wedge\ \alpha\geqslant\frac{1}{2}\ \wedge\ \beta\geqslant\frac{1}{2}(1-\lambda)\ \wedge\ \gamma,\delta\geqslant 0\right.\\
&\left.\wedge\left(\alpha-\frac{1}{2}\right)\left[\beta-\frac{1}{2}(1-\lambda)\right]\geqslant\left(\min\{\min\{\sqrt{\alpha\beta},\sqrt{\gamma\delta}\}-\frac{1}{2}\sqrt{1-\lambda},0\}\right)^2\right\}\\
&\quad=\min\{A,B\},
\end{aligned}
\tag{E5}
$$

where

$$
\begin{aligned}
A\coloneqq\min\Bigg\{&\frac{1}{2}(\alpha+\beta+\sqrt{(\alpha-\beta)^2+4x^2})\colon\alpha+\frac{2x^2}{\lambda}\geqslant\beta+\frac{\lambda}{2}\ \wedge\ \alpha\geqslant\frac{1}{2}\ \wedge\ \beta\geqslant\frac{1}{2}(1-\lambda)\ \wedge\ x\geqslant 0\\
&\wedge\left(\alpha-\frac{1}{2}\right)\left[\beta-\frac{1}{2}(1-\lambda)\right]\geqslant\left(\min\{\min\{\sqrt{\alpha\beta},x\}-\frac{1}{2}\sqrt{1-\lambda},0\}\right)^2\Bigg\},
\end{aligned}
\tag{E6}
$$

$$
\begin{aligned}
B\coloneqq\min\Bigg\{&\beta+\frac{1}{2}\lambda\colon\alpha+\frac{2x^2}{\lambda}\leqslant\beta+\frac{\lambda}{2}\ \wedge\ \alpha\geqslant\frac{1}{2}\ \wedge\ \beta\geqslant\frac{1}{2}(1-\lambda)\ \wedge\ x\geqslant 0\\
&\wedge\left(\alpha-\frac{1}{2}\right)\left[\beta-\frac{1}{2}(1-\lambda)\right]\geqslant\left(\min\{\min\{\sqrt{\alpha\beta},x\}-\frac{1}{2}\sqrt{1-\lambda},0\}\right)^2\Bigg\}.
\end{aligned}
\tag{E7}
$$

The first equality comes from the following two observations

$$
V\in\overrightarrow{\mathrm{PPT}}\Rightarrow V'\in\overrightarrow{\mathrm{PPT}}',
\tag{E8}
$$

$$
V-\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}}\geqslant 0\Rightarrow V'-\pi_{\mathcal{N}_\lambda^{(\mathrm{ad})}},
\tag{E9}
$$

and from the inequality $\|\mathrm{Tr}_B\, V\|_\infty\ \geqslant\ \|\mathrm{Tr}_B\, V'\|_\infty$, where V, V' are generic matrices of the form

$$
V=\begin{pmatrix}a_{11} & a_{12} & a_{13} & a_{14}\\ a_{21} & a_{22} & a_{23} & a_{24}\\ a_{31} & a_{32} & a_{33} & a_{34}\\ a_{41} & a_{42} & a_{43} & a_{44}\end{pmatrix},\qquad V'=\begin{pmatrix}a_{11} & 0 & 0 & a_{14}\\ 0 & a_{22} & 0 & 0\\ 0 & 0 & a_{33} & 0\\ a_{41} & 0 & 0 & a_{44}\end{pmatrix}.
\tag{E10}
$$

The second equality is just a rearrangement of the previous expression, whereas in the third equality we exploit equation (E4). The fourth equality can be obtained by expanding the matrix inequality previously found, and in the fifth equality we used the following relation

$$\min_{\phi\in\mathbb{R}} \left| \xi e^{i\phi} - \frac{1}{2}\sqrt{1-\lambda} \right|^2 = \left(\xi - \frac{1}{2}\sqrt{1-\lambda}\right)^2, \tag{E11}$$

which holds for $\xi \geqslant 0$. In the sixth and seventh equalities we used respectively

$$x, y \geqslant 0 \Rightarrow \min_{0\leqslant\xi\leqslant x} (\xi - y)^2 = \min\{x - y, 0\}^2, \tag{E12}$$

and

$$\alpha + \beta \geqslant x + y \wedge (\alpha - x)(\beta - y) \geqslant 0 \;\Leftrightarrow\; \alpha \geqslant x \wedge \beta \geqslant y. \tag{E13}$$

