Advances in the theory of channel simulation: from quantum communication to quantum sensing

Riccardo Laurenza

PhD

University of York

September 2018

Abstract

In this thesis we investigate the fundamental limitations that the laws of the quantum nature impose on the performance of quantum communications, quantum metrology and quantum channel discrimination. In a quantum communication scenario, the typical tasks are represented by the simple transmission of quantum bits, the distribution of entanglement and the sharing of quantum secret keys. The ultimate rates for each of these protocols are given by the two-way quantum capacities of the quantum channel which are in turn defined by considering the most general adaptive strategies that can be implemented over the channel. To assess these quantum capacities, we combine the simulation of quantum channels, suitably generalized to systems of arbitrary dimension, with quantum teleportation and the relative entropy of entanglement. This procedure is called teleportation stretching. Relying on this, we are able to reduce any adaptive protocols into simpler block ones and to determine the tightest upper bound on the two-way quantum capacities. Remarkably, we also prove the existence of a particular class of quantum channel for which the lower and the upper bounds coincide. By employing a slight modification of the teleportation scheme, allowing the two parties to share a multi-copy resource state, we apply our technique to simplify adaptive protocols for quantum metrology and quantum channel discrimination. In the first case we show that the modified teleportation stretching implies a quantum Cramér-Rao bound that follows asymptotically the Heisenberg scaling. In the second scenario we are able to derive the only known so far fundamental lower bound on the probability of error affecting the discrimination of two arbitrary finite-dimensional quantum channels.

Contents

List of Figures

List of Tables

Acknowledgements

I am deeply grateful to my supervisor Prof. Stefano Pirandola for his precious guidance during my PhD. He gave me the opportunity to grow as a researcher and to face exciting challenges at the frontiers of the quantum information theory. He taught me a lot and working with him has been a great privilege. I also want to thank Prof. Samuel L. Braunstein for all the invaluable discussions I had with him and for all the insightful suggestions he gave me. I would also like to express my gratitude to Prof. Edwin Handcock for all the useful advices he provided during these years. I am grateful also to my other closest collaborators Dr. Carlo Ottaviani and Dr. Cosmo Lupo. Without their fundamental help I would have not achieved all my results. I am also indebt to them for all the moments spent together talking about physics and life in general, contributing to create a more pleasant working environment. A special thank goes also to the other colleagues in the quantum information group at the University of York, Dr. Gaetana Spedalieri, Thomas Cope, Panagiotis Papanastasiou, Zhiwei Wang, Jason Pereira. It's been a pleasure to share knowledge and discussions with them. My intellectual debt is to Prof. Claudio Cereda who made me experience for the first time the fascination for quantum mechanics.

Ringraziamenti

Il mio piú sentito ringraziamento va ai miei genitori. A mia madre Anita, perché per quanto poco abbia avuto la possibilitá di accompagnarmi in questo mondo ha fatto in tempo a lasciare un segno indelebile dei suoi insegnamenti. A mio padre Mario, per tutto il supporto incondizionato che mi ha dato in questi anni e aver permesso cosi che potessi formarmi personalmente e raggiungere i miei traguardi. Saró inoltre sempre grato a mia sorella Margherita perché é la migliore sorella che abbia mai potuto desiderare e per aver dato vita a due splendide creature che ogni volta mi riempiono di infinita gioia.

A Nico e Dige saró sempre grato per avermi regalato due amicizie uniche e profonde. Sono certo che potró sempre contare sulla vostra complicitá e che vi vorró costantemente come compagni al mio fianco, sfruttando a pieno tutta la ricchezza che mi ha sempre dato il vostro sguardo, mai banale, sul mondo. Vi voglio un bene enorme.

Un grazie di cuore é per Ale, per tutte le indimenticabili avventure che ha portato nella mia vita e per avermi compreso piú del dovuto.

Ringrazio e abbraccio tutti gli altri amici fondamentali che in questi anni mi hanno fatto sentire il loro calore. Camilla, Giulia, Finch, Anní, Patrick, Maste, Fede, Ste. Anche se magari non ci siamo sentiti spesso sappiate che avete sempre trovato un posto nei miei pensieri e tornare a casa per rincontrarvi ogni volta é stato fonte di immenso piacere.

Author's declaration

I declare that the research described in this thesis is original work, which I undertook at the University of York during 2015 - 2018. This work has not previously been presented for an award at this, or any other, University. All the work presented here has been done under the guidance and supervision of Professor Stefano Pirandola and in close collaboration with the other listed authors. The work presented in this Thesis is based on the collection of papers listed below, jointly written with collaborators. For each item the primary author is the first listed author.

- [1] S. Pirandola, R. Laurenza, C. Ottaviani and L. Banchi "Ultimate limits of repeaterless quantum communications", *Nature Communications* **8**, 15043 (2017). See also [2] *arXiv preprint:1510.08863v1.*

  Here, I computed the analytical formulas of the bounds for the discrete variable channels, besides studying the classical communication cost associated with the protocols. Then, I contributed to the study of the bosonic Gaussian channels by performing numerical investigations. See "*Author contributions*" in [1] for details on the contributions of each author.
  The content of this paper is presented in Chapter 2 and Appendix B.

  See also
  [3] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieris and L. Banchi "Theory of channel simulation and bounds for private communication", *Quantum Sci. Technol.* **3**, 035009 (2018).

- [4] S. Pirandola, R. Laurenza and S. L. Braunstein "Teleportation simulation of bosonic Gaussian channels: Strong and uniform convergence", *The European Physical Journal D* **72** (9), 162 (2018).

Together with my co-authors, I contributed to refine the understanding of the convergence properties of continuous-variable teleportation under various topologies. In particular, I performed the analytical calculations proving Lemma A.1.1 for the main canonical forms of bosonic Gaussian channels.
The content of this paper is presented at the end of Chapter 1, in Chapter 2 and Appendix A.

- [5] R. Laurenza, S. L. Braunstein and S. Pirandola "Finite-resource teleportation stretching for continuous variable systems", *Scientific reports* **8** (1), 15267 (2018).

  Here I computed the finite-energy resource upper bounds to the secret-key capacity of all the bosonic Gaussian channels investigated.
  The content of this paper is presented in Chapter 3.

- [6] R. Laurenza, S. Tserkis, S. L. Braunstein, T. C. Ralph and S. Pirandola "Tight finite-resource bounds for private communication over Gaussian channels," *arXiv preprint:* 1808.00608, (2018). PRA press.

  Together with my co-authors, I contributed to the refinement of the finite-resource upper bounds for the secret key capacity of bosonic Gaussian channels. I also derived the non-asymptotic behaviour of the upper bound (in the number of channel uses) for the specific case of the thermal-loss channel.
  The content of this paper is presented in Chapter 3.

- [7] R. Laurenza and S. Pirandola "General bounds for sender-receiver capacities in multipoint quantum communications," *Phys. Rev. A*, **96**, 032318, (2017).

  Together with my co-author, I contributed to determine the bounds for the secret key capacities of the multi-user communication schemes presented in the paper. In particular, I have carried out the explicit calculations for thermal-loss broadcast channel.
  The content of this paper is presented in Chapter 4.

- [8] R. Laurenza, C. Lupo, G. Spedalieri, S. L Braunstein and S. Pirandola "Channel simulation in quantum metrology," *Quantum Meas. Quantum Metrol.*, **5**, 1-12, (2018).

Here I investigated the quantum Cramér-Rao bound for adaptive quantum parameter estimation by using finite-energy resource states.
The content of this paper is presented in Chapter 5.

- [9] S. Pirandola, R. Laurenza and C. Lupo "Fundamental limits to quantum channel discrimination," *arXiv preprint:* 1803.02834, (2018).

  Here I helped and contributed to the derivation of the basic simulation error which is involved in the protocol of port-based teleportation. This error is crucial in the following derivations which lead to the fundamental lower bound for the discrimination of two arbitrary discrete-variable quantum channels. Then, I also contributed to derive the ultimate limits for adaptive quantum illumination.
  The content of this paper is presented in Chapter 5.

Introduction

In the last few decades, quantum information [10–13] has provided a huge speed-up to the practical implementation of quantum technologies. The huge interest devoted to this broad area of research mainly comes from the fact that the employment of quantum systems, such as atoms and photons, allows to outperform several different task that are already implemented on current technology. Moreover the size of computer's components has been pushed down to a regime where quantum features must be taken into account. Several quantum algorithms have been demonstrated that, by exploiting quantum information processing, the speed of computing is greatly enhanced [14, 15]. Quantum communication protocols such as quantum teleportation [16–20] and quantum cryptography [21, 22] provide new and innovative techniques for the manipulation and the transmission of the information that allow to improve the efficiency and the security of communications.

In the first part of this thesis, we consider quantum communication over quantum channels which is one of the central topics of the theory. In this scenario, the most typical tasks include the reliable transmission of quantum information, quantum key distribution (QKD) and the sharing of entanglement, whose importance is at the core of the implementation of quantum teleportation, which is also a crucial tool for the setting up of a realistic quantum Internet [23, 24]. Unfortunately, in practical implementations, one has to cope with the fundamental problem of the interactions between the quantum carriers of the information and the sorrounding environment. Such interactions lead to typical phenomena of noise and decoherence that may rapidly weaken the purely quantum features of the systems involved [25]. For this reason, the performance of any point-to-point quantum and private communication scheme suffers from fundamental limitations that increase with the distance between parties and a potential way to overcome this hindrance is to resort to quantum repeaters [26, 27]. In this context, it is of prominent importance then to have a complete understanding of the optimal rates that are achievable by two remote parties connected by a quantum channel. To assess this problem, we need to consider the most general strategies allowed by quantum mechanics. This means that on the one hand we must not put any constrain on the local operations (LOs), which need to be arbitrary and completely general, whereas on the other, we assume that the parties are assisted by unlimited two-way classical communication (CC), i.e. feed-forward and feedback, by means of which the users can update their local quantum systems before and after each transmission along the channel. The optimal rates are also known as the *two-way quantum capacities* of the quantum channel, with different definitions depending on the operational task we are considering. Namely we investigate the two-way capacities at which two remote parties can distribute entanglement (D_2), transmit quantum information (Q_2) and generate secret keys (K) over many uses of a quantum channel. Despite the theoretical advances in this field [28–31], very little is known in the theory about these quantum capacities. In fact, their determination is extremely hard since they are defined through the optimization over all the possible adaptive strategies and then by taking the limit in the number of channel uses going to infinite. The best route to follow is then represented by finding suitable lower [32,33] and upper bounds [34] that usually are built on quantum information measures as well as entanglement monotones [35].

In our work we first build a novel upper bound on the two-way capacities which is given in terms of the relative entropy of entanglement (REE) [36]. Such an upper bound is then simplified through a completely innovative and powerful methodology. This allows to reduce any adaptive protocol of a given task into a simpler protocol with the same task but with a block structure, meaning that the output can be written in terms of the tensor product of many copies of suitable quantum states. This has been called by us *stretching* of the protocol, where the meaning will be clearer later. To develop such a technique we first refine and expand the tool of quantum channel LOCC-simulation [37–39] in order to include into the description any quantum channel in both the discrete (DV) and the continuous variable (CV) setting. Following this approach the action of a quantum channel on an input state is directly translated into the action of a generic LOCC over the tensor product between the input and a suitable resource state. When the quantum channel commutes with the group of teleportation unitaries (i.e. they are teleportation covariant), we are able to identify the LOCC in the simulation with quantum teleportation and the resource state with the (asymptotic) Choi state of the same channel. Through this, we then show that the two-way capacities of an arbitrary channel are actually upper-bounded by a single letter quantity, i.e. the relative entropy of entanglement computed over the (asymptotic) Choi state. The results of our methdology are quite remarkable. In fact, on the one hand, we find the tightest upper bounds on the two-way capacities known so far, on the other, we show that for a particular class of channel acting on either finite and infinite dimensional Hilbert spaces, by showing coincidence between the lower and the upper bounds, we exactly determine their two-way capacities. An important example is given by the bosonic lossy channel with transmissivity η, for which all the two-way quantum capacities are equal to $-\log_2(1-\eta)$ corresponding to $\simeq 1.44\eta$ bits per channel use at long distances (i.e high losses). This result completely characterizes the fundamental rate-loss scaling of any point-to-point QKD protocol through a lossy communication line, such as an optical fibre or a free-space link.

In the second part of this thesis we extend our approach to other fundamental areas of quantum information theory. In particular we consider quantum metrology and quantum channel discrimination. Quantum metrology [40, 41] deals with the estimation of unknown physical parameters that are encoded in quantum states or in quantum channels. We are here interested in the latter case-scenario, where we are given a black-box implementing some parameter-dependent transformation. We probe the box n times thus building a parameter estimator whose error variance decreases as a function of n. For some quantum channels this error variance scales as $\sim n^{-1/2}$, known as the *standard quantum limit*. This is not a fundamental quantum bound since it can be obtained also in a classical setting. By exploiting truly quantum features like entanglement among the probing devices employed for the measurements, it can be shown that the performance is greatly improved with a scaling that follows the behaviour $\sim n^{-1}$, known as the *Heisenberg scaling* [41]. In order to understand which scaling limits a given quantum channel it is essential to adopt the most general quantum protocols of parameter estimation that are allowed by quantum mechanics. These involve the use of unlimited entanglement and are inevitably adaptive, i.e., they may involve the use of joint quantum operations (instead of LOCC) where the inputs to the box are optimised as a result of all the previous rounds. This is the main difficulty of the analysis and once again channel simulation is the most powerful tool that we invoke to reduce the complexity. By applying our channel simulation technique, in fact, the authors of Ref. [42] provide a *no-go* theorem for Heisenberg scaling when considering teleportation covariant channels. Here in this thesis we slightly modify the simulation described above by substituting standard quantum teleportation with *port-based* teleportation (PBT) [43–45], where a multi-copy state is employed as the resource of entanglement. By applying this PBT-simulation to adaptive quantum metrology over a finite-dimensional channel, we prove an ultimate bound which asymptotically follows the Heisenberg scaling.

Port-based teleportation simulation turns out to be fundamental also in the setting of quantum channel discrimination (QCD). In this context, the goal is to distinguish between two or more quantum transformations acting on the state of a quantum system. There are practical problems related to QCD where the quantum features have been shown to provide better results with respect to classical strategies. Typical examples are represented by the readout of digital memories, a protocol that undergoes the name of *quantum reading* [46, 47], the resolution of single-photon diffraction diffraction-limited optical systems [48–50] and *quantum illumination* [51–54], a protocol for sensing the presence of an low-reflectivity target in a thermal noisy environment. Usually the strategies for QCD involve optimizations over the input states and the output detection measurements. The ultimate performance in terms of the probability of error must be addressed by considering adaptiveness in the protocols, where feedback from the output is exploited to update the input. Here the LOCC that we have in quantum communication are substituted with quantum operations that may also include the use of entanglement among the registers of the users' local quantum systems. While on the one hand we know how to bound the error probability for the discrimination of quantum states [55], a similar bound is missing for the probability of error affecting the discrimination of quantum channels. Here we build such a bound by relying on the reduction of an adaptive protocol for QCD to a block one over multiple copies of the channel's Choi state. This is obtained by employing port-based teleportation at the core of channel simulation and as a direct application of this result we derive such a bound for the ultimate performance of adaptive quantum illumination.

Chapter 1

Preliminaries

In this Chapter we review some basic and fundamental concepts in quantum information theory with a major focus on continuous variable systems. Quantum channels and quantum teleportation are exhaustively discussed.

1.1 Gaussian quantum information

1.1.1 Bosonic systems and Gaussian states

In a wide part of this thesis we willl be dealing with continuous variable (CV) systems, i.e. quantum mechanical systems that can be described by an infinite dimensional Hilbert space. Quantum harmonic oscillators (bosonic modes), which do correspond to the quantized radiation modes of the electromagnetic field, are a good example of CV quantum systems. The infinite dimensionality of the underlying Hilbert space calls for a description of these systems through quantum operators with continuous eigenspectra.

Let us consider a system of N bosons labeled by k associated with N-tensor product Hilbert space $\mathcal{H}^{\otimes N} = \bigotimes_{k=1}^{N} \mathcal{H}_k$ and described by N pairs of bosonic fields operators (also called ladder operators) $\{\hat{a}_i, \hat{a}_i^\dagger\}_{i=1}^N$ which satisfy the bosonic commutation relations

$$[\hat{a}_k, \hat{a}_l^\dagger] = \delta_{kl} \ . \tag{1.1}$$

The Hilbert space of this system is separable and infinite-dimensional. This is due to the fact that the single-mode Hilbert space $\mathcal{H}_k$ is spanned by the countable Fock's basis $\mathbf{B} = \{|n_k\rangle\}_{n_k=1,\ldots,\infty}$, where the elements $|n_k\rangle$ are the eigenstates of the number operator $\hat{n}_k|n_k\rangle = n_k|n_k\rangle$, with $\hat{n}_k := \hat{a}_k^\dagger \hat{a}_k$ and n_k describing the number of photons in mode k. The action of the bosonic operators is well defined on these vectors, in fact we can start from the vacuum state $|0_k\rangle$, which describes the mode k with zero photons, and by applying n_k times the creation operator $\hat{a}_k^\dagger$ we get

$$|n_k\rangle = \frac{1}{\sqrt{n_k!}}(\hat{a}_k^\dagger)^{n_k}|0_k\rangle \tag{1.2}$$

and in particular

$$\hat{a}_k^\dagger|n_k\rangle = \sqrt{n_k+1}|n_k+1\rangle \ . \tag{1.3}$$

In the same manner the annihilation operator $\hat{a}_k$ applied n_k times to the number state $|n_k\rangle$ gives the vacuum state

$$|0_k\rangle = \frac{1}{\sqrt{n_k!}}\hat{a}_k^{n_k}|n_k\rangle \ , \tag{1.4}$$

and in particular

$$\hat{a}_k|n_k\rangle = \sqrt{n_k}|n_k-1\rangle \ . \tag{1.5}$$

At this point, one can introduce the vector of operators $\hat{\mathbf{r}} = (\hat{a}_1, \hat{a}_1^\dagger, \ldots, \hat{a}_N, \hat{a}_N^\dagger)$ so that the bosonic commutation relations of Eq. (1.1) can be recast in the following form

$$[\hat{r}_l, \hat{r}_m] = \Omega_{lm} \quad (l, m = 1\ldots, 2N) \ , \tag{1.6}$$

where the $2N \times 2N$ matrix $\mathbf{\Omega}$ is defined by

$$\mathbf{\Omega} := \bigoplus_{k=1}^{N} \omega \quad \omega := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ , \tag{1.7}$$

and is referred to as the *symplectic form.* We can introduce another type of field operator by relying on the bosonic field operators introduced above. These are obtained from the cartesian decomposition of $\hat{a}_k$ and $\hat{a}_k^\dagger$ which read as follows

$$\hat{a}_k := \frac{1}{2}(\hat{q}_k + i\hat{p}_k) \qquad \hat{a}_k^\dagger := \frac{1}{2}(\hat{q}_k - i\hat{p}_k) \ , \tag{1.8}$$

from which we can derive

$$\hat{q}_k = \hat{a}_k + \hat{a}_k^\dagger, \ \hat{p}_k = i(\hat{a}_k^\dagger - \hat{a}_k) \ . \tag{1.9}$$

These are the quadrature field operators, usually arranged in the vector of operators $\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n)$ and represent dimensionless observables of the system behaving like the momentum and the position operators of the quantum harmonic oscillator since they satisfy the canonical commutation relations

$$[\hat{x}_i, \hat{x}_j] = 2i\Omega_{ij} \ . \tag{1.10}$$

The quadrature operators just introduced have continuous eigenspectra, with non square integrable eigenstates, i.e. unphysical states, which read as follows

$$\hat{q}|q\rangle = q|q\rangle \ , \quad \hat{p}|p\rangle = p|p\rangle \ , \tag{1.11}$$

with $q, p \in \mathbb{R}$. They form two bases since they satisfy orthogonality and completeness relations respectively given by

$$\langle q|q'\rangle = \delta(q-q') \ , \quad \langle p|p'\rangle = \delta(p-p') \tag{1.12}$$

and

$$\int_{-\infty}^{\infty} |q\rangle\langle q| \ dq = \mathbb{I} \ , \quad \int_{-\infty}^{\infty} |p\rangle\langle p| \ dp = \mathbb{I} \ . \tag{1.13}$$

These two orthonormal sets $\{|q\rangle\}_{q\in\mathbb{R}}$ and $\{|p\rangle\}_{p\in\mathbb{R}}$ are mutually connected to each other by Fourier transform, namely

$$|q\rangle = (2\sqrt{\pi})^{-1} \int_{-\infty}^{\infty} e^{-ipq}|p\rangle \ dp \ , \quad |p\rangle = (2\sqrt{\pi})^{-1} \int_{-\infty}^{\infty} e^{ipq}|q\rangle \ dq \ . \tag{1.14}$$

1.1.2 Phase space representation

We can give an equivalent description of quantum states in terms of *phase-space* variables such as the quadratures introduced above. The phase space description can be understood by the introduction of the so-called Wigner function which allows to describe the dynamics of quantum systems in terms of a *quasi*-probability distibution. Quantum dynamics is therefore translated into the evolution of the phase-space distribution in a classical-like fashion. The Wigner distribution is bounded and normalized and enables the computation of mean values and variances of the quadratures but, as opposed to a classical probability distribution, it can take on negative values.

We begin by considering the set of displacement operators for N-bosons

$$D(\boldsymbol{\gamma}) = \bigotimes_{k=1}^{N} D_k(\gamma_k) \ , \tag{1.15}$$

whose action on the mode operators defined in the previous section is described via the following transformation

$$D(\boldsymbol{\gamma})^{\dagger}\hat{a}_k D(\boldsymbol{\gamma}) = \hat{a}_k + \gamma_k \ . \tag{1.16}$$

In Eq. (1.15) the column vector $\boldsymbol{\gamma}$ is given by $\boldsymbol{\gamma} = (\gamma_1, \ldots, \gamma_N)^T$, $\gamma_k \in \mathbb{C}$ and $D(\gamma_k) := \exp(\gamma_k \hat{a}_k^{\dagger} - \gamma_k^* \hat{a}_k)$ are the single-mode displacement operators. We also define the vector

$\boldsymbol{\gamma}^\dagger = (\gamma_1^*, \ldots, \gamma_N^*)$. An N-mode bosonic system is uniquely described by its quantum state, i.e. a positive operator $\hat{\rho}$ with unit trace acting on the corresponding Hilbert space, $\hat{\rho} : \mathcal{H}^{\otimes N} \to \mathcal{H}^{\otimes N}$. We denote with the symbol $\mathcal{D}(\mathcal{H}^{\otimes N})$ the space of density operators on $\mathcal{H}^{\otimes N}$. The operators $D(\boldsymbol{\gamma})$ belong to a complete set since any $\hat{\rho} \in \mathcal{D}(\mathcal{H}^{\otimes N})$ can be written as follows

$$\hat{\rho} = \int_{\mathbb{C}^N} \frac{d^{2N}\boldsymbol{\gamma}}{\pi^{2N}} \operatorname{Tr}[\hat{\rho} D(\boldsymbol{\gamma})] D(\boldsymbol{\gamma})^\dagger \ , \tag{1.17}$$

and in it we identify the *characteristic* function of the operator $\hat{\rho}$ as

$$\chi(\boldsymbol{\gamma}) = \operatorname{Tr}[\hat{\rho} D(\boldsymbol{\gamma})] \ . \tag{1.18}$$

This is introduced also as the moment-generating function of $\hat{\rho}$ since its derivatives in the origin of the complex plane provide the simmetrically ordered moments of the mode operators, namely

$$(-)^m \frac{\partial^{n+m}}{\partial \gamma_j^n \partial \gamma_k^{*m}} \chi(\boldsymbol{\gamma})\big|_{\boldsymbol{\gamma}=0} = \operatorname{Tr}\left\{\hat{\rho}\mathcal{S}\left[(\hat{a}_j^\dagger)^n \hat{a}_k^m\right]\right\} \ , \tag{1.19}$$

where we have introduced the symmetrization $\mathcal{S}$ so that for example $\mathcal{S}[\hat{a}^\dagger\hat{a}^2] = (\hat{a}^2\hat{a}^\dagger + \hat{a}^\dagger\hat{a}^2 + \hat{a}^\dagger\hat{a})/3$. Any operator density operator $\hat{\rho}$ has an equivalent representation in terms of the Wigner function, which is introduced via the Fourier transform of the characteristic function, i.e.

$$W(\boldsymbol{\alpha}) = \int_{\mathbb{C}^N} \frac{d^{2N}\boldsymbol{\gamma}}{(2\pi)^{2N}} \exp\left\{\boldsymbol{\gamma}^\dagger\boldsymbol{\alpha} + \boldsymbol{\alpha}^\dagger\boldsymbol{\gamma}\right\} \chi(\boldsymbol{\gamma}) \ , \tag{1.20}$$

where $\boldsymbol{\alpha} = (a_1, \ldots, a_N)$ with $a_k := q_k + ip_k$. Since the characteristic function defined in (1.18) is square integrable, the Wigner distribution is a well behaved probability distribution, normalized since $1 = \operatorname{Tr}\hat{\rho} = \int_{\mathbb{C}^N} d^{2N}\boldsymbol{\alpha} W(\boldsymbol{\alpha})$, and it can be exploited to give expectation values of the simmetrically ordered moments following the receipt

$$\operatorname{Tr}\left\{\hat{\rho}\mathcal{S}\left[(\hat{a}^\dagger)^n \hat{a}^m\right]\right\} = \int_{\mathbb{C}^N} d^{2N}\boldsymbol{\alpha}\, W(\boldsymbol{\alpha}) a^m a^{*n} \ , \tag{1.21}$$

which can be straightforwardly derived from Eq. (1.19). We can equivalently represent the Wigner function of Eq. (1.20) in Cartesian coordinates. Let us introduce the vector of quadrature operators

$$\hat{\mathbf{x}} = (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_N, \hat{p}_N) \ , \tag{1.22}$$

and the vector of the corresponding eigenvalues

$$\mathbf{x} = (q_1, p_1, \ldots, q_N, p_N) \ , \tag{1.23}$$

which are continuous variable that span a real symplectic space $\mathcal{K} := (\mathbb{R}^{2N}, \boldsymbol{\Omega})$. The Wigner representation can then be expressed as follows

$$W(\mathbf{x}) = \int_{\mathbb{R}^{2N}} \frac{d^{2N}\boldsymbol{\xi}}{(2\pi)^{2N}} \exp\left\{-i\mathbf{x}^T\boldsymbol{\xi}\right\} \chi(\boldsymbol{\xi}) \ , \tag{1.24}$$

with the generic vector $\boldsymbol{\xi} \in \mathbb{R}^{2N}$ and where $\chi(\boldsymbol{\xi}) = \mathrm{Tr}[\hat{\rho}D(\boldsymbol{\xi})]$ with the Weyl operator defined by $D(\boldsymbol{\xi}) := \exp\left\{i\hat{\mathbf{x}}^T\boldsymbol{\xi}\right\}$. From now on we will work with Cartesian coordinates having in mind that the two representation of Eq. (1.20) and (1.24) are equivalent. By means of the Wigner representation we can characterize a wide class of quantum states within the continuous variable setting. Among these there are those belonging to the set of Gaussian states which are completely characterized by the first two statistical moments of Eq. (1.21) and whose Wigner funtion is non-negative.

1.1.3 Gaussian states and Gaussian unitaries

Gaussian states for N-mode bosonic systems are at the core of quantum communication and computation with continuous variables system. These states have been deeply studied and commonly employed since they can be reproduced in the laboratory with the present technologies relying on which we can implement evolution of quantum systems that are described by Hamiltonians at most second-order polynomial in the quantum field operators. Such Hamiltonians generate unitaries transformation that preserve the Gaussian features of the quantum state in input.

An N-mode quantum state $\hat{\rho}$ is Gaussian if its Wigner representation is Gaussian, i.e.

$$W(\mathbf{x}) = \frac{\exp\left[-\frac{1}{2}(\mathbf{x}-\bar{\mathbf{x}})^T\mathbf{V}^{-1}(\mathbf{x}-\bar{\mathbf{x}})\right]}{(2\pi)^N\sqrt{\det\mathbf{V}}} \ , \tag{1.25}$$

$$\chi(\boldsymbol{\xi}) = \exp\left[-\frac{1}{2}\boldsymbol{\xi}^T\mathbf{V}\boldsymbol{\xi} - i(\boldsymbol{\Omega}\bar{\mathbf{x}})^T\boldsymbol{\xi}\right] \ , \tag{1.26}$$

where the first statistical moment, or mean value is given by $\bar{\mathbf{x}} := \langle\hat{\mathbf{x}}\rangle = \mathrm{Tr}\,\hat{\rho}\hat{\mathbf{x}}$ and it can be set to zero without losing generality. The second statistical moment is represented by the so-called $2N \times 2N$ *covariance matrix* (CM) $\mathbf{V}$ whose generic element V_{ij} is defined by means of the second statistical moment, symmetrized according to Eq. (1.21)

$$\begin{aligned}\langle(\hat{x}_i\hat{x}_j+\hat{x}_j\hat{x}_i)/2\rangle &= \mathrm{Tr}[\hat{\rho}(\Delta\hat{x}_i\Delta\hat{x}_j+\Delta\hat{x}_j\Delta\hat{x}_i)/2] \\ &= \int_{\mathbb{R}^{2N}} W(\mathbf{x})x_ix_jd^{2N}\mathbf{x} \\ &=: V_{ij}\ . \end{aligned} \tag{1.27}$$

In particular the diagonal elements of the covariance matrix represent the variances of the quadrature operators, i.e. $V_{ii}=\langle(\Delta\hat{x}_i)^2\rangle=\langle\hat{x}_i^2\rangle-\langle\hat{x}_i\rangle^2$. Like any matrix describing physical correlations, the matrix $\mathbf{V}$ must be real, symmetric and positive and must satisfy the uncertainty principle [56, 57]

$$\mathbf{V}+i\mathbf{\Omega}\geq 0\ , \tag{1.28}$$

which directly follows from the non-negativity of the density operator $\hat{\rho}$ and the commutation relation in Eq. (1.10). The inequality in Eq. (1.28) implies that $\mathbf{V}$ is positive definite. Gaussian states turn out to be completely characterized by the first two moments $\bar{\mathbf{x}}$ and $\mathbf{V}$, i.e. we have $\hat{\rho}=\hat{\rho}(\bar{\mathbf{x}},\mathbf{V})$. Now we are in the position to characterize the discrete transformations on Gaussian states and to specify the corresponding transformations on the quadrature operators in the phase-space description.

Reversible transformations are represented by unitary operations U, with $U^\dagger=U^{-1}$ acting on a generic state according to $\hat{\rho}\to U\hat{\rho}U^\dagger$. Furthermore such a transformation is defined to be Gaussian if it preserves the Gaussian features of a quantum state. These Gaussian unitaries are generated through exponentiation $U=\exp\left(-i\hat{H}/2\right)$ with Hamiltonian operators $\hat{H}$ that are linear and bilinear in the field mode, i.e., upon introducing the vectors of creation and annihilation operators, $\hat{\mathbf{a}}:=(\hat{a}_1,\ldots,\hat{a}_N)^T$ and $\hat{\mathbf{a}}^\dagger:=(\hat{a}_1^\dagger,\ldots,\hat{a}_N^\dagger)$, these Hamiltonians can be written as

$$\hat{H}=i(\hat{\mathbf{a}}^\dagger\mathbf{g}+\hat{\mathbf{a}}^\dagger\mathbf{G}\hat{\mathbf{a}}+\hat{\mathbf{a}}^\dagger\mathbf{G}'\hat{\mathbf{a}}^{\dagger T})+h.c.\ , \tag{1.29}$$

where $\mathbf{g}\in\mathbb{C}^N$, whereas both $\mathbf{G}$ and $\mathbf{G}'$ are $N\times N$ complex matrices. In the Heisenberg picture, the field operators transfroms according to the following unitary transformation, usually referred to as Bogoliubov transformation

$$\hat{a}\to U^\dagger\hat{a}U=\mathbf{A}\hat{a}+\mathbf{B}\hat{a}^\dagger+\mathbf{g} \tag{1.30}$$

with $N\times N$ complex matices $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{A}\mathbf{B}^T=\mathbf{B}\mathbf{A}^T$. The Gaussian transformations on the quadrature operators imposed by the Hamiltonians as in Eq. (1.29) can be expressed through the following affine map

$$(\mathbf{S},\mathbf{d}) \; : \; \hat{\mathbf{x}} \to \mathbf{S}\hat{\mathbf{x}} + \mathbf{d} \ , \tag{1.31}$$

where $\mathbf{d} \in \mathbb{R}^{2N}$ and the $2N \times 2N$ real matrix $\mathbf{S}$ is a *symplectic* transformation. This means that the commutation relations of Eq. (1.10) are preserved by the transformation $\mathbf{S}$, a property that follows from the fact that the symplectic form $\mathbf{\Omega}$ is left invariant by the action of $\mathbf{S}$, i.e.

$$\mathbf{S}\mathbf{\Omega}\mathbf{S}^T = \mathbf{\Omega} \ . \tag{1.32}$$

Clearly the vector $\mathbf{x} \in \mathcal{K}(\mathbb{R}^{2N}, \mathbf{\Omega})$ of eigenvalues of the quadrature operators $\hat{\mathbf{x}}$ must transform according the same rule, i.e. $(\mathbf{S},\mathbf{d}) \; : \; \mathbf{x} \to \mathbf{S}\mathbf{x} + \mathbf{d}$. In this way we can conclude that an arbitrary Gaussian unitary $U_{\mathbf{S},\mathbf{d}}$ acting on the Hilbert space $\mathcal{H}$ of the system is equivalent to a symplectic affine map $(\mathbf{S},\mathbf{d})$ which acts on the corresponding phase space $\mathcal{K}$. Such a map is composed by two different element, namely the phase space displacement vector $\mathbf{d} \in \mathbb{R}^{2N}$ corresponding to the displacement operator $D(\mathbf{d})$, and the symplectic transformation $\mathbf{S}$ corresponding to a canonical unitary map $U_{\mathbf{S}}$ in the Hilbert space. Thus we can always write $U_{\mathbf{S},\mathbf{d}} = D(\mathbf{d})U_{\mathbf{S}}$. The statistical moments of a Gaussian state transform accordingly as

$$\bar{\mathbf{x}} \to \mathbf{S}\bar{\mathbf{x}} + \mathbf{d} \ , \tag{1.33}$$

$$\mathbf{V} \to \mathbf{S}\mathbf{V}\mathbf{S}^T \ , \tag{1.34}$$

which completely characterize the action of a Gaussian unitary $U_{\mathbf{S},\mathbf{d}}$ over a Gaussian state $\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$.

We give some examples of some Gaussian states and Gaussian unitaries for single and two bosonic modes which are the most commonly employed in continuous variable quantum information and which will be playing a central role in this thesis.

- *Vacuum and thermal state* - The vaccum state $|0\rangle$ is a Gaussian state with zero mean photon number, i.e. $\bar{n} = 0$, and it is defined as the eigenstate of the annihilation operator with null eigenvalue $\hat{a}|0\rangle = 0$. It is characterized by a covariance matrix (CM) equal to the identity operator $\mathbf{I}$, so that the position and momentum operator have noise variance equal to one, i.e. $V(\hat{q}) = V(\hat{p}) = 1$, known also as the *quantum shot-noise*. Another fundamental Gaussian state is represented by the thermal state. This is a state $\hat{\rho}_{th}$ that maximizes the von Neumann entropy defined as

$$S := -\operatorname{Tr} \hat{\rho} \ln \hat{\rho} \tag{1.35}$$

This can be written in the number-state representation as

$$\hat{\rho}_{th}(\bar{n}) = \sum_{n=0}^{\infty} \frac{\bar{n}^n}{(\bar{n}+1)^{n+1}} |n\rangle\langle n| \ . \tag{1.36}$$

The Gaussian Wigner function of $\hat{\rho}_{th}$ is characterized by zero mean value and covariance matrix given by $\mathbf{V} = (2\bar{n}+1)\mathbf{I}$.

- *Coherent states* - Coherent states $|\alpha\rangle$ are the eigenstates of the annihilation operator, i.e. $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, where $\alpha = (q+ip)/2$ is the complex amplitude. Their decomposition on the number state basis reads

$$|\alpha\rangle = e^{-\frac{1}{2}|\alpha|^2} \sum_{n=0}^{\infty} \frac{\alpha^n}{\sqrt{n!}} |n\rangle \ . \tag{1.37}$$

Coherent states can be generated by acting with a displacement operator $D(\alpha)$ on the vacuum, i.e. $D(\alpha)|0\rangle$. The operator $D(\alpha)$ is the single-mode version of the one introduced in Sec. (1.1.2) but now we can introduce it as a Gaussian unitary generated by the linear term in the Hamiltonian of Eq. (1.29), namely we have

$$D(\alpha) = \exp\left(\alpha\hat{a}^\dagger - \alpha^*\hat{a}\right) \tag{1.38}$$

In the Heisenberg picture, based on the prescription of Eq. (1.30), the annihilation operator undergoes the transformation $\hat{a} \to \hat{a} + \alpha$, whereas the quadrature operator vector undergo the transformation $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + \mathbf{d}_\alpha$ with $\mathbf{d}_\alpha = (q,p)^T$. The mean values of a coherent state is $\bar{\mathbf{x}} = \mathbf{d}_\alpha$, and as for the vacuum state, the CM of a coherent state is given by the identity $\mathbf{V} = \mathbf{I}$.

- *Squeezed states* - The single-mode squeezing operator $S(r)$ is a Gaussian unitary which is generated by the quadratic term in the Hamiltonian of Eq. (1.29) proportional to $\hat{a}^{\dagger 2}$ and to $\hat{a}^2$

$$S(r) = \exp\left\{\frac{r}{2}[\hat{a}^2 - \hat{a}^{\dagger 2}]\right\} \tag{1.39}$$

with $r \in \mathbb{R}$ the squeezing parameter. In the Heisenberg picture the annihilation operator evolves according to $\hat{a} \to (\cosh r)\hat{a} - (\sinh r)\hat{a}^\dagger$ and the quadrature operators are transformed by the symplectic map $\hat{\mathbf{x}} \to \mathbf{S}(r)\hat{\mathbf{x}}$ with $\mathbf{S}(r) = \begin{pmatrix} e^{-r} & 0 \\ 0 & e^{r} \end{pmatrix}$.

If we apply the operator $S(r)$ to the vacuum $|0\rangle$ we get

$$|0,r\rangle = (\cosh r)^{-1} \sum_{n=0}^{\infty} \frac{(2n)!}{2^n n!} \tanh r^n |2n\rangle \ , \tag{1.40}$$

which is the squeezed vacuum state with covariance matrix $\mathbf{V} = \mathbf{S}(r)\mathbf{S}(r)^T = \mathbf{S}(2r)$ with one variance squeezed below the quantum shot-noise and the other anti-squeezed above the quantum shot-noise.

- *Two-mode squeezing and EPR states* - The squeezing operator of two modes a and b is the Gaussian unitary defined as

$$S_2(r) = \exp\left[\frac{r}{2}\left(\hat{a}\hat{b} - \hat{a}^\dagger\hat{b}^\dagger\right)\right] \ , \tag{1.41}$$

with r quantifying two-mode squeezing. In the Heisenberg picture the transformation of the quadrature operators $\hat{\mathbf{x}} = (\hat{q}_a, \hat{p}_a, \hat{q}_b, \hat{p}_b)^T$ is given by the following symplectic map

$$\hat{\mathbf{x}} \to \mathbf{S}_2(r)\hat{\mathbf{x}} \quad \text{and} \quad \mathbf{S}_2(r) = \begin{pmatrix} \cosh r\mathbf{I} & \sinh r\mathbf{Z} \\ \sinh r\mathbf{Z} & \cosh r\mathbf{I} \end{pmatrix} \ , \tag{1.42}$$

with $\mathbf{Z} := \mathrm{diag}(1, -1)$. At this stage the Einstein-Podolsky-Rosen (EPR) state also called two-mode squeezed vacuum (TMSV) is obtained by applying $S_2(r)$ to a two-mode vacuum state. A TMSV Φ^μ is a Gaussian state with zero mean value and covariance matrix given by

$$\mathbf{V}^\mu = \begin{pmatrix} \mu\mathbf{I} & \sqrt{\mu^2-1}\mathbf{Z} \\ \sqrt{\mu^2-1}\mathbf{Z} & \mu\mathbf{I} \end{pmatrix} \tag{1.43}$$

where $\mu = \cosh 2r$ is the noise variance in the quadrature and once defined $\hat{q}_- := (\hat{q}_a - \hat{q}_b)/\sqrt{2}$ and $\hat{p}_+ := (\hat{p}_a + \hat{p}_b)/\sqrt{2}$, from Eq. (1.43) we can easily verify that $V(\hat{q}_-) = V(\hat{p}_+) = e^{-2r}$.

The Gaussian Wigner function of a TMSV reads as follows

$$W[\Phi^\mu](x) = 4\pi^{-2}\exp\left[-x^T(\mathbf{V}^\mu)^{-1}x\right] \ , \tag{1.44}$$

where $x = (q_a, p_a, q_b, p_b)^T$. We notice that in the limit of infinite squeezing, i.e. $\mu \to +\infty$, this Wigner function approaches a delta-like expression [19]

$$W[\Phi^\mu](x) \to \aleph\delta(q_a - q_b)\delta(p_a + p_b) \tag{1.45}$$

with $\aleph$ a normalization factor. Thus, the infinite-energy limit of TMSV states $\lim_\mu \Phi^\mu$ defines the asymptotic CV EPR state Φ, i.e. $\Phi = \lim_\mu \Phi^\mu$, with perfect correlations $\hat{q}_a = \hat{q}_b$ and $\hat{p}_a = -\hat{p}_b$.