Finally, in order to obtain the last equality we observed that

$$\min_{\delta\geqslant\frac{1}{2}\lambda} \max\left\{\alpha + \frac{x^2}{\delta}, \beta + \delta\right\} = \begin{cases} \frac{1}{2}(\alpha + \beta + \sqrt{(\alpha-\beta)^2 + 4x^2}), & \text{for } \alpha + \frac{2x^2}{\lambda} \geqslant \beta + \frac{\lambda}{2}, \\ \beta + \frac{1}{2}\lambda, & \text{for } \alpha + \frac{2x^2}{\lambda} \leqslant \beta + \frac{\lambda}{2}. \end{cases} \tag{E14}$$

From this analysis it follows that equation (E1) is proven if we can show that $A = 1 - \frac{1}{2}\lambda$ and $B \geqslant 1 - \frac{1}{2}\lambda$. This is what we do in the following.

E.1. Proof of $A = 1 - \frac{1}{2}\lambda$

Note that the choices $\alpha = \frac{1}{2}$, $\beta = \frac{1}{2}(1-\lambda)$, and $x = \frac{1}{2}\sqrt{1-\lambda}$ satisfy the conditions appearing in equation (E6), providing

$$\frac{1}{2}(\alpha + \beta + \sqrt{(\alpha-\beta)^2 + 4x^2}) = 1 - \frac{1}{2}\lambda, \tag{E15}$$

so that $A \leqslant 1 - \frac{1}{2}\lambda$.

In order to derive the converse inequality, we first rewrite A as

$$\begin{aligned} A = \min\Bigg\{ & \frac{1}{2}\left[a + b + 1 - \frac{1}{2}\lambda + \sqrt{\left(a - b + \frac{1}{2}\lambda\right)^2 + 4x^2}\right] : a + \frac{2x^2}{\lambda} \geqslant b \;\wedge\; a, b, x \geqslant 0 \\ & \wedge ab \geqslant \left(\min\left\{\min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b + \frac{1}{2}(1-\lambda)\right]}, x\right\} - \frac{1}{2}\sqrt{1-\lambda}, 0\right\}\right)^2 \Bigg\} \end{aligned} \tag{E16}$$

$$\begin{aligned} \geqslant \min\Bigg\{ & \frac{1}{2}\left[a + b + 1 - \frac{1}{2}\lambda + \sqrt{\left(a - b + \frac{1}{2}\lambda\right)^2 + 4x^2}\right] : a, b, x \geqslant 0 \\ & \wedge ab \geqslant \left(\min\left\{\min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b + \frac{1}{2}(1-\lambda)\right]}, x\right\} - \frac{1}{2}\sqrt{1-\lambda}, 0\right\}\right)^2 \Bigg\} \end{aligned} \tag{E17}$$

$$= \min\{A_1, A_2\}, \tag{E18}$$

where

$$\begin{aligned} A_1 := \min\Bigg\{ & \frac{1}{2}\left[a + b + 1 - \frac{1}{2}\lambda + \sqrt{\left(a - b + \frac{1}{2}\lambda\right)^2 + 4x^2}\right] : a, b, x \geqslant 0 \\ & \wedge \min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b + \frac{1}{2}(1-\lambda)\right]}, x\right\} \geqslant \frac{1}{2}\sqrt{1-\lambda}\Bigg\}, \end{aligned} \tag{E19}$$

$$\begin{aligned} A_2 := \min\Bigg\{ & \frac{1}{2}\left[a + b + 1 - \frac{1}{2}\lambda + \sqrt{\left(a - b + \frac{1}{2}\lambda\right)^2 + 4x^2}\right] : a, b, x \geqslant 0 \\ & \wedge ab \geqslant \left(\min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b + \frac{1}{2}(1-\lambda)\right]}, x\right\} - \frac{1}{2}\sqrt{1-\lambda}\right)^2 \\ & \wedge \min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b + \frac{1}{2}(1-\lambda)\right]}, x\right\} \leqslant \frac{1}{2}\sqrt{1-\lambda}\Bigg\}. \end{aligned} \tag{E20}$$

The equality in equation (E16) follows from the definition of A in equation (E6), by substituting $\alpha \to a + \frac{1}{2}$ and $\beta \to b + \frac{1}{2}(1-\lambda)$, and in order to obtain the following inequality we drop a condition on the parameters a, b, x. Then, the equality in equation (E18) can be proven by dividing the parameter region into two sub-regions:

one such that $\min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left(b+\frac{1}{2}(1-\lambda)\right)},\, x\right\} \geqslant \frac{1}{2}\sqrt{1-\lambda}$, and one such that the converse inequality holds.

As next step, we show that both A_1 and A_2 are larger than $1-\frac{1}{2}\lambda$. In particular, we can explicitly evaluate A_1 as

$$\begin{aligned} A_1 &= \min\left\{\frac{1}{2}\left(a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+(1-\lambda)}\right):\right. \\ &\quad \left.\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \geqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge\ a,\, b \geqslant 0\right\} \\ &= \min\left\{\frac{1}{2}\left(a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+(1-\lambda)}\right):\right. \\ &\quad \left.\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \geqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge\ a = b = 0\right\} = 1-\frac{1}{2}\lambda. \end{aligned} \tag{E21}$$

The two equalities can be respectively shown by noticing that the quantity being minimised is a monotonically increasing function of $x \geqslant 0$ and of $a,\ b \geqslant 0$. In order to show that $A_2 \geqslant 1-\frac{1}{2}\lambda$, it is convenient to write

$$A_2 = \min\{A_3,\, A_4\}, \tag{E22}$$

where we divide the parameter region into two sub-regions, depending on the ordering between $\sqrt{(a+\frac{1}{2})\left[b+\frac{1}{2}(1-\lambda)\right]}$ and x, that is:

$$\begin{aligned} A_3 \coloneqq \min&\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+4x^2}\right]:\, a,\, b,\, x \geqslant 0\right. \\ &\wedge ab \geqslant \left(\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}-\frac{1}{2}\sqrt{1-\lambda}\right)^2 \ \wedge\ \sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \leqslant \frac{1}{2}\sqrt{1-\lambda} \\ &\left.\wedge\ \sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \leqslant x\right\} \\ = \min&\left\{\frac{1}{2}\left(1-\frac{1}{2}\lambda+\sqrt{\frac{\lambda^2}{4}+4x^2}\right):\, \frac{1}{2}\sqrt{1-\lambda} \leqslant x \ \wedge\ x \geqslant 0\right\} = 1-\frac{1}{2}\lambda, \end{aligned} \tag{E23}$$

and

$$\begin{aligned} A_4 \coloneqq \min&\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+4x^2}\right]:\, a,\, b,\, x \geqslant 0\right. \\ &\left.\wedge ab \geqslant \left(x-\frac{1}{2}\sqrt{1-\lambda}\right)^2 \ \wedge\ x \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge\ \sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \geqslant x\right\} \\ \geqslant \min&\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+4x^2}\right]:\, a,\, b,\, x \geqslant 0\right. \\ &\left.\wedge ab \geqslant \left(\frac{1}{2}\sqrt{1-\lambda}-x\right)^2 \ \wedge\ x \leqslant \frac{1}{2}\sqrt{1-\lambda}\right\} \\ = \min&\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+4x^2}\right]:\, a,\, b,\, x \geqslant 0\right. \\ &\left.\wedge\ \frac{1}{2}\sqrt{1-\lambda}-\sqrt{ab} \leqslant x \leqslant \frac{1}{2}\sqrt{1-\lambda}\right\} \\ = \min&\{A_5,\, A_6\}, \end{aligned} \tag{E24}$$

where we further expanded A_4 in terms of A_5 and A_6, depending on the ordering between $\frac{1}{2}\sqrt{1-\lambda}$ and $\sqrt{ab}$:

$$\begin{aligned}
A_5 &:= \min\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+4x^2}\right]: a,\, b,\, x \geqslant 0\right. \\
&\left. \wedge\, \frac{1}{2}\sqrt{1-\lambda}-\sqrt{ab} \leqslant x \leqslant \frac{1}{2}\sqrt{1-\lambda} \;\wedge\; \frac{1}{2}\sqrt{1-\lambda} \geqslant \sqrt{ab}\right\} \\
&= \min\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+(\sqrt{1-\lambda}-2\sqrt{ab})^2}\right]:\right. \\
&\left. \frac{1}{2}\sqrt{1-\lambda} \geqslant \sqrt{ab} \;\wedge\; a,\, b \geqslant 0\right\} \\
&\geqslant \min\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+(\sqrt{1-\lambda}-2\sqrt{ab})^2}\right]: a,\, b \geqslant 0\right\} \\
&= \min\left\{\frac{1}{2}\left[x+1-\frac{1}{2}\lambda+\sqrt{\left(1-\frac{1}{2}\lambda\right)^2+x^2+x(y\lambda-2\sqrt{1-\lambda}\sqrt{1-y^2})}\right]:\right. \\
&\left. 1 \geqslant y \geqslant -1 \wedge x \geqslant 0\right\} \\
&= \min\left\{\frac{1}{2}\left[x+1-\frac{1}{2}\lambda+|1-\frac{1}{2}\lambda-x|\right]: x \geqslant 0\right\} = 1-\frac{1}{2}\lambda,
\end{aligned} \tag{E25}$$