- *Beam splitter* - The beam splitter transformation is one of the most important example of Gaussian untary for two bosonic modes a and b with respective annihilation operators $\hat{a}$ and $\hat{b}$. This Gaussian unitary is defined via

$$BS(\varphi) = \exp\left[\varphi(\hat{a}^\dagger\hat{b} - \hat{a}\hat{b}^\dagger)\right] \ , \tag{1.46}$$

where the quantity φ determines the transmissivity τ of the beam splitter through the relation $\tau = \cos^2\varphi \in [0,1]$. Again, in the Heisenberg picture, the annihilation operators are transformed by the linear Bogoliubov transformation

$$\begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \to \begin{pmatrix} \sqrt{\tau} & \sqrt{1-\tau} \\ -\sqrt{1-\tau} & \sqrt{\tau} \end{pmatrix} \begin{pmatrix} \hat{a} \\ \hat{b} \end{pmatrix} \ , \tag{1.47}$$

which corresponds to the following symplectic transformation on the quadrature operators $\hat{\mathbf{x}} = (\hat{q}_a, \hat{p}_a, \hat{q}_b, \hat{p}_b)^T$

$$\hat{\mathbf{x}} \to \mathbf{B}(\tau)\hat{\mathbf{x}} \quad , \quad \mathbf{B}(\tau) := \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix} \ . \tag{1.48}$$

According to a fundamental theorem by Williamson [58–60], for any N-mode Gaussian state there always exists a symplectic transformation $\mathbf{S}$ by means of which the CM $\mathbf{V}$ of the state can be diagonalized, i.e.

$$\mathbf{V} = \mathbf{S}\boldsymbol{\nu}\mathbf{S}^T \ , \tag{1.49}$$

where $\boldsymbol{\nu} = \mathrm{diag}(\nu_1, \nu_1, \ldots, \nu_N, \nu_N)$ and the quantities ν_k's represent the *symplectic spectrum* of $\mathbf{V}$. These symplectic eigenvalues are clearly invariant under symplectic transformation and satisfy $\sqrt{\det\mathbf{V}} = \prod_{k=1}^N \nu_k$, since we have that $\det\mathbf{S} = 1$ being $\mathbf{S}$ symplectic. In terms of density operators, the decomposition of Eq. (1.49) corresponds to a decomposition in terms of thermal states and canonical Gaussian unitaries $U_{\mathbf{S},\mathbf{d}} =$ and reads as follows

$$\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V}) = U_{\mathbf{S},\mathbf{d}} \left(\bigotimes_{k=1}^N \hat{\rho}_{th}(\bar{n}_k)\right) U_{\mathbf{S},\mathbf{d}}^\dagger \tag{1.50}$$

where $\rho_{th}(\bar{n}_k)$ has been introduced in Eq. (1.36) and the mean thermal number $\bar{n}_k$ is related to the symplectic spectrum according to $\nu_k = 2\bar{n}_k + 1$.

The symplectic spectrum contains the most essential informations about the relative Gaussian state and it provides a powerful and straightforward way to express its fundamental properties. For instance, the von Neumann entropy of a Gaussian state can be written [61, 62]

$$S(\hat{\rho}) = \sum_{k=1}^{N} g(\nu_k) \ , \tag{1.51}$$

where

$$g(x) := \left(\frac{x+1}{2}\right) \log \left(\frac{x+1}{2}\right) - \left(\frac{x-1}{2}\right) \log \left(\frac{x-1}{2}\right) \ . \tag{1.52}$$

In particular, by applying the diagonalization in Eq. (1.49) to Eq. (1.28) we can recast the uncertainty principle into the following simpler form

$$\mathbf{V} > 0 \text{ and } \nu_k \geq 1 \ , \tag{1.53}$$

i.e. the covariance matrix must be positive definite with all the symplectic eigenvalues greater or equal than 1.

Consider now a Gaussian state $\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$ describing two bosonic modes ($N = 2$). For this kind of states there exist a simple analytical characterization. To see this, let us write the covariance matrix into the following block form

$$\mathbf{V} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix} \ , \tag{1.54}$$

where $\mathbf{A} = \mathbf{A}^T$, $\mathbf{B} = \mathbf{B}^T$ and $\mathbf{C}$ are 2×2 real matrices. The Williamson diagonalization leads to the diagonal CM $\mathbf{V} = \nu_+ \mathbf{I} \oplus \nu_- \mathbf{I}$, where the two symplectic eigenvalues ν_+ and ν_- assume the following expression [60]

$$\nu_\pm = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4 \det \mathbf{V}}}{2}} \ , \tag{1.55}$$

with $\Delta := \det \mathbf{A} + \det \mathbf{B} + 2 \det \mathbf{C}$. Is is easy to check that, in this case, the uncertainty principle of Eq. (1.28) corresponds to the following bona-fide conditions

$$\mathbf{V} > 0 \ , \quad \det \mathbf{V} \geq 1 \quad \text{and} \quad \Delta \leq 1 + \det \mathbf{V} \ . \tag{1.56}$$

There is a class of two-mode Gaussian states whose covariance matrix can be put in standard form, i.e.

$$\mathbf{V} = \begin{pmatrix} a\mathbf{I} & \mathbf{C} \\ \mathbf{C}^T & b\mathbf{I} \end{pmatrix} \ , \quad \mathbf{C} = \mathrm{diag}(c, c') \ , \tag{1.57}$$

with $a, b, c, c' \in \mathbb{R}$ satisfying the bona-fide conditions stated above.

1.2 Quantum channels

In this section we introduce the formalism of quantum channels which are at the core of the description of any physical process involving a mapping from an initial to a final state of a quantum system [10]. In a quantum communication scenario, quantum channels are employed to model the noise to which the transmission of information between parties is subjected. Such a noise is generated by the coupling of the quantum information carriers with external and often uncontrolled degrees of freedom and leads to losses and decoherence which are typically described by non-unitary quantum channels. Throughout this Thesis we will deal only with memoryless quantum channel, i.e. channels that act indipendently and identically over a sequence of information carriers. The memoryless condition is the simplest modelization of the input-output mapping induced by noise and it is sufficient to describe the most common scenarios where consecutive information transmissions do not retain memories of the previous ones. For an exaustive review over memory channel see Ref. [63].

We start by reviewing the general definition of quantum channels by considering only finite dimensional Hilbert spaces and then we proceed by describing single-mode Gaussian channels for CV systems.

Let us consider the mapping $\mathcal{E}$ acting on quantum state $\rho_A \in \mathcal{D}(\mathcal{H}_A)$ as

$$\rho_A \mapsto \rho_B = \mathcal{E}(\rho_A) \in \mathcal{D}(\mathcal{H}_B) \tag{1.58}$$

where we recall that $\mathcal{D}(\mathcal{H})$ is the space of non-negative, unit trace operators (density operators) defined on the Hilbert space $\mathcal{H}$. Since the output state ρ_B must be a genuine quantum state, we need to require the map $\mathcal{E}$ to be completely positive and trace preserving (CPTP), i.e. it satisfies the following properties [64, 65]

- The map $\mathcal{E}$ acts linearily over mixtures of density operators, i.e. mixtures of input states are sent into mixtures of corresponding outputs

$$\mathcal{E}\left(\sum_i p_i \rho_A^i\right) = \sum_i p_i \mathcal{E}(\rho_A^i) \ , \tag{1.59}$$

  with p_i the probability associated to ρ_A^i.

- $\mathcal{E}$ must preserve the normalization of the input state, or otherwise stated it must be trace preserving, i.e. $\operatorname{Tr} \rho_B = 1$.

- The map $\mathcal{E}$ must be positive, i.e. positivity of the density operator ρ_A is preserved under the action of $\mathcal{E}$.
- When ρ_A is a part of a joint state $\rho_{AA'}$ of system A and an ancillary system A', positivity by itself is not enough to assure the positivity of the extended map $\mathcal{E}\otimes\mathcal{I}_{A'}$. We need then to require the condition of *complete positivity*

$$\mathcal{E}\otimes\mathcal{I}_{A'}(\rho_{AA'}) \geq 0 \tag{1.60}$$

A linear map satisfying the previous properties can also be written through operational representations. One of these is given by the Stinespring dilation [66], i.e. it can be proved that a map is CPTP if and only if it can be described by a unitary interaction between the input ρ_A and an external environment which is represented by the state φ_E. This environment is not necessarily the physical environment determining the system's evolution, but it may rather correspond to a mathematical artifact. Then the output of the channel can be recovered by tracing out the environmental degrees of freedom after the unitary evolution, i.e., by taking $B = A$ for simplicity, we have

$$\mathcal{E}(\rho_A) = \mathrm{Tr}_E\left[U_{AE}(\rho_A\otimes\varphi_E)U^\dagger_{AE}\right] \ , \tag{1.61}$$

The channel representation through the Stinespring dilation is not unique but if we purify the environment state, i.e. $\varphi_E = |\varphi\rangle_E\langle\varphi|$, it can be shown that the choice of U_{AE} is unique up to partial isometries on system E .

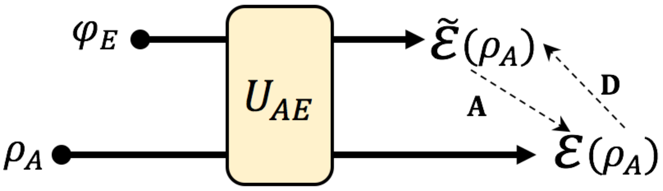

Figure 1.1: Stinespring dilation of a quantum channel $\mathcal{E}$. The input state ρ_A interacts with the environmental state φ_E by means of a unitary evolution U_{AE}.

Another useful representation is given by the Kraus decomposition, stated as a theorem in [67] which allows to represent the CPTP map $\mathcal{E}$ as an operator sum

$$\mathcal{E}(\rho_A) = \sum_j K_j\rho_A K_j^\dagger \tag{1.62}$$

where the set $\{K_j\}$ is given by operators on $\mathcal{H}_A$ satisfying the condition $\sum_j K_j^\dagger K_j = \mathbb{I}_A$. The choice of operators K_j is not unique, in fact if we introduce the new set of operators $\widetilde{K}_l$ satisfying $K_j = \sum_l U_{jl}\widetilde{K}_l$ with unitary transformation U_{jl} then we can give the equivalent decomposition

$$\mathcal{E}(\rho_A) = \sum_j \widetilde{K}_j \rho_A \widetilde{K}_j^\dagger \ . \tag{1.63}$$

In association with the Stinespring dilation we have the notion of *complementary* channel of $\mathcal{E}$. This is a CPTP map $\widetilde{\mathcal{E}} : \mathcal{D}(\mathcal{H}_A) \mapsto \mathcal{D}(\mathcal{H}_E)$ which is defined through the following transformation

$$\widetilde{\mathcal{E}}(\rho_A) = \mathrm{Tr}_A \left[U_{AE}(\rho_A \otimes |\varphi\rangle_E\langle\varphi|) U_{AE}^\dagger \right] \ . \tag{1.64}$$

The purity of $|\varphi\rangle_E\langle\varphi|$ guarantees the uniqueness of the complementary channel $\widetilde{\mathcal{E}}$ up to an isometric transformation on the environment E [68, 69]. We are now able to introduce another fundamental property of quantum channels. In fact, it can happen that the two outputs $\mathcal{E}(\rho_A)$ and $\widetilde{\mathcal{E}}(\rho_A)$ are connected by CPTP maps (see Fig. 1.1) and in this case we say that the quantum channel is *degradable* or *antidegradable*. A quantum channel is called degradable [70] if there exist a CPTP map $\mathbf{D}$ such that the environmental output $\widetilde{\mathcal{E}}(\rho_A)$ can be retrieved from the system output $\mathcal{E}$, namely we can write $\widetilde{\mathcal{E}} = \mathbf{D} \circ \mathcal{E}$. Viceversa a quantum channel is antidegradable [68] if we can identify a CPTP map $\mathbf{A}$ such that $\mathcal{E} = \mathbf{A} \circ \widetilde{\mathcal{E}}$.

1.3 Gaussian channels and canonical forms

A bosonic Gaussian channel is a channel that can be expressed as in Eq. (1.61), where U_{AE} is now a Gaussian unitary and ϕ_E a Gaussian state. Such a channel is described by a CPTP map $\mathcal{G}$ which preserves the Gaussian character of the states in input. Let us consider an arbitrary multi-mode Gaussian state $\hat{\rho}(\bar{\mathbf{x}}, \mathbf{V})$. Under the action of a Gaussian channel, the characteristic funtion transforms according to [71]

$$\mathcal{G}\chi(\boldsymbol{\xi}) \mapsto \chi(\mathbf{T}\boldsymbol{\xi}) \exp\left(-\frac{1}{2}\boldsymbol{\xi}^T \mathbf{N}\boldsymbol{\xi} + i\mathbf{d}^T\boldsymbol{\xi}\right) \tag{1.65}$$

where $\mathbf{d} \in \mathbb{R}^{2N}$ is a displacement, while $\mathbf{T}$ and $\mathbf{N} = \mathbf{N}^T$ are $2N \times 2N$ real matrices which must satisfy the following inequality

$$\mathbf{N} + i\boldsymbol{\Omega} - i\mathbf{T}\boldsymbol{\Omega}\mathbf{T}^T \geq 0 \ , \tag{1.66}$$

directly coming from the requirement of complete positivity of the map $\mathcal{G}$. In terms of the first two statistical moments the transformation given in Eq. (1.65) can be equivalently written as [62]

$$\bar{\mathbf{x}} \to \mathbf{T}\bar{\mathbf{x}} + \mathbf{d} \ , \ \mathbf{V} \to \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N} \ . \tag{1.67}$$

Note that if we identify $\mathbf{N} = 0$ and $\mathbf{T} = \boldsymbol{S}$ with the symplectic transformation $\boldsymbol{S}$, the Gaussian channel corresponds to a Gaussian unitary $U_{\boldsymbol{S},\mathbf{d}}$.

An arbitrary one-mode Gaussian channel takes in input a single bosonic mode and its action is fully characterized by the transformation in Eq. (1.67) with $\mathbf{d} \in \mathbb{R}^2$ and the 2×2 real matrices $\mathbf{T}$ and $\mathbf{N}$ satisfying the following conditions

$$\mathbf{N} = \mathbf{N}^T \geq 0 \ , \ \det \mathbf{N} \geq (\det \mathbf{T} - 1)^2 \ , \tag{1.68}$$

where the latter is straightforwardly derived from the relation (1.66) specified to a single mode, i.e. $N = 1$. Of fundamental importance is the classification of one-mode Gaussian channel which relies on the decomposition of the mathematical structure of $\mathcal{G}$ in terms of the so-called canonical form. According to Ref. [71] , corresponding to any physical Gaussian channel $\mathcal{G} = \mathcal{G}[\mathbf{T}, \mathbf{N}, \mathbf{d}]$, there exist non-unique Gaussian unitaries W and U such that

$$\mathcal{G}(\rho) = W \left[\mathcal{C}(U \rho U^\dagger) \right] W^\dagger \ . \tag{1.69}$$

Here the CPTP map $\mathcal{C}$ is called *canonical form* and it is a simplified Gaussian channel $\mathcal{C} = \mathcal{C}[\mathbf{d}_c, \mathbf{T}_c, \mathbf{N}_c]$ with $\mathbf{d}_c = 0$ and diagonal matrices $\mathbf{T}_c$ and $\mathbf{N}_c$. The action of the map $\mathcal{C}$ on the characteristic function can be written as

$$\mathcal{C} : \chi(\boldsymbol{\xi}) \mapsto \chi(\mathbf{T}_c \boldsymbol{\xi}) \exp\left(-\frac{1}{2} \boldsymbol{\xi}_c^T \mathbf{N}_c \boldsymbol{\xi} \right) \ . \tag{1.70}$$

There are three quantities which are left invariant under the acion of the Gaussian unitaries, namely $\det \mathbf{T}$, $\mathrm{rank}(\mathbf{T})$, $\mathrm{rank}(\mathbf{N})$. Depending on the values of these quantities we can have six different expression for diagonal matrices $\mathbf{T}_c$ and $\mathbf{N}_c$ and therefore sic different classes of canonical forms $\mathcal{C}[\mathbf{T}_c, \mathbf{N}_c]$ denoted by A_1, A_2, B_1, B_2, C and D. Following Ref. [69] we give in Table 1.1 the classification of the various canonical forms. In the Table we have set $\mathbf{Z} = \mathrm{diag}(1, -1)$, $\mathbf{I}$ the identity matrix and $\mathbf{0}$ the null matrix. $\tau := \det \mathbf{T}$ is the generalized transmissivity, $\bar{n}$ the thermal number of the envirnment and ξ is the additive noise.

$\tau := \det \mathbf{T}$	rank($\mathbf{T}$)	rank($\mathbf{N}$)	class	$\mathbf{T}_c$	$\mathbf{N}_c$
0	0	2	A_1	$\mathbf{0}$	$(2\bar{n}+1)\mathbf{I}$
0	1	2	A_2	$\frac{\mathbf{I}+\mathbf{Z}}{2}$	$(2\bar{n}+1)\mathbf{I}$
1	2	1	B_1	$\mathbf{I}$	$\frac{\mathbf{I}-\mathbf{Z}}{2}$
1	2	$\neq 1$	B_2	$\mathbf{I}$	$\xi\mathbf{I}$
$0<\tau\neq 1$	2	2	C	$\sqrt{\tau}\mathbf{I}$	$\|1-\tau\|(2\bar{n}+1)\mathbf{I}$
$\tau<0$	2	2	D	$\sqrt{-\tau}\mathbf{I}$	$(1-\tau)(2\bar{n}+1)\mathbf{I}$

Table 1.1: Classification of canonical forms

We can also introduce the following symplectic invariant

$$r := \frac{\text{rank}(\mathbf{T})\,\text{rank}(\mathbf{N})}{2} \tag{1.71}$$

which is referred to as the *rank* of the Gaussian channel [11,72]. Then the three invariants $\{\tau, r, \bar{n}\}$ identify a unique canonical form $\mathcal{C} = \mathcal{C}[\tau, r, \bar{n}]$ and in particular the pair $\{\tau, r\}$ completely determine the class of the form. Following this new prescription we can build a refined classification which is given in Table 1.2.

τ	r	class	$\mathbf{T}_c$	$\mathbf{N}_c$	$\mathcal{C}[\tau,r,\bar{n}]$
0	0	A_1	$\mathbf{0}$	$(2\bar{n}+1)\mathbf{I}$	$\mathcal{C}[0,0,\bar{n}]$
0	1	A_2	$\frac{\mathbf{I}+\mathbf{Z}}{2}$	$(2\bar{n}+1)\mathbf{I}$	$\mathcal{C}[0,1,\bar{n}]$
1	1	B_1	$\mathbf{I}$	$\frac{\mathbf{I}-\mathbf{Z}}{2}$	$\mathcal{C}[1,1,0]$
1	2	$B_2(\neq \text{Id})$	$\mathbf{I}$	$\xi\mathbf{I}$	$\mathcal{C}[1,2,\xi]$
1	0	$B_2(= \text{Id})$	$\mathbf{I}$	$\mathbf{0}$	$\mathcal{C}[1,0,0]$
$(0,1)$	2	C(Att)	$\sqrt{\tau}\mathbf{I}$	$(1-\tau)(2\bar{n}+1)\mathbf{I}$	$\mathcal{C}[\tau,2,\bar{n}]$
>1	2	C(Amp)	$\sqrt{\tau}\mathbf{I}$	$(\tau-1)(2\bar{n}+1)\mathbf{I}$	$\mathcal{C}[\tau,2,\bar{n}]$
<0	2	D	$\sqrt{-\tau}\mathbf{Z}$	$(1-\tau)(2\bar{n}+1)\mathbf{I}$	$\mathcal{C}[\tau,2,\bar{n}]$

Table 1.2: Refined classification of canonical forms

The class A_1, B_2 and C, following the common terminology, are known as phase-insensitive since they act symmetrically on the two input quadratures. The canonical forms A_2, B_1 and D (conjugate of the amplifier)are all phase-sensitive. Class A_1 represents forms that are completely depolarizing channels replacing the input states with thermal states. The class B_2 is known as the additive-noise channel which transforms the quadrature as

$\hat{\mathbf{x}} \rightarrow \hat{\mathbf{x}}+\boldsymbol{\xi}$, where $\boldsymbol{\xi}$ is Gaussian noise with covariance matrix given by $\bar{n}\mathbf{I}$. B_2 includes also the identity channel (Id) for $r = 0$ and it is the quantum straightforward generalization of the classical Gaussian channel. The class C involves canonical forms characterized by transmissivities $0 < \tau \neq 1$ and it can be divided into two subclasses. In fact it can describe an *amplifier* for $\tau > 1$. The phase-insensitive amplifier desribes an optical process where the input signals are amplified and thermal noise is added, i.e. the quadratures transform as $\hat{\mathbf{x}} \rightarrow \sqrt{\tau}\hat{\mathbf{x}} + \sqrt{\tau - 1}\hat{\mathbf{x}}_{th}$. On the other hand for $0 < \tau < 1$ the canonical form in the C class is the one describing *attenuators*, i.e. lossy channels. In this case the input signals are attenuated and combined with thermal noise, i.e. we have $\hat{\mathbf{x}} \rightarrow \sqrt{\tau}\hat{\mathbf{x}} + \sqrt{1 - \tau}\hat{\mathbf{x}}_{th}$. These kind of channels are the most important ones since they are the basic model to describe the losses along communication lines such as optical fibers.

1.3.1 Stinespring dilation of a canonical form

Any canonical form $\mathcal{C}[\tau, r, \bar{n}]$, except for the form B_2, can be equivalently expressed by a physical representation involving a unitary interaction between the input single bosonic mode a described by the state ρ_a and a single environmental bosonic mode e described by the mixed state ρ_e. This means that $\mathcal{C}[\tau, r, \bar{n}]$ can be dilated to a canonical unitary $\hat{U}_{ae}$ mixing the input ρ_a with a thermal state $\rho_e(\bar{n})$ with thermal number $\bar{n}$ and covariance matrix $\mathbf{V}_e = (2\bar{n} + 1)\mathbf{I}$, i.e. we can write

$$\mathcal{C} : \ \rho_a \mapsto \mathcal{C}(\rho_a) = \mathrm{Tr}_e \left[\hat{U}_{ae}(\rho_a \otimes \rho_e(\bar{n}))\hat{U}^{\dagger}_{ae}\right] \ , \tag{1.72}$$

where

$$\hat{U}_{ae} \begin{pmatrix} \hat{x}_a \\ \hat{x}_e \end{pmatrix} \hat{U}^{\dagger}_{ae} = \mathbf{M} \begin{pmatrix} \hat{x}_a \\ \hat{x}_e \end{pmatrix} \tag{1.73}$$

with $\mathbf{M}$ symplectic matrix (see Fig. 1.2). By writing $\mathbf{M}$ into blockform

$$\mathbf{M} = \begin{pmatrix} \mathbf{m}_1 & \mathbf{m}_2 \\ \mathbf{m}_3 & \mathbf{m}_4 \end{pmatrix} , \tag{1.74}$$

we have that

$$\hat{x}_a \rightarrow \hat{x}_b := \mathbf{m}_1\hat{x}_a + \mathbf{m}_2\hat{x}_e \ , \tag{1.75}$$

$$\hat{x}_e \rightarrow \hat{x}_{e'} := \mathbf{m}_3\hat{x}_a + \mathbf{m}_4\hat{x}_e \ . \tag{1.76}$$

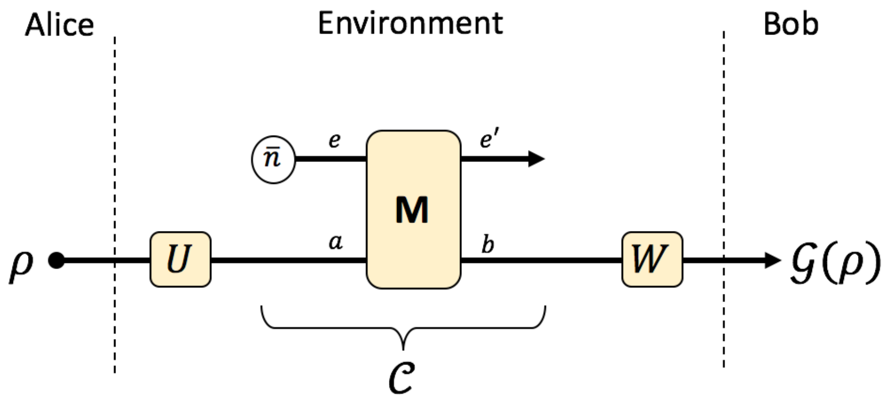

Figure 1.2: Single-mode dilation of a canonical form $\mathcal{C} = \mathcal{C}[\tau, r, \bar{n}]$. The forms of all the classes, apart from B_2, can be represented by a single-mode thermal state interacting with the input via a two-mode symplectic transformation $\mathcal{M}$. This is also the physical representation of a non-additive Gaussian channel up to the input and output unitaries U and W. This is Fig 2 from Ref. [3].

Then, one can easily verify that Eq. (1.72) corresponds to the following input-output transformation of the characteristic function

$$\chi_a(\boldsymbol{\xi}) \to \chi_a(\mathbf{m}_1^T \boldsymbol{\xi}) \exp\left[-\frac{1}{2}(2\bar{n}+1)\left|\mathbf{m}_2^T \boldsymbol{\xi}\right|^2\right] . \tag{1.77}$$

Then, by setting $\mathbf{m}_2^T = \sqrt{\mathbf{N}_c/(2\bar{n}+1)}\mathbf{O}$, with $\mathbf{O}^T = \mathbf{O}^{-1}$ orthogonal matrix, Eq. (1.77) assume the form of Eq. (1.70). The bona fide condition given by Eq. (1.68) is guaranteed by the fact that the matrix $\mathbf{M}$ is symplectic. In fact the symplectic nature of $\mathbf{M}$ implies that $\det \mathbf{m}_1 + \det \mathbf{m}_2 = 1$, so that we have

$$\det \mathbf{N}_c = (2\bar{n}+1)^2 (\det \mathbf{m}_2)^2 \tag{1.78}$$

$$= (2\bar{n}+1)^2 (\det \mathbf{m}_1 - 1)^2 \tag{1.79}$$

$$= (2\bar{n}+1)^2 (\det \mathbf{T}_c - 1)^2 \geq (\det \mathbf{T}_c - 1)^2 . \tag{1.80}$$

The orthogonal matrix $\mathbf{O}$ introduced above is chosen in way such that the symplectic character of $\mathbf{M}$ is preserved. Such a condition restricts also the choice for $\mathbf{m}_3$ and $\mathbf{m}_4$ which are fixed up to local unitaries.

We can now conclude that any canonical form with the exception of the B_2 class (see next section) can be represented by a single-mode physical representation $\{\mathbf{M}(\tau, r), \rho_e(\bar{n})\}$ where the symplectic matrix is completely determined by the class $\{\tau, r\}$ and the environmental state is determined by the thermal number $\bar{n}$. In terms of the second order statistical moment, the input state described by the CM $\mathbf{V}_a$ transforms according to

$$\mathbf{V}_a \to \mathrm{Tr}_e \left[\mathbf{M}(\tau, r) \left(\mathbf{V}_a \oplus (2\bar{n}+1)\mathbf{I}_e\right) \mathbf{M}(\tau, r)^T\right] \tag{1.81}$$

where $\oplus$ is the matrix direct sum and the partial trace Tr_e is interpreted as deletionof rows and columns relating to mode e.

The explicit expression of the symplectic matrices $\mathbf{M}(\tau, r)$ for the different forms are given [69]

$$\mathbf{M}(0<\tau<1,2) = \mathbf{M}(C) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & \sqrt{\tau}\mathbf{I} \end{pmatrix}, \tag{1.82}$$

which describes a beam-splitter,

$$\mathbf{M}(\tau>1,2) = \mathbf{M}(C) = \begin{pmatrix} \sqrt{\tau}\mathbf{I} & \sqrt{\tau-1}\mathbf{Z} \\ \sqrt{\tau-1}\mathbf{Z} & \sqrt{\tau}\mathbf{I} \end{pmatrix}, \tag{1.83}$$

which describes an amplifier,

$$\mathbf{M}(\tau<0,2) = \mathbf{M}(D) = \begin{pmatrix} \sqrt{-\tau}\mathbf{Z} & \sqrt{1-\tau}\mathbf{I} \\ -\sqrt{1-\tau}\mathbf{I} & -\sqrt{-\tau}\mathbf{Z} \end{pmatrix}, \tag{1.84}$$

describing the complementary of an amplifier. Furthermore for the remaining classes we have [69]

$$\mathbf{M}(0,0) = \mathbf{M}(A_1) = \begin{pmatrix} \mathbf{0} & \mathbf{I} \\ \mathbf{I} & \mathbf{0} \end{pmatrix}, \tag{1.85}$$

$$\mathbf{M}(0,1) = \mathbf{M}(A_2) = \begin{pmatrix} \frac{\mathbf{I}+\mathbf{Z}}{2} & \mathbf{I} \\ \mathbf{I} & \frac{\mathbf{Z}-\mathbf{I}}{2} \end{pmatrix}, \tag{1.86}$$

$$\mathbf{M}(1,1) = \mathbf{M}(B_1) = \begin{pmatrix} \mathbf{I} & \frac{\mathbf{I}+\mathbf{Z}}{2} \\ \frac{\mathbf{I}-\mathbf{Z}}{2} & \mathbf{I} \end{pmatrix}. \tag{1.87}$$

1.3.1.1 Asymptotic dilation of the B_2 form

The B_2 canonical form $\mathcal{C}[1, 2, \xi]$ corresponding to the additive-noise Gaussian channel can be dilated into a two-mode environment [69] or alternatively it can be described through an asymptotic single-mode dilation. In fact, consider the dilation of the attenuator channel, which is a beam-splitter $\hat{U}_{ae}^{BS}(\tau)$ with transmissivity τ coupling the input mode a with the environment e initialized in the state $\rho_e(\bar{n})$ with mean photon number $\bar{n}$. In order to achieve this dilation, we can consider a thermal state with $\bar{n}_{\tau,\xi} := \left[\xi(1-\tau)^{-1} - 1\right]/2$ so that we get $\xi = (1-\tau)(2\bar{n}_{\tau,\xi}+1)$. Then, by taking the limit for $\tau \to 1$, i.e. $\bar{n}_{\tau,\xi} \to \infty$ we can represent the B_2 form as

$$\mathcal{C}[1,2,\xi](\rho_a) = \lim_{\tau \to 1} \mathrm{Tr}_e \left\{ \hat{U}_{ae}^{BS}(\tau) \left[\rho_a \otimes \rho_e(\bar{n}_{\tau,\xi})\right] U_{ae}^{BS}(\tau)^{\dagger} \right\} \ . \tag{1.88}$$

In this manner we are able to realize the asymptotic transformations $\bar{\mathbf{x}} \to \bar{\mathbf{x}}$ and $\mathbf{V} \to \mathbf{V} + \boldsymbol{\xi}\mathbf{I}$.

1.4 Quantum Teleportation

We now introduce and characterize quantum teleportation, which is one of the fundamental primitive of quantum information science and a neat example of how entanglement is an essential resource for the perfect accomplishement of the task which would be otherwise impossible. Besides being a powerful theoretical tool, teleportation plays a crucial role also in the development of many potential practical implementation of quantum communication technologies. Continuous variable teleportation in particular is a central tool in optical quantum communications, ranging from realistic implementation of quantum key distribution, e.g. via swapping in untrusted relays [26, 73–75], to quantum networking and quantum Internet [17, 23]. In this research work, teleportation represents one of the essential building block since it is at the core of the development of a particular quantum channel simulation, where, as we will see, it is exploited as a theoretical tool in combination with functionals, monotonic under trace-preserving quantum operations or local operations and classical communication, to provide simplification of fundamental characterizing various quantum informational tasks.

Quantum teleportation exploits entanglement and classical communication in order to transfer an unknown quantum state ρ_C from a sender Alice to a remote receiver without the presence of a physical connection. To do so, Alice and Bob must share, prior to teleportation, a bipartite quantum state ρ_{AB} that is exploited as the resource of quantum correlations. The first version of quantum teleportation was introduced in the seminal paper of Bennet C. H. *et al.* [16] for qubits. More generally [76], in an ideal scenario, for quantum systems with finite dimension d (qudits), in order to perfectly teleport an unknown quantum state ρ_C the two users need to exploit as the resource for quantum correlations a maximally entangled state, also usually referred to as the EPR state, $\Phi_{AB} = |\Phi\rangle\langle\Phi|_{AB}$,

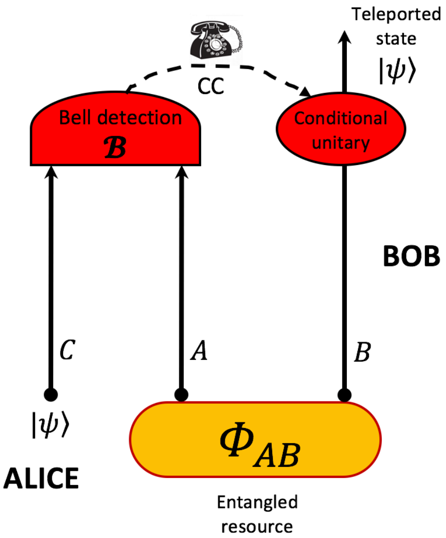

Figure 1.3: Teleportation protocol. Alice wants to teleport to Bob an unknown input state $|\psi\rangle_C$ with the aid of an EPR pair Φ_{AB} shared with Bob. To achieve this task Alice implement a Bell measurement on input system C and the arm A of the EPR state. After that, she communicates through a classical channel (dashed arrow) her outcome to Bob who performs a suitable conditional unitary transformation on his EPR system B in order to reconstruct the input state $|\psi\rangle$.

where

$$|\Phi\rangle_{AB} := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A |k\rangle_B \ . \tag{1.89}$$

For qubits, this state clearly reduces to the usual Bell state pair $(|00\rangle_{AB} + |11\rangle_{AB})/\sqrt{2}$. At the initial stage the total uncorrelated state is expressed by the product $|\phi\rangle_{tot} \equiv |\psi\rangle_C \otimes |\Phi\rangle_{AB}$. The information transfer from Alice to Bob is possible since at Alice's side, the input state of system C is coupled with the EPR's subsystem A through a collective measurement described by a *Bell detection*, here indicated with the symbol $\mathcal{B}$. This measurement corresponds to a projection onto the orthonormal Bell basis $\{|\Phi^k\rangle_{CA}\}_{k=0}^{d^2-1}$ with d^2 possible outcomes k with equal probabilities $p_k = d^{-2}$. The Bell detection can be described as a positive-operator valued measure (POVM) with measurement operators given by

$$M_k = (U_k \otimes \mathcal{I})^\dagger \Phi_{CA} (U_k \otimes \mathcal{I}) \tag{1.90}$$

where $\Phi_{CA} = |\Phi\rangle\langle\Phi|_{CA}$ has the same form of the Bell state in Eq. (1.89) and the operator U_k is one of the d^2 teleportation unitaries. Before proceeding with the description of the teleportation strategy we better characterize the set of unitary operators.

This is a group of d^2 generalized Pauli operators $\mathbb{U}_d = \{U_k\}$ where we assume k is a multi-index $k = (a, b)$ with $a, b \in \mathbb{Z}_d := \{0, \ldots, d-1\}$. Namely we define $U_{ab} := X^a Z^b$ through the non-Hermitian unitary operators X and Z acting on the computational basis $\{|j\rangle\}$ in the following manner

$$X|j\rangle = |j \oplus 1\rangle \ , \ Z|j\rangle = \omega^j |j\rangle \text{ with } \omega := \exp(2i\pi/d) \ , \tag{1.91}$$

and satisfying the generalized commutation relation

$$Z^b X^a = \omega^{ab} X^a Z^b \ . \tag{1.92}$$

The set of finite-dimensional operators $D(j, a, b) := \omega^j X^a Z^b$ with $j, a, b, \in \mathbb{Z}_d$ is identified with the Weyl-Heisenberg group of displacements operators, which for $d = 2$ (qubits) reduces to the group $\mathcal{S}_2 = \{\mathcal{I}, X, XZ, Z\}$ and the group $\pm 1 \times \{\mathcal{I}, X, XZ, Z\}$, where

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{1.93}$$

are the Pauli qubits operators.

It is important to note that, at any dimension (finite or infinite), the teleportation unitaries satisfy

$$U_k U_\ell = e^{i\phi(k,l)} U_f, \tag{1.94}$$

where U_f is another teleportation unitary and $\phi(k, \ell)$ is a phase. In fact, for finite d, let us write k and ℓ as multi-indices, i.e., $k = (a, b)$ and $\ell = (s, t)$. From $U_{ab} = X^a Z^b = \sum_n \omega^{nb} |n \oplus a\rangle\langle n|$, we see that $U_{ab} U_{st} = \omega^{sb} U_{a\oplus s, b\oplus t}$. Then, for infinite d, we know that the displacement operators satisfy $D(u)D(v) = e^{uv^* - u^* v} D(u + v)$, for any two complex amplitudes u and v.

Now, let us represent a teleportation unitary as

$$\mathcal{U}_g(\rho) := U_g \rho U_g^\dagger. \tag{1.95}$$

It is clear that we have $\mathcal{U}_{a,b} \circ \mathcal{U}_{s,t} = \mathcal{U}_{a\oplus s, b\oplus t}$ for DV systems, and $\mathcal{U}_u \circ \mathcal{U}_v = \mathcal{U}_{u+v}$ for CV systems. Therefore $\mathcal{U}_g$ satisfies the group structure

$$\mathcal{U}_g \circ \mathcal{U}_h = \mathcal{U}_{g\cdot h} \quad (g, h \in G), \tag{1.96}$$

where G is a product of two groups of addition modulo d for DVs, while G is the translation group for CVs. Thus, the (multi-)index of the teleportation unitaries can be taken from the abelian group G.

After Alice's Bell detection, for any classical outcome k, Bob's EPR subsystem B is projected onto the state $|\psi\rangle_B$ which is related to ρ_C through $|\psi\rangle_B = U_k|\psi\rangle_C$. At this stage, in order to complete the teleportation, Alice has to communicate to Bob, through a classical channel, the two bits of classical information resulting from her measurement process. By doing so Bob can apply the inverse unitary U_k^{-1} to retreive the teleported state $|\psi\rangle_{out} = |\psi\rangle_C$. In an ideal scenario, by employing an EPR entanglement recource the output state perfectly coincides with the input state on Alice's side, or otherwise stated the teleportation protocol simulates the identity channel. This is no more valid in a more realistic scenario where the entanglement available to the two users is limited and in this case Bob's output state ρ_{out} is "close" to Alice's input ρ_{in} by an amount quantified by the *quantum fidelity* F [10] which is defined as

$$F(\rho_{in}, \rho_{out}) := \overline{\mathrm{Tr}\,[\sqrt{\rho_{in}}\rho_{out}\sqrt{\rho_{in}}]} \in [0,1] \ , \tag{1.97}$$

where the bar stands for averaging over all the possible outcomes of the Bell measurement. Thus if Alice and Bob share an arbitrary bipartite not maximally-entangled state, teleportation simulates a noisy channel from the input C to the output B. Furthermore, it is important to notice that if Alice and Bob make no use of an entanglement resource, they can achieve only imperfect teleportation. This is indeed a classical teleportation strategy which can be achieved by Alice measuring directly the input state and sending her results to Bob who aim at reconstructing the input state simply by means of the classical information received by Alice. This strategy can give a maximum fidelity $F_{cl} = 2/3$, and as a consequence the benchmark $F > F_{cl}$ tells us that we are in the regime of genuine quantum teleportation [77, 78].

1.4.1 Continuous variable teleportation

So far we have considered a discrete variable (DV) scenario for qudits which are described by finite-dimensional Hilbert spaces. We now aim at describing the protocol of quantum teleportation in the framework of continuous variable ($d = +\infty$). The advantages of a CV quantum teleportation stem from an experimental point of view. In fact, the DV teleportation described in the previous section is very hard to be implemented in a laboratory due to the Bell-state discrimination which is difficult to achieve with linear-passive devices such as beam splitters and photodetectors. CV teleportation seems to overcome this difficulty since the CV version of the Bell projection is obtained through passive linear optics and homodyne detections, whose outcomes can be asymptotically discriminated in a perfect manner. Continuous variable teleportation is conceptually analogous to the DV protocol since it is based on the same constitutive elements. The first proposal of quantum teleportation of continuous variable was given by Vaidman in Ref. [18] and then refined in a more realistic scenario by Braunstein and Kimble in Ref. [19]. The protocol *á la* Vaidman (see Fig. 1.4) depicts the ideal situation in which the entanglement shared between Alice and Bob is an ideal EPR state of mode A and B with perfect correlations, i.e. with quadratures satisfying

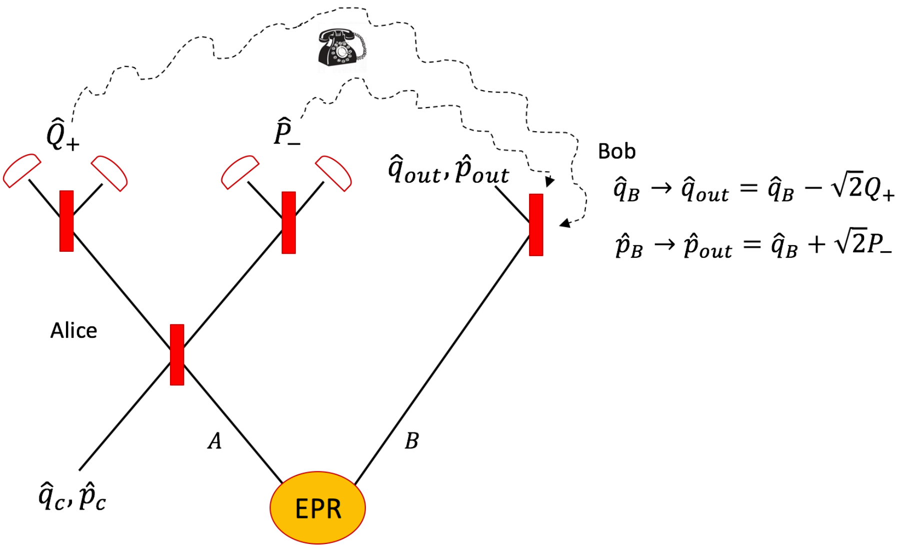
$\hat{Q}_+$
$\hat{P}_-$
$\hat{q}_{out}, \hat{p}_{out}$
Bob
$\hat{q}_B \rightarrow \hat{q}_{out} = \hat{q}_B - \sqrt{2}Q_+$
$\hat{p}_B \rightarrow \hat{p}_{out} = \hat{q}_B + \sqrt{2}P_-$
Alice
A
B
$\hat{q}_c, \hat{p}_c$
EPR

Figure 1.4: Ideal CV quantum teleportation using an ideal asymptotic EPR state shared between Alice and Bob as the resource for entanglement [18]. See the main text for explanation.

$$\hat{q}_A - \hat{q}_B = \hat{p}_A + \hat{p}_B = 0 \ . \tag{1.98}$$

Alice wants to teleport the unknown input state ρ_c with quadratures $\hat{q}_c, \hat{p}_c$. The Bell measurement on Alice's side in the CV setting is composed by two consecutive operations on her local modes. Namely, these are represented by a beam splitter mixing and a homodyne detection. These two steps realize the ideal CV Bell-detection $\mathcal{B}$ which can be seen as a projection on displaced EPR state. In the former, Alice combines the input mode with her half A of the EPR pair through a balanced beam splitter whose action on the quadratures of the two modes is given by the following transformation

$$\hat{Q}_{\pm} = \frac{\hat{q}_A \pm \hat{q}_c}{\sqrt{2}} \quad , \quad \hat{P}_{\pm} = \frac{\hat{p}_A \pm \hat{p}_c}{\sqrt{2}} \ , \tag{1.99}$$

where $\hat{Q}_{\pm}$ and $\hat{P}_{\pm}$ are the quadratures of modes + and − at the output of the beam splitter. After that Alice measures via homodyne detection the two commuting quadratures $\hat{Q}_-$ and $\hat{P}_+$ with respective outcomes Q_- and P_+, so that now her state reads

$$\hat{q}_A = \hat{q}_c + \sqrt{2}Q_- \quad , \quad \hat{p}_A = -\hat{p}_C + \sqrt{2}P_+ \ . \tag{1.100}$$

EPR correlations of Eq. (1.98) are such that Bob's quadrature are instantaneously projected into

$$\hat{q}_B = \hat{q}_c + \sqrt{2}Q_- \quad , \quad \hat{p}_B = \hat{p}_c - \sqrt{2}P_+ \ . \tag{1.101}$$

Alice now classically communicates the classical outcome of her measurement (Q_-, P_+) to Bob by sending the complex variable $\alpha = Q_- + iP_+$. In this way he can apply a suitable conditional displacement $D(-\alpha)$ on his mode B thus retreiving the input state of mode C

$$\hat{q}_B \to \hat{q}_{out} = \hat{q}_B - \sqrt{2}Q_- = \hat{q}_c \tag{1.102}$$

$$\hat{p}_B \to \hat{p}_{out} = \hat{p}_B + \sqrt{2}P_+ = \hat{p}_c \ . \tag{1.103}$$

As one can easily notice the fidelity of the overall teleportation process is $F = 1$. The protocol just described is clearly an ideal protocol since it relies on an energy unbounded EPR state. This idealization is removed by the Braunstein-Kimble (BK) version of CV teleportation, therefore allowing for a realistic and practical implementation of teleportation.