$$\begin{aligned}
A_6 &:= \min\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+4x^2}\right]: a,\, b,\, x \geqslant 0\right. \\
&\left. \wedge\, \frac{1}{2}\sqrt{1-\lambda}-\sqrt{ab} \leqslant x \leqslant \frac{1}{2}\sqrt{1-\lambda} \;\wedge\; \frac{1}{2}\sqrt{1-\lambda} \leqslant \sqrt{ab}\right\} \\
&= \min\left\{\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+|a-b+\frac{1}{2}\lambda|\right]: \frac{1}{2}\sqrt{1-\lambda} \leqslant \sqrt{ab} \;\wedge\; a,\, b \geqslant 0\right\} \\
&= \min\left\{\frac{1}{2}\left[\sqrt{4x^2+y^2}+1-\frac{1}{2}\lambda+|y+\frac{1}{2}\lambda|\right]: \frac{1}{2}\sqrt{1-\lambda} \leqslant x \;\wedge\; x \geqslant 0\right\} \\
&= \min\left\{\frac{1}{2}\left[\sqrt{1-\lambda+y^2}+1-\frac{1}{2}\lambda+|y+\frac{1}{2}\lambda|\right]\right\} = 1-\frac{1}{2}\lambda.
\end{aligned} \tag{E26}$$

In order to manipulate the expression of A_3, we first used the fact that

$$\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \leqslant \frac{1}{2}\sqrt{1-\lambda} \wedge a,\, b \geqslant 0 \Leftrightarrow a = 0 \wedge b = 0, \tag{E27}$$

and then we exploited the monotonicity of $\frac{1}{2}\left(1-\frac{1}{2}\lambda+\sqrt{\frac{\lambda^2}{4}+4x^2}\right)$ in x for $x \geqslant 0$. The inequalities appearing in the manipulations of A_4 and A_5 are obtained by dropping a condition on $a,\, b,\, x$ which restricts the minimisation region. In the first equalities written for A_5 and A_6 we used the monotonicity in x of the function

$$\frac{1}{2}\left[a+b+1-\frac{1}{2}\lambda+\sqrt{\left(a-b+\frac{1}{2}\lambda\right)^2+4x^2}\right], \tag{E28}$$

which is minimised for $x = 0$. In the third relation appearing in the manipulation of A_5 we changed variables as $a \to \frac{1}{2}(x+xy)$ and $b \to \frac{1}{2}(x-xy)$, whereas in the second relation appearing in the manipulation of A_6 we parametrised $a,\, b$ as $a \to \frac{1}{2}(y+\sqrt{4x^2+y^2})$ and $b \to \frac{1}{2}(-y+\sqrt{4x^2+y^2})$. Finally, the last equalities leading to the evaluation of A_5 and A_6 in equations (E25) and (E26) are respectively due to

$$\min_{-1 \leqslant y \leqslant 1}\left[y\lambda-2\sqrt{1-\lambda}\sqrt{1-y^2}\right] = -(2-\lambda), \tag{E29}$$

and

$$\min_{y}\left[\sqrt{1-\lambda+y^2}+\left|y+\frac{1}{2}\lambda\right|\right] = 1-\frac{1}{2}\lambda. \tag{E30}$$

Overall, we have been able to show that $A_1 = 1-\frac{1}{2}\lambda$, and that A_2 can be written as the minimum among quantities larger than or equal to $1-\frac{1}{2}\lambda$. Therefore, from equation (E18) it follows that $A = 1-\frac{1}{2}\lambda$, as desired.

E.2. Proof of $B \geqslant 1 - \frac{1}{2}\lambda$

We start by writing the values of α and β appearing in the definition of B in equation (E7) as $\alpha \to a + \frac{1}{2}$ and $\beta \to b + \frac{1}{2}(1-\lambda)$. Then, we divide the parameter region into two sub-regions depending on the ordering between $\min\left\{\sqrt{(a+\frac{1}{2})\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\}$ and $\frac{1}{2}\sqrt{1-\lambda}$. This leaves us with

$$\begin{aligned} B = \min\Bigg\{ & b + \frac{1}{2} : ab \geqslant \left(\min\left\{\min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\} - \frac{1}{2}\sqrt{1-\lambda}, 0\right\}\right)^2 \\ & \wedge\, a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ = \min\{B_1, B_2\}, \end{aligned} \tag{E31}$$

where

$$\begin{aligned} B_1 \coloneqq \min\Bigg\{ & b + \frac{1}{2} : ab \geqslant 0 \ \wedge\ \min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\} \geqslant \frac{1}{2}\sqrt{1-\lambda} \\ & \wedge\, a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ = \min\Bigg\{ & b + \frac{1}{2} : \sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \geqslant \frac{1}{2}\sqrt{1-\lambda} \\ & \wedge\, x \geqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge\ a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ \geqslant \min\Bigg\{ & b + \frac{1}{2} : x \geqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge\ a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ = \min\Bigg\{ & b + \frac{1}{2} : a + \frac{1-\lambda}{\lambda} \leqslant b \ \wedge\ a \geqslant 0\Bigg\} \\ = \min\Bigg\{ & b + \frac{1}{2} : \frac{1-\lambda}{\lambda} \leqslant b\Bigg\} = \frac{1}{\lambda}\left(1 - \frac{1}{2}\lambda\right) \geqslant 1 - \frac{1}{2}\lambda, \end{aligned} \tag{E32}$$

and

$$\begin{aligned} B_2 \coloneqq \min\Bigg\{ & b + \frac{1}{2} : ab \geqslant \left(\min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\} - \frac{1}{2}\sqrt{1-\lambda}\right)^2 \\ & \wedge \min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\} \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge\ a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ = \min\Bigg\{ & b + \frac{1}{2} : \sqrt{ab} \geqslant \frac{1}{2}\sqrt{1-\lambda} - \min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\} \\ & \wedge \min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\} \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge\ a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ \geqslant \min\Bigg\{ & b + \frac{1}{2} : \sqrt{ab} \geqslant \frac{1}{2}\sqrt{1-\lambda} - \min\left\{\sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]}, x\right\} \\ & \wedge\, a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ = \min\Bigg\{ & b + \frac{1}{2} : \sqrt{ab} \geqslant \frac{1}{2}\sqrt{1-\lambda} - x \ \wedge\ \sqrt{ab} \geqslant \frac{1}{2}\sqrt{1-\lambda} - \sqrt{\left(a+\frac{1}{2}\right)\left[b+\frac{1}{2}(1-\lambda)\right]} \\ & \wedge\, a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ \geqslant \min\Bigg\{ & b + \frac{1}{2} : \sqrt{ab} \geqslant \frac{1}{2}\sqrt{1-\lambda} - x \ \wedge\ a + \frac{2x^2}{\lambda} \leqslant b \ \wedge\ a, b, x \geqslant 0\Bigg\} \\ = \min\{B_3, B_4\}. \end{aligned} \tag{E33}$$

The inequalities appearing in the above manipulations are obtained by dropping conditions on a, b, x which restrict the minimisation region. Moreover, B_3 and B_4 are obtained by splitting the parameter region into two sub-regions, defined according to the ordering between $\sqrt{ab}$ and $\frac{1}{2}\sqrt{1-\lambda}$. More precisely, we can write

$$\begin{aligned} B_3 &:= \min\left\{b+\frac{1}{2}: x \geqslant \frac{1}{2}\sqrt{1-\lambda}-\sqrt{ab} \ \wedge \ \sqrt{ab} \geqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ a+\frac{2x^2}{\lambda} \leqslant b \ \wedge \ a, b, x \geqslant 0\right\} \\ &= \min\left\{b+\frac{1}{2}: \sqrt{ab} \geqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ a \leqslant b \ \wedge \ a, b \geqslant 0\right\} \\ &= \min\left\{b+\frac{1}{2}: b \geqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ b \geqslant 0\right\} = \frac{1}{2}\sqrt{1-\lambda}+\frac{1}{2} \geqslant 1-\frac{1}{2}\lambda, \end{aligned} \tag{E34}$$