The BK protocol exploits as resource for teleportation a TMSV state Φ^{μ}, defined in Eq. (1.43). As we have already discussed, the ideal EPR state can be defined as the asyptotic state $\Phi_{EPR} := \lim_{\mu} \Phi^{\mu}$ in terms of a diverging sequence of TMSV states. Similarly the CV Bell-detection is energy unbounded. To handle this we may consider a finite-energy version of Alice's measurement which is a *quasi*-projection onto displaced TMSV states. This defines a Gaussian POVM $\mathcal{B}^{\mu}$ with measurement operators given by

$$M_k^{\mu} = \pi^{-1}[D(-k) \otimes \mathcal{I}]\Phi^{\mu}_{C,A}[D(k) \otimes \mathcal{I}] \ . \tag{1.104}$$

At this stage the ideal CV Bell-detection $\mathcal{B}$ is defined through $\mathcal{B} := \lim_{\mu} \mathcal{B}^{\mu}$ and it is clear that we cannot achieve unit fidelity teleportation for any finite values of the squeezing

μ which characterizes both the entanglement resource and the Bell detection. One has perfect teleportation in the limit of infinite μ. In other words, if for finite μ the output state on Bob's side ρ_B is the teleported μ-dependent version ρ_c^μ of the input ρ_c, then we can write the following limit in the trace norm [19, 20]

$$\lim_{\mu \to +\infty} ||\rho_c^\mu - \rho_c|| = 0 \tag{1.105}$$

which is equivalent to

$$\lim_{\mu \to +\infty} F(\rho_c^\mu, \rho_c) = 1 \ . \tag{1.106}$$

In this Thesis, CV teleportation must be always interpreted *a la* Braunstein-Kimble. We always have to consider first a finite energy resources $(\Phi^\mu, \mathcal{B}^\mu)$ leading to the computation of a μ-dependent output and then we perform the limit $\mu \to +\infty$. Furthermore, any funtional of the output of the protocol must be computed on the finite squeezing sequence Φ^μ and then we take the limit for infinite μ.

1.5 Convergence of continuous variable teleportation

Here we complete the discussion about the Braunstein-Kimble CV teleportation by describing the different forms of convergence in different topologies that can be associated with this protocol. These properties will turn out to be fundamental in Chapter 2 for the development of the channel simulation of bosonic channels and to prove that the simulation of Gaussian channels converge uniformly under specific conditions.

1.5.1 Strong convergence

We have seen in the previous section that teleportation has an LOCC structure where the two local operations are represented by the CV Bell detection $\mathcal{B}^\mu$ and the conditional displacement $D(-\alpha)$ respectively on Alice's and Bob's side. Let us denote by $\mathcal{T}$ the overall LOCC associated with the BK protocol. Let us also include an ancillary system in the description so that Alice's state ρ_c that has to be teleported is a part of a bipartite state ρ_{Rc}, with $\rho_c = \mathrm{Tr}_R[\rho_{Rc}]$, where R is an arbitrary multimode system. The action of $\mathcal{T}$ on a TMSV state Φ^μ_{AB} result in a global channel $\mathcal{I}^\mu$ which is point-wise (local) approximation of the identity channel $\mathcal{I}$. This means that, for any energy-bounded input state $\rho_{Rc} \in \mathcal{D}_N$, where

$$\mathcal{D}_N := \{\rho_{Rc} | \, \mathrm{Tr}(\hat{N}\rho_{Rc}) \leq N\} \ , \tag{1.107}$$

with $\hat{N}$ the total number operator for the mode c and the reference modes R, we have the output

$$\rho^{\mu}_{Rc} := \mathcal{I}_R \otimes \mathcal{I}^{\mu}_c(\rho_{Rc}) = \mathcal{I}_R \otimes \mathcal{T}_{cAB}(\rho_{Rc} \otimes \Phi^{\mu}_{AB}) \ . \tag{1.108}$$

Then, as above, we can write the following trace-norm point-wise limit

$$\lim_{\mu} ||\mathcal{I}_R \otimes \mathcal{I}^{\mu}_c(\rho_{Rc}) - \rho_{Rc}|| = 0 \ , \tag{1.109}$$

which directly implies the convergence in the strong topology, i.e.

$$\sup_{\rho_{Rc}} \lim_{\mu} ||\mathcal{I}_R \otimes \mathcal{I}^{\mu}_c(\rho_{Rc}) - \rho_{Rc}|| = 0 \ . \tag{1.110}$$

Let us notice that in Ref. [19], Eq. (4) and (8), there is a convolution between the Wigner function W_{in} of an arbitrary normalized input state and the Gaussian kernel G_{σ}, where σ goes to zero for increasing squeezing r (and ideal homodyne detectors). Taking the limit for large r, the teleportation fidelity goes to 1 as we can also see from Eq. (11) of [19]. This is just a standard delta-like limit that does not really need explicit steps to be shown and fully provides the strong convergence of the BK protocol.

1.5.2 Bounded-uniform convergence

Consider now an energy-constrained state $\rho_{Rc} \in \mathcal{D}_N$. Then we can introduce the energy-constrained diamond distance between two generic bosonic channels $\mathcal{E}$ and $\mathcal{E}'$, defined as [1, Eq. (98)]

$$||\mathcal{E} - \mathcal{E}'||_{\diamond N} := \sup_{\rho_{Rc} \in \mathcal{D}_N} ||\mathcal{I}_R \otimes \mathcal{E}_c(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{E}'_c(\rho_{Rc})|| \tag{1.111}$$

In Ref. [79, 80] the authors give alternate definition of energy-constrained diamond norm. Now due to the point-wise limit in Eq. (1.109) and the fact that the set $\mathcal{D}_N$ is compact we can easily conclude that for any finite value of the energy N

$$\lim_{\mu \to +\infty} ||\mathcal{I}^{\mu} - \mathcal{I}||_{\diamond N} = 0 \ . \tag{1.112}$$

Thus, from Eq. (1.112), we see that the BK teleportation converges to the identity channel in the bounded-uniform topology.

1.5.3 Non-uniform convergence

The BK protocol does not uniformly converge to the identity channel. In fact, if we remove the energy constraint in Eq. (1.112) we get

$$\lim_{\mu \to +\infty} ||\mathcal{I}^{\mu} - \mathcal{I}||_{\diamond} = 2 \ , \tag{1.113}$$

where

$$||\mathcal{E}-\mathcal{E}'||_{\diamond}=\lim_{N\to\infty}||\mathcal{E}-\mathcal{E}'||_{\diamond N} \tag{1.114}$$

$$=\sup_{\rho_{Rc}}||\mathcal{I}_R\otimes\mathcal{E}_c(\rho_{Rc})-\mathcal{I}_R\otimes\mathcal{E}'_c(\rho_{Rc})|| \tag{1.115}$$

is the standard diamond distance between two arbitrary bosonic channels [3]. In order to prove Eq. (1.113) we first notice that when applied to an energy-constrained quantum state, the μ-approximated identity channel $\mathcal{I}^{\mu}$ is locally equivalent to an additive-noise Gaussian channel, i.e. in the notation of Table 1.2 the form B_2, with added noise equal to $\xi=2(\mu-\sqrt{\mu^2-1})$ (see for example Ref. [81]). Now let us consider as the input of the teleportation process a TMSV state $\Phi^{\widetilde{\mu}}_{Rc}$ with CM $V^{\widetilde{\mu}}$ of the form as in Eq. (1.43). Then it is straightforward to compute the CM of the state $\rho^{\mu,\widetilde{\mu}}_{Rc}:=\mathcal{I}_R\otimes\mathcal{I}_{C^{\mu}}(\Phi^{\widetilde{\mu}}_{Rc})$, and we get

$$V^{\mu,\widetilde{\mu}}=\begin{pmatrix}\widetilde{\mu}\mathbf{I} & \sqrt{\widetilde{\mu}^2-1}\mathbf{Z}\\ \sqrt{\widetilde{\mu}^2-1}\mathbf{Z} & (\widetilde{\mu}+\xi)\mathbf{I}\end{pmatrix}. \tag{1.116}$$

By employing the formula for the quantum fidelity between arbitrary Gaussian states given in Ref. [82] we obtain the following expression

$$F\left(\rho^{\mu,\widetilde{\mu}}_{Rc},\Phi^{\widetilde{\mu}}_{Rc}\right)=\left\{1-4\widetilde{\mu}\left[\sqrt{4\mu^2-1}+\widetilde{\mu}-2\mu(1+4\mu\widetilde{\mu}-2\widetilde{\mu}\sqrt{4\mu^2-1})\right]\right\}^{-1/4}. \tag{1.117}$$

Note that for any finite μ, the above fidelity has the expansion $F\left(\rho^{\mu,\widetilde{\mu}}_{Rc},\Phi^{\widetilde{\mu}}_{Rc}\right)\simeq O(\widetilde{\mu}^{-1/2})$ which combined with the Fuchs-van de Graaf inequalities [83]

$$2[1-F(\rho,\sigma)]\leq||\rho-\sigma||\leq 2\sqrt{1-F(\rho,\sigma)^2} \tag{1.118}$$

we obtain for any finite value of the energy μ the expansion $||\rho^{\mu,\widetilde{\mu}}_{Rc}-\Phi^{\widetilde{\mu}}_{Rc}||\geq 2-O(\widetilde{\mu}^{-1/2})$ which directly leads to

$$\lim_{\widetilde{\mu}\to\infty}\left\|\mathcal{I}_R\otimes\mathcal{I}^{\widetilde{\mu}}_c(\Phi^{\widetilde{\mu}}_{Rc})-\Phi^{\widetilde{\mu}}_{Rc}\right\|=2\ , \tag{1.119}$$

and this is equivalent for any μ to Eq. (1.113) so that this complete the proof. In conclusion we observe that the limit in the energy μ of the resource state Φ^{μ}_{AB} and the limit in the energy $\widetilde{\mu}$ of the input $\Phi^{\widetilde{\mu}}_{Rc}$ of the teleportation do not commute. In fact, by performing first the limit in μ in Eq. (1.117) we get $F(\rho^{\mu,\widetilde{\mu}}_{Rc},\Phi^{\widetilde{\mu}}_{Rc})\simeq O(\mu^{-1})$. Due to this non-commutation between the two different limits we, i.e.

$$\lim_{\mu\to\infty}\left[\lim_{\widetilde{\mu}\to\infty}F\left(\rho^{\mu,\widetilde{\mu}}_{Rc},\Phi^{\widetilde{\mu}}_{Rc}\right)\right]\neq\lim_{\widetilde{\mu}\to\infty}\left[\lim_{\mu\to\infty}F\left(\rho^{\mu,\widetilde{\mu}}_{RC},\Phi^{\widetilde{\mu}}_{Rc}\right)\right]\ , \tag{1.120}$$

the strong convergence of Eq. (1.110) and the uniform non-convergence of Eq. (1.113) do not coincide. This also implies that the following joint limits

$$\lim_{\mu,\widetilde{\mu}} F\left(\rho_{Rc}^{\mu,\widetilde{\mu}}, \Phi_{Rc}^{\widetilde{\mu}}\right) \quad , \quad \limsup_{\mu,\widetilde{\mu}} F\left(\rho_{Rc}^{\mu,\widetilde{\mu}}, \Phi_{Rc}^{\widetilde{\mu}}\right) \tag{1.121}$$

are not defined.

Chapter 2

Channel simulation and bounds for quantum and private communications

One of the crucial contribution of this Thesis is undoubtely represented by the development of the simulation of quantum channel through local operation and classical communication (LOCC) with a particular focus on quantum teleportation. Precursory ideas of quantum channel simulation by means of teleportation can be found in [37, 84] where it has been developed for Pauli channels and then later in [39,85] for other classes of channels in finite dimension. Another type of simulation [86] is the deterministic version of a programmable quantum gate array [38], and it was introduced for discrete variable channels and based on joint quantum operations. For this reason it cannot be employed in a quantum communication scenario which is characterized by a LOCC structure.

Here we extend the teleportation simulation of quantum channels to continuous variable systems and we design the most general channel simulation in a quantum communication setting e.g. able to simulate the amplitude damping channel, impossible to simulate with previous approaches. This simulation will be based on completely arbitrary LOCCs and may involve systems in either finite or infinite dimension. We then show the fundamental role of our simulation method in the derivation of tight upper bounds on the maximum achievable rates for quantum communication protocols implemented over quantum channels.

The ideal performances of quantum protocols in a point-to-point scenario are inevitably affected by the interactions between the quantum information carriers and the external environment. These interactions are at the core of decoherence phenomena that may rapidly degrade the quantum features of the system involved. To surpass this limitation one may resort to the implementation of quantum repeaters. An open problem is then to determine the ultimate point-to-point limits that we can reach without the use of these devices in order to have also a better understanding of the actual benchmarks that quantum repeaters need to surpass in order to be considered beneficial.

This chapter investigates this basic problem and establishes the optimal rates of repeaterless quantum communications in the most relevant settings. Here we consider two remote parties connected by a quantum channel, who may exploit unlimited two-way classical communication (CC) and adaptive local operations (LOs), briefly called adaptive LOCCs. In this general scenario, we determine the maximum achievable rates for transmitting quantum information (two-way quantum capacity Q_2), distributing entanglement (two-way entanglement distribution capacity D_2) and generating secret keys (secret key capacity K), through the most fundamental quantum channels. The two-way assisted capacities are benchmarks for quantum repeaters because they are derived by removing any restriction from the point-to-point protocols between the remote parties, who may perform the most general strategies allowed by quantum mechanics in the absence of pre-shared entanglement. Clearly these ultimate limits cannot be achieved by imposing restrictions on the number of channel uses or enforcing energy constraints. To achieve our results we suitably combine the relative entropy of entanglement (REE) [36, 87, 88] with teleportation in a novel reduction method which completely simplifies quantum protocols based on adaptive LOCCs. The first step is to show that two-way capacities cannot exceed a bound based on the REE. The second step is the application of a technique, dubbed “teleportation stretching”, which is valid at any dimension. This allows us to reduce any adaptive protocol to a block form, so that the REE bound becomes a single-letter quantity. In this way, we upperbound the two-way capacities of bosonic Gaussian channels [11], Pauli channels, erasure channels and amplitude damping channels [10]. Before our results, only the Q_2 of the erasure channel was known [89]. It took about 20 years to find the other two-way capacities, which should give an idea of the novelty of our reduction method. All these results and methods have been established in [1].

2.1 Adaptive quantum protocols and two-way quantum capacities

We start by describing the most general adaptive protocol for quantum or private communication over an arbitrary quantum channel $\mathcal{E}$. Such adaptive protocols are the most general strategies we need to consider in order to explore the ultimate performances of quantum channels for quantum and private communications. These strategies are characterized by subsequent transmissions of quantum systems through $\mathcal{E}$, intervealed by local operations with the assistance of classical communication which is two-way, i.e. forward and feedback, and by means of which the involved parties may interactively update their quantum systems in real time.

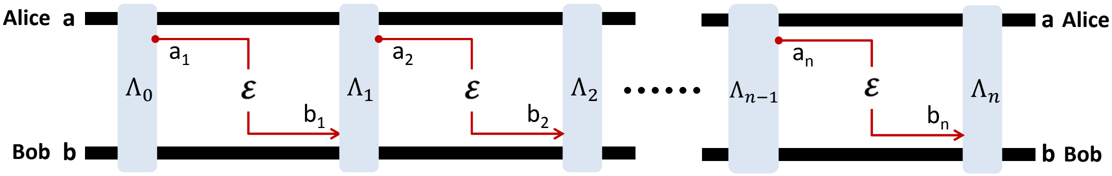

Figure 2.1: General adaptive quantum protocol assisted by local operations and feedback classical communication (LOCC). Each transmission $a_i \to b_i$ takes part between two rounds of LOCC Λ_{i-1} and Λ_i. After n transmissions, we end up with a sequence of adaptive LOCCs $\mathcal{P} = \{\Lambda_0, \dots, \Lambda_n\}$ characterizing the protocol. The corresponding output is represented by the state $\rho^n_{\mathbf{ab}}$ for Alice and Bob. This is adapted from Fig. 1 in Ref. [1].

Let us consider two parties Alice and Bob, which are connected by an arbitrary quantum memoryless channel (see Sec. 1.2) that is described by a completely positive trace-preserving (CPTP) map $\mathcal{E}$. Alice and Bob want to implement the most general adaptive protocol for private and quantum communication tasks over the channel $\mathcal{E}$. At the very initial stage the two users own two local register $\mathbf{a} = \{a_1, a_2, \cdots, a_n\}$ and $\mathbf{b} = \{b_1, b_2, \cdots, b_n\}$ consisting in two countable sets of quantum systems a_i and b_i.

The main steps of an adaptive protocol can be summed up as follows and the reader may refer to Fig. 2.1 for a schematic representation

- Alice and Bob start with the preparation of the initial state $\rho^0_{\mathbf{ab}}$, by means of an adaptive LOCC Λ_0 which is applied to their register $\mathbf{a}$ and $\mathbf{b}$.

- Alice selects a quantum system $a_1 \in \mathbf{a}$ and sends it through the channel $\mathcal{E}$. This procedure generates on Bob's side, the output system b_1 which is then included in the local register, i.e. $b_1\mathbf{b} \to \mathbf{b}$. At this stage, the second LOCC Λ_1 is performed on the two local register producing the output

$$\rho^1_{\mathbf{ab}} = \Lambda_1(\rho^0_{\mathbf{ab}}) \tag{2.1}$$

- The second transmission $\mathbf{a} \ni a_2 \overset{\mathcal{E}}{\to} b_2$ then takes place, followed by another adaptive LOCC Λ_2. This procedure is now iterated for a number n of uses of the channel giving rise to a sequence $\mathcal{P} := \{\Lambda_0 \dots \Lambda_n\}$ of adaptive local operations and classical communications which provides the output $\rho^n_{\mathbf{ab}}$ and characterizes the protocol.

Suppose now that the aim of the adaptive protocol implemented by Alice and Bob is to distribute entanglement, i.e. the parties aim at distributing ebits (units of entanglement). Let us introduce the family of maximally entangled states $\{\phi_n\}_{n\in\mathbb{N}}$ parametrized by the number of channel uses n

$$\phi_n := \frac{1}{\sqrt{d_n}} \sum_{i=0}^{d_n-1} |i\rangle_A |i\rangle_B \ . \tag{2.2}$$

Then we say that the adaptive protocol outlined above distributes entanglement at a rate equal to R_n, if the output $\rho^n_{\mathbf{ab}}$ is ϵ-close to a target state ϕ_n having a number of ebits equal to $nR_n = \log_2 d_n$. In other words if we can write $\|\rho^n_{\mathbf{ab}} - \phi_n\| \leq \epsilon$ in trace norm with $\epsilon \to 0$. The two-way entanglement distribution capacity $D_2(\mathcal{E})$ of the quantum channel $\mathcal{E}$ is then defined by taking the limit of R_n for large number of transmissions n and optimizing over all the possible adaptive protocols $\mathcal{P}$ (see Ref. [34] for a similar approach), namely we have

$$D_2(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{n\to\infty} R_n \ . \tag{2.3}$$

This capacity is equal to the two-way quantum capacity $Q_2(\mathcal{E})$, i.e. the maximum achievable rate for transmitting quantum information, i.e. qubits, and this is true since an ebit can teleport a qubit and viceversa with a qubit is possible distribute an ebit. If the aim of the protocol is to implement Quantum Key Distribution (QKD), then ϕ_n is a private state [90, 91] (see next section) and the generic two-way quantum capacity is the secret key capacity $K(\mathcal{E})$ which is equal to the private capacity $P_2(\mathcal{E})$ (capacity for the private transmission of classical bits). Since a maximally entangled state is a specific type of private state, entanglement distillation is a specific version of key distillation, thus we can write the following relations between all the different capacities

$$Q_2 = D_2 \leq P_2 = K \ . \tag{2.4}$$

In the following discussions we collectively use the symbol $\mathcal{C}(\mathcal{E})$ to refer to these different two-way assisted quantum capacities.

2.1.1 Private state and size of the shield system

We now want to better characterize the structure of a private state and to do so we introduce the notion of the shield system which plays a central role in its definition. Let us consider two local registers **a** and **b** for Alice and Bob, decomposed as $\mathbf{a} = AA'$ and $\mathbf{b} = BB'$ respectively. Here A and B are the local key systems each with dimension equal to d_K, whereas A' and B' together provide the so-called *shield system*, whose dimension is indicated with d_S and can in principle be arbitrary (it could be infinite for bosonic systems). The total dimension d of of the registers is therefore $d = d_K^2 d_S$. A generic private state is a state with the following structure

$$\phi_{ABA'B'} = U(\Phi_{AB} \otimes \chi_{A'B'})U^\dagger \ , \tag{2.5}$$

where the maximally entangled state Φ_{AB} is given by

$$\Phi_{AB} = |\Phi\rangle_{AB}\langle\Phi| \quad \text{with} \quad |\Phi\rangle_{AB} = 1/\sqrt{d_K} \sum_{i=0}^{d_K-1} |i\rangle_A |i\rangle_B \ , \tag{2.6}$$

while $\chi_{A'B'}$ is the shielding state protecting the key from an eavesdropper Eve. In Eq. (2.5) the control unitary U referred to as *twisting* unitary takes the form [91]

$$U = \sum_{i,j=0}^{d_K-1} |i\rangle_A\langle i| \otimes |j\rangle_B\langle j| \otimes U_{A'B'}^{ij} \tag{2.7}$$

with arbitrary unitary operators $U_{A'B'}^{ij}$. It is possible to prove [91] that a dilation of a private state into an environment E (owned by Eve) has the form

$$\phi_{ABA'B'E} = d_{\mathrm{K}}^{-1} \sum_{i,j=0}^{d_{\mathrm{K}}-1} |ii\rangle_{AB} \langle jj| \otimes U_{A'B'}^{ii} \chi_{A'B'E} (U_{A'B'}^{jj})^\dagger \ , \tag{2.8}$$

where $\chi_{A'B'} = \mathrm{Tr}_E(\chi_{A'B'E})$. By performing local measurements on the key system AB and tracing out the shield $A'B'$, Alice and Bob share an ideal private state which shares no correlation with the eavesdropper, i.e. it is completely factorized from system E [90]

$$\tau_{ABE} = d_{\mathrm{K}}^{-1} \sum_{i=0}^{d_{\mathrm{K}}-1} |i\rangle_A \langle i| \otimes |i\rangle_B \langle i| \otimes \tau_E, \tag{2.9}$$

with τ_E an arbitrary state for Eve's system. The shared randomness in the final classical systems A and B provides $\log_2 d_K$ secret bits so that the n-use target state ϕ_n of the adaptive protocol described above is such that

$$\log_2 d_K = nR_n \ , \tag{2.10}$$

with the local dimension d_K giving the number of secret bits and it is exponential in the number of transmission n in both DV and CV scenarios. The dimension d_S of the shield system $A'B'$ can in principle be arbitrary. The total dimension of the private state is $d_P = d_K^2 d_S$. In a key distillation protocol, where Alice and Bob start from n shared copies $\rho_{AB}^{\otimes n}$ and apply LOCCs to approximate a private state ϕ_n, the size of the shield d_S grows with the number of classical bits exchanged in their CCs. In fact, Eve may store all these bits in her local register and a private state can be approximated by the parties only if the dimension of Eves register is smaller than the dimension of the shield system. This is implied by Eq. (2.9) as explained in ref. [91, Section III]. The dimension d_S of the shield system $A'B'$, for DV system, is at most exponential in n. In fact there exist the following result originally proven in Ref. [34] and also discussed in Ref. [92]

Lemma 2.1.1 (Shield system's dimension [34, 92]) *The increase in the shield size d_S is at most exponential in the number n of channel uses, i.e. $\log_2 d_S \leq cn$ for some constant c. In particular, this means that for any protocol we can design an approzimate protocol with the same asymptotic rate but keeping the increase of d_S at most exponential.*

We give an idea of the proof stressing the meaningful steps. For a detailed proof of this Lemma see Ref [34] and its re-adapted version of our work in Ref. [1].

Suppose Alice and Bob are running a key generation prtotocol $\mathcal{P}_n$ with a large number of channel uses n and a rate equal to R_n. For any $\epsilon > 0$, there exists a number n_0 such that the truncated protocol has a rate R_{n_0} satisfying $R_{n_0} \geq R_n - \epsilon$. Now Alice and Bob repeat the truncated protocol a number of times $m = n/n_0$, so that they collect m copies of the state $\rho_{\mathbf{ab}}^{n_0}$. By performing one-way key distillation with these copies they achieve an average key rate (per channel use) [34, 92]

$$\widetilde{R}_n \geq (1-8\epsilon)(R_n - \epsilon) - 4\frac{H_2(\epsilon)}{n_0} \ , \tag{2.11}$$

where we have introduced the binary Shannon entropy

$$H_2(x) := -x\log_2 x - (1-x)\log_2(1-x) \ , \tag{2.12}$$

At this stage it is important to note that Alice and Bob can achieve the average rate $\widetilde{R}_n$ by using an amount of one-way classical communication which is linear in the block number $m < n$. In fact, the communication cost (bits per block) associated with the one-way key distillation of Alice and Bob's copies $(\tilde{\rho}^{n_0}_{AB})^{\otimes m}$ is equal to the conditional (Shannon) entropy $S(A|B)$ between the two classical finite-dimensional systems A and B [93]. This overhead is bounded by $\log_2 \dim \mathcal{H}_{A,B} = l_{n_0}$ classical bits per block, so that it scales at most linearly as ml_{n_0}. Therefore, by decreasing ε, we get a sequence of protocols whose classical communication scales linearly in m while their rates approach R according to Eq. (2.11). Correspondingly, the size of the shield grows at most exponentially in m. Thus, for DV systems, this lemma allows to restrict the definition of $\mathcal{C}(E)$ in Eq. (2.3) to adaptive protocols $\mathcal{P}$ for which the dimension of the shield system grows at most exponentially. For CV system this lemma still applies after a suitable truncation of the underlying Hilbert space [1, Supp. Note 3].

2.2 Lower bound at any dimension

In order to assess the various capacities $\mathcal{C}(\mathcal{E})$ defined in Eq. (2.3) and specified in Eq. (2.4) we need to resort to suitable lower and upper bounds that are usually built upon information and entanglement measures. The lower bound is a well established result. In fact, from below, we may use the coherent [94,95] or reverse coherent [32,33] information which are defined through the following specific strategy. Consider a quantum channel $\mathcal{E}$ applied to some input state ρ_A of system A. Let us introduce the purification $|\psi\rangle_{RA}$ of ρ_A by means of an auxiliary system R. We can therefore consider the output $\rho_{RB} = \mathcal{I} \otimes \mathcal{E}(|\psi\rangle_{RA}\langle\psi|)$. By definition, the coherent information is

$$I_{\mathrm{C}}(\mathcal{E}, \rho_A) = I(A\rangle B)_{\rho_{RB}} = S(\rho_B) - S(\rho_{RB}) \ , \tag{2.13}$$

where $\rho_B := \mathrm{Tr}_R(\rho_{RB})$ and $S(\rho) := -\mathrm{Tr}(\rho \log_2 \rho)$ is the von Neumann entropy. Similarly, the reverse coherent information is given by

$$I_{\mathrm{RC}}(\mathcal{E}, \rho_A) = I(A\langle B)_{\rho_{RB}} = S(\rho_R) - S(\rho_{RB}) \ , \tag{2.14}$$

where $\rho_R := \mathrm{Tr}_B(\rho_{RB})$.

When the input state ρ_A is a maximally-mixed state, its purification is a maximally-entangled state Φ_{RA}, so that ρ_{RB} is the Choi matrix of the channel, i.e. $\rho_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi_{RA})$.

We then define the coherent information of the channel as

$$I_{\mathrm{C}}(\mathcal{E}) := I_{\mathrm{C}}\left(\mathcal{E}, \frac{\mathbb{I}}{d}\right) = I(A\rangle B)_{\rho_{\mathcal{E}}} \ . \tag{2.15}$$

Similarly, its reverse coherent information is

$$I_{\mathrm{RC}}(\mathcal{E}) := I_{\mathrm{RC}}\left(\mathcal{E}, \frac{\mathbb{I}}{d}\right) = I(A\langle B)_{\rho_{\mathcal{E}}} \ . \tag{2.16}$$

Note that for unital channels, i.e., channels preserving the identity $\mathcal{E}(I) = I$, we have $I_{\mathrm{C}}(\mathcal{E}) = I_{\mathrm{RC}}(\mathcal{E})$. This is just a consequence of the fact that, the reduced states ρ_A and ρ_R of a maximally entangled state Φ_{RA} is a maximally-mixed state I/d, where d is the dimension of the Hilbert space (including the limit for $d \to +\infty$). If the channel is unital, also the reduced state $\rho_B = \mathcal{E}(\rho_A)$ is maximally-mixed. As a result, $S(\rho_B) = S(\rho_A) = S(\rho_R)$ and we may write $I_{\mathrm{C}}(\mathcal{E}) = I_{\mathrm{RC}}(\mathcal{E}) := I_{(\mathrm{R})\mathrm{C}}(\mathcal{E})$.

In the specific case of discrete-variable systems ($d < +\infty$), we have $S(\rho_R) = \log_2 d$ and therefore

$$I_{(\mathrm{R})\mathrm{C}}(\mathcal{E}) = \log_2 d - S(\rho_{\mathcal{E}}) \ . \tag{2.17}$$

In particular, for unital qubit channels ($d = 2$), one has

$$I_{(\mathrm{R})\mathrm{C}}(\mathcal{E}) = 1 - S(\rho_{\mathcal{E}}) \ . \tag{2.18}$$

The latter two formulas will be exploited to compute the coherent information of discrete-variable channels.

The coherent information is an achievable rate for *forward* one-way entanglement distillation [93]. Similarly, the reverse coherent information is an achievable rate for *backward* one-way entanglement distillation [32] (i.e., assisted by a single and final CC from Bob to Alice). In fact, thanks to the hashing inequality [93], we may write

$$\max\{I_{\mathrm{C}}(\mathcal{E}), I_{\mathrm{RC}}(\mathcal{E})\} = \max\{I(A\rangle B)_{\rho_{\mathcal{E}}}, I(A\langle B)_{\rho_{\mathcal{E}}}\} \leq D_1(\rho_{\mathcal{E}}). \tag{2.19}$$

where $D_1(\rho_{\mathcal{E}})$ is the entanglement which is distillable from the Choi matrix $\rho_{\mathcal{E}}$ of the channel, by means of one-way forward or backward classical communication [93]. In the next section we are going to extend the inequality in Eq. (2.19) to energy-constrained bosonic state. To do so we will exploit the continuity of the (reverse) coherent information in the limit of infinite dimension, moreover we need the following truncation argument in order to connect continuous-variable and discrete-variable states.

Suppose we are given m bosonic modes with Hilbert space $\mathcal{H}^{\otimes m}$ and $\mathcal{D}(\mathcal{H}^{\otimes m})$ the set of density operators. If $\hat{N}_i$ is the number operator of the i-th mode, the total energy operator reads $\hat{H} = \sum_{i=1}^m \hat{N}_i$. We can then define the following compact set of energy-constrained states

$$\mathcal{D}_E(\mathcal{H}^{\otimes m}) := \left\{ \rho \in \mathcal{D}(\mathcal{H}^{\otimes m}) | \operatorname{Tr}(\rho \hat{H}) \leq E \right\} . \tag{2.20}$$

We can always find a finite-dimensional projector P_d (the detailed proof of this statement is in [1, Supp. Note 1]) that projects the state $\rho \in \mathcal{D}(\mathcal{H}^{\otimes m})$ onto the d-dimensional support of the m-mode Hilbert space with probability

$$\operatorname{Tr}(\rho P_d) \geq 1 - \widetilde{\gamma} \ , \quad \widetilde{\gamma} := \frac{E}{\sqrt[m]{d} - 1} \ , \tag{2.21}$$

in this way generating a d-dimensional truncated state $\delta = P_d \rho P_d / \operatorname{Tr}(\rho P_d)$ such that

$$D(\rho, \delta) \leq \sqrt{\widetilde{\gamma}} \ . \tag{2.22}$$

The projector P_d can be constructed in the following way. Consider the degenerate eigenvalues of the operator $\hat{H}$ and sort them in increasing order $h_0 \leq h_1 \leq \cdots \leq h_n \leq \cdots$. Each of these eigenvalues is given by $\sum_{i=1}^m N_i$ where N_i counts the number of photons in the i-th mode. The corresponding eigenstates can be written as $|\tilde{h}_n\rangle = |N_1\rangle \otimes \cdots \otimes |N_m\rangle$, i.e.

$$\begin{aligned} |\tilde{h}_0\rangle &= |0\rangle \otimes |0\rangle \cdots \otimes |0\rangle \ , \quad (h_0 = 0), \\ |\tilde{h}_1\rangle &= |1\rangle \otimes |0\rangle \cdots \otimes |0\rangle \ , \quad (h_1 = 1), \\ |\tilde{h}_2\rangle &= |0\rangle \otimes |1\rangle \cdots \otimes |0\rangle \ , \quad (h_2 = 1), \\ &\vdots \qquad\qquad\qquad\qquad\qquad \vdots \end{aligned} \tag{2.23}$$

If we define the projector associated with the eigenvector $|\tilde{h}_n\rangle$ as $P_n := |\tilde{h}_n\rangle\langle\tilde{h}_n|$, then the d-dimensional truncation projector P_d is given by

$$P_d := \sum_{n=0}^{d-1} P_n \ . \tag{2.24}$$

2.2.1 Hashing inequality in infinite dimension

Let us consider the state ρ_{AB} of two-bosonic modes A and B having $\leq \bar{n}$ mean photons each, we can apply a projector P_d to obtain the d-dimensional truncated state $\delta_{AB} = P_d \rho_{AB} P_d / \operatorname{Tr}(\rho_{AB} P_d)$ such that

$$D(\rho_{AB}, \delta_{AB}) \leq \sqrt{\gamma}, \quad \gamma := \frac{2\bar{n}}{\sqrt{d} - 1} \ , \tag{2.25}$$

According to ref. [96, Lemma 17], the trace-distance condition $D(\rho,\delta) \leq \sqrt{\gamma} < 1/6$ implies that the coherent information $I(A\rangle B) = -S(A|B)$ satisfies

$$|I(A\rangle B)_\rho - I(A\rangle B)_\delta| \leq 16\sqrt{\gamma}\log_2\left[\frac{2e(\bar{n}+1)}{1-\sqrt{\gamma}}\right] + 32H_2(3\sqrt{\gamma}) \ , \tag{2.26}$$

where H_2 has been introduced in Eq. (2.12). For any $\bar{n}$, the limit $d \to +\infty$ implies that $\gamma \to 0$ and therefore

$$|I(A\rangle B)_\rho - I(A\rangle B)_\delta| \to 0 \ . \tag{2.27}$$

The reverse coherent information $I(A\langle B) = -S(B|A)$ satisfies an equivalent limit. Thus for any $\bar{n}$, the coherent and reverse coherent information are continuous in the limit of infinite dimension and the hashing inequality [93] is extended to bosonic systems with constrained energy. This means that $I(A\rangle B)_\rho$ ($I(A\langle B)_\rho$) represents an achievable rate for the distillable entanglement of the energy-bounded bosonic state ρ via forward (backward) CCs.

We can extend all these definitions in order to give a formulation for asymptotic states thus including into the description CV systems for which the maximally entangled state is itself asymptotic (energy-unbounded). In fact, as we already noticed at the end of Sec. 1.4.1, this is realized as $\Phi := \lim_{\mu\to\infty}\Phi^\mu$, i.e. as the infinite energy limit of a sequence of two-mode squeezed vacuum states Φ^μ. The parameter $\mu = \bar{n} + 1/2$ quantifies both the squeezing and the local energy, i.e. the mean total thermal photon number $\bar{n}$ in each mode.

The Choi matrix of a bosonic channel $\mathcal{E}$ is then defined as the following asymptotic state

$$\rho_{\mathcal{E}} := \lim_{\mu\to\infty}\rho^\mu_{\mathcal{E}} \quad , \quad \rho^\mu_{\mathcal{E}} = \mathcal{I}\otimes\mathcal{E}(\Phi^\mu). \tag{2.28}$$

Correspondingly, the computation of the (reverse) coherent information of the channel is performed as a limit, i.e., we have

$$I_{\mathrm{C}}(\mathcal{E}) = I(A\rangle B)_{\rho_{\mathcal{E}}} := \lim_{\mu\to\infty} I(A\rangle B)_{\rho^\mu_{\mathcal{E}}} \ , \tag{2.29}$$

$$I_{\mathrm{RC}}(\mathcal{E}) = I(A\langle B)_{\rho_{\mathcal{E}}} := \lim_{\mu\to\infty} I(A\langle B)_{\rho^\mu_{\mathcal{E}}} \ . \tag{2.30}$$

As we will see afterwards in the technical derivations of Appendix B, for bosonic Gaussian channels the functionals $I(A\rangle B)_{\rho^\mu_{\mathcal{E}}}$ and $I(A\langle B)_{\rho^\mu_{\mathcal{E}}}$ are continuous, monotonic and bounded in μ. Therefore, the previous limits are finite and we can continuously extend the hashing inequality of Eq. (2.19) to the asymptotic Choi matrix $\rho_{\mathcal{E}}$ of a Gaussian channel, for which we may set $D_1(\rho_{\mathcal{E}}) := \lim_{\mu\to\infty} D_1(\rho^{\mu}_{\mathcal{E}})$.

Due to the hashing inequality, the quantities $I_{\mathrm{C}}(\mathcal{E})$ and $I_{\mathrm{RC}}(\mathcal{E})$ are achievable rates for one-way entanglement distillation. Therefore, they also represent achievable rates for key generation, just because an ebit is a particular type of secret bit. In particular, ref. [33] proved that $I_{\mathrm{RC}}(\mathcal{E})$ is an achievable lower bound for quantum key distribution (QKD) through a Gaussian channel without the need of preliminary entanglement distillation. In fact, $I_{\mathrm{RC}}(\mathcal{E})$ can be computed as the asymptotic key rate of a coherent protocol where:

(i) Alice prepares TMSV states $\Phi^{\mu}_{AA'}$ sending A' to Bob;

(ii) Bob heterodynes each output mode B and sends final CCs back to Alice;

(iii) Alice measures all her modes A by means of an optimal coherent detection that reaches the Holevo bound.

The achievable rate of this coherent protocol is given by a generalized Devetak-Winter rate [93] where Alice and Bobs mutual information is replaced by their Holevo bound [33]. Because Eve holds the entire purification of Alice and Bob's Gaussian output state $\rho^{\mu}_{\mathcal{E}}$ and Bob's detections are rank-1 measurements, this rate is equal to the reverse coherent information $R_{\mathrm{DW}} = I(A\langle B)_{\rho^{\mu}_{\mathcal{E}}}$ computed on Alice and Bob's output. Then, by taking the limit of $\mu \to +\infty$, one obtains $K(\mathcal{E}) \geq I_{\mathrm{RC}}(\mathcal{E})$.