and

$$\begin{aligned} B_4 &:= \min\left\{b+\frac{1}{2}: x \geqslant \frac{1}{2}\sqrt{1-\lambda}-\sqrt{ab} \ \wedge \ \sqrt{ab} \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ a+\frac{2x^2}{\lambda} \leqslant b \ \wedge \ a, b, x \geqslant 0\right\} \\ &= \min\left\{b+\frac{1}{2}: \sqrt{ab} \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ a+\frac{2\left(\frac{1}{2}\sqrt{1-\lambda}-\sqrt{ab}\right)^2}{\lambda} \leqslant b \ \wedge \ a, b \geqslant 0\right\} \\ &= \min\left\{b+\frac{1}{2}: \sqrt{ab} \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ \frac{1}{2}\sqrt{1-\lambda}-\sqrt{ab} \leqslant \sqrt{\frac{\lambda}{2}}\sqrt{b-a} \ \wedge \ b \geqslant a \ \wedge \ a \geqslant 0\right\} \\ &= \min\left\{\frac{1}{2}(1+y^2+\sqrt{4x^2+y^4}): x \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ \frac{1}{2}\sqrt{1-\lambda}-x \leqslant \sqrt{\frac{\lambda}{2}}y \ \wedge \ x, y \geqslant 0\right\} \\ &= \min\left\{\frac{1}{2}(1+y^2+\sqrt{4x^2+y^4}): x \leqslant \frac{1}{2}\sqrt{1-\lambda} \ \wedge \ \frac{1}{2}\sqrt{1-\lambda}-x = \sqrt{\frac{\lambda}{2}}y \ \wedge \ x \geqslant 0\right\} \\ &= \min\left\{\frac{1}{2}[1+y^2+\sqrt{(\sqrt{1-\lambda}-\sqrt{2\lambda}y)^2+y^4}]: 0 \leqslant y \leqslant \sqrt{\frac{1-\lambda}{2\lambda}}\right\} \\ &\geqslant \min_{y\in\mathbb{R}}\left\{\frac{1}{2}[1+y^2+\sqrt{(\sqrt{1-\lambda}-\sqrt{2\lambda}y)^2+y^4}]\right\} \\ &= \min_{z\in\mathbb{R}}\left\{\frac{1}{2}+\frac{1}{4}(1-\lambda)\lambda\left[z^2+\sqrt{\frac{4(1-\lambda z)^2}{(1-\lambda)\lambda^2}+z^4}\right]\right\} \\ &= \frac{1}{2}+\frac{1}{4}(1-\lambda)\lambda\left[1+\sqrt{\frac{4(1-\lambda)^2}{(1-\lambda)\lambda^2}+1}\right] = 1-\frac{1}{2}\lambda. \end{aligned} \tag{E35}$$

In the third equality of the manipulations performed on B_4 we changed variables as $b \to \frac{1}{2}(y^2+\sqrt{4x^2+y^4})$ and $a \to \frac{1}{2}(-y^2+\sqrt{4x^2+y^4})$, whereas in the fourth equality we used the fact that $\frac{1}{2}(1+y^2+\sqrt{4x^2+y^4})$ is a monotonic function of y when $y \geqslant 0$. The seventh and eighth relations appearing in the manipulation of B_4, instead, are respectively obtained by changing variable as $y \to \sqrt{\frac{(1-\lambda)\lambda}{2}}z$ and by exploiting the fact that $z^2+\sqrt{\frac{4(1-\lambda z)^2}{(1-\lambda)\lambda^2}+z^4}$ is minimised at $z=1$ for $0<\lambda<1$.

Overall, this shows that $B \geqslant 1-\frac{1}{2}\lambda$ and the proof is concluded.

ORCID iDs

Luca Rigovacca https://orcid.org/0000-0002-6260-9239

References

[1] Wilde M M 2013 *Quantum Information Theory* 1st edn (New York: Cambridge University Press) (https://doi.org/10.1017/CBO9781139525343)
[2] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Secure key from bound entanglement *Phys. Rev. Lett.* **94** 160502
[3] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2009 General paradigm for distilling classical key from quantum states *IEEE Trans. Inf. Theory* **55** 1898–929
[4] Horodecki R, Horodecki P, Horodecki M and Horodecki K 2009 Quantum entanglement *Rev. Mod. Phys.* **81** 865–942
[5] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3

[6] Bennett C H, Brassard G and Mermin N D 1992 Quantum cryptography without Bell's theorem *Phys. Rev. Lett.* **68** 557–9
[7] Bennett C H, Brassard G, Crépeau C, Jozsa R, Peres A and Wootters W K 1993 Teleporting an unknown quantum state via dual classical and Einstein–Podolsky–Rosen channels *Phys. Rev. Lett.* **70** 1895–9
[8] Horodecki M, Oppenheim J and Winter A 2005 Partial quantum information *Nature* **436** 673–6
[9] Takeoka M, Guha S and Wilde M M 2014 Fundamental rate-loss tradeoff for optical quantum key distribution *Nat. Commun.* **5** 5235
[10] Munro W J, Stephens A M, Devitt S J, Harrison K A and Nemoto K 2012 Quantum communication without the necessity of quantum memories *Nat. Photon.* **6** 777–81
[11] Azuma K, Tamaki K and Lo H-K 2015 All-photonic quantum repeaters *Nat. Commun.* **6** 6787
[12] Azuma K, Tamaki K and Munro W J 2015 All-photonic intercity quantum key distribution *Nat. Commun.* **6** 10171
[13] Takeoka M, Guha S and Wilde M M 2014 The squashed entanglement of a quantum channel *IEEE Trans. Inf. Theory* **60** 4987–98
[14] Pirandola S, Laurenza R, Ottaviani C and Banchi L 2017 Fundamental limits of repeaterless quantum communications *Nat. Commun.* **8** 15043
[15] Christandl M and Müller-Hermes A 2017 Relative entropy bounds on quantum, private and repeater capacities *Commun. Math. Phys.* **353** 821–52
[16] Goodenough K, Elkouss D and Wehner S 2016 Assessing the performance of quantum repeaters for all phase-insensitive gaussian bosonic channels *New J. Phys.* **18** 063005
[17] Wilde M M, Tomamichel M and Berta M 2017 Converse bounds for private communication over quantum channels *IEEE Trans. Inf. Theory* **63** 1792–817
[18] Kaur E and Wilde M M 2017 Upper bounds on secret key agreement over lossy thermal bosonic channels arXiv: 1706.04590
[19] Cope T P W, Hetzel L, Banchi L and Pirandola S 2017 Simulation of non-Pauli channels *Phys. Rev.* A **96** 022323
[20] Laurenza R, Braunstein S L and Pirandola S 2017 Finite-resource teleportation stretching for continuous-variable systems arXiv: 1706.06065
[21] Christandl M and Winter A 2004 Squashed entanglement: an additive entanglement measure *J. Math. Phys.* **45** 829–40
[22] Huang Y 2014 Computing quantum discord is np-complete *New J. Phys.* **16** 033027
[23] Kimble H J 2008 The quantum internet *Nature* **453** 1023–30
[24] Azuma K, Mizutani A and Lo H-K 2016 Fundamental rate-loss tradeoff for the quantum internet *Nat. Commun.* **7** 13523
[25] Munro W J, Azuma K, Tamaki K and Nemoto K 2015 Inside quantum repeaters *IEEE J. Sel. Top. Quantum Electron.* **21** 78–90
[26] Schoute E, Mancinska L, Islam T, Kerenidis I and Wehner S 2016 Shortcuts to quantum network routing arXiv: 1610.05238
[27] Sangouard N, Simon C, de Riedmatten H and Gisin N 2011 Quantum repeaters based on atomic ensembles and linear optics *Rev. Mod. Phys.* **83** 33–80
[28] Peev M *et al* 2009 The SECOQC quantum key distribution network in Vienna *New J. Phys.* **11** 075001
[29] Stucki D *et al* 2011 Long-term performance of the SwissQuantum quantum key distribution network in a field environment *New J. Phys.* **13** 123001
[30] Sasaki M *et al* 2011 Field test of quantum key distribution in the tokyo QKD network *Opt. Express* **19** 10387–409
[31] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dušek M, Lütkenhaus N and Peev M 2009 The security of practical quantum key distribution *Rev. Mod. Phys.* **81** 1301–50
[32] Pirandola S 2016 Capacities of repeater-assisted quantum communications, arXiv:1601.00966
[33] Cover T 1972 Broadcast channels *IEEE Trans. Inf. Theory* **18** 2–14
[34] Yard J, Hayden P and Devetak I 2011 Quantum broadcast channels *IEEE Trans. Inf. Theory* **57** 7147–62
[35] Seshadreesan K P, Takeoka M and Wilde M M 2016 Bounds on entanglement distillation and secret key agreement for quantum broadcast channels *IEEE Trans. Inf. Theory* **62** 2849–66
[36] Bäuml S and Azuma K 2017 Fundamental limitation on quantum broadcast networks *Quantum Sci. Technol.* **2** 024004
[37] Laurenza R and Pirandola S 2017 General bounds for sender-receiver capacities in multipoint quantum communications *Phys. Rev.* A **96** 032318
[38] Takeoka M, Seshadreesan K P and Wilde M M 2016 Unconstrained distillation capacities of a pure-loss bosonic broadcast channel *2016 IEEE ISIT* pp 2484–8
[39] Takeoka M, Seshadreesan K P and Wilde M M 2017 Unconstrained capacities of quantum key distribution and entanglement distillation for pure-loss bosonic broadcast channels *Phys. Rev. Lett.* **119** 150501
[40] Berta M and Wilde M M 2017 Amortization does not enhance the max-rains information of a quantum channel arXiv: 1709.04907
[41] Umegaki H 1962 Conditional expectation in an operator algebra: IV. Entropy and information *Kodai Math. Sem. Rep.* **14** 59–85
[42] Datta N 2009 Min- and max-relative entropies and a new entanglement monotone *IEEE Trans. Inf. Theory* **55** 2816–26
[43] Lindblad G 1974 Expectations and entropy inequalities for finite quantum systems *Commun. Math. Phys.* **39** 111–9
[44] Vedral V and Plenio M B 1998 Entanglement measures and purification procedures *Phys. Rev.* A **57** 1619–33
[45] Datta N 2009 Max-relative entropy of entanglement, alias log robustness *Int. J. Quantum Inf.* **07** 475–91
[46] Bennett C H, DiVincenzo D P, Smolin J A and Wootters W K 1996 Mixed-state entanglement and quantum error correction *Phys. Rev.* A **54** 3824–51
[47] Gottesman D and Chuang I L 1999 Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations *Nature* **402** 390–3
[48] Horodecki P, Horodecki M and Horodecki R 1998 General teleportation channel, singlet fraction and quasi-distillation *Phys. Rev.* A **60** 1888
[49] Knill E, Laflamme R and Milburn G J 2001 A scheme for efficient quantum computation with linear optics *Nature* **409** 46–52
[50] Wolf M M, Pérez-García D and Giedke G 2007 Quantum capacities of bosonic channels *Phys. Rev. Lett.* **98** 130501
[51] Niset J, Fiurášek J and Cerf N J 2009 No-go theorem for gaussian quantum error correction *Phys. Rev. Lett.* **102** 120501
[52] Müller-Hermes A 2012 Transposition in quantum information theory *Master's Thesis* Technical University of Munich
[53] Christandl M, Schuch N and Winter A 2010 Highly entangled states with almost no secrecy *Phys. Rev. Lett.* **104** 240405
[54] Christandl M, Schuch N and Winter A 2012 Entanglement of the antisymmetric state *Commun. Math. Phys.* **311** 397–422
[55] Azuma K and Kato G 2017 Aggregating quantum repeaters for the quantum internet *Phys. Rev.* A **96** 032332
[56] Synak-Radtke B and Horodecki M 2006 On asymptotic continuity of functions of quantum states *J. Phys. A: Math. Gen.* **39** L423
[57] Wilde M M 2016 Squashed entanglement and approximate private states *Quantum Inf. Process.* **15** 4563–80
[58] Müller-Lennert M, Dupuis F, Szehr O, Fehr S and Tomamichel M 2013 On quantum Rényi entropies: A new generalization and some properties *J. Math. Phys.* **54** 122203
[59] Wilde M M, Winter A and Yang D 2014 Strong converse for the classical capacity of entanglement-breaking and hadamard channels via a sandwiched rényi relative entropy *Commun. Math. Phys.* **331** 593–622