2.3 General weak converse upper bound for private communication

We are now ready to establish the fundamental upper bound on the various two-way capacities of Eq. (2.4). In order to build such an upper bound we resort to the definition of the relative entropy of entanglement (REE) suitably extended from quantum states to quantum channel. Let us recall that the REE of a quantum state ρ is defined as [36,87,88]

$$E_R(\rho) := \inf_{\sigma_s} S(\rho||\sigma_s) \tag{2.31}$$

where the infimum is take over the set of all separable states σ_s and $S(\rho||\sigma_s) := \mathrm{Tr}\left[\rho(\log_2\rho - \log_2\sigma_s)\right]$ is the relative entropy [87]. Its regularized version in terms of the REE computed over n copies of ρ is given by

$$E_R^\infty(\rho) := \lim_{n\to\infty} \frac{1}{n} E_R(\rho^{\otimes n}) \leq E_R(\rho) \ . \tag{2.32}$$

Now, if we consider a DV quantum channel with Choi matrix $\rho_{\mathcal{E}} := \mathcal{I} \otimes \mathcal{E}(\Phi)$, where $\mathcal{I}$ is the identity channel and Φ is maximally entangled as in Eq. (1.89), we can define the REE of the channel $\mathcal{E}$ as [1]

$$E_R(\mathcal{E}) := \sup_\rho E_R[\mathcal{I} \otimes \mathcal{E}(\rho)] \geq \mathbf{\Phi}(\mathcal{E}) \ , \tag{2.33}$$

where we have introduced the *entanglement flux* of the channel $\mathcal{E}$ which is in turn given by the REE of the Choi state $\rho_{\mathcal{E}}$

$$\mathbf{\Phi}(\mathcal{E}) := E_R(\rho_{\mathcal{E}}) \ . \tag{2.34}$$

The inequality in Eq. (2.33) is clear. By extending all the previous definition to CV systems, we note that, given two sequences of states σ_1^μ and σ_2^μ such that $\|\sigma_k^\mu - \sigma_k\| \overset{\mu\to\infty}{\longrightarrow} 0$, for $k = 1, 2$, the relative entropy between the two limit states σ_1 and σ_2 satisfies, at any dimension, the lower semi-continuity property [97]

$$S(\sigma_1 \| \sigma_2) \leq \liminf_{\mu\to\infty} S(\sigma_1^\mu \| \sigma_2^\mu) \ . \tag{2.35}$$

Relying on this we can define the REE of an asymptotic state $\sigma := \lim_{\mu\to\infty} \sigma^\mu$ as follows [1]

$$E_{\mathrm{R}}(\sigma) := \inf_{\sigma_s^\mu} \liminf_{\mu\to+\infty} S(\sigma^\mu || \sigma_s^\mu), \tag{2.36}$$

where σ_s^μ is an arbitrary sequence of separable states such that $||\sigma_s^\mu - \sigma_s|| \overset{\mu\to\infty}{\longrightarrow} 0$ for some separable σ_s. A straightforward implication of Eq. (3.26) is that the entanglement flux of Eq. (2.34) can be introduced also for bosonic channels in the following way

$$\mathbf{\Phi}(\mathcal{E}) := \inf_{\sigma_s^\mu} \liminf_{\mu\to+\infty} S(\rho_{\mathcal{E}}^\mu \| \sigma_s^\mu) \ . \tag{2.37}$$

where $\rho_{\mathcal{E}}^\mu$ is the *quasi*-Choi matrix defined in Eq. (2.28).

Now that we have clarified how REE is defined for quantum states and asymptotic states, including Choi matrices, we can provide the following fundamental upper bound on the two-way capacities of an arbitrary quantum channel.

Theorem 2.3.1 (general weak converse [1]) *At any dimension, finite or infinite, the generic two-way capacity of a quantum channel $\mathcal{E}$ is upper bounded by the REE bound*

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}^\bigstar(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{n\to\infty} \frac{E_{\mathrm{R}}(\rho_{\mathbf{ab}}^n)}{n}. \tag{2.38}$$

where $\rho_{\mathbf{ab}^n}$ is the output of an n-use protocol $\mathcal{P}$.

There are three different but equivalent proofs for this theorem. The first one assumes an exponential growth of the shield system in the target private as explained in the previous section. The second proof simultaneously applies to both DV and CV systems, and relies on the physical assumption that the energy of the output state grows at most exponentially in the number n of channel uses. Another proof is completely independent from the shield system. Here we decided to show only the first proof which was the first given in [2] back in 2015 and it is a re-adaptation of the arguments of Refs. [34,92]. For the other two proofs the reader may refer to [1], where they were given for the sake of completeness.

Proof: Let us start by assuming that the output state $\rho^n_{\mathbf{ab}}$ in Alice and Bob's registers has total finite dimension $d_{\mathbf{ab}}$. Given $\rho^n_{\mathbf{ab}}$ and ϕ_n such that $\|\rho^n_{\mathbf{ab}} - \phi_n\| \leq \varepsilon \leq 1/3$, we may write the Fannes-type inequality [98]

$$E_{\mathrm{R}}(\phi_n) \leq E_{\mathrm{R}}(\rho^n_{\mathbf{ab}}) + 2\varepsilon \log_2 d_{\mathbf{ab}} + f(\varepsilon) \ , \tag{2.39}$$

where $f(\varepsilon) := 4\varepsilon - 2\varepsilon \log_2 \varepsilon$. This result is also known as asymptotic continuity of the REE. An alternate version states that $\|\rho^n_{\mathbf{ab}} - \phi_n\| \leq \varepsilon \leq 1/2$ implies [99]

$$E_{\mathrm{R}}(\phi_n) \leq E_{\mathrm{R}}(\rho^n_{\mathbf{ab}}) + 4\varepsilon \log_2 d_{\mathbf{ab}} + 2H_2(\varepsilon) \ , \tag{2.40}$$

where H_2 is the binary Shannon entropy. Note that the total dimension $d_{\mathbf{ab}}$ of the output state may always be considered to be greater than or equal to the dimension d_{P} of the private state. The latter involves two key systems (with total dimension d^2_{K}) and a shield system (with total dimension d_{S}), so that $d_{\mathrm{P}} = d^2_{\mathrm{K}} d_{\mathrm{S}}$. The logarithm of the dimension d_{K} determines the key rate, while the extra dimension d_{S} is needed to shield the key and can be assumed to grow exponentially in n (see Sec. 2.1.1 for full details). According to ref. [90], we may write

$$E_{\mathrm{R}}(\phi_n) \geq K(\phi_n) = \log_2 d_{\mathrm{K}} := nR^{\varepsilon}_n, \tag{2.41}$$

where $K(\phi_n)$ is the distillable key of ϕ_n. Therefore, from Eq. (2.40), we find

$$R^{\varepsilon}_n \leq \frac{E_{\mathrm{R}}(\rho^n_{\mathbf{ab}}) + 4\varepsilon \log_2 d_{\mathbf{ab}} + 2H_2(\varepsilon)}{n} \ . \tag{2.42}$$

For some sufficiently high $\alpha \geq 2$, let us set

$$\log_2 d_{\mathbf{ab}} \leq \alpha n R^{\varepsilon}_n \ . \tag{2.43}$$

Then the previous inequality becomes

$$R_n^\varepsilon \leq \frac{E_{\mathrm{R}}(\rho_{\mathbf{ab}}^n) + 2H_2(\varepsilon)}{n(1-4\varepsilon\alpha)} \ . \tag{2.44}$$

Taking the asymptotic limit first in n and then in $\varepsilon \to 0$, we derive

$$\lim_{n\to\infty} R_n \leq \lim_{n\to\infty} n^{-1} E_{\mathrm{R}}(\rho_{\mathbf{ab}}^n) \ , \tag{2.45}$$

whose optimization over adaptive protocols $\mathcal{P}$ leads to the following weak converse bound for the key generation capacity

$$K(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{n\to\infty} R_n \leq E_{\mathrm{R}}^{\bigstar}(\mathcal{E}) := \sup_{\mathcal{P}} \lim_{n\to\infty} n^{-1} E_{\mathrm{R}}(\rho_{\mathbf{ab}}^n) \ . \tag{2.46}$$

When $\rho_{\mathbf{ab}}^n$ is a CV bosonic state, we may consider an LOCC truncation channel $T^{\otimes}$ which maps the state into a DV state $\tilde{\rho}_{\mathbf{ab}}^n = T^{\otimes}(\rho_{\mathbf{ab}}^n)$ supported in a subspace with cut-off α, so that the effective dimension is $2^{\alpha n R_n^\varepsilon}$ as in Eq. (2.43). The LOCC truncation channel $T^{\otimes}$ can be defined as follows.

Let us consider the local POVM $\Pi_{ij} := \Pi_i^{\mathbf{a}} \otimes \Pi_j^{\mathbf{b}}$ where the two local projections are given by

$$\Pi_0^{\mathbf{a(b)}} = P_d^{\mathbf{a(b)}} \ , \quad \Pi_1^{\mathbf{a(b)}} = I^{\mathbf{a(b)}} - P_d^{\mathbf{a(b)}} \ , \tag{2.47}$$

where P_d has been defined in Eq. (2.24). Therefore, the channel $T^{\otimes}$ is defined in the following manner

$$T^{\otimes}(\rho_{\mathbf{ab}}) := \sum_{i,j\in\{0,1\}} \mathcal{E}_{ij}(\Pi_{ij}\rho_{\mathbf{ab}}\Pi_{ij}^{\dagger}) \ , \tag{2.48}$$

with

$$\mathcal{E}_{ij} = \begin{cases} \mathcal{I}_{\mathbf{a}} \otimes \mathcal{I}_{\mathbf{b}} & \text{for } i=j=0 \\ \mathcal{E}_{\mathbf{a}}^* \otimes \mathcal{E}_{\mathbf{b}}^* & \text{otherwise} \ , \end{cases} \tag{2.49}$$

and the channels $\mathcal{E}_{\mathbf{a(b)}}^*$ are two damping channels giving $m_{\mathbf{a}}$- ($m_{\mathbf{b}}$-)mode vacuum state for any given input. In other words, Alice and Bob apply the projections of Eq. (2.47) and then communicate their outcomes to each other by using a single bit of classical information for each one-way CC. At this stage, if both parties project onto the local d-dimensional support, then they apply an identity channel $\mathcal{I}_{\mathbf{a(b)}}$. On the other hand, if one between Alice and Bob projects outside the local support, they both apply a damping channel $\mathcal{E}^*$ which maps any input state into a fixed output within the support. This output state can always be chosen as the vacuum state.

The CV-to-DV mapping just described is large enough to leave the private state ϕ_n invariant, i.e., $\phi_n = T^{\otimes}(\phi_n)$. Because $\|\tilde{\rho}^n_{\mathbf{ab}} - \phi_n\| \leq \|\rho^n_{\mathbf{ab}} - \phi_n\| \leq \varepsilon$, we can then repeat the previous derivation and write Eq. (2.46) for $\tilde{\rho}^n_{\mathbf{ab}}$. Then, we introduce the upper-bound $E_{\mathrm{R}}(\tilde{\rho}^n_{\mathbf{ab}}) \leq E_{\mathrm{R}}(\rho^n_{\mathbf{ab}})$, which derives from the monotonicity of the REE under trace-preserving LOCCs (such as $T^{\otimes}$). For clarity, this derivation can be broken down into the following steps

$$E_{\mathrm{R}}(\tilde{\rho}^n_{\mathbf{ab}}) \overset{(1)}{=} S(\tilde{\rho}^n_{\mathbf{ab}}||\tilde{\sigma}^{\mathrm{opt}}_s) \overset{(2)}{\leq} S(\tilde{\rho}^n_{\mathbf{ab}}||\sigma'_s) \overset{(3)}{\leq} S(\rho^n_{\mathbf{ab}}||\sigma^{\mathrm{opt}}_s) = E_{\mathrm{R}}(\rho^n_{\mathbf{ab}}) \ , \tag{2.50}$$

where (1) we use the optimal separable state $\tilde{\sigma}^{\mathrm{opt}}_s$ which is the closest to $\tilde{\rho}^n_{\mathbf{ab}}$ in terms of relative entropy; (2) we introduce the non-optimal separable state $\sigma'_s = T^{\otimes}(\sigma^{\mathrm{opt}}_s)$, where σ^{opt}_s is the separable state closest to $\rho^n_{\mathbf{ab}}$ (because $T^{\otimes}$ is a LOCC, it preserves the separability of input states); and (3) we exploit the fact that the relative entropy cannot increase under trace-preserving LOCCs, which holds in arbitrary dimension [88,97]. Thus, we may write Eq. (2.46) where $E_{\mathrm{R}}(\rho^n_{\mathbf{ab}})$ is directly computed on the bosonic state $\rho^n_{\mathbf{ab}}$.■

Having established the upper bound $E^{\bigstar}_{\mathrm{R}}(\mathcal{E})$, we need a strategic methodology to simplify it in order to make it a function of a single letter quantity and thus in principle computable. Such a strategy is given by teleportation stretching which is in turn based on suitable simulation of quantum channels.

2.4 Simulation of quantum channels

In Sec. 1.4 we described the quantum teleportation protocol and we have seen that its structure consists in local operations, Bell detection on Alice's side and Bob's unitary correction, plus classical communication from Alice to Bob. We also noticed that for maximally entangled resource state, the teleported output perfectly correspond to the input. If we perform teleportation over an arbitrary mixed resource state σ of systems A and B, the teleported state on Bob's side will result in the output of a certain quantum channel $\mathcal{E}$ from Alice to Bob, as explained in Fig. 2.2, panel (**a**). More generally any implementation through an arbitrary LOCC $\mathcal{T}$ and a resource state σ simulates the output of a quantum channel, see Fig 2.2, panel (**b**).

Thus at any finite dimension d , we define the channel $\mathcal{E}$ to be "σ-stretchable" if its action on an input state ρ can be written in terms of a trace-preserving LOCC $\mathcal{T}$ as follows [1]

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma) \ . \tag{2.51}$$

Note that for any given quantum channel, we can always find a suitable LOCC $\mathcal{T}$ and a resource state σ that acheive the simulation in Eq. (2.51). For example we can trivially decompose the channel as $\mathcal{E} = \mathcal{I} \otimes \mathcal{E}$ and include the map $\mathcal{E}$ into Alice's LO, so that the we can simulate the identity map $\mathcal{I}$ by means of teleportation over the ideal EPR pair $\sigma := \Phi$. Therefore the problem is to characterize the best resource state for the specific purpose under study. In infinite dimension, the LOCC simulation should involve the limits $\mathcal{T} := \lim_{\mu\to\infty} \mathcal{T}^\mu$ and $\sigma := \lim_{\mu\to\infty} \sigma^\mu$ of sequences of LOCCs $\mathcal{T}^\mu$ and resource states σ^μ. Then, for any finite μ, the simulation $(\mathcal{T}^\mu, \sigma^\mu)$ provides the approximated channel $\mathcal{E}^\mu$ through $\mathcal{E}^\mu(\rho) := \mathcal{T}^\mu(\rho \otimes \sigma^\mu)$ [1] which defines the quantum channel $\mathcal{E}$ as the point-wise limit (more details on the bosonic channel simulation in the next subsection)

$$\mathcal{E}(\rho) = \lim_{\mu\to\infty} \mathcal{E}^\mu(\rho) \ . \tag{2.52}$$

Among all the possible simulations, we need to identify the best resource state that optimizes the functional under study. In our case the best results are achieved when the resource state σ is identified with the Choi matrix of the channel, i.e. $\sigma = \rho_{\mathcal{E}}$ (see Fig 2.2, panel (**c**)). In fact, a simple criterion to characterize a good LOCC simulation for a quantum channel is given by *teleportation covariance.*

Definition 2.4.1 (Tele-covariance [1]) A quantum channel $\mathcal{E}$ is defined to be teleportation covariant if, for any teleportation unitary U, i.e. Pauli unitary in DVs and phase-space displacement in CVs (refer to Sec. 1.4), we may write

$$\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger \tag{2.53}$$

for some other unitary V.

The key property of a teleportation covariant channel is that the input teleportation unitaries can be pushed out of the channel, where they become other correctable unitaries. Because of this property, the transmission of a quantum system through the channel can be simulated by a generalized teleportation protocol over the Choi matrix of the channel. More precisely we can state the following

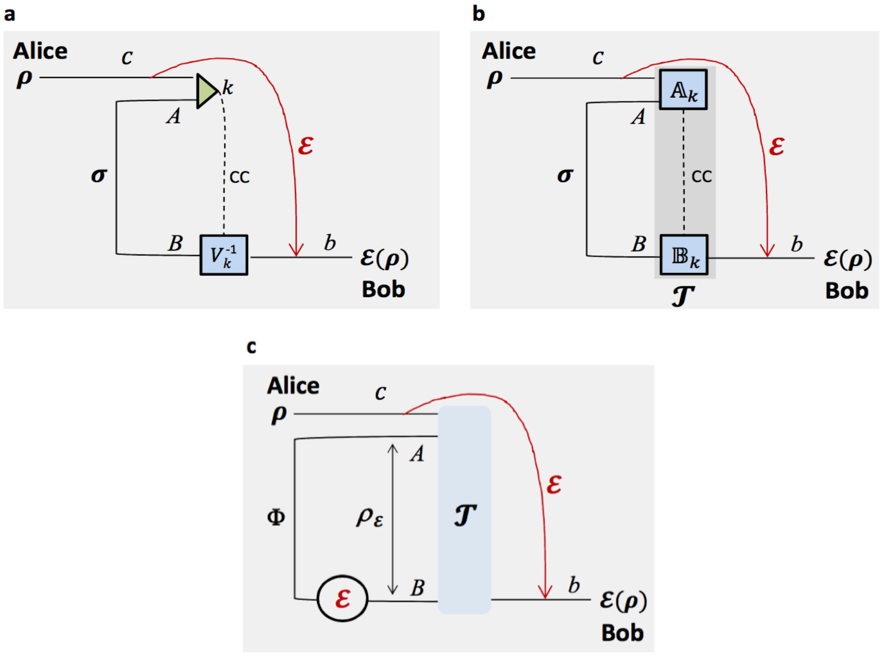

Figure 2.2: Generalization of teleportation-simulation of quantum channels to LOCC-simulation. (**a**) Scheme of generalized teleportation of an input state ρ of a d-dimensional system c by using a resource state σ shared by systems A and B, with respective dimensions d and d' (finite or infinite). Input c and A are subject to a Bell detection (triangle) with random outcome k. This outcome is associated with a projection onto a maximally entangled state up to an associated teleportation unitary U_k which is a Pauli operator for $d < +\infty$ and a phase-displacement for $d = +\infty$ (see Sec 1.4 for the basics of quantum teleportation and the characterization of the teleportation unitaries). The classical outcome k is communicated to Bob, who conditionally applies a correction unitary V_k^{-1} to his system B with output b. In general, V_k does not necessarily belong to the set $\{U_k\}$. On average, this teleportation LOCC defines a teleportation channel $\mathcal{E}$ from a to b. It is clear that this construction also teleports part a of an input state involving ancillary systems. (**b**) We can replace the teleportation LOCC (Bell detection and unitary corrections) with an arbitrary LOCC $\mathcal{T}$ consisting of a quantum operation $\mathbb{A}_k$ on Alice's side applied to systems c and A, the classical communication of the outcome k and then another quantum operation $\mathbb{B}_k$ that Bob applies to his system B. By averaging over the variable k, so that $\mathcal{T}$ is certainly trace-preserving, we achieve the simulation $\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \sigma)$ for any input state ρ. In this case we say that $\mathcal{E}$ is σ-stretchable. The LOs $\mathbb{A}_k$ and $\mathbb{B}_k$ are arbitrary quantum operations that may involve other local ancillas and also have extra labels (due to additional local measurements), in which case $\mathcal{T}$ is assumed to be averaged over all these labels. (**c**) The most important case is when channel $\mathcal{E}$ can be simulated by a trace-preserving LOCC $\mathcal{T}$ applied to its Choi matrix $\rho_\mathcal{E} := \mathcal{I} \otimes \mathcal{E}(\Phi)$, with Φ being an EPR state. In this case, we say that the channel is "Choi-stretchable". These definitions are suitably extended to bosonic channels. This Figure is adapted from [1, Fig. 2.2].

Proposition 2.4.1 (Choi stretchability [1]) A teleportation covariant channel is *Choi-stretchable*, i.e. it can be simulated by using its Choi matrix $\rho_{\mathcal{E}}$. For a DV channel this means

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \rho_{\mathcal{E}}) \tag{2.54}$$

where $\mathcal{T}$ is now the teleportation LOCC. For a CV channel this means

$$\mathcal{E}(\rho) = \lim_{\mu \to \infty} \mathcal{E}^{\mu}(\rho) \ , \quad \mathcal{E}^{\mu}(\rho) = \mathcal{T}^{\mu}(\rho \otimes \rho^{\mu}_{\mathcal{E}}) \tag{2.55}$$

where $\mathcal{T}^{\mu}$ is the LOCC of the BK teleportation protocol and the sequence $\rho^{\mu}_{\mathcal{E}}$ defines the asymptotic Choi matrix for large μ.

In Fig. 2.3 we give a graphical depiction of how teleportation covariance implies Choi stretchability. Teleportation covariant channels belong to a wide class including all Pauli channels and erasure channels in DVs, and bosonic channels in CVs (see Sec. 2.7 for the definitions of these quantum channels).

2.4.1 Simulation of bosonic Gaussian channel

In this section we better describe the technical details of the simulation for bosonic channels and how to handle carefully its different topologies of convergence which are straightforwardly derived from the considerations made in Sec. 1.5 regarding the convergence of the Braunstein-Kimble teleportation protocol. In particular we discuss how the teleportation simulation of bosonic channels uniformly converges only for the specific class of Gaussian channels. The proof of this statement is left to Appendix A to not overload the discussion here.

Strong convergence in the teleportation simulation of bosonic channels

To begin let us consider a teleportation covariant bosonic channel $\mathcal{E}$. This means that for any random phase-space displacement $D(-\alpha)$, we can write the corresponding of Eq. (2.51), i.e.

$$\mathcal{E}[D(-\alpha)\rho D(\alpha)] = V_{\alpha}\mathcal{E}(\rho)V_{\alpha}^{\dagger} \ , \tag{2.56}$$

with V_{α} an output unitary. To correctly formulate the simulation for this type of channel we start from a μ-energy BK protocol $(\mathcal{T}^{\mu}, \Phi^{\mu})$. From Sec. 1.5 we know that this results

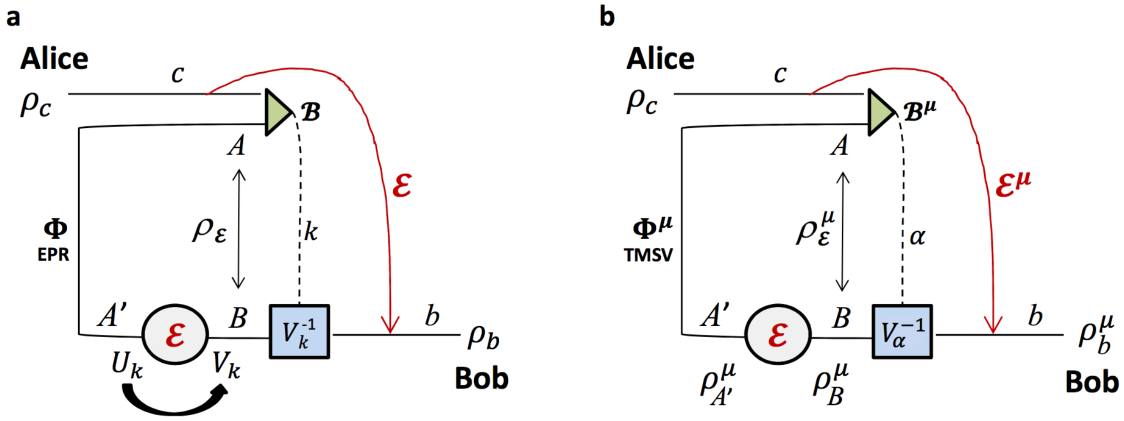

Figure 2.3: Teleportation-covariant channels are Choi-stretchable. (**a**) Consider the teleportation of an input state ρ_c with the EPR state $\Phi_{AA'}$ of systems A and A' as resource for entanglement. The Bell detection $\mathcal{B}$ on systems a and A teleports the input state onto A', up to a random teleportation unitary, i.e., $\rho_{A'} = U_k \rho_c U_k^\dagger$. By invoking the teleportation covariance of $\mathcal{E}$, we can map U_k into an output unitary V_k so that we may write $\rho_B = \mathcal{E}(\rho_{A'}) = \mathcal{E}(U_k\rho_c U_k^\dagger) = V_k \mathcal{E}(\rho_c) V_k^\dagger$. Once Bob receives the CC from Alice with the information about the outcome k, he applies V_k^{-1}, so that $\rho_b = V_k^{-1}\rho_B(V_k^{-1})^\dagger = \mathcal{E}(\rho_c)$. Globally, the process describes the simulation of channel $\mathcal{E}$ by means of a generalized teleportation protocol over the Choi matrix $\rho_{\mathcal{E}}$. (**b**) The procedure is also valid for CV systems. For a bosonic mode c in input , we consider a TMSV state Φ^μ and a corresponding quasi-projection $\mathcal{B}^\mu$ onto displaced TMSV states. At finite energy μ, the teleportation process from c to A' is imperfect with some output $\rho_{A'}^\mu \neq \rho_{A'} = U_\alpha \rho_c U_\alpha^\dagger$. However, as we noticed in Eq. (1.105), for any $\varepsilon > 0$ and input state ρ_c, there is a sufficiently large value of μ such that $||\rho_{A'}^\mu - \rho_{A'}|| \leq \varepsilon$. Consider the transmitted state $\rho_B^\mu = \mathcal{E}(\rho_{A'}^\mu)$. Because the trace distance decreases under channels, we have $||\rho_B^\mu - \rho_B|| \leq ||\rho_{A'}^\mu - \rho_{A'}|| \leq \varepsilon$. After the application of the correction unitary V_α^{-1}, we get the output state ρ_b^μ which satisfies $||\rho_b^\mu - \mathcal{E}(\rho_c)|| \leq \varepsilon$. Taking the asymptotic limit of large μ, we achieve $||\rho_b^\mu - \mathcal{E}(\rho_c)|| \to 0$ for any input ρ_c, therefore achieving the perfect asymptotic simulation of the channel. The asymptotic teleportation-LOCC is therefore $(\mathcal{B}, \rho_{\mathcal{E}}) := \lim_{\mu\to\infty}(\mathcal{B}^\mu, \rho_{\mathcal{E}}^\mu)$ where $\rho_{\mathcal{E}}^\mu := \mathcal{I} \otimes \mathcal{E}(\Phi^\mu)$. The result is trivially extended to the presence of ancillas. This is Fig. 3 from [1].

in a μ-approximated identity channel $\mathcal{I}^{\mu}$. Suppose now that after this channel Bob applies the bosonic channel $\mathcal{E}$. Then we consider the following channel composition

$$\mathcal{E}^{\mu} = \mathcal{E} \circ \mathcal{I}^{\mu} \ . \tag{2.57}$$

Then for any input state ρ_{Rc}, we may write the the output state as

$$\mathcal{I}_R \otimes \mathcal{E}_c^{\mu}(\rho_{Rc}) = \mathcal{I}_R \otimes \mathcal{E}_B \circ \mathcal{T}_{cAB}(\rho_{Rc} \otimes \Phi_{AB}^{\mu}) \ . \tag{2.58}$$

By employing the teleportation covariance of $\mathcal{E}$ we can commute it with the displacement $D(-\alpha)$, up to redefining the teleportation corrections as V_α. By including the unitaries V_α into the LOCC $\mathcal{T}$, the latter changes into a new LOCC $\widetilde{\mathcal{T}}$ and therefore the resource state now reads

$$\rho_{\mathcal{E}}^{\mu} := \mathcal{I}_A \circ \mathcal{E}_B(\Phi_{AB}^{\mu}) \ , \tag{2.59}$$

We can re-write the teleportation simulation of the output as follows

$$\mathcal{I}_R \otimes \mathcal{E}_c^{\mu}(\rho_{Rc}) = \mathcal{I}_R \otimes \widetilde{\mathcal{T}}_{cAB}\left[\rho_{Rc} \otimes \left(\rho_{\mathcal{E}}^{\mu}\right)_{AB}\right] \ . \tag{2.60}$$

Now, by exploiting the composition in Eq. (2.57) and the monotonicity of the trace distance under the action of CPTP maps [10], we get

$$\begin{aligned}\|\mathcal{I}_R \otimes \mathcal{E}_c^{\mu}(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{E}_c(\rho_{Rc})\| &= \|\mathcal{I}_R \otimes \mathcal{E}_c \circ \mathcal{I}_c^{\mu}(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{E}_c \circ \mathcal{I}_c(\rho_{Rc})\| \\ &\leq \|\mathcal{I}_R \otimes \mathcal{I}_c^{\mu}(\rho_{Rc}) - \rho_{Rc}\| \overset{\mu\to\infty}{\to} 0 \ ,\end{aligned} \tag{2.61}$$

where in the last limit we exploited Eq. (1.109). As a consequence, for any bipartite energy-costrained input state ρ_{Rc} we can write the following point-wise limit

$$\lim_{\mu\to\infty} \|\mathcal{I}_R \otimes \mathcal{E}_c^{\mu}(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{E}_c(\rho_{Rc})\| = 0 \ . \tag{2.62}$$

The strong convergence in the simulation of teleportation covariant bosonic channels (not necessarily Gaussian) directly follows from the above limit. In fact, since Eq. (2.62) is valid for any bipartite energy-costrained input state ρ_{Rc}, we may write

$$\sup_{\rho_{Rc}} \lim_{\mu\to\infty} \|\mathcal{I}_R \otimes \mathcal{E}_c^{\mu}(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{E}_c(\rho_{Rc})\| = 0 \tag{2.63}$$

which states that the teleportation simulation $\mathcal{E}^{\mu}$ strongly converges to the corresponding bosonic channel $\mathcal{E}$.

Bounded-uniform convergence in the teleportation simulation of bosonic channels

Consider now an energy constrained input alphabet $\mathcal{D}_N$ as in Eq. (1.107) and the energy-constrained diamond distance defined in Eq. (1.111). Given the teleportation-covariant bosonic channel $\mathcal{E}$ and its teleportation simulation $\mathcal{E}^\mu$ introduced in Eq. (2.60), we define the error of the simulation as

$$\delta(\mu, N) := \|\mathcal{E}^\mu - \mathcal{E}\|_{\diamond N} \ , \tag{2.64}$$

which satisfies

$$\begin{aligned}\delta(\mu, N) &= \sup_{\rho_{Rc} \in \mathcal{D}_N} \|\mathcal{I}_R \otimes \mathcal{E}_c^\mu(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{E}_c(\rho_{Rc})\| \\ &\leq \sup_{\rho_{Rc} \in \mathcal{D}_N} \|\mathcal{I}_R \otimes \mathcal{I}_c^\mu(\rho_{Rc}) - \rho_{Rc}\| \\ &=: \|\mathcal{I}^\mu - \mathcal{I}\|_{\diamond N}\end{aligned} \tag{2.65}$$

where in the inequality we have once again exploited the monotonicity of the trace norm under CPTP maps. Thus, relying on Eq. (1.112), we can conclude that for any finite N we have

$$\lim_{\mu \to \infty} \delta(\mu, N) = 0 \ , \tag{2.66}$$

so that any teleportation simulation $\mathcal{E}^\mu$ of a teleportation covariant bosonic channel $\mathcal{E}$ converges to it in the energy-bounded diamond norm [1, 4].
At this stage we ask whether is possible to remove the energy constrain, i.e. whether we can have uniform convergence ($N \to \infty$). Indeed, as we show in the next, if a bosonic Gaussian channel satisfies a particular condition, it can be simulated by teleportation according to the uniform topology.

Uniform convergence in the teleportation simulation of bosonic Gaussian channels

We have already seen from Eqs. (1.110) and (1.113) that for the identity channel $\mathcal{I}$ the teleportation simulation with the BK protocol strongly but not uniformly converges. This non convergence affects also the teleportation simulation of many Gaussian channels, especially those that can be represented as Gaussian unitaries and those that can be reduced to the B_1 (see Table 1.2) via unitary transformations. Nevertheless, the following theorem [4] establishes the exact condition that a single-mode Gaussian channel must satisfy in order to be simulated by teleportation according to the uniform topology

Theorem 2.4.2 *Consider a single-mode bosonic Gaussian channel* $\mathcal{G}[\mathbf{T}, \mathbf{N}, \mathbf{d}]$ *and its teleportation simulation*

$$\mathcal{G}^{\mu}(\rho) = \tilde{\mathcal{T}}_{cAB}\left[\rho_c \otimes (\rho^{\mu}_{\mathcal{G}})_{AB}\right], \tag{2.67}$$

where $\tilde{\mathcal{T}}_{cAB}$ *is the LOCC of a modified BK protocol implemented over the resource state* $\rho^{\mu}_{\mathcal{G}} := \mathcal{I} \otimes \mathcal{G}(\Phi^{\mu})$*, with* Φ^{μ} *being a TMSV state with energy* μ*. Then, we have uniform convergence*

$$\lim_{\mu \to \infty} \|\mathcal{G}^{\mu} - \mathcal{G}\|_{\diamond} = 0, \tag{2.68}$$

if and only if the noise matrix $\mathbf{N}$ *of the Gaussian channel* $\mathcal{G}$ *has full rank, i.e.,* $\operatorname{rank}(\mathbf{N}) = 2$*.*

The proof of this theorem will be given in Appendix A.

2.5 Teleportation stretching

Having analyzed in full details the teleportation simulation of quantum channels in both DV and CV scenarios, we can now plug it into the structure of the arbitrary adaptive protocol, described in Sec. 2.1, in this way we achieve the protocol-reduction into a simpler block one. This procedure has been dubbed *teleportation stretching* in its original formulation [1]. Although the teleportation stretching technique is similar for DV and CV channels, we leave the two descriptions separated (see next section for bosonic channels) in order to better focus the attention on the subtleties coming from the asymptotic simulation for CV channels.

The main steps of the teleportation stretching are depicted in Fig. 2.4 and they develope as follows

- Panel **(a)** - Consider the ith transmission through a DV channel $\mathcal{E}$, where the input $(i-1)$th register state is given by $\rho^{i-1}_{\mathbf{ab}} := \rho_{\mathbf{a}a_i\mathbf{b}}$. After transmission through $\mathcal{E}$ and the adaptive LOCC Λ_i, the register state is updated to $\rho^{i}_{\mathbf{ab}} = \Lambda_i \circ (\mathcal{I}_{\mathbf{a}} \otimes \mathcal{E} \otimes \mathcal{I}_{\mathbf{b}})(\rho_{\mathbf{a}a_i\mathbf{b}})$.
- Panel **(b)** - We employ the simulation of the channel $\mathcal{E}$ by means of a LOCC $\mathcal{T}$ and a resource state σ according to Eq. (2.51).
- Panel **(c)** - The simulation LOCC $\mathcal{T}$ can be combined with the adaptive LOCC Λ_i into a single "extended" LOCC Δ_i while the distribution of the resource state σ can

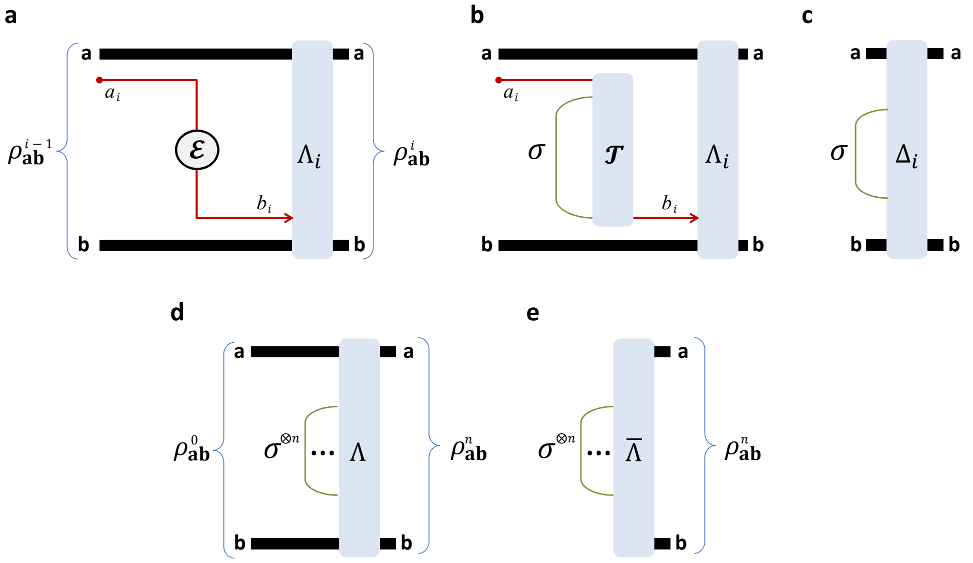

Figure 2.4: Teleportation stretching of an adaptive quantum protocol. See the main text for the explanation. This is Fig. 4 in [1].

be anticipated in time (i.e. it is “stretched”out of the adaptive LOCC), so that we can write $\rho_{\mathbf{ab}}^{i} = \Delta_i(\rho_{\mathbf{ab}}^{i-1} \otimes \sigma)$.

- Panel **(d)** - We iterate the previous steps for all transmissions, so as to stretch n copies $\sigma^{\otimes n}$ and collapse all the extended LOCCs $\Delta_n \circ \ldots \circ \Delta_1$ into a single LOCC Λ. In other words, we may write $\rho_{\mathbf{ab}}^{n} = \Lambda(\rho_{\mathbf{ab}}^{0} \otimes \sigma^{\otimes n})$.

- Panel **(e)** - Finally, the preparation of the separable state $\rho_{\mathbf{ab}}^{0}$ can be included into Λ. We average over all local measurements present in Λ, so that we may write the output state as $\rho_{\mathbf{ab}}^{n} = \bar{\Lambda}(\sigma^{\otimes n})$ for a trace-preserving LOCC $\bar{\Lambda}$. More precisely, for any sequence of outcomes $\mathbf{u}$ with probability $p(\mathbf{u})$, there is conditional LOCC $\Lambda_{\mathbf{u}}$ with output $\rho_{\mathbf{ab}}^{n}(\mathbf{u}) = p(\mathbf{u})^{-1}\Lambda_{\mathbf{u}}(\sigma^{\otimes n})$. Thus, the mean output state $\rho_{\mathbf{ab}}^{n}$ is generated by $\bar{\Lambda} = \sum_{\mathbf{u}} \Lambda_{\mathbf{u}}$.

For discrete variable channels we have thus shown the following fundamental result on the reduction of an arbitrary adaptive protocol for quantum communication.

Lemma 2.5.1 (*Stretching* [1]) *Consider arbitrary n transmissions through a channel $\mathcal{E}$ which is stretchable into a resource state σ. The output of an adaptive protocol can be decomposed into the block form*

$$\rho_{\mathbf{ab}}^{n} = \bar{\Lambda}(\sigma^{\otimes n}) \ , \tag{2.69}$$

for some trace-preserving LOCC $\bar{\Lambda}$. If the channel $\mathcal{E}$ is Choi-stretchable, then we may write

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes n}) \ . \tag{2.70}$$

In the next section we show that this Lemma is valid also in infinite dimension, i.e. it holds also for bosonic channels.

2.5.1 Teleportation stretching with bosonic channels

Here we discuss how an asymptotic bosonic channel simulation $(\mathcal{T},\sigma) = \lim_\mu(\mathcal{T}^\mu,\sigma^\mu)$ leads to an asymptotic version of Lemma 2.5.1. Let us consider the output state $\rho^n_{\mathbf{ab}}$ after n adaptive uses of a bosonic channel $\mathcal{E}$ and the simulated output $\rho^{n,\mu}_{\mathbf{ab}}$, which is obtained by replacing $\mathcal{E}$ with its imperfect version $\mathcal{E}^\mu$. Explicitly, we may write

$$\rho^n_{\mathbf{ab}} = \Lambda_n \circ \mathcal{E} \circ \Lambda_{n-1} \cdots \circ \Lambda_1 \circ \mathcal{E}(\rho^0_{\mathbf{ab}}), \tag{2.71}$$

with its approximate version

$$\rho^{n,\mu}_{\mathbf{ab}} = \Lambda_n \circ \mathcal{E}^\mu \circ \Lambda_{n-1} \cdots \circ \Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}}), \tag{2.72}$$

where it is understood that $\mathcal{E}$ and $\mathcal{E}^\mu$ are applied to system a_i in the i-th transmission, i.e., $\mathcal{E} = \mathcal{I}_{\mathbf{a}} \otimes \mathcal{E}_{a_i} \otimes \mathcal{I}_{\mathbf{b}}$.

Assume that the mean photon number of the total register states $\rho^n_{\mathbf{ab}}$ and $\rho^{n,\mu}_{\mathbf{ab}}$ is bounded by some large but yet finite value $N(n)$. For instance, we may consider a sequence $N(n) = N(0)+nt$, where $N(0)$ is the initial photon contribution and t is the channel contribution, which may be negative for energy-decreasing channels (like the thermal-loss channel) or positive for energy-increasing channels (like the quantum amplifier). We then prove the following inequality [1]

$$\left\|\rho^n_{\mathbf{ab}} - \rho^{n,\mu}_{\mathbf{ab}}\right\| \leq \sum_{i=0}^{n-1} \|\mathcal{E} - \mathcal{E}^\mu\|_{\diamond N(i)} \ . \tag{2.73}$$

by means of a "peeling"argument through which all the LOCCs are peeled out. In fact, for $n = 2$, we may write

$$\begin{aligned}
\|\rho^2_{\mathbf{ab}} - \rho^{2,\mu}_{\mathbf{ab}}\| &= \|\Lambda_2 \circ \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho^0_{\mathbf{ab}}) - \Lambda_2 \circ \mathcal{E}^\mu \circ \Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}})\| \\
&\overset{(1)}{\leq} \|\mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho^0_{\mathbf{ab}}) - \mathcal{E}^\mu \circ \Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}})\| \\
&\overset{(2)}{\leq} \|\mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho^0_{\mathbf{ab}}) - \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}})\| + \|\mathcal{E} \circ \Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}}) - \mathcal{E}^\mu \circ \Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}})\| \\
&\overset{(3)}{\leq} \|\mathcal{E}(\rho^0_{\mathbf{ab}}) - \mathcal{E}^\mu(\rho^0_{\mathbf{ab}})\| + \|\mathcal{E}[\Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}})] - \mathcal{E}^\mu[\Lambda_1 \circ \mathcal{E}^\mu(\rho^0_{\mathbf{ab}})]\| \\
&\overset{(4)}{\leq} \|\mathcal{E} - \mathcal{E}^\mu\|_{\diamond N(0)} + \|\mathcal{E} - \mathcal{E}^\mu\|_{\diamond N(1)} \ , \qquad (2.74)
\end{aligned}$$

where: (1) we use monotonicity under Λ_2; (2) we use the triangle inequality; (3) we use monotonicity with respect to $\mathcal{E} \circ \Lambda_1$; and (4) we use the definition of Eq. (1.111) assuming $a' = a_i$ and the energy bound $N(n)$. Generalization to arbitrary n is just a matter of technicality. By using Eq. (2.66) we may write that, for any bound $N(n)$ and $\varepsilon \geq 0$, there is a sufficiently large μ such that $\|\mathcal{E} - \mathcal{E}^\mu\|_{\diamond N(n)} \leq \varepsilon$, so that Eq. (2.73) becomes

$$\left\|\rho^n_{\mathbf{ab}} - \rho^{n,\mu}_{\mathbf{ab}}\right\| \leq n\varepsilon \ . \qquad (2.75)$$

By applying teleportation stretching we derive $\rho^{n,\mu}_{\mathbf{ab}} = \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})$, where $\bar{\Lambda}_\mu$ includes the original LOCCs Λ_i and the teleportation LOCCs $\mathcal{T}^\mu$. Thus, Eq. (2.75) implies

$$\left\|\rho^n_{\mathbf{ab}} - \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})\right\| \leq n\varepsilon, \qquad (2.76)$$

or, equivalently, $\left\|\rho^n_{\mathbf{ab}} - \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})\right\| \xrightarrow{\mu} 0$. Therefore, given an adaptive protocol with arbitrary register energy, and performed n times through a bosonic channel $\mathcal{E}$ with asymptotic simulation, we may write its output state as the (trace-norm) limit [1]

$$\rho^n_{\mathbf{ab}} = \lim_{\mu\to\infty} \bar{\Lambda}_\mu(\sigma^{\mu\otimes n}). \qquad (2.77)$$

This means that we may formally write the asymptotic stretching $\bar{\Lambda}(\sigma^{\otimes n}) := \lim_{\mu\to\infty} \bar{\Lambda}_\mu(\sigma^{\mu\otimes n})$ for an asymptotic channel simulation $(\mathcal{T}, \sigma) := \lim_{\mu\to\infty}(\mathcal{T}^\mu, \sigma^\mu)$ so that Lemma 2.5.1 holds at any dimension, finite or infinite. To conclude this Section we note that teleportation stretching reduces an adaptive protocol performing an arbitrary task (quantum communication, entanglement distribution or key generation) into an equivalent block protocol, whose output state $\rho^n_{\mathbf{ab}}$ is the same but suitably decomposed as in Eq. (2.69) for any number n of channel uses. In particular, for Choi-stretchable channels, the output is decomposed into a tensor-product of Choi matrices. An essential feature which makes the technique applicable to many contexts is the fact that the adaptive-to-block reduction maintains task and output of the original protocol so that, e.g., adaptive key generation is reduced to block key generation and not entanglement distillation.

2.6 Single letter upper bound

The combination of the general weak upper bound (Theorem 2.3.1 in Sec. 2.3) with the teleportation stretching (Lemma 2.5.1) is the key ingredient that gives the insight of our entire reduction method. In fact, let us compute the REE of the output state $\rho^n_{\mathbf{ab}}$, decomposed as in Eq. (2.69). Using the monotonicity of the REE under trace-preserving LOCCs, we derive

$$E_{\mathrm{R}}(\rho^n_{\mathbf{ab}}) \leq E_{\mathrm{R}}(\sigma^{\otimes n}), \tag{2.78}$$

where the complicated $\bar{\Lambda}$ is fully discarded. Then, by replacing Eq. (2.78) into Eq. (2.38) and by invoking the subadditivity of the REE under tensor product, we can ignore the supremum and the limit in the definition of $E^{\bigstar}_{\mathrm{R}}(\mathcal{E})$ and get the simple single-letter bound

$$E^{\bigstar}_{\mathrm{R}}(\mathcal{E}) \leq E^{\infty}_{\mathrm{R}}(\sigma) \leq E_{\mathrm{R}}(\sigma). \tag{2.79}$$

Thus, we can state the following main result.

Theorem 2.6.1 (one-shot REE bound [1]) *Let us stretch an arbitrary quantum channel $\mathcal{E}$ into some resource state σ, according to Eq. (2.51). Then, we may write*

$$\mathcal{C}(\mathcal{E}) \leq E^{\infty}_{\mathrm{R}}(\sigma) \leq E_{\mathrm{R}}(\sigma). \tag{2.80}$$

Moreover, if $\mathcal{E}$ is Choi-stretchable, we have

$$\mathcal{C}(\mathcal{E}) \leq E^{\infty}_{\mathrm{R}}(\rho_{\mathcal{E}}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E}). \tag{2.81}$$

In particular, for DV channels, we may also write the following simplified version for this Theorem

Proposition 2.6.1 ([1]) *For a Choi-stretchable channel $\mathcal{E}$ in finite dimension, we may write the chain*

$$K(\mathcal{E}) = K(\rho_{\mathcal{E}}) \leq E^{\infty}_{\mathrm{R}}(\rho_{\mathcal{E}}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E}), \tag{2.82}$$

where $K(\rho_{\mathcal{E}})$ is the distillable key of $\rho_{\mathcal{E}}$.

Note that, for bosonic channels, since the Choi matrix $\rho_{\mathcal{E}}$ is energy-unbounded, its distillable key $K(\rho_{\mathcal{E}})$ is not well-defined and we cannot directly write the equality $K(\mathcal{E}) = K(\rho_{\mathcal{E}})$. By contrast, we know how to extend $E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}})$ to bosonic channels and to show $K(\mathcal{E}) \leq E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}})$ at any dimension. This is the more general procedure of Theorem 2.6.1 which first exploits the general REE bound $K(\mathcal{E}) \leq E_{\mathrm{R}}^{\bigstar}(\mathcal{E})$ and then simplifies $E_{\mathrm{R}}^{\bigstar}(\mathcal{E}) \leq E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}})$ by means of teleportation stretching at any dimension.

In order to prove the equality $K(\mathcal{E}) = K(\rho_{\mathcal{E}})$ we first show that $K(\mathcal{E}) \leq K(\rho_{\mathcal{E}})$ and then the opposite inequality. Consider a key-generation protocol described by a sequence $\mathcal{L}$ of adaptive LOCCs (implicitly assumed to be averaged). If the protocol is implemented over a Choi-stretchable channel $\mathcal{E}$ in finite dimension d, its stretching allows us to write the output as $\rho_{\mathbf{ab}}^{n} = \bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right)$ for a trace-preserving LOCC $\bar{\Lambda}$. Since any LOCC-sequence $\mathcal{L}$ is transformed into $\bar{\Lambda}$, any key-generation protocol through $\mathcal{E}$ becomes a key distillation protocol over copies of the Choi matrix $\rho_{\mathcal{E}}$. For large n, this means $K(\mathcal{E}) \leq K(\rho_{\mathcal{E}})$. To derive the opposite inequality, consider Alice sending EPR states through the channel, so that the shared output will be $\rho_{\mathcal{E}}^{\otimes n}$. There exists an optimal LOCC on these states which reaches the distillable key $K(\rho_{\mathcal{E}})$ for large n. This is a specific key-generation protocol over $\mathcal{E}$, so that we may write $K(\rho_{\mathcal{E}}) \leq K(\mathcal{E})$. Thus, for a d-dimensional Choi-stretchable channel, we find

$$K(\mathcal{E}) = K(\rho_{\mathcal{E}}) \leq E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}}), \tag{2.83}$$

where we also exploit the fact that the distillable key of a DV state is bounded by its regularized REE [90]. It is also clear that $E_{\mathrm{R}}^{\infty}(\rho_{\mathcal{E}}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E})$, where the latter equality is demonstrated in the proof of Theorem 2.6.1, which is the following.

Proof: Given the asymptotic stretching of the output state $\rho_{\mathbf{ab}}^{n}$ as in Eq. (2.77), the simplification of the REE bound $E_{\mathrm{R}}(\rho_{\mathbf{ab}}^{n})$ explicitly goes as follows

$$\begin{aligned} E_{\mathrm{R}}(\rho_{\mathbf{ab}}^{n}) &= \inf_{\sigma_s} S(\rho_{\mathbf{ab}}^{n}||\sigma_s) \\ &\overset{(1)}{\leq} \inf_{\sigma_s^{\mu}} S\left[\lim_{\mu\to\infty} \bar{\Lambda}_{\mu}(\sigma^{\mu\otimes n}) \;||\; \lim_{\mu} \sigma_s^{\mu}\right] \\ &\overset{(2)}{\leq} \inf_{\sigma_s^{\mu}} \liminf_{\mu\to+\infty} S\left[\bar{\Lambda}_{\mu}(\sigma^{\mu\otimes n}) \;||\; \sigma_s^{\mu}\right] \\ &\overset{(3)}{\leq} \inf_{\sigma_s^{\mu}} \liminf_{\mu\to+\infty} S\left[\bar{\Lambda}_{\mu}(\sigma^{\mu\otimes n}) \;||\; \bar{\Lambda}_{\mu}(\sigma_s^{\mu})\right] \\ &\overset{(4)}{\leq} \inf_{\sigma_s^{\mu}} \liminf_{\mu\to+\infty} S\left(\sigma^{\mu\otimes n} \;||\; \sigma_s^{\mu}\right) \\ &\overset{(5)}{=} E_{\mathrm{R}}(\sigma^{\otimes n}), \end{aligned} \tag{2.84}$$

where: (1) σ_s^μ is a generic sequence of separable states that converges in trace norm, i.e., such that there is a separable state $\sigma_s := \lim_{\mu\to\infty} \sigma_s^\mu$ so that $\|\sigma_s - \sigma_s^\mu\| \overset{\mu}{\to} 0$; (2) we use the lower semi-continuity of the relative entropy [97]; (3) we use that $\bar{\Lambda}_\mu(\sigma_s^\mu)$ are specific types of converging separable sequences within the set of all such sequences; (4) we use the monotonicity of the relative entropy under trace-preserving LOCCs; and (5) we use the definition of REE for asymptotic states given in Eq. (3.26).

Thus, from Theorem 2.3.1, we may write the following upper bound for the two-way capacity of a bosonic channel

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}^{\bigstar}(\mathcal{E}) \leq \lim_{n\to\infty} n^{-1} E_{\mathrm{R}}(\sigma^{\otimes n}) = E_{\mathrm{R}}^{\infty}(\sigma). \tag{2.85}$$

The supremum over all adaptive protocols which defines $E_{\mathrm{R}}^{\bigstar}(\mathcal{E})$ disappears in the right hand side of Eq. (2.85). The resulting bound applies to both energy-constrained protocols and the limit of energy-unconstrained protocols. The proof of the further condition $E_{\mathrm{R}}^{\infty}(\sigma) \leq E_{\mathrm{R}}(\sigma)$ in Eq. (2.80) comes from the subadditivity of the REE over tensor product states. This subadditivity also holds for a tensor product of asymptotic states; it is proven by restricting the minimization on tensor-product sequences $\sigma_s^{\mu\otimes n}$ in the corresponding definition of the REE. Let us now prove Eq. (2.81). The two inequalities in Eq. (2.81) are simply obtained by using $\sigma = \rho_{\mathcal{E}}$ for a Choi-stretchable channel (where the Choi matrix is intended to be asymptotic for a bosonic channel). Then we show the equality $E_{\mathrm{R}}(\rho_{\mathcal{E}}) = E_{\mathrm{R}}(\mathcal{E})$. By restricting the optimization in $E_{\mathrm{R}}(\mathcal{E})$ to an input EPR state Φ, we get the direct part $E_{\mathrm{R}}(\mathcal{E}) \geq E_{\mathrm{R}}(\rho_{\mathcal{E}})$. For CVs, this means to choose an asymptotic EPR state $\Phi := \lim_{\mu\to\infty} \Phi^\mu$, so that

$$\mathcal{I} \otimes \mathcal{E}(\Phi) := \lim_{\mu\to\infty} \mathcal{I} \otimes \mathcal{E}(\Phi^\mu) = \lim_{\mu\to\infty} \rho_{\mathcal{E}}^\mu := \rho_{\mathcal{E}}, \tag{2.86}$$

and therefore

$$E_{\mathrm{R}}(\mathcal{E}) \geq E_{\mathrm{R}}(\rho_{\mathcal{E}}) := \inf_{\sigma_s^\mu} \liminf_{\mu\to+\infty} S\left(\rho_{\mathcal{E}}^\mu \,||\, \sigma_s^\mu\right). \tag{2.87}$$

For the converse part, consider first DVs. By applying teleportation stretching to a single use of the channel $\mathcal{E}$, we may write $\mathcal{I} \otimes \mathcal{E}(\rho) = \bar{\Lambda}(\rho_{\mathcal{E}})$ for a trace-preserving LOCC $\bar{\Lambda}$. Then, the monotonicity of the REE leads to

$$E_{\mathrm{R}}(\mathcal{E}) = \sup_\rho E_{\mathrm{R}}[\mathcal{I} \otimes \mathcal{E}(\rho)] = \sup_\rho E_{\mathrm{R}}[\bar{\Lambda}(\rho_{\mathcal{E}})] \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}). \tag{2.88}$$

For CVs, we have an asymptotic stretching $\mathcal{I} \otimes \mathcal{E}(\rho) = \lim_{\mu\to\infty} \sigma^{\mu}$ where $\sigma^{\mu} := \bar{\Lambda}_{\mu}(\rho^{\mu}_{\mathcal{E}})$. Therefore, we may write

$$\begin{aligned} E_{\mathrm{R}}[\mathcal{I} \otimes \mathcal{E}(\rho)] &= \inf_{\sigma^{\mu}_{s}} \liminf_{\mu\to+\infty} S(\sigma^{\mu}||\sigma^{\mu}_{s}) \\ &\leq \inf_{\sigma^{\mu}_{s}} \liminf_{\mu\to+\infty} S[\bar{\Lambda}_{\mu}(\rho^{\mu}_{\mathcal{E}})||\bar{\Lambda}_{\mu}(\sigma^{\mu}_{s})] \\ &\leq \inf_{\sigma^{\mu}_{s}} \liminf_{\mu\to+\infty} S(\rho^{\mu}_{\mathcal{E}}||\sigma^{\mu}_{s}) = E_{\mathrm{R}}(\rho_{\mathcal{E}}). \end{aligned} \tag{2.89}$$

Since this is true for any ρ, it also applies to the supremum and, therefore, to the channel's REE $E_{\mathrm{R}}(\mathcal{E})$. ■

We have therefore reached our goal and found single-letter bounds. In particular, note that $E_{\mathrm{R}}(\rho_{\mathcal{E}})$ measures the entanglement distributed by a single EPR state, so that we may call it the "entanglement flux" of the channel $\Phi(\mathcal{E}) := E_{\mathrm{R}}(\rho_{\mathcal{E}})$. Remarkably, there is a sub-class of Choi-stretchable channels for which $E_{\mathrm{R}}(\rho_{\mathcal{E}})$ coincides with the lower bound $D_1(\rho_{\mathcal{E}})$ in Eq. (2.19). We call these "distillable channels". We establish all their two-way capacities as $\mathcal{C}(\mathcal{E}) = E_{\mathrm{R}}(\rho_{\mathcal{E}})$. They include lossy channels, quantum-limited amplifiers, dephasing and erasure channels. See Fig. 2.5.

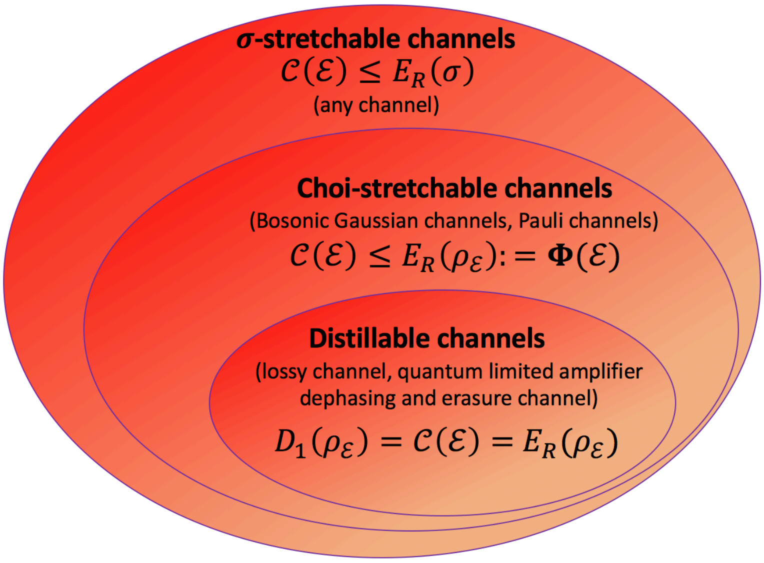
σ-stretchable channels
$\mathcal{C}(\mathcal{E}) \leq E_R(\sigma)$
(any channel)
Choi-stretchable channels
(Bosonic Gaussian channels, Pauli channels)
$\mathcal{C}(\mathcal{E}) \leq E_R(\rho_{\mathcal{E}}) := \mathbf{\Phi}(\mathcal{E})$
Distillable channels
(lossy channel, quantum limited amplifier
dephasing and erasure channel)
$D_1(\rho_{\mathcal{E}}) = \mathcal{C}(\mathcal{E}) = E_R(\rho_{\mathcal{E}})$

Figure 2.5: Classification of σ-stretchable, Choi-stretchable and distillable channels in DVs and CVs. This is adapted from [1, Fig. 5].

2.7 Ultimate limits in quantum channel communications

2.7.1 Discrete variable channels

We now study the ultimate rates for quantum communication, entanglement distribution and secret key generation through qubit channels, with generalizations to any finite dimension. For any DV channel $\mathcal{E}$ from dimension d_A to dimension d_B, we may write the dimensionality bound $\mathcal{C}(\mathcal{E}) \leq \min\{\log_2 d_A, \log_2 d_B\}$. This is because we may always decompose the channel into $\mathcal{I} \circ \mathcal{E}$ (or $\mathcal{E} \circ \mathcal{I}$), include $\mathcal{E}$ in Alice's (or Bob's) LOs and stretch the identity map into a Bell state with dimension d_B (or d_A).
In the following we provide our results for DV channels, with technical details available in Appendix B.

2.7.1.1 Pauli channels

A general error model for the transmission of qubits is represented by the class of Pauli channels

$$\mathcal{P}(\rho) = p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z, \tag{2.90}$$

where X, Y, and Z are Pauli operators and $\mathbf{p} := \{p_k\}$ is a probability distribution. It is easy to check that this channel is Choi-stretchable and its Choi matrix is Bell-diagonal. We compute its entanglement flux as (see Appendix B.1 for the discussion on how to deal with the optimization over the set of separable states in Eq. (2.31)) [1, Eq. (33)]

$$\mathbf{\Phi}(\mathcal{P}) = 1 - H_2(p_{\max}), \tag{2.91}$$

if $p_{\max} := \max\{p_k\} \geq 1/2$, while zero otherwise. Since the channel is unital, we have that $I_{\mathrm{C}}(\mathcal{P}) = I_{\mathrm{RC}}(\mathcal{P}) = 1 - H(\mathbf{p})$, where H is the Shannon entropy. Thus, the two-way capacity of a Pauli channel satisfies

$$1 - H(\mathbf{p}) \leq \mathcal{C}(\mathcal{P}) \leq \mathbf{\Phi}(\mathcal{P}). \tag{2.92}$$

This can be easily generalized to arbitrary finite dimension (see Sec. B.1.2 in Appendix B). Consider the depolarising channel, which is a Pauli channel shrinking the Bloch sphere. With probability p, an input state becomes the maximally-mixed state

$$\mathcal{P}_{\text{depol}}(\rho) = (1-p)\rho + pI/2. \tag{2.93}$$

Setting $\kappa(p) := 1 - H_2\left(3p/4\right)$, we may then write [1, Eq. (36)]

$$\kappa(p) - \frac{3p}{4}\log_2 3 \leq \mathcal{C}(\mathcal{P}_{\text{depol}}) \leq \kappa(p), \tag{2.94}$$

for $p \leq 2/3$, while 0 otherwise (see Fig. 2.6a). The result can be extended to any dimension $d \geq 2$. A qudit depolarising channel is defined as in Eq. (2.93) up to using the mixed state I/d. Setting $f := p(d^2-1)/d^2$ and $\kappa(d,p) := \log_2 d - H_2(f) - f\log_2(d-1)$, we find [1, Eq. (37)]

$$\kappa(d,p) - f\log_2(d+1) \leq \mathcal{C}(\mathcal{P}_{\text{depol}}) \leq \kappa(d,p), \tag{2.95}$$

for $p \leq d/(d+1)$, while zero otherwise.

Consider now the dephasing channel. This is a Pauli channel which deteriorates quantum information without energy decay, as it occurs in spin-spin relaxation or photonic scattering through waveguides. It is defined as

$$\mathcal{P}_{\text{deph}}(\rho) = (1-p)\rho + pZ\rho Z, \tag{2.96}$$

where p is the probability of a phase flip. We can easily check that the two bounds of Eq. (2.92) coincide, so that this channel is distillable and its two-way capacities are [1, Eq. (39)]

$$\begin{aligned} \mathcal{C}(\mathcal{P}_{\text{deph}}) &= D_2(\mathcal{P}_{\text{deph}}) = Q_2(\mathcal{P}_{\text{deph}}) \\ &= K(\mathcal{P}_{\text{deph}}) = 1 - H_2(p). \end{aligned} \tag{2.97}$$

Note that this also proves $Q_2(\mathcal{P}_{\text{deph}}) = Q(\mathcal{P}_{\text{deph}})$, where the latter was derived in ref. [70]. For an arbitrary qudit with computational basis $\{|j\rangle\}$, the generalized dephasing channel is defined as

$$\mathcal{P}_{\text{deph}}(\rho) = \sum_{i=0}^{d-1} P_i Z^i \rho (Z^\dagger)^i, \tag{2.98}$$

where P_i is the probability of i phase flips, with a single flip being $Z\,|j\rangle = e^{ij2\pi/d}\,|j\rangle$. This channel is distillable and its two-way capacities are functionals of $\mathbf{P} = \{P_i\}$ and are given by [1, Eq. (41)]

$$\mathcal{C}(\mathcal{P}_{\text{deph}}) = \log_2 d - H(\mathbf{P}). \tag{2.99}$$

2.7.1.2 Quantum erasure channel

A simple decoherence model is the erasure channel. This is described by

$$\mathcal{E}_{\text{erase}}(\rho) = (1-p)\rho + p\,|e\rangle\,\langle e|\,, \tag{2.100}$$

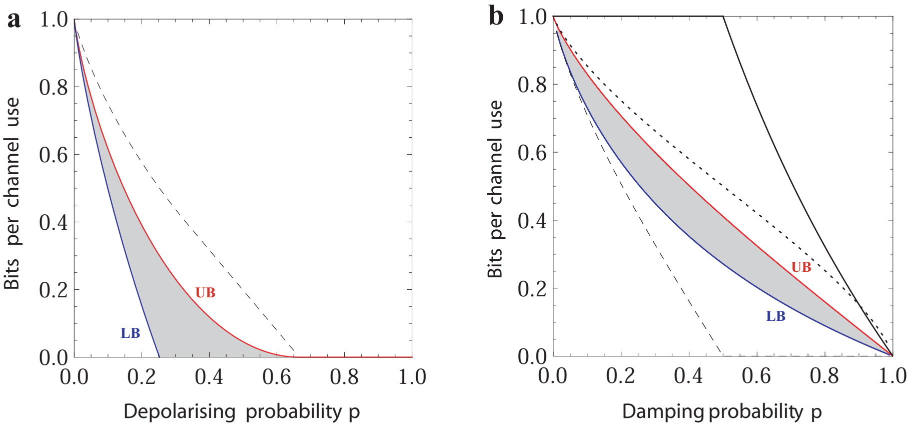

Figure 2.6: Two-way capacities of basic qubit channels. (**a**) Two-way capacity of the depolarising channel $\mathcal{P}_{\text{depol}}$ with arbitrary probability p. It is contained in the shadowed region specified by the bounds in Eq. (2.94). We also depict the best known bound based on the squashed entanglement [100] (dashed). (**b**) Two-way capacity of the amplitude damping channel $\mathcal{E}_{\text{damp}}$ for arbitrary damping probability p. It is contained in the shadowed area identified by the lower bound (LB) of Eq. (2.106) and the upper bound (UB) of Eq. (2.107). We also depict the bound of Eq. (2.105) (upper solid line), which is good only at high dampings; and the bound $C_{\text{A}}(\mathcal{E}_{\text{damp}})/2$ of ref. [100] (dotted line), which is computed from the entanglement-assisted classical capacity C_{A}. Finally, note the separation of the two-way capacity $\mathcal{C}(\mathcal{E}_{\text{damp}})$ from the unassisted quantum capacity $Q(\mathcal{E}_{\text{damp}})$ (dashed line). This is Fig 8 from [1].

where p is the probability of getting an orthogonal erasure state $|e\rangle$. We already know that $Q_2(\mathcal{E}_{\text{erase}}) = 1 - p$ [89]. Therefore we compute the secret key capacity.
Following ref. [89], one shows that $D_1(\rho_{\mathcal{E}_{\text{erase}}}) \geq 1 - p$. In fact, suppose that Alice sends halves of EPR states to Bob. A fraction $1 - p$ will be perfectly distributed. These good cases can be identified by Bob applying the measurement $\{|e\rangle\langle e|, I - |e\rangle\langle e|\}$ on each output system, and communicating the results back to Alice in a single and final CC. Therefore, they distill at least $1 - p$ ebits per copy. It is then easy to check that this channel is Choi-stretchable and we compute $\mathbf{\Phi}(\rho_{\mathcal{E}_{\text{erase}}}) \leq 1 - p$. Thus, the erasure channel is distillable and we may write [1, Eq. (43)]

$$\mathcal{C}(\mathcal{E}_{\text{erase}}) = K(\mathcal{E}_{\text{erase}}) = 1 - p. \tag{2.101}$$

In arbitrary dimension d, the generalized erasure channel is defined as in Eq. (2.100), where ρ is now the state of a qudit and the erasure state $|e\rangle$ lives in the extra $d + 1$ dimension. We can easily generalize the previous derivations to find that this channel is distillable and [1, Eq. (44)]

$$K(\mathcal{E}_{\text{erase}}) = (1 - p)\log_2 d. \tag{2.102}$$

Note that the latter result can also be obtained by computing the squashed entanglement of the erasure channel, as shown by the independent derivation of ref. [100].

2.7.1.3 Amplitude damping channel

An important model of decoherence in spins or optical cavities is energy dissipation or amplitude damping [101,102]. The action of this channel on a qubit is

$$\mathcal{E}_{\text{damp}}(\rho) = \textstyle\sum_{i=0,1} A_i \rho A_i^\dagger, \tag{2.103}$$

where $A_0 := |0\rangle\langle 0| + \sqrt{1-p}\,|1\rangle\langle 1|$, $A_1 := \sqrt{p}\,|0\rangle\langle 1|$, and p is the damping probability. Note that $\mathcal{E}_{\text{damp}}$ is not teleportation-covariant. However, it is decomposable as

$$\mathcal{E}_{\text{damp}} = \mathcal{E}_{\text{CV}\to\text{DV}} \circ \mathcal{E}_{\eta(p)} \circ \mathcal{E}_{\text{DV}\to\text{CV}}, \tag{2.104}$$

where $\mathcal{E}_{\text{DV}\to\text{CV}}$ teleports the original qubit into a single-rail bosonic qubit [78]; then, $\mathcal{E}_{\eta(p)}$ is a lossy channel with transmissivity $\eta(p) := 1 - p$; and $\mathcal{E}_{\text{CV}\to\text{DV}}$ teleports the single-rail qubit back to the original qubit. Thus, $\mathcal{E}_{\text{damp}}$ is stretchable into the asymptotic Choi matrix of the lossy channel $\mathcal{E}_{\eta(p)}$. This shows that we need a dimension-independent theory even for stretching DV channels.

From Theorem 2.6.1 we get $\mathcal{C}(\mathcal{E}_{\rm damp}) \leq \mathbf{\Phi}(\mathcal{E}_{\eta(p)})$, implying [1, Eq. (47)]

$$\mathcal{C}(\mathcal{E}_{\rm damp}) \leq \min\{1, -\log_2 p\}, \tag{2.105}$$

while the reverse coherent information implies [32]

$$\max_u \{H_2\left(u\right) - H_2\left(up\right)\} \leq \mathcal{C}(\mathcal{E}_{\rm damp}). \tag{2.106}$$

The bound in Eq. (2.105) is simple but only good for strong damping ($p > 0.9$). A shown in Fig. 2.6b, we find a tighter bound using the squashed entanglement [1, Eq. (49)], i.e.,

$$\mathcal{C}(\mathcal{E}_{\rm damp}) \leq H_2\left(\frac{1}{2} - \frac{p}{4}\right) - H_2\left(1 - \frac{p}{4}\right). \tag{2.107}$$

2.7.2 Bosonic Gaussian channels

Here we give the analytical expression of the ultimate rates for quantum and secure communication through bosonic Gaussian channels. The detailed calculation of such expressions are left in the Appendix B (Sec. B.2). Refer also to Sec. 1.3 for the characterization of Gaussian channels.

We have shown that bosonic Gaussian channels are Choi-stretchable and that their two-way quantum capacities can be upper-bounded as [1, Eq. (18)]

$$\mathcal{C}(\mathcal{E}) \leq \mathbf{\Phi}(\mathcal{E}) \leq \liminf_{\mu \to \infty} S(\rho^{\mu}_{\mathcal{E}} \| \tilde{\sigma}^{\mu}_{s}) \ , \tag{2.108}$$

for a suitable converging sequence of separable states $\tilde{\sigma}^{\mu}_{s}$. For Gaussian channels, the sequences in the above equation involve Gaussian states, for which we easily compute the relative entropy. In fact, for any two Gaussian states, ρ_1 and ρ_2, we prove in Appendix B(Sec. B.2.1) the general formula $S(\rho_1||\rho_2) = \Sigma(V_1, V_2) - \Sigma(V_1, V_1)$, where Σ is given by a simple functional of their statistical moments, namely [1, Theorem 7]

$$\Sigma(V_1, V_2) := \frac{1}{2\ln 2}\left\{\ln\det\left(V_2 + \frac{i\mathbf{\Omega}}{2}\right) + \mathrm{Tr}\left[V_1 G(V_2)\right]\right\} \ , \tag{2.109}$$

where $G(V) = 2i\mathbf{\Omega}\coth^{-1}(2Vi\mathbf{\Omega})$ is the so-called Gibbs matrix of the Gaussian state with covariance matrix V.

The optimization over the set of all the separable states appearing in the definition of the

REE is here circumvented by choosing a good separable candidate state. This is given by a two-mode Gaussian state with CM given by

$$\mathbf{V} = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix} , \tag{2.110}$$

with

$$c = c_{\text{sep}} := \sqrt{(a - \frac{1}{2})(b - \frac{1}{2})} , \tag{2.111}$$

which defines the maximally-correlated separable Gaussian state. It is straightforward to check that this state entails the maximum correlations among all the separable states, e.g., as quantified by its quantum discord [103].

2.7.2.1 Pure loss channel

This Gaussian channel is the standard model to describe losses in optical communications through free-space links or telecom fibres. The lossy channel $\mathcal{E}_\eta$ is characterized by a transmissivity parameter η, which quantifies the fraction of input photons that survives at the output. It is represented by a beam splitter mixing the input signal witha zero-temperature environment (backgorund thermal noise is negligible at optical and telecom frequencies). For $\mathcal{E}_\eta$ we compute the entanglement flux $\mathbf{\Phi}(\eta) \leq -\log_2(1-\eta)$. This coincides with the reverse coherent information of this channel $I_{\text{RC}}(\eta)$, first derived in Ref. [33]. Thus, we find that this channel is distillable and all its two-way capacities are given by [1, Eq. (19)]

$$\mathcal{C}(\eta) = D_2(\eta) = Q_2(\eta) = K(\eta) = -\log_2(1-\eta). \tag{2.112}$$

Interestingly, this capacity coincides with the maximum discord [104] that can be distributed, since we may write [105] $I_{\text{RC}}(\eta) = D(B|A)$, where the latter is the discord of the (asymptotic) Gaussian Choi matrix $\rho_{\mathcal{E}_\eta}$ [103]. We also prove the strict separation $Q_2(\eta) > Q(\eta)$, where Q is the unassisted quantum capacity [94, 95].

Expanding Eq. (2.112) at high loss $\eta \simeq 0$, we find

$$\mathcal{C}(\eta) \simeq \eta / \ln 2 \simeq 1.44\eta \text{ (bits per channel use)}, \tag{2.113}$$

or about η nats per channel use. This completely characterizes the fundamental rate-loss scaling which rules long-distance quantum optical communications in the absence of quantum repeaters. It is important to remark that our work also proves the achievability of this

scaling. This is a major advance with respect to existing literature, where previous studies with the squashed entanglement [106] only identified a non-achievable upper bound.
In Fig. 2.7, we compare the scaling of Eq. (2.113) with the maximum rates achievable by current QKD protocols.
The capacity in Eq. (2.112) is also valid for two-way quantum communication with lossy channels, assuming that η is the maximum transmissivity between the forward and feedback channels. It can also be extended to a multiband lossy channel, for which we write $\mathcal{C} = -\sum_i \log_2(1-\eta_i)$, where η_i are the transmissivities of the various bands or frequency components. For instance, for a multimode telecom fibre with constant transmissivity η and bandwidth W, we have [1, Eq. (21)]

$$\mathcal{C} = -W \log_2(1-\eta). \tag{2.114}$$

Finally, note that free-space satellite communications may be modeled as a fading lossy channel, i.e., an ensemble of lossy channels $\mathcal{E}_{\eta_i}$ with associated probabilities p_i [107]. In particular, slow fading can be associated with variations of satellite-Earth radial distance [108, 109]. For a fading lossy channel $\{\mathcal{E}_{\eta_i}, p_i\}$, we may write [1, Eq. (22)]

$$\mathcal{C} \leq -\sum_i p_i \log_2(1-\eta_i) \ . \tag{2.115}$$

Quantum communications with Gaussian noise

The fundamental limit of the lossy channel bounds the two-way capacities of all channels decomposable as $\mathcal{E} = \mathcal{E}'' \circ \mathcal{E}_\eta \circ \mathcal{E}'$ where $\mathcal{E}_\eta$ is a lossy component while $\mathcal{E}'$ and $\mathcal{E}''$ are extra channels. A channel $\mathcal{E}$ of this type is stretchable with resource state $\sigma = \rho_{\mathcal{E}_\eta} \neq \rho_{\mathcal{E}}$ and we may write $\mathcal{C}(\mathcal{E}) \leq -\log_2(1-\eta)$. For Gaussian channels, such decompositions are known but we achieve tighter bounds if we directly stretch them using their own Choi matrix.

2.7.2.2 Thermal loss channel

This Gaussian channel can be modeled as a beamsplitter with transmissivity η in a thermal background with $\bar{n}$ mean photons. Its action on input quadratures $\hat{\mathbf{x}} = (\hat{q}, \hat{p})$ is given by $\hat{\mathbf{x}} \to \sqrt{\eta}\hat{\mathbf{x}} + \sqrt{1-\eta}\hat{\mathbf{x}}_E$ with E being a thermal mode. This channel is central for microwave communications [118–121] but also important for CV QKD at optical and telecom frequencies, where Gaussian eavesdropping via entangling cloners results into a thermal-loss channel [11].

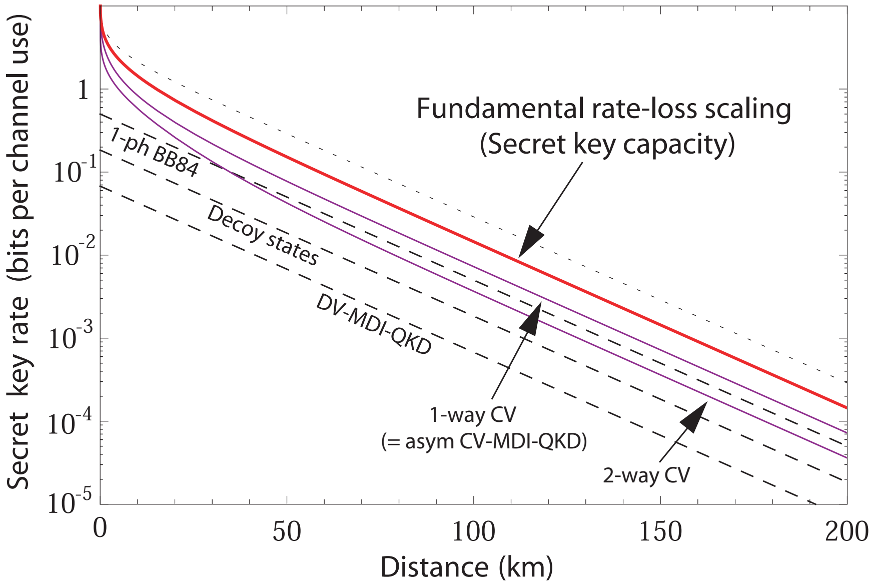

Figure 2.7: Ideal performances in QKD. We plot the secret key rate (bits per channel use) versus Alice-Bob's distance (km) at the loss rate of 0.2 dB per km. The secret key capacity of the channel (red line) sets the fundamental rate limit for point-to-point QKD in the presence of loss. Compare this capacity with a previous non-achievable upperbound [106] (dotted line). We then show the maximum rates that are potentially achievable by current protocols, assuming infinitely long keys and ideal conditions, such as unit detector efficiencies, zero dark count rates, zero intrinsic error, unit error correction efficiency, zero excess noise (for CVs), and large modulation (for CVs). In the figure, we see that ideal implementations of CV protocols (purple lines) are not so far from the ultimate limit. In particular, we consider: (i) One-way no-switching protocol [110], coinciding with CV-MDI-QKD [75,111] in the most asymmetric configuration (relay approaching Alice). For high loss ($\eta \simeq 0$), the rate scales as $\eta/\ln 4$, which is just $1/2$ of the capacity. Same scaling for the one-way switching protocol of ref. [112]; (ii) Two-way protocol with coherent states and homodyne detection [113,114] which scales as $\simeq \eta/(4\ln 2)$ for high loss (thermal noise is needed for two-way to beat one-way QKD [113]). For the DV protocols (dashed lines), we consider: BB84 with single-photon sources [21] with rate $\eta/2$; BB84 with weak coherent pulses and decoy states [115] with rate $\eta/(2e)$; and DV-MDI-QKD [116,117] with rate $\eta/(2e^2)$. This is Fig. 6 from [1]

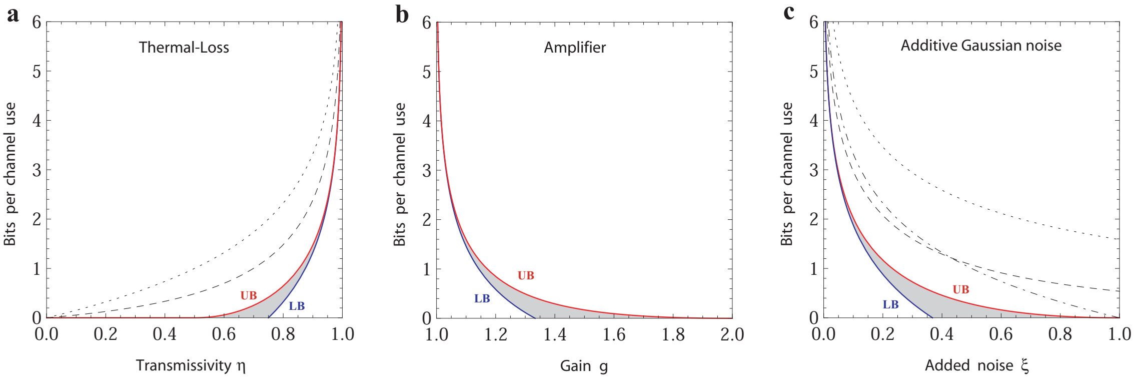

Figure 2.8: Two-way capacities for Gaussian channels in terms of the relevant channel parameters. (**a**) Two-way capacity $\mathcal{C}(\eta, \bar{n})$ of the thermal-loss channel as a function of transmissivity η for $\bar{n} = 1$ thermal photon. It is contained in the shadowed area identified by the lower bound (LB) and upper bound (UB) of Eq. (2.118). Our upper bound is clearly tighter than those based on the squashed entanglement, computed in ref. [106] (dotted) and ref. [100] (dashed). Note that $\mathcal{C}(\eta, \bar{n}) \simeq -\log_2(1-\eta)-h(\bar{n})$ at high transmissivities. For $\bar{n} = 0$ (lossy channel) the shadowed region shrinks into a single line. (**b**) Two-way capacity $\mathcal{C}(g, \bar{n})$ of the amplifier channel as a function of the gain g for $\bar{n} = 1$ thermal photon. It is contained in the shadowed specified by the bounds in Eq. (2.120). For small gains, we have $\mathcal{C}(g, \bar{n}) \simeq \log_2[g/(g-1)] - h(\bar{n})$. For $\bar{n} = 0$ (quantum-limited amplifier) the shadowed region shrinks into a single line. (**c**) Two-way capacity $\mathcal{C}(\xi)$ of the additive-noise Gaussian channel with added noise ξ. It is contained in the shadowed region specified by the bounds in Eq. (2.123). For small noise, we have $\mathcal{C}(\xi) \simeq -1/\ln 2 - \log_2 \xi$. Our upper bound is much tighter than those of ref. [106] (dotted), ref. [100] (dashed), and ref. [62] (dot-dashed). This is Fig. 7 from [1]

For an arbitrary thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$ we apply our reduction method and compute the entanglement flux [1, Eq. (23)]

$$\mathbf{\Phi}(\eta,\bar{n}) \leq -\log_2\left[(1-\eta)\eta^{\bar{n}}\right] - h(\bar{n}), \tag{2.116}$$

for $\bar{n} < \eta/(1-\eta)$, while zero otherwise. Here we set

$$h(x) := (x+1)\log_2(x+1) - x\log_2 x. \tag{2.117}$$

Combining this result with the lower bound given by the reverse coherent information, we write the following inequalities for the two-way capacity of this channel [1, Eq. (25)]

$$-\log_2(1-\eta) - h(\bar{n}) \leq \mathcal{C}(\eta,\bar{n}) \leq \mathbf{\Phi}(\eta,\bar{n}). \tag{2.118}$$

As shown in Fig. 2.8a, the two bounds tend to coincide at sufficiently high transmissivity. We clearly retrieve the previous result of the lossy channel for $\bar{n} = 0$.