[60] Beigi S 2013 Sandwiched Rényi divergence satisfies data processing inequality *J. Math. Phys.* **54** 122202
[61] Devetak I, Junge M, King C and Ruskai M B 2006 Multiplicativity of completely bounded p-norms implies a new additivity result *Commun. Math. Phys.* **266** 37–63
[62] Christandl M and Winter A 2005 Uncertainty, monogamy, and locking of quantum correlations *IEEE Trans. Inf. Theory* **51** 3159–65
[63] Horodecki K, Horodecki M, Horodecki P and Oppenheim J 2005 Locking entanglement with a single qubit *Phys. Rev. Lett.* **94** 200501
[64] Briegel H J, Browne D E, Dur W, Raussendorf R and Van den Nest M 2009 Measurement-based quantum computation *Nat. Phys.* **5** 19–26
[65] Yokoyama S, Ukai R, Armstrong S C, Sornphiphatphong C, Kaji T, Suzuki S, Yoshikawa J-i, Yonezawa H, Menicucci N C and Furusawa A 2013 Ultra-large-scale continuous-variable cluster states multiplexed in the time domain *Nat. Photon.* **7** 982–6
[66] Horodecki M, Horodecki P and Horodecki R 1996 Separability of mixed states: necessary and sufficient conditions *Phys. Lett.* A **223** 1–8