2.7.2.3 Quantum amplifier

This channel $\mathcal{E}_{g,\bar{n}}$ is described by $\hat{\mathbf{x}} \to \sqrt{g}\hat{\mathbf{x}} + \sqrt{g-1}\hat{\mathbf{x}}_E$, where $g > 1$ is the gain and E is the thermal environment with $\bar{n}$ mean photons. We compute [1, Eq. (26)]

$$\mathbf{\Phi}(g,\bar{n}) \leq \log_2\left(\frac{g^{\bar{n}+1}}{g-1}\right) - h(\bar{n}), \tag{2.119}$$

for $\bar{n} < (g-1)^{-1}$, while zero otherwise. Combining this result with the coherent information [62], we get [1, Eq. (27)]

$$\log_2\left(\frac{g}{g-1}\right) - h(\bar{n}) \leq \mathcal{C}(g,\bar{n}) \leq \Phi(g,\bar{n}), \tag{2.120}$$

whose behavior is plotted in Fig. 2.8b.

In the absence of thermal noise ($\bar{n} = 0$), the previous channel describes a quantum-limited amplifier $\mathcal{E}_g$, for which the bounds in Eq. (2.120) coincide. This channel is therefore distillable and its two-way capacities are [1, Eq. (28)]

$$\mathcal{C}(g) = D_2(g) = Q_2(g) = K(g) = -\log_2(1-g^{-1}). \tag{2.121}$$

In particular, this proves that $Q_2(g)$ coincides with the unassisted quantum capacity $Q(g)$ [62, 122]. The result of Eq. (2.121) sets the fundamental limit for key generation, entanglement distribution and quantum communication with amplifiers. A trivial consequence is that infinite amplification is useless for communication since $\mathcal{C}_{\text{amp}}(\infty) \to 0$. For an amplifier with typical gain 2, the maximum achievable rate for quantum communication is just 1 qubit per use.

2.7.2.4 Additive-noise Gaussian channel

This channel respresents the simplest model of bosonic decoherence and it can be seen as the direct extension of the classical model of a Gaussian channel to the quantum regime. It can be seen as the action of a random Gaussian displacement over incoming states. In terms of input-output transformations, it is described by $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + (z, z)^T$ where z is a classical Gaussian variable with zero mean and variance $\xi \geq 0$. For this channel $\mathcal{E}_\xi$ we find the entanglement flux [1, Eq. (29)]

$$\mathbf{\Phi}(\xi) \leq \frac{\xi - 1}{\ln 2} - \log_2 \xi, \tag{2.122}$$

for $\xi < 1$, while zero otherwise. Including the lower bound given by the coherent information [62], we get [1, Eq. (30)]

$$-\frac{1}{\ln 2} - \log_2 \xi \leq \mathcal{C}(\xi) \leq \mathbf{\Phi}(\xi) \ . \tag{2.123}$$

In Fig. 2.8c, see its behavior and how the two bounds tend to rapidly coincide for small added noise.

It is interesting to note how quantum communication rapidly degrades when we compose quantum channels. For instance, a quantum-limited amplifier with gain 2 can transmit $Q_2 = 1$ qubit per use from Alice to Bob. This is the same amount which can be transmitted from Bob to Charlie, through a lossy channel with transmissivity 1/2. By using Bob as a quantum repeater, Alice can therefore transmit at least 1 qubit per use to Charlie. If we remove Bob and we compose the two channels, we obtain an additive-noise Gaussian channel with variance $\xi = 1/2$, which is limited to $Q_2 \lesssim 0.278$ qubits per use.

2.8 Cost of classical communication

It is important to discuss the cost associated with the CCs. In fact, in order to achieve its performance, an optimal protocol will need a certain number of classical bits per channel use. Furthermore, the physical transmission of these bits is ultimately restricted by the speed of light. It is therefore essential to consider these aspects in order to translate a capacity, which is expressed in terms of target-bits (e.g. secret bits) per channel use, into a practical throughput, which is expressed in terms of target-bits per second. Consider the case of a bosonic lossy channel which is the most important for quantum optical communications.

By definition, an adaptive protocol is assisted by unlimited and two-way CCs. This is a very general formulation but it has an issue for practical applications: An adaptive protocol, which may be optimal in terms of target-bits per channel use, may have zero throughput in terms of target-bits per second, just due the fact that its implementation may require infinite rounds of feed-forward and feedback CCs in each channel use. The existence of such protocol is not excluded by the TGW bounds [106], which are non-tight and do not have control on the CCs. By contrast, this problem is completed solved by our bound.

In fact, for any distillable channel $\mathcal{E}$ (e.g., bosonic lossy channel, quantum-limited amplifier, dephasing or erasure channel), the generic two-way capacity $\mathcal{C}(\mathcal{E})$ is equal to $D_1(\mathcal{E})$. This means that an optimal protocol achieving the capacity is non-adaptive and it does not involve infinite rounds of CCs, but just a single round of forward or backward CCs.

For the specific case of a bosonic lossy channel, with transmissivity η, we find that an optimal key-generation protocol, achieving the repeaterless bound $K(\eta) = -\log_2(1-\eta)$, can be implemented by using backward CCs. In fact, an optimal key-generation protocol is the following: Alice prepares TMSV states $\Phi^{\mu}_{AA'}$ sending A' to Bob; Bob heterodynes each output mode, with outcome Y, and sends final CCs back to Alice; Alice measures all her modes A by means of an optimal coherent detection. Taking the limit for large μ, the key rate of the parties achieves the bound $K(\eta)$.

Because this is a generalized Devetak-Winter rate (in reverse reconciliation), the amount of CCs required by the protocol (bits per channel use) is equal to the following conditional entropy [93]

$$\gamma_{\mathrm{CC}} := S(Y|A) = S(Y) - [S(A) - S(A|Y)], \tag{2.124}$$

where $S(Y) = H(Y)$ is the Shannon entropy of Bob's outcomes Y, while $S(A)$ and $S(A|Y)$ are the von Neumann entropies of Alice's reduced state ρ_A and conditional state $\rho_{A|Y}$. These quantities are all easily computable for any finite value of μ. By taking the limit for large μ, we derive the asymptotic cost

$$\gamma_{\mathrm{CC}}(\eta) = \frac{2\eta\log_2\pi + (2\eta-3)\log_2(3-2\eta) + 3\log_2 3}{2\eta} \leq \log_2(3\pi e) \approx 4.68 \text{ classical bits/use}, \tag{2.125}$$

where the latter bound is achieved for low transmissivities (long-distances), i.e., $\gamma_{\mathrm{CC}}(\eta \simeq 0) \simeq \log_2(3\pi e)$. According to Eq. (2.125), at any transmissivity η, Bob needs to send Alice no more than $\log_2(3\pi e)$ classical bits per channel use.

Consider a practical scenario where the rounds of the protocol are not infinite but yet a very large number, e.g., $n = 10^9$, so that the performance of such a large block of data is close to the asymptotic one. The amount of classical bits to be transmitted is linear in n, and the total cost is no larger than 4.68×10^9 bits, i.e., less than 1 gigabyte per block. Assuming the existence of a broadband classical channel between Alice and Bob, the extra time associated with the transmission of this classical overhead can be made negligible (for instance, it may happen at the beginning of the second large block of quantum communication). Assuming that the procedures of error correction and privacy amplification are also sufficiently fast within the block, then the final achievable throughput (secret-bits per second) will only depend on the capacity $K(\eta)$ (secret-bits per use) multiplied by the clock of the system (uses per second). Clearly, this is a simplified reasoning which does not consider other technical issues.

Chapter 3

Finite-energy resource bounds for private communication over Gaussian channels

So far we have seen that, since they are teleportation covariant, bosonic Gaussian channels can be simulated by means of continuous variable teleportation over their asymptotic Choi matrices. As discussed in the previous Chapter, a bosonic Choi matrix is defined by propagating half of a two-mode squeezed vacuum state through the channel, and then taking the limit for infinite energy. This results in an energy-unbounded and therefore unphysical state. Thus at finite energy, the simulation is imperfect with an associated simulation error that must be carefully handled and propagated at the output of the adaptive protocols (see the discussions leading to Eq. (2.75) and (2.76)). In order to circumvent the limit for infinite energy and the employment of asymptotic Choi matrices, we provide an alternative way to simulate bosonic Gaussian channels. This is obtained by implementing the CV teleportation protocol over a suitably-defined class of finite-energy Gaussian states. This approach removes the limit in the energy in the resource state, even though it survives at the level of the CV Bell detection, which is defined in Eq. (1.104) as an asymptotic Gaussian measurement, whose limit realizes an ideal projection onto displaced EPR states.

Following the strategy described in the previous Chapter, here we combine two types of finite-energy simulation of phase-insensitive Gaussian channels with teleportation stretching and the relative entropy of entanglement in order to derive non-asymtotic upper bounds on the secret key capacity of these channels.

We first consider the finite-energy simulation developed in Refs. [81, 123, 124], and we show [5] how this gives upper bounds on $K(\mathcal{E})$ that roughly approximate the asymptotic ones.

More recently, Ref. [125] derived a more general class of resource states for the perfect teleporatation simulation of bosonic Gaussian channels and studied their performance in term of the entanglement of formation. Here we adopt also these resource states which can be parametrized in terms of their purity and optimized with respect to the REE. We therefore derive [6] upper bounds to the secret-key capacity of bosonic channels which can be made as close as possible to the infinite-energy ones of the previous Chapter.

3.1 Simulation of Gaussian channels with finite-energy resource states

Recently, Ref. [81] has shown that all single-mode phase-insensitive Gaussian channels can be simulated by applying CV teleportation to a particular class of Gaussian states as the resource. We extensively described Gaussian channels in Sec. 1.3, here we recall some of their characterizing properties for the sake of clarity. Consider a single-mode Gaussian state with mean value $\bar{x}$ and covariance matrix (CM) $\mathbf{V}$. As we already know, the action of a single-mode Gaussian channel can be expressed in terms of the statistical moments as (see also Eq. (1.67))

$$\bar{x} \to \mathbf{T}\bar{x}, \quad \mathbf{V} \to \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N}, \tag{3.1}$$

where $\mathbf{T}$ and $\mathbf{N} = \mathbf{N}^T$ are 2×2 real matrices satisfying the conditions of Eq. (1.68) [11]. In particular, as shown in Table 1.2, the class of phase-insensitive is characterized by diagonal matrices, i.e.

$$\mathbf{T} = \sqrt{\eta}\mathbf{I}, \quad \mathbf{N} = v\mathbf{I} \tag{3.2}$$

where $\eta \in \mathbb{R}$ is a transmissivity parameter, while $v \geq 0$ represents the added noise.

Suppose now that Alice and Bob are implementing a BK protocol for CV teleportation with a generic quantum resource given by a two-mode Gaussian state with zero first statistical moment and covariance matrix that in standard form reads

$$\mathbf{V}_{AB} = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix} . \tag{3.3}$$

The input state to be teleported has displacement d_c and covariance matrix $\mathbf{V}_c$. By repeating the procedure depicted in Sec. 1.4.1, contrary to what happens in Eqs. (1.102) and (1.103), once Bob applies the final conditional displacement he ends up with an output state that does not coincide with the input and reads

$$\hat{q}_B \to \hat{q}_{out} = \hat{q}_B - g\sqrt{2}Q_- \tag{3.4}$$

$$\hat{p}_B \to \hat{p}_{out} = \hat{p}_B + g\sqrt{2}P_+ \tag{3.5}$$

where g is Bob's gain for the transformation from photocurrent to output field [126] which is set to $g = 1$ for a maximally entangled resource. At this stage, once the teleportation process has taken place, the statistical moment of the output state can be computed as in Refs. [127,128] and they can be given in terms of the statistical moments of the inputs and of the resource state of Eq. (3.3). It can be shown then that CV teleportation is equivalent to a phase-insensitive channel characterized by Eq. (3.2) with parameters related to the protocol and its resource state as follows

$$\sqrt{\eta} = g \quad , \quad v = ag^2 - 2cg + b \ . \tag{3.6}$$

Viceversa, by fixing the phase-insensitive Gaussian channel, i.e. fixing the pair (η, v), the problem is to find the resource state CM that simulates the corresponding channel with finite mean energy. By solving this, imposing also minimum entanglement, as measured by the logarithmic negativity [35, 129], the authors of [81] prove that a phase-insensitive Gaussian channel $\mathcal{E}_{\eta,v}$ can be simulated as follows

$$\mathcal{E}_{\eta,v}(\rho) = \mathcal{T}_\eta(\rho \otimes \sigma_v), \tag{3.7}$$

where $\mathcal{T}_\eta$ is the Braunstein-Kimble protocol with gain $\sqrt{\eta}$, and σ_v is a zero-mean two-mode Gaussian state with CM

$$\mathbf{V}(\sigma_v) = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \tag{3.8}$$

where [81]

$$a = \frac{2b + (\eta - 1)e^{-2r}}{2\eta}, \quad c = \frac{2b - e^{-2r}}{2\sqrt{\eta}}, \tag{3.9}$$

$$b = \frac{-|\eta - 1| + \eta e^{2r} + e^{-2r}}{2[-e^{2r}|\eta - 1| + \eta + 1]}, \tag{3.10}$$

and the entanglement parameter $r \geq 0$ is connected to the channel parameter via the relation

$$v = \frac{e^{-2r}}{2}(\eta + 1). \tag{3.11}$$

To conclude we further observe that, in the simulation of Eq. (3.7), a Braunstein-Kimble protocol with an ideal CV Bell detection obtained as a limit for infinite energy (see Eq. 1.104) is exploited. This means that the finite-energy feature of the simulation is only at the level of the resource state.

We also notice that the expressions of Eq. (3.10) diverge for the pure-loss and the pure amplifier channel so that these two channels cannot be simulated using that resource state (more details later on). Fortunately, this issue is removed by the finite-energy simulation we are describing in the following and which has been derived by Tserkis *et al.* in Ref. [125].

In this work the same problem is adressed. The difference is that, as a quantifier of the entanglement, the entanglement of formation is employed. This allows to find a suitable class of resource states, with the same entanglement as the Choi state and minimum mean energy, that are able to simulate any phase-insensitive Gaussian channel.

In particular, Ref. [125] shows that we can simulate a phase-insensitive Gaussian channel as follows

$$\mathcal{E}_{\eta,v}(\rho) = \mathcal{T}_{\eta}(\rho \otimes \tilde{\sigma}_v), \tag{3.12}$$

where now the resource state $\tilde{\sigma}_v$ is characterized by the following CM

$$\mathbf{V}(\tilde{\sigma}_v) = \begin{pmatrix} \tilde{a}\mathbf{I} & \tilde{c}\mathbf{Z} \\ \tilde{c}\mathbf{Z} & \tilde{b}\mathbf{I} \end{pmatrix}, \tag{3.13}$$

with elements

$$\tilde{a} = \frac{|1-\eta|(\nu_+ - \nu_-) + (1+\eta)v - 2\gamma}{(1-\eta)^2}, \tag{3.14}$$

$$\tilde{b} = \frac{\eta|1-\eta|(\nu_+ - \nu_-) + (1+\eta)v - 2\gamma}{(1-\eta)^2}, \tag{3.15}$$

$$\tilde{c} = \frac{\tau|1-\eta|(\nu_+ - \nu_-) + 2\eta v - (1+\eta)\gamma}{\sqrt{\eta}(1-\eta)^2}, \tag{3.16}$$

where we have set

$$\gamma := \sqrt{\eta(v - |1-\eta|\nu_-)(v + |1-\eta|\nu_+)}. \tag{3.17}$$

Note that for $0 < \eta < 1$, we get states with $a \geq b$, while for $\eta > 1$ we get $a \leq b$. These elements are expressed in terms of the channel parameters, η and v, and may vary over the symplectic spectrum $\nu_{\pm}$ with the constraints

$$1/2 \leq \nu_- \leq \bar{n} + 1/2, \qquad \nu_- \leq \nu_+ \ , \tag{3.18}$$

where $\bar{n}$ is the mean thermal number of the Gaussian channel (thermal-loss or amplifier). Note that states with reversed symmetry for each case, i.e. $a \leq b$ for $\eta < 1$ and $a \geq b$ for $\eta > 1$, can be retrieved by interchanging the role of ν_- and ν_+.

According to Eq. (3.18), for thermal-loss and amplifier channels, we have some freedom in choosing $\nu_\pm$ so that there is an entire class over which we may optimize our upper bounds. One possible approach is fixing the purity $p = (\nu_- \nu_+)^{-1}$ of the resource state and optimizing over the remaining free parameter. Note that the asymptotic Choi matrix can be retrieved in the limit of $p \to 0$. In Sec. 3.3 we will see how this feature allows us to approximate the infinite-energy bounds as much as we want by using a small but yet non-zero value of the purity p.

For the special case of $\eta = 1$, we have an additive-noise Gaussian channel with added-noise variance $v > 0$. In this case, taking the limit $\eta \to 1$ for the class in Eqs. (3.14)-(3.16) we get the following parametrization

$$\tilde{a} = \frac{\nu_-^2 + 2\nu_-(\nu_+ - v) + (\nu_+ + v)^2}{4v}, \tag{3.19}$$

$$\tilde{b} = \frac{\nu_-^2 + 2\nu_-(\nu_+ + v) + (\nu_+ - v)^2}{4v}, \tag{3.20}$$

$$\tilde{c} = \frac{(\nu_- + \nu_+ - v)(\nu_- + \nu_+ + v)}{4v}. \tag{3.21}$$

3.2 Finite-resource teleportation stretching of an adaptive protocol

Here we plug the two previous finite-resource simulations into the tool of teleportation stretching. By following the recipe of Sec. 2.5 and 2.6, we show how to use the finite-resource simulation to simplify an adaptive protocol and reduce the REE bound to a single-letter quantity.

Assume that the adaptive protocol described in Sec. 2.1 is performed over a phase-insensitive Gaussian channel $\mathcal{E}_{\eta,v}$, so that we may use the simulation of Eq. (3.7), where $\mathcal{T}_\eta$ is the Braunstein-Kimble protocol with gain $\sqrt{\eta}$ and σ_v is a zero-mean two-mode Gaussian state, specified by Eqs. (3.8)-(3.11). The line of reasoning is clearly the same also for the resource $\tilde{\sigma}_v$ specified by Eq.s (3.14)-(3.16). We may re-organize an adaptive protocol in such a way that each transmission through $\mathcal{E}_{\eta,v}$ is replaced by its resource state σ_v. At the same time, each teleportation-LOCC $\mathcal{T}_\eta$ is included in the adaptive LOCCs of the protocol, which are all collapsed into a single LOCC $\bar{\Lambda}_\eta$ (trace-preserving after averaging over all measurements). In this way, we may decompose the output state $\rho^n_{\mathbf{ab}} := \rho_{\mathbf{ab}}(\mathcal{E}^{\otimes n}_{\eta,v})$ as [5]

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}_\eta(\sigma_v^{\otimes n}) \ . \tag{3.22}$$

The computation of $E_R(\rho^n_{\mathbf{ab}})$ can now be remarkably simplified. In fact, we may write

$$\begin{aligned} E_R(\rho^n_{\mathbf{ab}}) &= \inf_{\sigma_{\text{sep}}} S(\rho^n_{\mathbf{ab}}||\sigma_{\text{sep}}) \\ &\overset{(1)}{\leq} \inf_{\sigma_{\text{sep}}} S[\bar{\Lambda}_\eta(\sigma_v^{\otimes n})||\bar{\Lambda}_\eta(\sigma_{\text{sep}})] \\ &\overset{(2)}{\leq} \inf_{\sigma_{\text{sep}}} S(\sigma_v^{\otimes n}||\sigma_{\text{sep}}) = E_R(\sigma_v^{\otimes n}), \end{aligned} \tag{3.23}$$

where: (1) we consider the fact that $\bar{\Lambda}_\eta(\sigma_{\text{sep}})$ form a subset of specific separable states, and (2) we use the monotonicity of the relative entropy under the trace-preserving LOCC $\bar{\Lambda}_\eta$. Therefore, by replacing in Eq. (2.38), we get rid of the optimization over the protocol (disappearing with $\bar{\Lambda}_\eta$) and we may write

$$K(\mathcal{E}_{\eta,v}) \leq \lim_n \frac{E_R(\sigma_v^{\otimes n})}{n} := E_R^\infty(\sigma_v) \leq E_R(\sigma_v) \ , \tag{3.24}$$

where we use the fact that the regularized REE is less than or equal to the REE. Thus, we may write the following theorem:

Theorem 3.2.1 ([5]) *Consider a phase-insensitive bosonic Gaussian channel $\mathcal{E}_{\eta,v}$, which is stretchable into a two-mode Gaussian state σ_v as given in Eqs. (3.8)-(3.11). Its secret-key capacity must satisfy the bound*

$$K(\mathcal{E}_{\eta,v}) \leq E_R(\sigma_v) := \inf_{\sigma_{sep}} S(\sigma_v||\sigma_{sep}) \ . \tag{3.25}$$

It is interesting to note that the new bound in Eq. (3.25) cannot beat the asymptotic bound established in the previous Chapter for bosonic channels, i.e.,

$$K(\mathcal{E}_{\eta,v}) \leq \inf_{\sigma^\mu_{\text{sep}}} \liminf_{\mu\to+\infty} S(\rho^\mu_{\mathcal{E}_{\eta,v}}||\sigma^\mu_{\text{sep}}), \tag{3.26}$$

where $\rho^\mu_{\mathcal{E}_{\eta,v}}$ is a Choi-approximating sequence, and σ^μ_{sep} is an arbitrary sequence of separable states converging in trace norm. This can be seen from a quite simple argument. In fact, according to Eqs. (2.28) and (3.7), we may write

$$\begin{aligned} \rho^\mu_{\mathcal{E}_{\eta,v}} &= \mathcal{I}\otimes\mathcal{E}_{\eta,v}(\Phi^\mu) \\ &= \mathcal{I}\otimes\mathcal{T}_\eta(\Phi^\mu\otimes\sigma_v) = \Delta(\sigma_v), \end{aligned} \tag{3.27}$$

where Δ is a trace-preserving LOCC. Therefore, $E_R(\rho^{\mu}_{\mathcal{E}_{\eta,v}}) \leq E_R(\sigma_v)$ and this relation is inherited by the bounds above. Notwithstanding this *no go* for the finite-resource simulation, we show that its performance is good and reasonably approximates the infinite-energy bounds that are found via Eq. (3.26).

3.3 Finite-resource bounds for phase insensitive Gaussian channels

We now proceed by computing the REE in Eq. (3.25) for the class of single-mode phase-insensitive Gaussian channels. For this, we exploit the formula of Eq. (2.109), which has been derived in [82].

Again, the computation of the REE involves an optimization over the set of separable states. Following the recipe of Sec. 2.7.2, we may construct a good candidate directly starting from the CM in Eq. (3.8). This separable state has CM with the same diagonal blocks as in Eq. (3.8), but where the off-diagonal term is replaced as follows (see Eq. (2.111))

$$c \rightarrow c_{\text{sep}} := \sqrt{(a-1/2)(b-1/2)} \ . \tag{3.28}$$

By using this separable state σ^*_{sep} we may write the further finite-resource upper bounds for both σ_v and $\tilde{\sigma}_v$

$$K(\mathcal{E}_{\eta,v}) \leq E_R(\sigma_v) \leq E^*_R(\sigma_v) = S(\sigma_v||\sigma^*_{\text{sep}}) =: \Psi(\mathcal{E}) \ , \tag{3.29}$$

$$K(\mathcal{E}_{\eta,v}) \leq E_R(\tilde{\sigma}_v) \leq E^*_R(\tilde{\sigma}_v) = S(\tilde{\sigma}_v||\sigma^*_{\text{sep}}) \ . \tag{3.30}$$

In particular for Eq. (3.30) we can fix the purity p and derive a further upper bound on the secret key capacity. To do so, let us call $\mathcal{S}_p$ the set of resource states $\tilde{\sigma}_v$ with purity equal to p and satisfying Eqs. (3.14)-(3.16). Then, for any p we have

$$K(\mathcal{E}_{\eta,v}) \leq \Upsilon_p := \min_{\tilde{\sigma}_v \in \mathcal{S}_p} S(\tilde{\sigma}_v\|\sigma^*_{\text{sep}}) \ . \tag{3.31}$$

Since for $p \rightarrow 0$, the resource state $\tilde{\sigma}_v$ approaches the Choi state of the channel, we clearly have that $\Upsilon_{p\rightarrow 0}$ coincides with the entanglement $\mathbf{\Phi}(\mathcal{E}_{\eta,v})$ flux of the channel.

In what follows, we compute these bound for the various types of phase-insensitive Gaussian channels and for the two different finite-energy parametrization of the resource states σ_v and $\tilde{\sigma}_v$.

3.3.1 Thermal-loss channel

In terms of the statistical moments, the action of the thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$ can be described by the matrices in Eq. (3.2) with parameter $v = (1-\eta)(\bar{n}+1/2)$. This means that the squeezing parameter r of the resource state reads

$$r = \frac{1}{2}\ln\left[\frac{\eta+1}{(2\bar{n}+1)\,(1-\eta)}\right] \ . \tag{3.32}$$

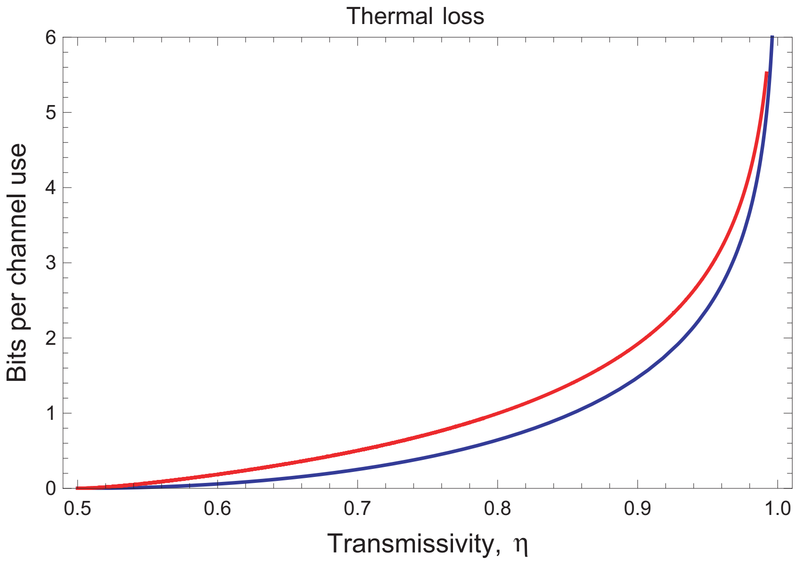

Figure 3.1: Finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ on the secret-key capacity of the thermal loss channel (red upper curve) as a function of the transmissivity η, compared with the infinite-energy bound $\mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}})$ (blue lower curve) derived in Eq. (2.116). The curves are plotted for $\bar{n} = 1$ thermal photons. This is Fig. 1 from Ref. [5].

By combining this relation with the ones in Eq. (3.10) and computing the relative entropy, we find[1] the finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ which is plotted in Fig. 3.1 and therein compared with the infinite-energy bound $\mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}})$ of Eq. (2.116), which we recall here

$$\mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}}) = -\log_2[(1-\eta)\eta^{\bar{n}}] - h(\bar{n}), \tag{3.33}$$

for $\bar{n} < \eta/(1-\eta)$ and zero otherwise, and we set $h(x) := (x+1)\log_2(x+1) - x\log_2 x$. It is clear that we have

$$K(\mathcal{E}_{\eta,\bar{n}}) \leq \mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}}) \leq \Psi(\mathcal{E}_{\eta,\bar{n}}), \tag{3.34}$$

[1] The analytical expresssion is too cumbersome to be reported in this Thesis

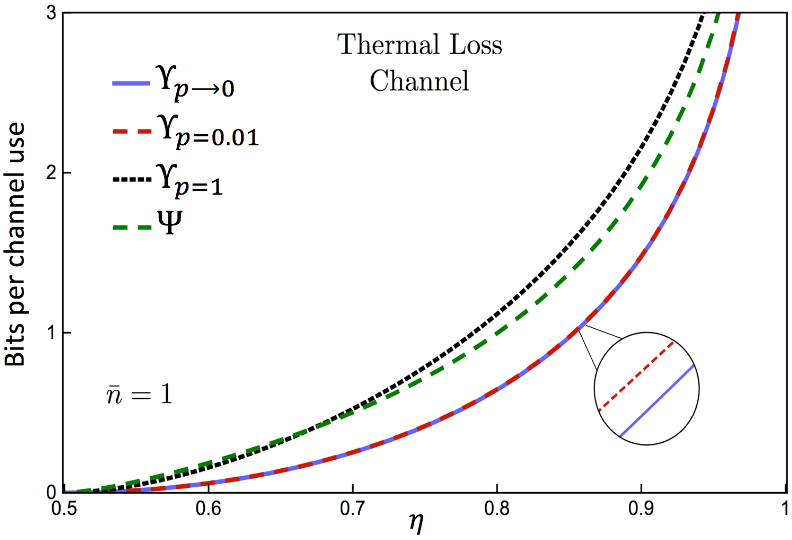

Figure 3.2: Finite-resource bound Υ_p on the secret-key capacity of the thermal loss channel. The blue line represents the infinite-energy bound $\Upsilon_{p\to 0} \equiv \mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}})$, while the green dashed line is the approximate finite-energy bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ of Fig. 3.1. We then show the optimized finite-energy upper bound Υ_p, plotted for purity $p=1$ (black dashed line) and $p=0.01$ (red dashed line). This is Fig. 3b from Ref. [6].

but the two upper bounds are reasonably close.

We then compute numerically the upper bound Υ_p for the thermal-loss channel, by fixing the purity p of the resource state and optimizing over the remaining free parameters $\tilde{a}$, $\tilde{b}$ and $\tilde{c}$ as in Eq. (3.31). As shown in Fig. 3.2, the finite-energy upper bound Υ_p rapidly approaches $\mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}})$ for decreasing purity p and due to the fact that $\mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}}) = \lim_{p\to 0}\Upsilon_p$ we can make the finite energy approximation, that relies on the resource $\tilde{\sigma}_v$, as close as needed.

3.3.2 Noisy amplifier channel

By repeating the previous calculations for the noisy (thermal) amplifier channel, we find the finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ plotted in Fig. 3.3 and where it is compared with the infinite-energy bound of Eq. (2.119), that we recall here

$$\mathbf{\Phi}(\mathcal{E}_{\eta,\bar{n}}) = \log_2\left(\frac{\eta^{\bar{n}+1}}{\eta-1}\right) - h(\bar{n}), \tag{3.35}$$

for $\bar{n} < (\eta-1)^{-1}$ and zero otherwise. In Fig. 3.4 we show the behaviour of Υ_p for the noisy amplifier.

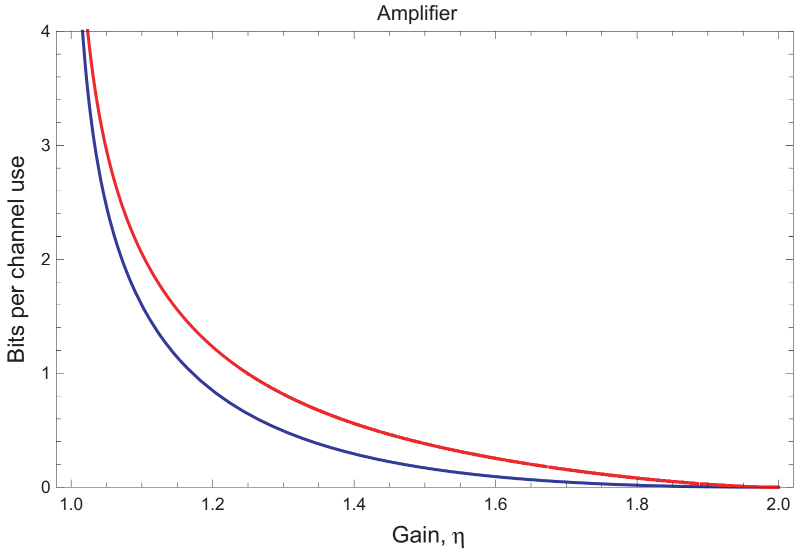

Figure 3.3: Finite-resource bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ on the secret-key capacity of the noisy amplifier channel (red upper curve) as a function of the gain η, compared with the optimal bound for infinite energy $\boldsymbol{\Phi}(\mathcal{E}_{\eta,\bar{n}})$ (blue lower curve). The two curves are plotted for $\bar{n} = 1$ thermal photons. This is Fig. 2 from [5].

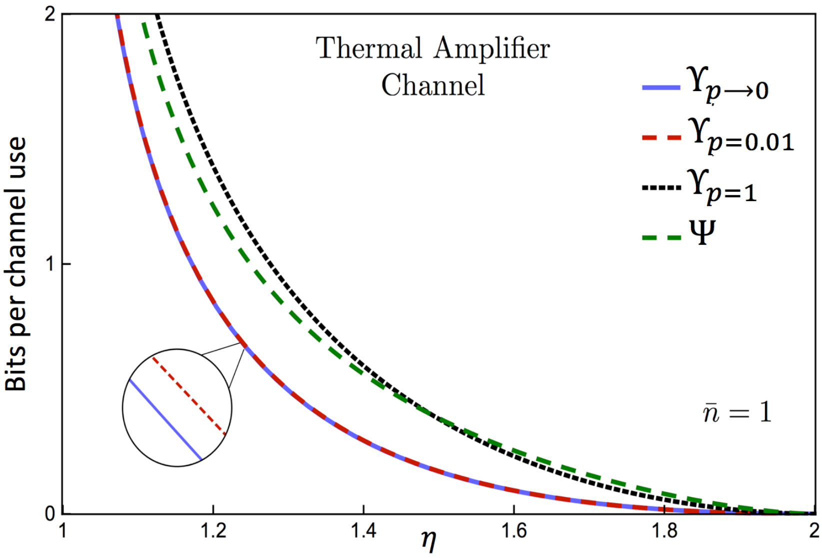

Figure 3.4: Finite-resource bound Υ_p on the secret-key capacity of the noisy amplifier channel. The blue line represents the infinite-energy bound $\Upsilon_{p\to0} \equiv \boldsymbol{\Phi}(\mathcal{E}_{\eta,\bar{n}})$, while the green dashed line is the approximate finite-energy bound $\Psi(\mathcal{E}_{\eta,\bar{n}})$ of Fig. 3.3. We then show the optimized finite-energy upper bound Υ_p, plotted for purity $p = 1$ (black dashed line) and $p = 0.01$ (red dashed line). Thermal noise is again equal to $\bar{n} = 1$. This is Fig. 3d from Ref. [6].

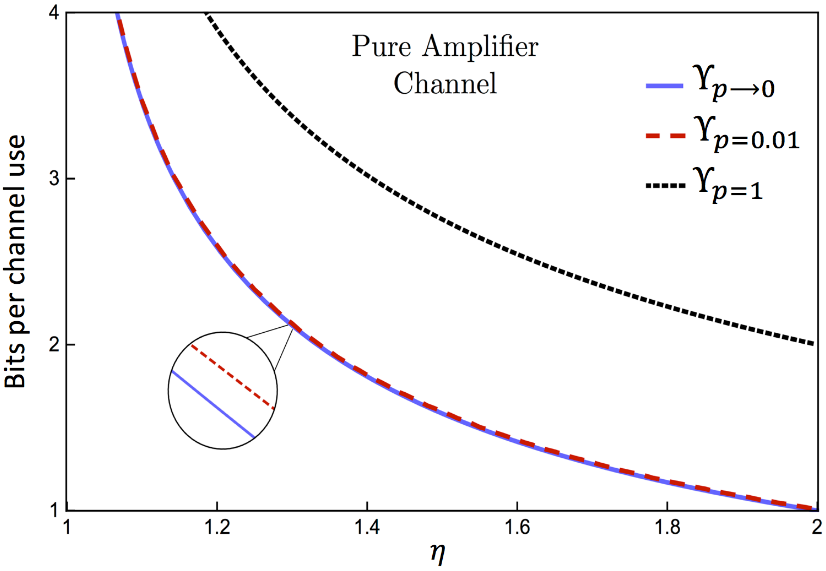

Figure 3.5: Finite-resource bound Υ_p on the secret-key capacity of the pure amplifier channel. The blue line represents the infinite-energy bound $\Upsilon_{p\to 0} \equiv K(\eta)$. We then show the optimized finite-energy upper bound Υ_p, plotted for purity $p = 1$ (black dashed line) and $p = 0.01$ (red dashed line). This is Fig. 3c from Ref. [6].

Pure amplifier channel

As we already mentioned, the resource state described by Eqs. (3.14)-(3.16) allows to simulate at finite-energy the pure amplifier channel. This channel is distillable, as we already know, and its secret key capacity is given by Eq. (2.121)

$$K(\eta) = -\log_2(1 - \eta^{-1}) \tag{3.36}$$

By computing Υ_p for the pure (quantum-limited) amplifier we obtain the plot of Fig. 3.5

3.3.3 Additive-noise Gaussian channel

This channel $\mathcal{E}_\xi$ is described by the matrices in Eq. (3.2) with $\eta = 1$ and $v = \xi$. The finite-resource bound $\Psi(\mathcal{E}_\xi)$ on the secret key capacity is plotted in Fig. 3.6 and compared with the infinite-energy bound of Eq. (2.122)

$$\mathbf{\Phi}(\mathcal{E}_\xi) = \frac{\xi - 1}{\ln 2} - \log_2 \xi, \tag{3.37}$$

for $\xi < 1$, while zero otherwise.

For the finite-energy upper bound Υ_p we employ the class of states specified in Eqs. (3.19)-(3.21). The corresponding behaviour is plotted in Fig. 3.7

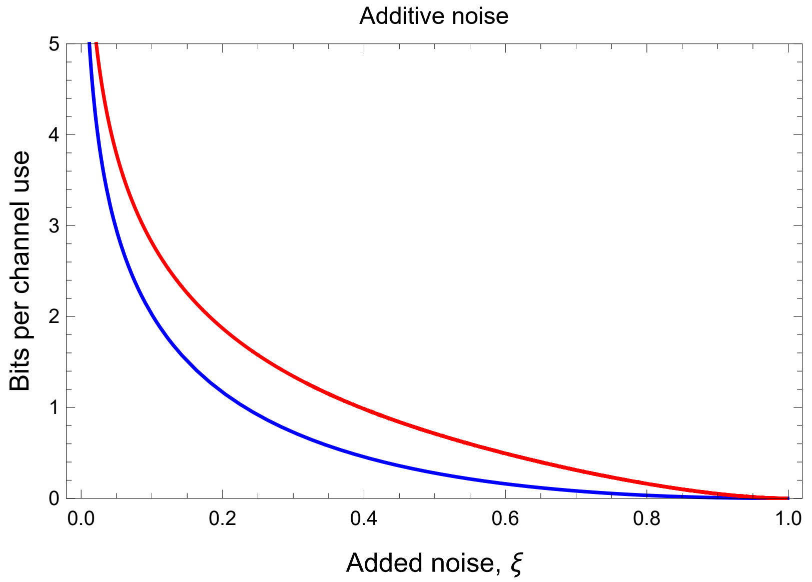

Figure 3.6: Finite-resource bound $\Psi(\mathcal{E}_\xi)$ on the secret-key capacity of the additive noise Gaussian channel (red upper curve) as a function of the added noise ξ, compared with the optimal bound for infinite energy $\mathbf{\Phi}(\mathcal{E}_\xi)$ (blue lower curve). This is Fig. 3 from Ref. [5].

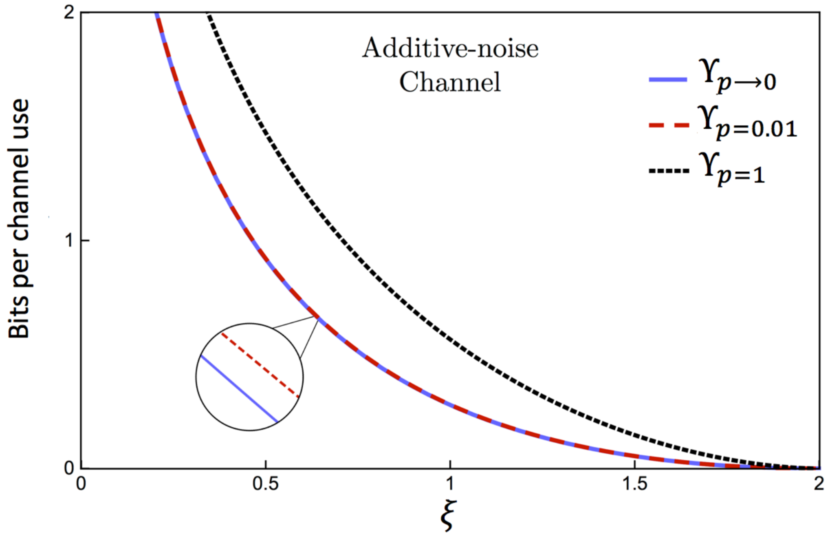

Figure 3.7: Upper bounds Υ_p to the secret-key capacity of the additive-noise Gaussian channel (secret bits per channel use versus added noise ξ). The lower blue line indicates the infinite-energy bound $\Upsilon_0 \equiv \mathbf{\Phi}(\mathcal{E}_\xi)$. Then, we show our improved finite-energy bound Υ_p which is plotted for purity $p = 1$ (black dashed line) and $p = 0.01$ (red dashed line). Note that the bound $\Psi(\mathcal{E}_\xi)$ coincides with the finite-bound $\Upsilon_{p=1}$. As we see for decreasing values of purity we can approximate Υ_0 as closely as we want, while keeping the energy of the resource state finite (despite being large). This is Fig. 4 from Ref. [6].

3.3.4 Pure-loss channel

Consider now the finite-resource teleportation simulation of a pure-losschannel. It is easy to check that we cannot use the parametrization inEq. (3.10). In fact, for a pure-loss channel, we have $v = (1-\eta)/2$ so that Eq. (3.11) provides $e^{2r} = (1+\eta)/(1-\eta)$. Replacing the latter in Eq. (3.10), we easily see that we have divergences (e.g., the denominator of b becomes zero). For the pure loss channel, we therefore use a different simulation, where the resource state is a two-mode squeezed state with CM [130]

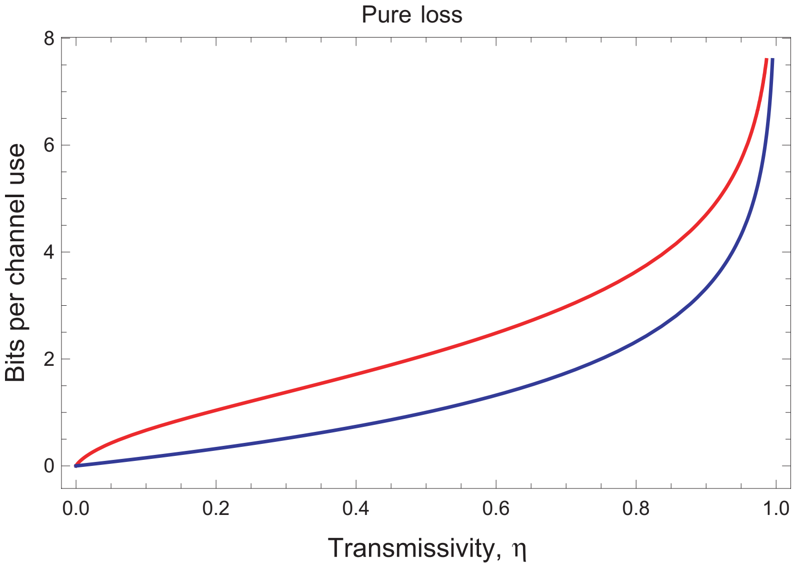

Figure 3.8: Finite-resource bound $\Psi(\mathcal{E}_\eta)$ on the secret-key capacity of the pure-loss channel (red upper curve) as a function of the transmissivity η, compared with its secret key capacity or PLOB bound $K(\eta) = -\log_2(1-\eta)$ (blue lower curve). This is Fig. 4 from Ref. [5].

$$\sigma_\eta = \begin{pmatrix} a\mathbf{I} & \sqrt{a^2 - 1/4}\mathbf{Z} \\ \sqrt{a^2 - 1/4}\mathbf{Z} & a\mathbf{I} \end{pmatrix}, \quad a = \frac{\eta + 1}{2(1-\eta)} . \tag{3.38}$$

By exploiting this resource state, we derive the bound $\Psi(\mathcal{E}_\eta)$ shown in Fig. 3.8, where it is compared with the secret-key capacity $K(\eta) = -\log_2(1-\eta)$ [1].

Regarding the computation of Υ_p we obtain the plot shown in Fig. 3.9.

3.4 Extension to repeater-assisted private communication

Here we extend the previous treatment to repeater-assisted private communication. We consider the basic scenario where Alice $\mathbf{a}$ and Bob $\mathbf{b}$ are connected by a chain of N quantum repeaters $\{\mathbf{r}_1, \dots, \mathbf{r}_N\}$, so that there are a total of $N+1$ quantum channels $\{\mathcal{E}_i\}$

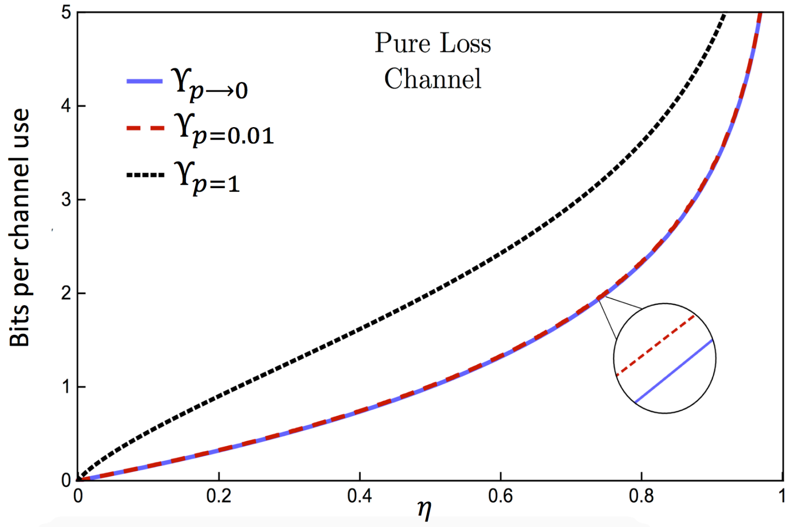

Figure 3.9: Finite-resource bound Υ_p of the pure-loss channel on the secret-key capacity of the pure-loss channel as a function of the transmissivity. Note that the bound $\Psi(\mathcal{E}_\eta)$ shown in Fig. 3.8 coincides with the finite-energy bound $\Upsilon_{p=1}$ (black dashed line). This is Fig. 3a from Ref. [6].

between them. Assume that these are phase-insensitive Gaussian channels $\mathcal{E}_i := \mathcal{E}_{\eta_i,\nu_i}$ with parameters (η_i, v_i). The most general adaptive protocol for key distribution through the chain is described in Ref. [27] and goes as follows.

Alice, Bob and all the repeaters prepare their local registers $\{\mathbf{a}, \mathbf{r}_1, \ldots, \mathbf{r}_N, \mathbf{b}\}$ into a global initial state ρ^0 by means of a network LOCC Λ_0, where each node in the chain applies LOs assisted by unlimited and two-way CCs with all the other nodes. In the first transmission, Alice picks a system $a_1 \in \mathbf{a}$ and sends it to the first repeater; after another network LOCC Λ_1, the first repeater communicates with the second repeater; then there is another network LOCC Λ_2 and so on, until Bob is eventually reached, which terminates the first use of the chain.

After n uses of the chain, we have a sequence of network LOCCs $\mathcal{L}$ defining the protocol and an output state $\rho^n_{\mathbf{ab}}$ for Alice and Bob which approximates some target private state with nR_n bits. By taking the limit for large n and optimizing over the protocols, we define the end-to-end or repeater-assisted secret-key capacity [27]

$$K(\{\mathcal{E}_i\}) = \sup_{\mathcal{L}} \lim_{n} R_n \ . \tag{3.39}$$

As shown in Ref. [27], we may extend the upper bound of Eq. (2.38). Then, we may use teleportation stretching and optimize over cuts of the chain, to simplify the bound to a single-letter quantity.

The network-reduction technique of Ref. [27] can be implemented by using the specific finite-resource simulation of Eq. (5.29), which leads to the following possible decompositions of the output state

$$\rho^n_{\mathbf{ab}} = \bar{\Lambda}_i(\sigma_{v_i}^{\otimes n}), \quad \text{for any } i = 1, \ldots, N, \tag{3.40}$$

where $\bar{\Lambda}_i$ is a trace-preserving LOCC and σ_{v_i} is the resource state associated with the ith Gaussian channel. By repeating the derivation of Ref. [27], this leads to

$$K(\{\mathcal{E}_i\}) \leq \min_i E_R(\sigma_{v_i}) \leq \min_i S(\sigma_{v_i}||\tilde{\sigma}_{i,\text{sep}}) := \Psi(\{\mathcal{E}_i\}) \ , \tag{3.41}$$

where Ψ is the upper bound coming from our choice of the separable state $\tilde{\sigma}_{i,\text{sep}}$ in the REE. This upper bound needs to be compared with the one $\Phi(\{\mathcal{E}_i\})$ obtained in the limit of infinite energy [27]. As an example, consider an additive-noise Gaussian channel with noise variance ξ. Let us split the communication line by using N "equidistant" repeaters, in such a way that each link is an additive-noise Gaussian channel $\mathcal{E}_i$ with the same variance $\xi_i = \xi/(N+1)$. It is easy to check that this is the optimal configuration for the repeaters. From Eq. (3.41), we derive $\Psi(\{\mathcal{E}_i\}) = \Psi(\mathcal{E}_{\xi/(N+1)})$. This bound is plotted in Fig. 3.10 where we can se an acceptable approximation of the corresponding infinite-energy bound $\Phi(\{\mathcal{E}_i\})$.

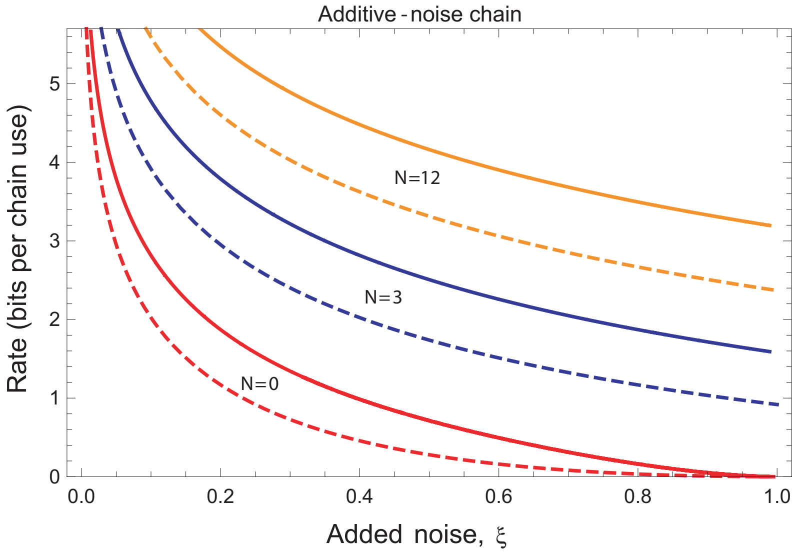

Figure 3.10: Secret-key capacity of a chain of N equidistant repeaters creating $N+1$ additive-noise Gaussian channels with variances $\xi_i = \xi/(N+1)$. We compare the finite-resource upper bound $\Psi(\{\mathcal{E}_i\})$ (solid lines) with the infinite-energy upper bound $\Phi(\{\mathcal{E}_i\})$ (dashed lines) for different values of N as a function of the overall added noise of the chain ξ. This is Fig. 5 from Ref. [5].

3.5 Finite number of channel uses

Consider an adaptive (n, ϵ)-protocol of key generation, meaning that Alice and Bob uses n times the channel and achieve a target state which is ϵ-close to a private state with $R_{n,\epsilon}$ secret bits. In particular, assume that the channel is a thermal-loss channel $\mathcal{L}$ with transmissivity τ and noise $v = 2\bar{n} + 1$. We can then simulate the channel by teleporting over our resource state $\hat{\rho}_{\tau,v}$; next we may apply teleportation stretching to the adaptive protocol, and compute the REE on its simplified output in order to get a single-letter upper bound to the n-use ϵ-secure secret-key capacity of the channel $K_{n,\epsilon}(\mathcal{L})$.

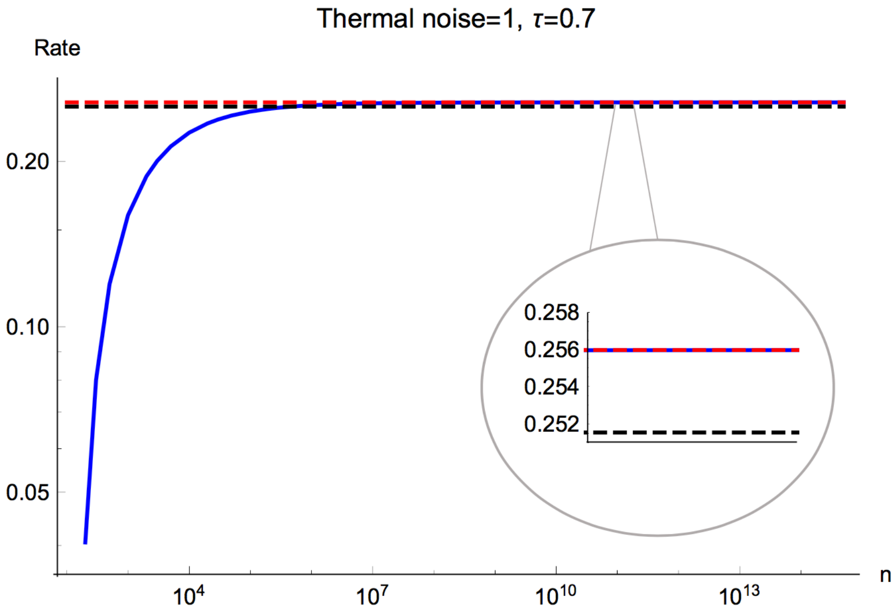

Figure 3.11: Upper bound to the n-use ϵ-secure secret-key capacity of the thermal-loss channel with $\tau = 0.7$ and $\bar{n} = 1$. We assume $\epsilon = 10^{-10}$ and purity $\mu = 10^{-4}$. We see how $\mathbf{\Phi}_n(\tau, v, \epsilon, p)$ (blue solid curve) tends to the asymptotic value Υ_p for large n (red dashed line), which is slightly above the infinite-energy bound Υ_0(black dashed line). This is Fig. A1 from Ref. [6].

Building on this recipe, one can write the following expansion in n

$$\begin{aligned} K_{n,\epsilon}(\mathcal{L}) &\leq \mathbf{\Phi}_n(\tau, v, \epsilon, \mu) \\ &:= \Upsilon_p + \sqrt{n^{-1}\mathcal{E}_V(\hat{\rho}'_{\tau,v})}F(\epsilon) + O\left(\frac{\log n}{n}\right), \end{aligned} \tag{3.42}$$

where Υ_p is the finite-energy bound asymptotic in n for fixed purity p computed over an optimal resource state $\hat{\rho}'_{\tau,v}$, $\mathcal{E}_V(\hat{\rho}'_{\tau,v})$ is its relative entropy variance, and F is the inverse of the cumulative Gaussian distribution, namely

$$F(\epsilon) = \sup\{a \in \mathbb{R}\ | f(a) \leq \epsilon\}\ , \tag{3.43}$$

$$f(a) = (2\pi)^{-1/2} \int_{-\infty}^{a} dx \exp(-x^2/2)\ . \tag{3.44}$$

In Fig. 3.11, we numerically plot the upper bound $\mathbf{\Phi}_n(\tau, v, \epsilon, p)$ versus n uses of a thermal-loss channel with transmissivity $\tau = 0.7$ and mean thermal number $\bar{n} = 1$, and assuming $\epsilon = 10^{-10}$. Our resource state is chosen with purity $p = 10^{-4}$ and optimized over the remaining free parameter. The non-asymptotic bound is compared with the asymptotic bound Υ_p and the infinite-energy bound Υ_0.

Chapter 4

Multi-point quantum communication

The goal of the present Chapter is to extend the “REE+teleportation” methodology [1] to a more complex communication scenario [7], in particular that of a single-hop quantum network, where multiple senders and/or receivers are involved. The basic configurations are represented by the quantum broadcast channel [131–133] where information is broadcast from a single sender to multiple receivers, and the quantum multiple-access channel [134], where multiple senders communicate with a single receiver. More generally, we also consider the combination of these two cases, where many senders communicate with many receivers in a sort of all-in-all quantum communication or quantum interference channel. In practical implementations, this may represent a quantum bus [135, 136] where quantum information is transmitted among an arbitrary number of qubit registers.

In all these multipoint scenarios, we characterize the most general protocols for entanglement distillation, quantum communication and key generation, assisted by adaptive LOCCs. This leads to the definition of the two-way capacities $\mathcal{C} = D_2$, Q_2, K between any pair of sender and receiver. We then consider those quantum channels (for broadcasting, multiple-accessing, and all-in-all communication) which are teleportation-covariant. For these channels, we can completely reduce an adaptive protocol into a block form involving a tensor product of Choi matrices. Combining this reduction with the REE, we then bound their two-way capacities by means of the REE of their Choi matrix, therefore extending the methods of Chapter 2 to multipoint communication.

Our upper bounds applies to both discrete-variable (DV) and continuous-variable (CV) channels. As an example, we consider the specific case of a 1-to-M thermal-loss broadcast channel through a sequence of beamsplitters subject to thermal noise. In particular, we discuss how that the two-way capacities Q_2, D_2 and K between the sender and each receiver are all bounded by the first point-to-point channel in the "multisplitter". This bottleneck result can be extended to other Gaussian broadcast channels. In the specific case of a lossy broadcast channel (without thermal noise), we find a straighforward extension of the fundamental rate-loss scaling, so that any sender-receiver capacity is bounded by $-\log_2(1-\eta)$ with η being the transmissivity of the first beamsplitter. These results have been achieved in Ref. [7].

4.1 Quantum broadcast channel

Here we consider quantum and private communication in a single-hop point-to-multipoint network. We adapt our techniques to bound the optimal rates that are achievable in adaptive protocols involving multiple receivers. For the sake of simplicity, we present the theory for non-asymptotic simulations. The theoretical treatment of asymptotic simulations goes along the lines described previously in Sec. 2.4.1 and is discussed afterwards. Consider a quantum broadcast channel $\mathcal{E}$ where Alice (local register $\mathbf{a}$) transmits a system $a \in \mathbf{a}$ to M different Bobs; the generic ith Bob (with $i = 1, \dots, M$) receives an output system b^i which may be combined with a local register $\mathbf{b}^i$ for further processing. Denote by $\mathcal{D}(\mathcal{H}_s)$ the space of density operators defined over the Hilbert space $\mathcal{H}_s$ of quantum system s. Then, the quantum broadcast channel is a completely-positive trace preserving (CPTP) map from Alice's input space $\mathcal{D}(\mathcal{H}_a)$ to the Bobs' output space $\mathcal{D}(\otimes_i \mathcal{H}_{b^i})$. The most general adaptive protocol over this channel goes as follows.

All the parties prepare their initial systems by means of a LOCC Λ_0. Then, Alice picks the first system $a_1 \in \mathbf{a}$ which is broadcast to all Bobs $a_1 \to \{b_1^i\}$ through channel $\mathcal{E}$. This is followed by another LOCC Λ_1 involving all parties. Bobs' ensembles are updated as $b_1^i \mathbf{b}^i \to \mathbf{b}^i$. Then, there is the second broadcast $\mathbf{a} \ni a_2 \to \{b_2^i\}$ through $\mathcal{E}$, followed by another LOCC Λ_2 and so on. After n uses, Alice and the ith Bob share an output state $\rho^n_{\mathbf{ab}^i}$ which is epsilon-close to a target state of nR_i^n bits. The generic broadcast capacity for the ith Bob is defined by maximizing the asymptotic rate over all the adaptive LOCCs $\mathcal{P} = \{\Lambda_0, \Lambda_1, \dots\}$, i.e., we have [7]

$$\mathcal{C}(\mathcal{E}_i) = \mathcal{C}^i := \sup_{\mathcal{P}} \lim_{n\to\infty} R_i^n \ , \tag{4.1}$$

where $\mathcal{E}_i$ is the channel from Alice to the i-th Bob. By specifying the adaptive protocol to a particular target state, i.e., to a particular task (entanglement distribution, reliable transmission of quantum information, key generation or deterministic transmission of secret bits), one derives the entanglement-distribution broadcast capacity (D_2^i), the quantum broadcast capacity (Q_2^i), the secret-key broadcast capacity (K^i), and the private broadcast capacity (P_2^i). These are all assisted by unlimited two-way CCs between the parties and it is easy to check that they must satisfy $D_2^i = Q_2^i \leq K^i = P_2^i$. In order to bound the previous capacities, let us introduce the notion of teleportation-covariant broadcast channel. It is explained for the case of two receivers, Bob and Charlie, with the extension to arbitrary M receivers being just a matter of technicalities. This is a broadcast channel which suitably commutes with teleportation. Formally, this means that, for any teleportation unitary U_k at the channel input, we may write [7]

$$\mathcal{E}(U_k \rho U_k^\dagger) = (B_k \otimes C_k)\mathcal{E}(\rho)(B_k \otimes C_k)^\dagger \ , \tag{4.2}$$

for unitaries B_k and C_k at the two outputs. If this is the case, it is immediate to prove that $\mathcal{E}$ can be simulated by a generalized teleportation protocol over its Choi matrix

$$\rho_{\mathcal{E}} = \mathcal{I}_A \otimes \mathcal{E}_{A'}(\Phi_{AA'}), \tag{4.3}$$

where the latter is defined by sending half of an EPR $\Phi_{AA'}$ through the broadcast channel. In other words, the broadcast channel is Choi-stretchable and its LOCC simulation is based on teleportation. See Fig. 4.1.

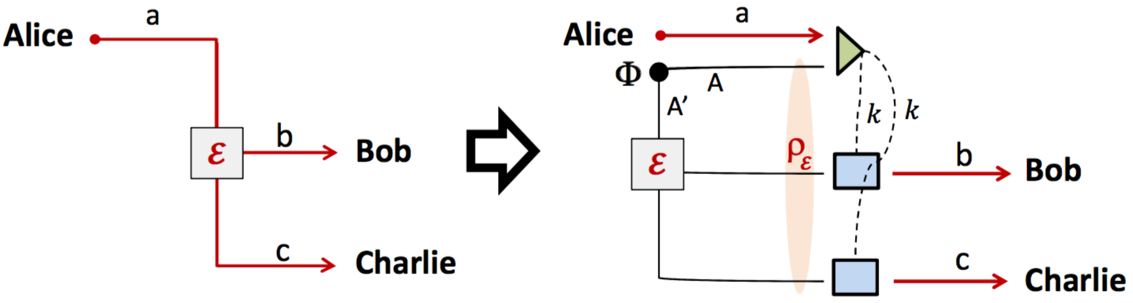

Figure 4.1: Simulation of a teleportation-covariant quantum broadcast channel. We may replace the broadcast channel $\mathcal{E} : a \to bc$ by teleportation over its Choi matrix $\rho_{\mathcal{E}}$, with CCs to Bob and Charlie, who will implement correction unitaries. The broadcast channel is therefore Choi-stretchable and its LOCC simulation is based on teleportation. This is Fig. 3 from Ref. [7].

We may now simplify any adaptive protocol performed over a teleportation-covariant broadcast channel. The steps of the procedure are shown in Fig. 4.2. As a result, the total output state of Alice, Bob and Charlie can be decomposed in the form

$$\rho^n_{\mathbf{abc}} := \rho_{\mathbf{abc}}(\mathcal{E}^{\otimes n}) = \bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right) \ , \tag{4.4}$$

where $\bar{\Lambda}$ is a trace-preserving LOCC. If we now trace one of the two receivers, e.g., Charlie, we still have a trace-preserving LOCC between Alice and Bob, and we may write the following

$$\rho^n_{\mathbf{ab}} = \mathrm{Tr}_{\mathbf{c}}\bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right) = \bar{\Lambda}_{\mathbf{a|bc}}\left(\rho_{\mathcal{E}}^{\otimes n}\right) \ , \tag{4.5}$$

where $\bar{\Lambda}_{\mathbf{a|bc}}$ is local with respect to the cut $\mathbf{a|bc}$ [7].

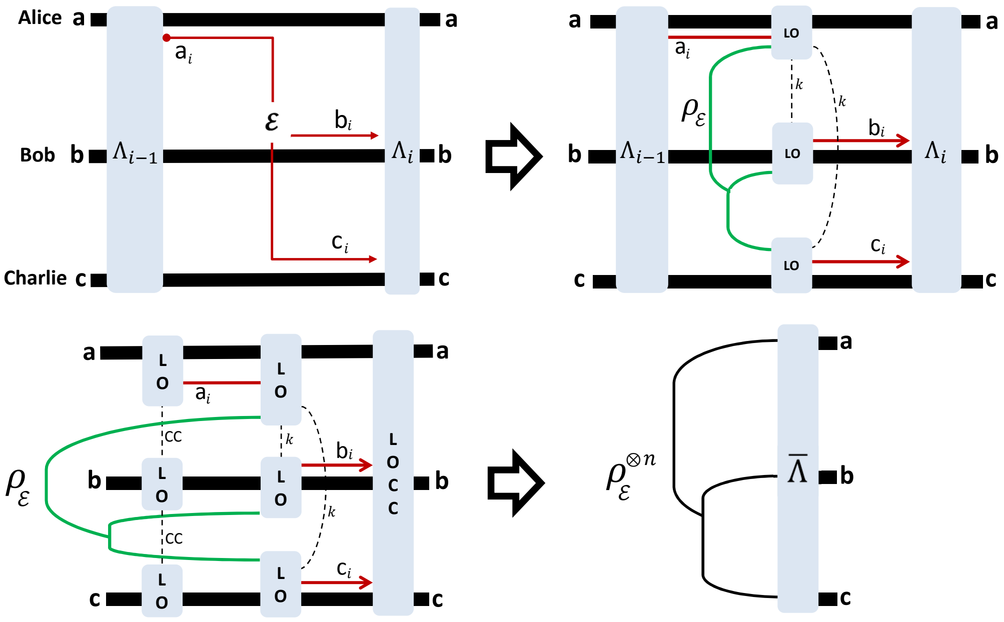

Figure 4.2: Stretching of an adaptive protocol over a teleportation-covariant quantum broadcast channel. **Top panels**. The generic ith transmission $a_i \rightarrow \{b_i, c_i\}$ over the broadcast channel $\mathcal{E}$ (red line) is replaced by a teleportation over its Choi matrix $\rho_{\mathcal{E}}$ (following the procedure shown in Fig. 4.1). The input system and the upper half of the Choi matrix are subject to a Bell detection which becomes part of Alice's LO (upper LO). The result of the Bell detection k is classically communicated to Bob and Charlie so that they can apply two correction unitaries which are then included into their respective LOs (middle and lower LOs). **Bottom panels**. The Choi matrix is stertched in time out of the adaptive LOCCs which are then collapsed into a single trace-preserving LOCC. After n uses, we can express the output in terms of n copies of the Choi matrix $\rho_{\mathcal{E}}$ of the broadcast channel, plus a trace-preserving single final LOCC $\bar{\Lambda}$ as in Eq. (4.4). This is Fig. 4 from Ref. [7].

Let us now compute the REE of Alice and Bob's output state $\rho^n_{\mathbf{ab}}$. Using Eq. (4.5) and the monotonicity of the REE under $\bar{\Lambda}_{\mathbf{a}|\mathbf{bc}}$, we derive

$$\begin{aligned} E_R(\rho^n_{\mathbf{ab}}) &:= \inf_{\sigma_s(\mathbf{a}|\mathbf{b})} S\left(\rho^n_{\mathbf{ab}}||\sigma_s\right) \\ &\leq \inf_{\sigma_s(\mathbf{a}|\mathbf{bc})} S\left(\rho^{\otimes n}_{\mathcal{E}}||\sigma_s\right) := E_{R(\mathbf{a}|\mathbf{bc})}(\rho^{\otimes n}_{\mathcal{E}}), \end{aligned} \tag{4.6}$$

where we call $E_{R(\mathbf{a}|\mathbf{bc})}$ the REE with respect to the bipartite cut $\mathbf{a}|\mathbf{bc}$. Note that the set of states $\{\sigma_s(\mathbf{a}|\mathbf{bc})\}$, separable between $\mathbf{a}$ and $\mathbf{bc}$, includes the set of states $\{\sigma_s(\mathbf{a}|\mathbf{b}|\mathbf{c})\}$ which are separable with respect to $\mathbf{a}$, $\mathbf{b}$ and $\mathbf{c}$. Therefore, we may write the further upper-bound

$$E_{R(\mathbf{a}|\mathbf{bc})}(\rho^{\otimes n}_{\mathcal{E}}) \leq \inf_{\sigma_s(\mathbf{a}|\mathbf{b}|\mathbf{c})} S\left(\rho^{\otimes n}_{\mathcal{E}}||\sigma_s\right) := E_R(\rho^{\otimes n}_{\mathcal{E}}). \tag{4.7}$$

For Alice and Bob ($i = B$), we can then exploit the weak converse bound in Eq. (2.38) where the optimization must be done over all the adaptive broadcast protocols. Combining this bound with Eqs. (4.6) and (4.7), we get

$$\mathcal{C}^B \leq \sup_{\mathcal{L}} \lim_n \frac{E_R(\rho^n_{\mathbf{ab}})}{n} \leq E^{\infty}_{R(\mathbf{a}|\mathbf{bc})}(\rho_{\mathcal{E}}) \leq E^{\infty}_R(\rho_{\mathcal{E}}), \tag{4.8}$$

where $E^{\infty}_R(\rho) := \lim_n n^{-1} E_R(\rho^{\otimes n})$ is the regularized version of the REE. Then, using the subadditive over tensor products, we may also write

$$E_R(\rho^n_{\mathbf{ab}}) \leq n E_{R(\mathbf{a}|\mathbf{bc})}(\rho_{\mathcal{E}}) \leq n E_R(\rho_{\mathcal{E}}), \tag{4.9}$$

which clearly leads to the single-letter upper bounds

$$\mathcal{C}^B \leq E_{R(\mathbf{a}|\mathbf{bc})}(\rho_{\mathcal{E}}) \leq E_R(\rho_{\mathcal{E}}). \tag{4.10}$$

We find the same bounds for the capacity of Alice and Charlie ($i = C$). In general, for arbitrary M receivers, we may extend the reasoning and write the following upper bounds for the capacity between Alice and the ith Bob [7]

$$\mathcal{C}^i \leq E_{R(\mathbf{a}|\mathbf{b}^1 \cdots \mathbf{b}^M)}(\rho_{\mathcal{E}}) \leq E_R(\rho_{\mathcal{E}}) := \mathbf{\Phi}(\mathcal{E}) \ , \tag{4.11}$$

where $\Phi(\mathcal{E})$ is the entanglement flux of the broadcast channel $\mathcal{E}$, defined as the REE of its Choi matrix $\rho_{\mathcal{E}}$.

4.1.1 Extension to continuous variables

By repeating the reasoning of Sec. 2.4.1 we can extend the simulation to bosonic broadcast channel. In fact, the error in the channel simulation can be propagated to the output state of the adaptive protocol, so that, for any energy constraint on the local registers, we may write the trace-norm limit

$$\left\| \rho^n_{\mathbf{abc}} - \bar{\Lambda}_\mu \left(\rho^{\mu \otimes n}_{\mathcal{E}} \right) \right\| \overset{\mu}{\to} 0, \tag{4.12}$$

where $\bar{\Lambda}_\mu$ is an imperfect stretching-LOCC associated with the imperfect teleportation LOCC $\mathcal{T}^\mu$. By tracing one of the outputs, e.g., Charlie, one gets

$$\left\| \rho^n_{\mathbf{ab}} - \bar{\Lambda}^{\mathbf{a}|\mathbf{bc}}_\mu \left(\rho^{\mu \otimes n}_{\mathcal{E}} \right) \right\| \overset{\mu}{\to} 0, \tag{4.13}$$

where $\bar{\Lambda}^{\mathbf{a}|\mathbf{bc}}_\mu$ is an imperfect stretching-LOCC associated with Alice and Bob, which is local with respect to the bipartite cut $\mathbf{a}|\mathbf{bc}$.

The next step is to extend the definition of REE to asymptotic states. In particular, we define

$$E_{R(\mathbf{a}|\mathbf{bc})}(\rho_{\mathcal{E}}) := \inf_{\sigma^\mu_s(\mathbf{a}|\mathbf{bc})} \liminf_{\mu \to +\infty} S(\rho^\mu_{\mathcal{E}} || \sigma^\mu_s), \tag{4.14}$$

where $\sigma^\mu_s(\mathbf{a}|\mathbf{bc})$ is an arbitrary converging sequence of states that is separable with respect to the cut $\mathbf{a}|\mathbf{bc}$. Then, we also define the entanglement flux of the bosonic broadcast channel as

$$\mathbf{\Phi}(\mathcal{E}) = E_R(\rho_{\mathcal{E}}) := \inf_{\sigma^\mu_s} \liminf_{\mu \to +\infty} S(\rho^\mu_{\mathcal{E}} || \sigma^\mu_s), \tag{4.15}$$

where σ^μ_s is an arbitrary converging sequence of separable states (with respect to all the local systems $\mathbf{a}|\mathbf{b}|\mathbf{c}$). By applying a direct extension of the weak converse bound in Eq. (2.38), we then derive the same result as in Eq. (4.10) for the capacity $\mathcal{C}^B$ between Alice and Bob, given that the REE quantities are suitably extended as in Eqs. (4.14) and (4.15). In general, for arbitrary M receivers, we have the corresponding extension of Eq. (4.11).

4.1.2 Thermal-loss quantum broadcast channel

Now that we have rigorously extended the treatment to CV systems, we study the example of a bosonic broadcast channel from Alice to M Bobs which introduces both loss and thermal noise. This is an optical scenario that may easily occur in practice. For instance, it may represent the practical implementation of a single-hop QKD network, where a party wants to share keys with several other parties for broadcasting private information. The latter may also be a common key to enable a quantum-secure conferencing among all the trusted parties.

One possible physical representation is a chain of $M+1$ beamsplitters with transmissivities $(\eta_0, \eta_1, \dots \eta_M)$ in which Alice's input mode A' subsequently interacts with $M+1$ modes

$(E_0, E_1, E_2, \ldots, E_M)$ described by thermal states $\rho_{E_i}(\bar{n}_i)$ with $\bar{n}_i$ mean number of photons. The M output modes $(B_1, B_2, \ldots, B_M)$ are then given to the different Bobs, with the extra modes E and E' being the leakage to the environment (or an eavesdropper). See Fig. 4.3 for a schematic representation of this thermal-loss broadcast channel $\mathcal{E} = \mathcal{E}_{A' \to B_1 \ldots B_M}$.

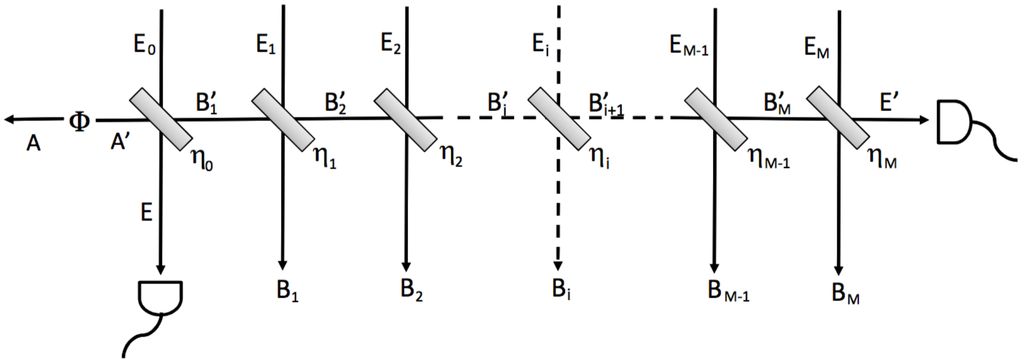

Figure 4.3: Thermal-loss quantum broadcast channel $\mathcal{E}_{A' \to B_1 \ldots B_M}$ from Alice (mode A') to M Bobs (modes $B_1, \ldots, B_M$), realized by a multi-splitter, i.e., a sequence of $M+1$ beamsplitters with transmissivities $(\eta_0, \eta_1, \ldots \eta_M)$. The environmental modes $E_0, E_1 \ldots, E_M$ are in thermal states. Modes E and E' describe leakage to the environment. This is Fig. 5 from Ref. [7].

The generic capacity $\mathcal{C}^i$ between Alice and the ith Bob is upper bounded by

$$\mathcal{C}^i \leq E_{R(A|B_1 \cdots B_M)}(\rho_{\mathcal{E}}) := \inf_{\sigma_s^\mu (A|B_1 \cdots B_M)} \liminf_{\mu \to +\infty} S(\rho_{\mathcal{E}}^\mu || \sigma_s^\mu), \tag{4.16}$$

where the state $\rho_{\mathcal{E}}^\mu := \mathcal{I}_A \otimes \mathcal{E}_{A' \to B_1 \ldots B_M}(\Phi_{AA'}^\mu)$ is the Choi-approximating state obtained by sending one half of a TMSV state $\Phi_{AA'}^\mu$, and $\sigma_s^\mu(A|B_1 \cdots B_M)$ is a converging sequence of states that are separable with respect to the cut $A|B_1 \cdots B_M$. Now notice that we may write

$$\rho_{\mathcal{E}}^\mu = \mathbf{L}_{A|B_1' E_1 \cdots E_M} \left[\rho_{\mathcal{E}_{A' \to B_1'}}^\mu \otimes \bigotimes_{i=1}^M \rho_{E_i}(\bar{n}_i) \right], \tag{4.17}$$

where $\rho_{\mathcal{E}_{A' \to B_1'}}^\mu := \mathcal{I}_A \otimes \mathcal{E}_{A' \to B_1'}(\Phi_{AA'}^\mu)$ is associated with the first beamsplitter, and $\mathbf{L}_{A|E_1 \cdots E_M}$ is a trace-preserving LOCC, local with respect to the cut $A|B_1' E_1 \cdots E_M$. Also note that, for any separable state $\sigma_s^\mu(A|B_1')$ we have that the output state

$$\tilde{\sigma}_s^\mu = \mathbf{L}_{A|B_1' E_1 \cdots E_M} \left[\sigma_s^\mu(A|B_1') \otimes \bigotimes_{i=1}^M \rho_{E_i}(\bar{n}_i) \right] \tag{4.18}$$

is separable with respect to the cut $A|B_1 \cdots B_M$. As a result we have that

$$\begin{aligned} E_{R(A|B_1\cdots B_M)}(\rho_{\mathcal{E}}) &\overset{(1)}{\leq} \inf_{\tilde{\sigma}^{\mu}_{s}(A|B_1\cdots B_M)} \liminf_{\mu\to+\infty} S(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s}) \\ &\overset{(2)}{\leq} \inf_{\sigma^{\mu}_{s}(A|B'_1)} \liminf_{\mu\to+\infty} S(\rho^{\mu}_{\mathcal{E}_{A'\to B'_1}}||\sigma^{\mu}_{s}) := \mathbf{\Phi}(\mathcal{E}_{A'\to B'_1}), \end{aligned} \tag{4.19}$$

where we use: (1) the fact that $\tilde{\sigma}^{\mu}_{s}(A|B_1 \cdots B_M)$ are specific types of $\sigma^{\mu}_{s}(A|B_1 \cdots B_M)$; and (2) monotonicity and additivity of the relative entropy with respect to the decompositions in Eqs. (4.17) and (4.18).

Because $\mathcal{E}_{A'\to B'_1}$ is a thermal-loss channel with transmissivity η_0 and mean photon number $\bar{n}_0$, we know its entanglement flux is bounded by

$$\mathbf{\Phi}(\mathcal{E}_{A'\to B'_1}) \leq -\log_2\left[(1-\eta_0)\eta_0^{\bar{n}_0}\right] - h(\bar{n}_0), \tag{4.20}$$

for $\bar{n}_0 < \eta_0/(1-\eta_0)$, while zero otherwise. Here we set

$$h(x) := (x+1)\log_2(x+1) - x\log_2 x. \tag{4.21}$$

Thus, we find that the capacity between Alice and the ith Bob must satisfy [7]

$$\mathcal{C}^i \leq \begin{cases} -\log_2\left[(1-\eta_0)\eta_0^{\bar{n}_0}\right] - h(\bar{n}_0) \quad \text{for } \bar{n}_0 < \frac{\eta_0}{1-\eta_0}, \\ \\ 0 \quad \text{for } \bar{n}_0 \geq \frac{\eta_0}{1-\eta_0}. \end{cases} \tag{4.22}$$

As expected, the first beamsplitter is a universal bottleneck which restricts the capacities between Alice and any of the receiving Bobs.

In the specific case of a lossy broadcast channel with no thermal noise ($n_i = 0$ for any i), we may specify Eq. (4.22) into the following simple bound

$$\mathcal{C}^i \leq -\log_2(1-\eta_0)\ . \tag{4.23}$$

Let us note that, contrary to another work [137], our analysis of the lossy broadcast channel builds upon a rigorous extension of channel simulation and teleportation stretching to CV systems, which includes a suitable generalization of the REE to asymptotic states.

Most importantly, notice that our derivation can be generalized to other bosonic broadcast channels, where the $M + 1$ beamsplitters are replaced by arbitrary Gaussian unitaries

$U_{A'E_0}, U_{B'_1E_1}, \ldots, U_{B'_M E_M}$. In this general case, we repeat the previous reasonings to find that the capacities must satisfy the bottleneck relation

$$\mathcal{C}^i \leq \mathbf{\Phi}(\mathcal{E}_{A' \to B'_1}), \tag{4.24}$$

where the latter is the entanglement flux of the first Gaussian channel $\mathcal{E}_{A' \to B'_1}$, determined by the action of the Gaussian unitary $U_{A'E_0}$ on the input mode A' and the thermal mode E_0.

4.2 Quantum multiple-access channel

Let us now study multipoint-to-point quantum communication, i.e., a quantum multiple-access channel from M senders (Alices) to a single receiver (Bob). This channel is a CPTP map from Alices' input space $\mathcal{D}(\otimes_i \mathcal{H}_{a^i})$ to Bob's output space $\mathcal{D}(\mathcal{H}_b)$. The most general adaptive protocol over this channel goes as follows. All the parties prepare their initial systems by means of a LOCC Λ_0. Then, the ith Alice picks the first system from her local ensemble, i.e., $a_1^i \in \mathbf{a}^i$. All Alice's input systems are sent through the quantum multiple-access channel $\mathcal{E}$ with output b_1 for Bob, i.e.,

$$a_1^1, \ldots, a_1^i, \ldots, a_1^M \overset{\mathcal{E}}{\to} b_1 \ . \tag{4.25}$$

This is followed by another LOCC Λ_1 involving all parties. Bob's ensemble is updated as $b_1\mathbf{b} \to \mathbf{b}$. Then, there is the second transmission $\{\mathbf{a}^i\} \ni \{a_2^i\} \to b_2$ through $\mathcal{E}$, followed by another LOCC Λ_2 and so on. After n uses, the ith Alice and Bob share an output state $\rho^n_{\mathbf{a}^i\mathbf{b}}$ which is epsilon-close to a target state with nR_i^n bits.

The generic multiple-access capacity for the ith Alice is defined by maximizing the asymptotic rate over all the adaptive LOCCs $\mathcal{P} = \{\Lambda_0, \Lambda_1, \ldots\}$, i.e., we have $\mathcal{C}^i := \sup_{\mathcal{P}} \lim_n R_i^n$. As before, by specifying the adaptive protocol to a particular task, one derives the entanglement distribution multiple-access capacity (D_2^i), the quantum multiple-access capacity (Q_2^i), the secret-key multiple-access capacity (K^i) and the private multiple-access capacity (P_2^i). These are all assisted by unlimited two-way CCs between the parties and satisfy $D_2^i = Q_2^i \leq K^i = P_2^i$.

Let us introduce the notion of teleportation-covariant multiple-access channel. For the sake of simplicity, this is explained for the case of two senders, with the extension to arbitrary M senders being just a matter of technicalities. We also consider the case of DV channels, with the extension to CV channels left implicit. A quantum multiple-access channel is teleportation-covariant if, for any teleportation unitaries, $U^1_{k_1}$ and $U^2_{k_2}$, we may write [7]

$$\mathcal{E}\left[(U^1_{k_1}\otimes U^2_{k_2})\rho(U^1_{k_1}\otimes U^2_{k_2})^\dagger\right]=V_k\mathcal{E}(\rho)V_k^\dagger, \tag{4.26}$$

for some unitary V_k, with k depending on both k_1 and k_2. If this is the case, then we can replace $\mathcal{E}$ with teleportation over its Choi matrix, which is defined by sending halves of two EPR states through the channel, i.e.,

$$\rho_{\mathcal{E}}=\mathcal{I}_{A^1A^2}\otimes\mathcal{E}_{A'^1A'^2}(\Phi_{A^1A'^1}\otimes\Phi_{A^2A'^2}). \tag{4.27}$$

See also Fig. 4.4 for further explanations.

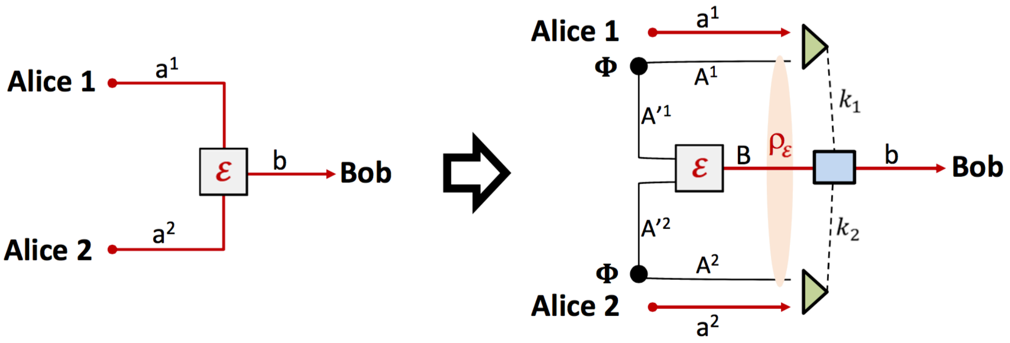

Figure 4.4: Simulation of a teleportation-covariant quantum multiple-access channel. We can replace the multiple-access channel $\mathcal{E}: a^1a^2\rightarrow b$ (left) by double teleportation over its tripartite Choi matrix $\rho_{\mathcal{E}}$ (right). This Choi matrix is obtained by sending halves (A'^1 and A'^2) of two EPR states Φ through $\mathcal{E}$, with output B. Then, systems a^1 and A^1 are subject to a Bell detection with outcome k_1. Similarly, systems a^2 and A^2 are subject to a Bell detection with outcome k_2. The outcomes are CCed to Bob who applies a correction unitary on system B. Since the channel is teleportation-covariant, i.e., it commutes with the teleportation unitaries according to Eq. (4.26), Bob's correction unitary V_k^{-1} on B re-generates the original channel $\mathcal{E}: a^1a^2\rightarrow b$. This is Fig. 6 from Ref. [7].

By using the channel simulation, we may fully simplify any adaptive protocol performed over a teleportation-covariant multiple-access channel $\mathcal{E}$. In fact, each transmission through $\mathcal{E}$ can be replaced by double teleportation on its Choi matrix $\rho_{\mathcal{E}}$, with the Bell detections and Bob's correction unitary being included in the LOCCs of the protocol. By stretching n uses of the adaptive protocol (see Fig. 4.5), we find that the total output state of Alice 1, Alice 2 and Bob reads [7]

$$\rho^n_{\mathbf{a}^1\mathbf{a}^2\mathbf{b}}=\bar{\Lambda}\left(\rho_{\mathcal{E}}^{\otimes n}\right). \tag{4.28}$$

If we now trace one of the two senders, e.g., Alice 2, we still have an LOCC between Alice 1 and Bob. In other words, we may write the following

$$\rho^n_{\mathbf{a}^1\mathbf{b}} = \bar{\Lambda}_{\mathbf{a}^1\mathbf{a}^2|\mathbf{b}}\left(\rho_{\mathcal{E}}^{\otimes n}\right), \tag{4.29}$$

where $\bar{\Lambda}_{\mathbf{a}^1\mathbf{a}^2|\mathbf{b}}$ is local with respect to the cut $\mathbf{a}^1\mathbf{a}^2|\mathbf{b}$. For Alice 1 and Bob ($i=1$), we can now write

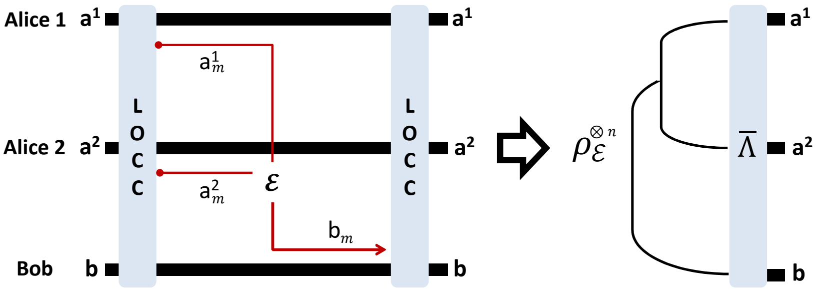

Figure 4.5: Teleportation stretching of an adaptive protocol implemented over a teleportation-covariant multiple-access channel (generic mth transmission shown on the left). After n uses, we can express the output in terms of n copies of the Choi matrix $\rho_{\mathcal{E}}$ of the quantum multiple-access channel, subject to a trace-preserving LOCC $\bar{\Lambda}$. This is Fig. 7 from Ref. [7].

$$\begin{aligned} E_R(\rho^n_{\mathbf{a}^1\mathbf{b}}) &:= \inf_{\sigma_s(\mathbf{a}^1|\mathbf{b})} S\left(\rho^n_{\mathbf{a}^1\mathbf{b}}||\sigma_s\right) \\ &\leq \inf_{\sigma_s(\mathbf{a}^1\mathbf{a}^2|\mathbf{b})} S\left(\rho_{\mathcal{E}}^{\otimes n}||\sigma_s\right) := E_{R(\mathbf{a}^1\mathbf{a}^2|\mathbf{b})}(\rho_{\mathcal{E}}^{\otimes n}) \\ &\leq \inf_{\sigma_s(\mathbf{a}^1|\mathbf{a}^2|\mathbf{b})} S\left(\rho_{\mathcal{E}}^{\otimes n}||\sigma_s\right) := E_R(\rho_{\mathcal{E}}^{\otimes n}). \end{aligned} \tag{4.30}$$

By applying the weak converse bound, we then derive [7]

$$\mathcal{C}^1 \leq \sup_{\mathcal{L}} \lim_{n} \frac{E_R(\rho^n_{\mathbf{a}^1\mathbf{b}})}{n} \leq E^\infty_{R(\mathbf{a}^1\mathbf{a}^2|\mathbf{b})}(\rho_{\mathcal{E}}) \leq E^\infty_R(\rho_{\mathcal{E}}), \tag{4.31}$$

and using the subadditivity of the REE over tensor products, it is easy to show the single-letter version

$$\mathcal{C}^1 \leq E_{R(\mathbf{a}^1\mathbf{a}^2|\mathbf{b})}(\rho_{\mathcal{E}}) \leq E_R(\rho_{\mathcal{E}}). \tag{4.32}$$

Note that we find the same bound for the other capacity for Alice 2 and Bob ($i=2$). The reasoning can be readily extended to arbitrary M senders, so that the capacity between the ith Alice and Bob reads [7]

$$\mathcal{C}^i \leq E_{R(\mathbf{a}^1\cdots\mathbf{a}^M|\mathbf{b})}(\rho_{\mathcal{E}}) \leq E_R(\rho_{\mathcal{E}}) := \mathbf{\Phi}(\mathcal{E}), \tag{4.33}$$

where $\mathbf{\Phi}(\mathcal{E})$ is the entanglement flux of the quantum multiple-access channel. As previously mentioned, the result can be extended to CV systems by employing asymptotic simulations and extending the notions.

4.3 All-in-all quantum communication

In this section we extend our technique to a single-hop quantum network involving multiple (M_A) senders and multiple (M_B) receivers, which is also known as quantum interference channel. This is a CPTP map from Alices' input space $\mathcal{D}(\otimes_{i=1}^{M_A}\mathcal{H}_{a^i})$ to Bobs' output space $\mathcal{D}(\otimes_{j=1}^{M_B}\mathcal{H}_{b^j})$. As a straightforward generalization of the previous cases, the most general adaptive protocol over this channel can be described as follows. At the initial stage the parties exploit a LOCC Λ_0 for their systems' preparation. Then, each Alice picks the first system from her local ensemble $a_1^i \in \mathbf{a}^i$. The inputs of all Alices are sent to all Bobs through channel $\mathcal{E}$ resulting into the outputs $\{b_1^i\}$, i.e.,

$$a_1^1, \dots, a_1^i, \dots, a_1^{M_A} \xrightarrow{\mathcal{E}} b_1^1, \dots, b_1^j, \dots, b_1^{M_B} \ . \tag{4.34}$$

After this first transmission, there is another LOCC Λ_1, after which all Bobs' ensembles are updated $b_1^j \mathbf{b}^j \to \mathbf{b}^j$. Next, there is the second transmission $\mathbf{a}^i \ni \{a_2^i\} \to \{b_2^j\}$ through $\mathcal{E}$, followed by another LOCC Λ_2 and so on. Thus, after n uses of the channel, the ith Alice and the jth Bob share an output state $\rho^n_{\mathbf{a}^i\mathbf{b}^j}$, which is ϵ-close to a target state of nR_{ij}^n bits. By maximizing the asymptotic rate over all the adaptive LOCCs $\mathcal{P} = \{\Lambda_0, \Lambda_1, \dots\}$ we can define the generic interference capacity for the ith Alice and the jth Bob as [7]

$$\mathcal{C}^{ij} := \sup_{\mathcal{P}} \lim_{n\to\infty} R_{ij}^n \ . \tag{4.35}$$

As usual, depending on the task, one specifies three different capacities assisted by unlimited two-way CCs: The entanglement distribution capacity (D_2^{ij}), the quantum capacity (Q_2^{ij}), the secret-key capacity (K^{ij}) and the private capacity (P_2^{ij}) of the quantum interference channel (with $D_2^{ij} = Q_2^{ij} \leq K^{ij} = P_2^{ij}$). As for the case of the broadcast and the multiple-access channels we bound these capacities by using REE+teleportation stretching. We proceed by considering two senders and two receivers being the extension to arbitrary M_A and M_B just a matter of technicalities. The definition of a teleportation-covariance quantum interference channel relies once again on the commutation with teleportation, i.e., for any teleportation unitaries $U_{k_1}^1$ and $U_{k_2}^2$ we must have [7]

$$\mathcal{E}\left[(U_{k_1}^1 \otimes U_{k_2}^2)\rho(U_{k_1}^1 \otimes U_{k_2}^2)^\dagger\right] = \mathcal{V}\mathcal{E}(\rho)\mathcal{V}^\dagger, \tag{4.36}$$

where $\mathcal{V} = V^1_{l_1} \otimes V^2_{l_2}$ for unitaries $V^1_{l_1}$ and $V^2_{l_2}$, with both l_1 and l_2 depending on k_1 and k_2. If this condition holds then the channel can be simulated by teleportation over its Choi matrix, which is formally defined as in Eq. (4.27). See Fig. 4.6 for this simulation. Thus, an adaptive protocol can be simplified since each use of channel $\mathcal{E}$ can be replaced by teleportation and both the Bell detections and Bobs' correction unitaries become part of the LOCCs. By stretching n uses of the channel (see Fig. 4.7), we have the following output state shared between Alice 1, Alice 2, Bob 1 and Bob 2

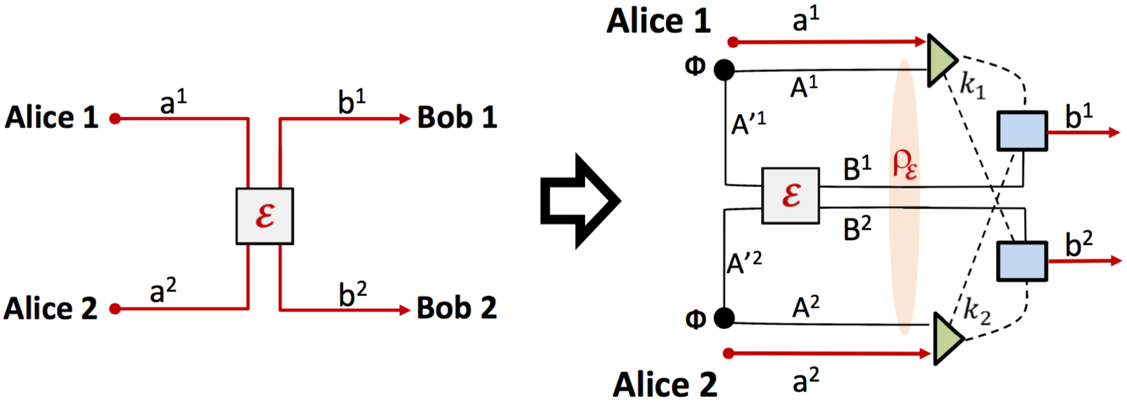

Figure 4.6: Simulation of a teleportation-covariant quantum interference channel. The channel $\mathcal{E} : a^1a^2 \rightarrow b^1b^2$ (left) can be simulated by its Choi matrix $\rho_{\mathcal{E}}$ (right). Systems a^1 and A^1 are subject to a Bell detection with outcome k_1. Similarly, systems a^2 and A^2 are subject to a Bell detection with outcome k_2. Both outcomes k_1 and k_2 are then classically communicated to Bob 1 and Bob 2 who apply two correction unitaries on B^1 and B^2. Since the channel is teleportation-covariant, i.e., it commutes with the teleportation unitaries according to Eq. (4.36), the two Bobs are able to recover the original channel $\mathcal{E} : a^1a^2 \rightarrow b^1b^2$ by applying correction unitaries $(V^1_{l_1})^{-1}$ and $(V^2_{l_2})^{-1}$. This is Fig. 8 from Ref. [7].

$$\rho_{\mathbf{a}^1\mathbf{a}^2\mathbf{b}^1\mathbf{b}^2} = \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes n}). \tag{4.37}$$

By tracing over one sender and one receiver, say Alice 2 and Bob 2, we then derive

$$\rho^n_{\mathbf{a}^1\mathbf{b}^1} = \bar{\Lambda}_{\mathbf{a}^1\mathbf{a}^2|\mathbf{b}^1\mathbf{b}^2}(\rho_{\mathcal{E}}^{\otimes n}) \ , \tag{4.38}$$

where $\bar{\Lambda}_{\mathbf{a}^1\mathbf{a}^2|\mathbf{b}^1\mathbf{b}^2}$ is a trace-preserving LOCC between Alice 1 and Bob 1, local with respect to the cut $\mathbf{a}^1\mathbf{a}^2|\mathbf{b}^1\mathbf{b}^2$.

It follows that the capacity for Alice 1 and Bob 1 ($i = j = 1$) is upper bounded by [7]

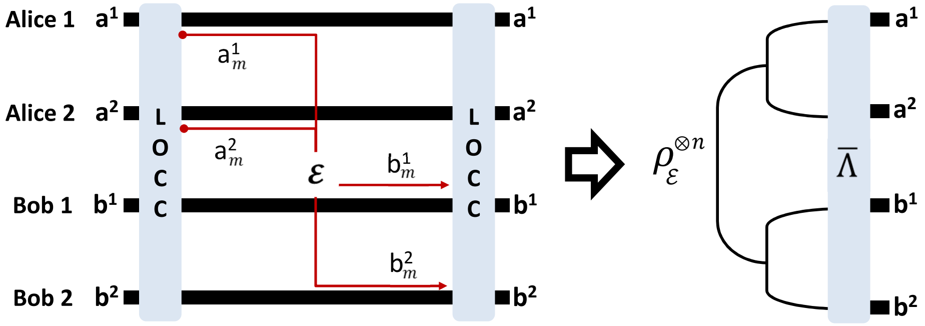

Figure 4.7: Teleportation stretching of an adaptive protocol over a quantum interference channel (generic mth transmission shown on the left). After n uses, we can express the output in terms of n copies of the Choi matrix $\rho_{\mathcal{E}}$ of the quantum interference channel, subject to a trace-preserving LOCC $\bar{\Lambda}$. This is Fig. 9 from Ref. [7].

$$\mathcal{C}^{11} \leq \sup_{\mathcal{L}} \lim_{n\to\infty} \frac{E_R(\rho^n_{\mathbf{a}^1\mathbf{b}^1})}{n} \leq E^{\infty}_{R(\mathbf{a}^1\mathbf{a}^2|\mathbf{b}^1\mathbf{b}^2)}(\rho_{\mathcal{E}}) \leq E^{\infty}_R(\rho_{\mathcal{E}}). \tag{4.39}$$

In terms of single-letter bounds we find

$$\mathcal{C}^{11} \leq E_{R(\mathbf{a}^1\mathbf{a}^2|\mathbf{b}^1\mathbf{b}^2)}(\rho_{\mathcal{E}}) \leq E_R(\rho_{\mathcal{E}}). \tag{4.40}$$

Clearly, we find the same result in all other cases, i.e., for any sender-receiver pair (i, j). In general, for arbitrary M_A senders and M_B receivers, we may write [7]

$$\mathcal{C}^{ij} \leq E_{R(\mathbf{a}^1\cdots\mathbf{a}^{M_A}|\mathbf{b}^1\cdots\mathbf{b}^{M_B})}(\rho_{\mathcal{E}}) \leq E_R(\rho_{\mathcal{E}}) := \mathbf{\Phi}(\mathcal{E}), \tag{4.41}$$

where $\Phi(\mathcal{E})$ is the entanglement flux of the quantum interference channel. The extension to CV systems exploits asymptotic simulations along the lines of Sec. 2.4.1.

Chapter 5

Ultimate performance of Quantum Metrology and Quantum Channel Discrimination

The level of generality at which we have developed quantum channel simulation and teleportation stretching is such that we can apply their combination to other contexts beside quantum communication. In particular, our methodology can be applied to simplify other types of adaptive protocols whose performances are given in terms of functionals that are monotonic under CPTP maps. In this Chapter we first review the results of Ref. [42] by showing how we can rely on our technique in order to bound the ultimate adaptive performance of quantum metrology. In the second part, by employing a different version of the standard teleportation protocol, namely the port-based teleportation (PBT), we are able to achieve a more powerful channel simulation that leads us to determine a universal lower bound for the probability of error affecting the discrimination of two arbitrary quantum channels.

Quantum metrology [138,139], also known as quantum parameter estimation, aims at optimally estimating unknown classical parameters which are encoded in quantum states as well as in quantum channels. Also in this setting, the ultimate limits of the performances must be addressed by considering the most general strategies for quantum parameter estimation that are allowed by quantum mechanics. These protocols are inevitably adaptive, involving joint quantum operations and an unlimited use of entanglement.

Let us start by formulating the general problem. Suppose that we have a black-box which is implementing a quantum transformation described by the quantum channel $\mathcal{E}_\theta$, where θ is an unknown classical parameter with a uniform prior probability distribution. In order to retrieve the best value for the parameter θ, we probe the box a number n of times obtaining the sequence of outcomes $\mathbf{x} = (x_1, x_2, \ldots, x_n)$. Statistically, this means that we generate an estimator $\tilde{\theta} = \tilde{\theta}(\mathbf{x})$, i.e. a mapping from the set of measurement outcomes into the space of parameters, such that its error variance $\delta\theta^2 = \langle(\tilde{\theta}(\mathbf{x}) - \theta)^2\rangle$ is minimal [139]. Here the average is assumed over the n probings of the box. We expect that the error variance or the standard deviation $\delta\theta$ to decrease with n. A fundamental question is then to determine which is the optimal scaling in n for a given quantum channel. We know that for certain channels the scaling is $\delta\theta \sim n^{-1/2}$, known as the "standard quantum limit"(SQL), and it is also what we expect in a completely classical setting. Remarkably, there are channels that behave fully quantum and this limit can be beaten. In fact, it is a known result [41] that the optimal limit that is reachable in the quantum realm is the "Heisenberg scaling"(HS), i.e. $\delta\theta \sim n^{-1}$. To decide if the estimation of the parameter in $\mathcal{E}_\theta$ is limited by the SQL or the HS we need to adopt adaptive protocols.

5.1 Protocols for quantum parameter estimation

In order to estimate the parameter θ with an optimal estimator $\tilde{\theta}$ characterized by minimal error variance $\delta\theta^2$, the simplest strategy is represented by a block protocol which can be *direct* or *ancillary-assisted*. In a block protocol of parameter estimation, the involved elementary operations are represented by the preparation of a suitable input state to probe the channel and the detection of the output of the channel by means of an optimal positive operator-valued measure (POVM). In a direct protocol, Fig 5.1 panel **a**, we prepare the same input state σ for all the n probings of the channel, and then the output state $\rho_\theta^{\otimes n} = \mathcal{E}_\theta(\sigma)^{\otimes n}$ is detected with a joint POVM.

In an assisted protocol, Fig 5.1 panel **b**, for each probing of the channel we use a joint state σ of the input system and an ancillary system. The total output state, which now reads $\rho_\theta^{\otimes n} = [(\mathcal{E}_\theta \otimes \mathcal{I})\sigma]^{\otimes n}$ is then jointly measured. Note that clearly an assisted protocol is equivalent to a direct one performed over the extended channel $\mathcal{E}_\theta \otimes \mathcal{I}$.

The most general adaptive protocol involves additional ingredients that complicate considerably the analysis. In fact, in such a setting each probing of the channel takes place between joint quantum operations and unlimited entanglement in principle could be distributed between the input and the output. Moreover, feedback may also be exploited

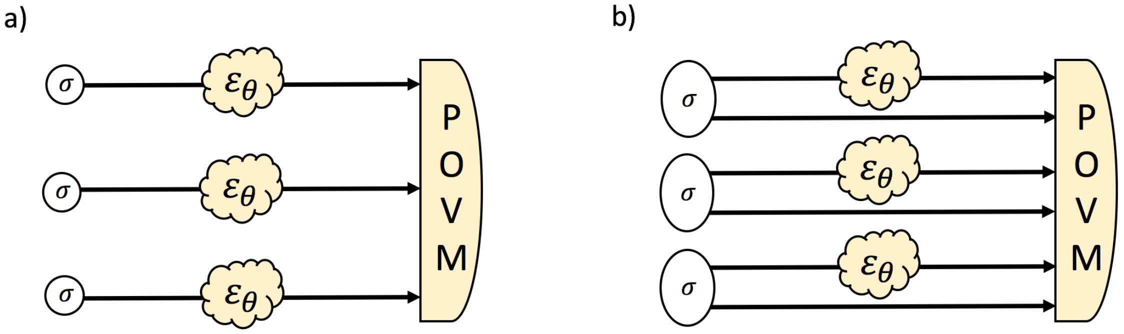

Figure 5.1: Block protocols for direct (panel **a**) and assisted (panel **b**) quantum parameter estimation. In both strategies, the n istances of the quantum channel $\mathcal{E}_\theta$ are identically and independently probed with the same input σ. At the output the quantum state has a tensor product structure and it is subjectd by an optimal POVM, whose outcome is post-processed into an (unbiased) estimator $\tilde{\theta}$.

in order to optimize the inputs for the next probings. An adaptive protocol for quantum metrology runs similarly to the one for quantum communication, described in Sec. 2.1. The main difference is that the trace-preserving LOCCs Λ_i are now substituted by joint quantum operations (QO) $\mathcal{Q}_i$ which can be assumed to be trace-preserving, since any non-trace preserving mapping can be postponed and included in the final collective POVM by following the principle of the deferred measurement [10].

After n adaptive probings, the output for Alice and Bob will result in the state ρ_θ^n which clearly depends on the sequence of QOs $\mathbb{Q} := \{\mathcal{Q}_0, \ldots, \mathcal{Q}_n\}$. The final step consists in detecting the final state with a joint POVM, whose outcome is then processed into the estimator $\tilde{\theta}$.

Suppose we implement an optimal adaptive protocol so that we are implicitly optimising over all the possible protocol $\mathbb{Q}$ and all the possible joint POVMs. The ultimate lower bound for the error variance $\delta\theta$ of any unbiasd estimator is given by the quantum Cramér-Rao bound (QCRB)

$$\delta\theta^2 \geq \frac{1}{\mathrm{QFI}(\rho_\theta^n)} \ , \tag{5.1}$$

where QFI is the quantum Fisher information [139], $\mathrm{QFI}(\rho_\theta^n) := \mathrm{Tr}(\mathcal{L}_\theta^2 \rho_\theta^n)$, and $\mathcal{L}_\theta$ is the symmetric logarithmic derivative (SLD) that can be represented as follows [139, 140]

$$\mathcal{L}_\theta \rho_\theta^n = \sum_{j,k:\lambda_j+\lambda_k>0} \frac{2}{\lambda_j + \lambda_k} \langle e_j | \frac{d\rho_\theta^n}{d\theta} | e_k \rangle | e_j \rangle \langle e_k | \tag{5.2}$$

once we have introduced the spectral decomposition of the output, i.e. $\rho_\theta^n = \sum_j \lambda_j\rangle |e_j\rangle\langle e_j|$. By relying on the definition of the quantum fidelity $F(\rho,\sigma) := \mathrm{Tr}\,\sqrt{\sqrt{\rho}\sigma\sqrt{\rho}}$ and taking the limit for $d\theta \to 0$, we can alternatively express the QFI as [139]

$$\mathrm{QFI}(\rho_\theta^n) = \lim_{d\theta\to 0} \frac{8[1 - F(\rho_\theta^n, \rho_{\theta+d\theta}^n)]}{d\theta^2} \ . \tag{5.3}$$

Two fundamental properties of the QFI are the following

- Monotonicity under the action of CPTP maps $\mathcal{M}$, i.e. quantum channels

$$\mathrm{QFI}[\mathcal{M}(\sigma_\theta)] \leq \mathrm{QFI}(\sigma_\theta) \ . \tag{5.4}$$

- Additivity over tensor product of states. Given two parameter-dependent states σ_θ and σ'_θ, we have

$$\mathrm{QFI}(\sigma_\theta \otimes \sigma'_\theta) = \mathrm{QFI}(\sigma_\theta) + \mathrm{QFI}(\sigma'_\theta) \ . \tag{5.5}$$

Note that a block protocol, direct or assisted, is restricted to the SQL. In fact, given that the output of such a strategy is a tensor product state $\rho_\theta^{\otimes n}$, by exploiting Eq. (5.5), we can write $\mathrm{QFI}(\rho_\theta^{\otimes n}) = n\mathrm{QFI}(\rho_\theta)$. In this way the associated QCRB becomes

$$\delta\theta^2 \geq \frac{1}{n\mathrm{QFI}(\rho_\theta)} \ . \tag{5.6}$$

In an adaptive protocol setting, the output state does not necessarily have a tensor product structure and the error variance could potentially behave differently from Eq. (5.6) and beat the SQL. However, as we will see in the next two sections, the characteristic feature of an adaptive protocol reduction into a block one, which allow us to write the output as a tensor product, automatically limits the performances of the protocol to the SQL. In Sec. 5.9 we will employ a slight modification of the channel simulation in order to cover quantum channels that beat the SQL.

5.2 Protocol reduction for co-programmable channels

By following the procedure devised in Ref. [42], we show that the reduction of any adaptive protocol for parameter estimation can be obtained when *co-programmable* channels are employed. We say that an ensemble $\mathbf{P}$ of quantum channels is *co-programmable* if, for any channel $\mathcal{E} \in \mathbf{P}$, we may write

$$\mathcal{E}(\rho) = \mathcal{S}(\rho \otimes \pi_{\mathcal{E}}) \ , \tag{5.7}$$

with the same joint quantum operation (trace preserving) $\mathcal{S}$ and a channel-dependent program state $\pi_{\mathcal{E}}$. For this class of channel is then possible to decompose the output of the protocol in terms of the tensor product of many copies of the program state. In this way, due to the considerations made at the end of the previous section, we have that quantum metrology with a co-programmable channel is limited by the SQL.

We have already mentioned programmability as a particular example of channel simulation. This idea was introduced in Ref. [38], where, in the context of quantum computation, the authors design a quantum gate array through which an arbitrary quantum channel is simulated by a universal unitary and a program state. With a finite number of systems for the program state, this kind of simulation can be only probabilistic. Viceversa, perfect simulation can be achieved by using ideally an infinite number of systems, this is a fundamental feature of *port-based* teleportation which we will describe later in Sec. 5.6.1. A deterministic simulation was given later in Ref. [141] for the particular class of co-programmable channels. Ref. [42] considered co-programmable channels in both discrete and continuous variable settings, also identifying the crucial connection with quantum teleportation.

Let us extend the notion of co-programmable quantum channel to the context of parameter estimation. Assume that the parametrised quantum channel $\mathcal{E}_\theta$ spans a family of co-programmable channels, so that, for any θ, we can write the following simulation

$$\mathcal{E}_\theta(\rho) = \mathcal{S}(\rho \otimes \pi_{\mathcal{E}_\theta}) \ . \tag{5.8}$$

By plugging this into the adaptive protocol, as we did for quantum communication, we can replace each istance of the channel with its simulation. Namely, each use of the channel $\mathcal{E}_\theta$ is substituted with its program state $\pi_{\mathcal{E}_\theta}$. Then all the program states are stretched back in time while all the simulators $\mathcal{S}$ collapse, together with the preparation of the initial state, into a single final QO $\boldsymbol{Q}$. Therefore we have [8, 42]

$$\rho_\theta^n = \boldsymbol{Q}(\pi_{\mathcal{E}_\theta}^{\otimes n}) \ . \tag{5.9}$$

As we already noticed, monotonicity and additivity of the QFI are enough to restrict the QCRB for the estimation of a parameter θ encoded in $\mathcal{E}_\theta$ to the SQL. In fact we may write [8, 42]

$$\mathrm{QFI}(\rho_\theta^n) = \mathrm{QFI}\left[\boldsymbol{Q}(\pi_{\mathcal{E}_\theta}^{\otimes n})\right] \leq \mathrm{QFI}(\pi_{\mathcal{E}_\theta}^{\otimes n}) = n\mathrm{QFI}(\pi_{\mathcal{E}_\theta}) \tag{5.10}$$

so that the error variance satisfies

$$\delta\theta^2 \geq \frac{1}{n\text{QFI}(\pi_{\mathcal{E}_\theta})} \ . \tag{5.11}$$

Note that this bound is not necessarily achievable since we do not know if the state $\pi_{\mathcal{E}_\theta}$ is generated by transmission of some input state through $\mathcal{E}_\theta$. Contrarily, for *jointly* teleportation covariant channel, the bound is always achievable, the optimal strategy is non-adaptive and it is defined by sending parts of maximally entangled states and then measuring the output Choi matrices. Joint teleportation-covariance means that we can write for any θ the following relation [8, 42]

$$\mathcal{E}_\theta(U\rho U^\dagger) = V\mathcal{E}_\theta(\rho)V^\dagger \ , \tag{5.12}$$

where the output unitaries V do not depend on the noise parameter, i.e. the ensemble of channels $\{\mathcal{E}_\theta\}$ is teleportation covariant with the same set of output correction unitaries, so that the noise parameter is uniquely associated with a environmental state dilating the channel. If Eq. (5.12) is valid, then Eq. (5.8) explicitly becomes

$$\mathcal{E}_\theta(\rho) = \mathcal{T}(\rho \otimes \rho_{\mathcal{E}_\theta}) \ , \tag{5.13}$$

where $\mathcal{T}$ is teleportation, independent from θ, which is in turn encoded in the channel's Choi matrix $\rho_{\mathcal{E}_\theta}$. The stretching is then repeated and we get [8, 42]

$$\rho^n_\theta = \boldsymbol{Q}\left(\rho^{\otimes n}_{\mathcal{E}_\theta}\right) \tag{5.14}$$

for some quantum channel $\boldsymbol{Q}$. This means that the estimation of a teleportation-covariant channel is limited by the SQL with a pre-factor given by the Choi matrix of the Channel, i.e. [8, 42]

$$\delta\theta^2 \geq \frac{1}{n\text{QFI}(\rho_{\mathcal{E}_\theta)}} \ . \tag{5.15}$$

As a consequence, teleportation simulation not only allows to compute explicitly the upper bound, but it also provides a matching lower bound. As a matter of facts, an optimal strategy that saturates the bound employs a block (assisted) estimation protocol where the maximally entangled state is used at the input of the channel in an identical and independent way. This strategy gives a QFI exactly equal to $n\text{QFI}(\rho_{\mathcal{E}_\theta})$, so that the QCRB in Eq. (5.15) is asymptotic achievable for large n. In Ref. [42], the authors gives analytical expressions for the QCRB of teleportation-covariant discrete variable channels. These are represented, as we learned, by the erasure, dephasing and depolarizing channels. More precisely, they satisfy joint teleportation covariance and the parameter θ is identified with the channel-defining probability p. For each family of these channels $\mathcal{E}_p$ the Choi matrix is computed, so that

$$\mathrm{QFI}(\rho_{\mathcal{E}_p}) = \frac{1}{p(1-p)} \tag{5.16}$$

and by using Eq. (5.15) we find that the adaptive estimation of p is bounded by the following asymptotically-achievable QCRB [42]

$$\delta p^2 \geq \frac{p(1-p)}{n} \ . \tag{5.17}$$

5.3 Teleportation stretching of adaptive metrology in continuous variables

To apply the methodology of Sec. 2.5.1 to adaptive parameter estimation, we need joint teleportation covariance for the family of channels $\mathcal{E}_\theta$ spanned by varying the parameter θ. If this is the case, then we may repeat the previous procedure and decompose the output state ρ_θ^n by using [42]

$$\left\| \rho_\theta^n - \boldsymbol{Q}_\mu(\rho_{\mathcal{E}_\theta}^{\mu\otimes n}) \right\| \leq n\epsilon_{\mu,N} \ , \tag{5.18}$$

for any θ, finite number of uses n and finite energy N. To evaluate the QFI of ρ_θ^n, we now exploit the connection with the Bures distance d_{B} and the trace distance D. In fact, for $d\theta \to 0$ we may write

$$\mathrm{QFI}(\rho_\theta^n) = \frac{4d_{\mathrm{B}}^2(\rho_\theta^n, \rho_{\theta+d\theta}^n)}{d\theta^2}, \tag{5.19}$$

where

$$\begin{aligned} d_{\mathrm{B}}(\rho,\sigma) &:= \sqrt{2[1-F(\rho,\sigma)]} \\ &\leq \sqrt{2D(\rho,\sigma)} = \sqrt{||\rho-\sigma||}. \end{aligned} \tag{5.20}$$

Using the triangle inequality for the Bures distance and properties of the fidelity (monotonicity under CPTP maps and multiplicativity over tensor products), we may write [42]

$$d_{\mathrm{B}}(\rho_\theta^n, \rho_{\theta+d\theta}^n) \leq \sqrt{2[1-(F_\theta^\mu)^n]} + 2\sqrt{n\delta(\mu,N)}, \tag{5.21}$$

where $F_\theta^\mu := F(\rho_{\mathcal{E}_\theta}^\mu, \rho_{\mathcal{E}_{\theta+d\theta}}^\mu)$. For any finite n and N, we may take the limit for large μ and write

$$d_{\mathrm{B}}(\rho_\theta^n, \rho_{\theta+d\theta}^n) \leq \lim_{\mu\to\infty} \sqrt{2[1-(F_\theta^\mu)^n]} = \sqrt{2[1-(F_\theta^\infty)^n]} \ , \tag{5.22}$$

where $F_\theta^\infty := \lim_{\mu\to\infty} F_\theta^\mu$. In other words, we have

$$\mathrm{QFI}(\rho_\theta^n) \leq \frac{8[1-(F_\theta^\infty)^n]}{d\theta^2}. \tag{5.23}$$

It is easy to check [42] that the upper bound is additive, so that

$$\mathrm{QFI}(\rho_\theta^n) \leq n\frac{8[1-F_\theta^\infty]}{d\theta^2} := n\mathrm{QFI}_\theta^\infty. \tag{5.24}$$

It is important to note that the upper bound does not depend on the specifics of the adaptive protocol and also on energy constraint N. Therefore, the bound is valid for all possible adaptive protocols, both constrained and unconstrained (i.e., we can safely remove the energy constraint at the end of the calculations). Also notice that the upper bound is asymptotically achievable by an unconstrained block (assisted) protocol, where n TMSV states Φ_μ are used to probe the channel, so that one collects the output product state $\rho_{\mathcal{E}_\theta}^{\mu\otimes n}$. By making an optimal measurement, we achieve

$$\mathrm{QFI}(\rho_{\mathcal{E}_\theta}^{\mu\otimes n}) = n\frac{8[1-F_\theta^\mu]}{d\theta^2}, \tag{5.25}$$

whose limit for large μ coincides with the upper bound in Eq. (5.24). Because, this protocol uses independent probing states, the QCRB is achievable for large n.

In conclusion, Eq. (5.24) is indeed the ultimate QFI achievable with adaptive estimation protocols. Thus, we may say that the optimal adaptive estimation of a noise parameter θ encoded in a teleportation-covariant bosonic channel $\mathcal{E}_\theta$ (so that the family is jointly tele-covariant) is limited to the SQL. In fact, it satisfies the asymptotically achievable QCRB [42]

$$\delta\theta^2 \geq (n\mathrm{QFI}_\theta^\infty)^{-1} \ , \tag{5.26}$$

where $\mathrm{QFI}_\theta^\infty$ is related to the asymptotic Choi matrix of the channel $\rho_{\mathcal{E}_\theta}$ according to the limit in Eq. (5.24).

Now let us consider a thermal loss-channel $\mathcal{E}_{\eta,\bar{n}}^{\mathrm{therm}}$, see Sec. 2.7.2.2, with transmissivity $\eta \in [0,1]$ and noise $\nu = (1-\eta)(\bar{n}+1/2)$. This channel is jointly teleportation-covariant in the thermal number. Therefore, if we consider the adaptive estimation of the parameter $\bar{n}$, which can be related to a measurement of temperature, by using Eq. (5.26) one computes [42]

$$\mathrm{QFI}_{\bar{n}}^\infty = \frac{1}{\bar{n}(\bar{n}+1)} \quad \Rightarrow \quad \delta\bar{n}^2 \geq \frac{\bar{n}(\bar{n}+1)}{n} \ . \tag{5.27}$$

We see that the QCRB does not depend on the loss parameter η, as long as it is less than 1. This implies that, for any $\eta < 1$, we achieve the same accuracy as we would get in a direct measurement of the environment ($\eta = 0$).

Consider now a noisy quantum amplifier $\mathcal{E}^{\mathrm{amp}}_{\eta,\bar{n}}$ which is defined by a gain $\eta > 1$ and noise $\nu = (\eta - 1)(\bar{n} + 1/2)$ with thermal number $\bar{n}$. This is teleportation covariant and jointly tele-covariant in the parameter $\bar{n}$. For the adaptive estimation of $\bar{n} > 0$, one gets [42] the same QCRB of Eq. (5.27). Finally, consider an additive-noise Gaussian channel $\mathcal{E}^{\mathrm{add}}_{\nu}$ which is defined by $\eta = 1$ and $\nu \geq 0$. This is joint teleportation covariant in the added noise ν, whose optimal adaptive estimation is bounded by [42] $\mathrm{QFI}^{\infty}_{\nu} = \nu^{-2}$ and therefore the QCRB

$$\delta\nu^2 \geq \nu^2/n \; . \tag{5.28}$$

5.4 Sub-optimal simulation of bosonic Gaussian channels

By following the recipe provided in Chapter 3, at this stage of the discussion, we are naturally led to compute finite-resource QCRBs for each single-mode Gaussian channel and to compare them with those obtained previously with the asymptotic Choi state. We are thus interested in finding a finite-energy resource state σ_ν that can simulate a phase-insensitive Gaussian channel $\mathcal{E}_{\eta,\nu}$ as in Eq. (3.7), i.e.

$$\mathcal{E}_{\eta,\nu}(\rho) = \mathcal{T}_{\eta}(\rho \otimes \sigma_\nu) \; , \tag{5.29}$$

It is worth remarking that there exist many finite-energy resource states that can simulate a given channel. Here we consider a choice for σ_ν different from the two described in Sec. 3.1 to derive weak converse upper bounds for the secret key capacity of phase-insensitive Gaussian channels. It is straightforward to verify that a phase-insensitive channel can be simulated with teleportation over the following Gaussian state with zero mean and CM [8]

$$\mathbf{V}(\sigma_\nu) = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix} , \tag{5.30}$$

with the following elements

$$a = \frac{1}{2}\cosh 2r, \;\; b = \frac{|1-\eta|}{2} + \frac{\eta}{2}\cosh 2r, \;\; c = \frac{\sqrt{\eta}}{2}\sinh 2r \; , \tag{5.31}$$

where

$$r = -\frac{1}{2}\ln\left[\frac{2\nu - |1-\eta|}{2\eta}\right] . \tag{5.32}$$

Note that the form of the simulation in Eq. (5.29) is such that the noise parameter ν only appears in the resource state σ_ν or, in other words, the teleportation LOCC $\mathcal{T}_\eta$ does not depend on ν. For this reason, the family of channels $\mathcal{E}_{\eta,\nu}$ with fixed η but varying ν is a family of jointly teleportation-simulable channels (which is a condition implied by the joint teleportation covariance). As a result, the adaptive estimation of the parameter ν can be completely simplified, so that the n-use output state of a comb reads $\rho_\nu^n = \Lambda_\eta(\sigma_\nu^{\otimes n})$ for some global quantum channel Λ_η which is independent from the unknown parameter ν. As a consequence, we may simplify the QFI of the output state ρ_ν^n and write the following QCRB for the adaptive estimation of ν [8]

$$\delta\nu^2 \geq \frac{1}{n\mathrm{QFI}(\sigma_\nu)} \ . \tag{5.33}$$

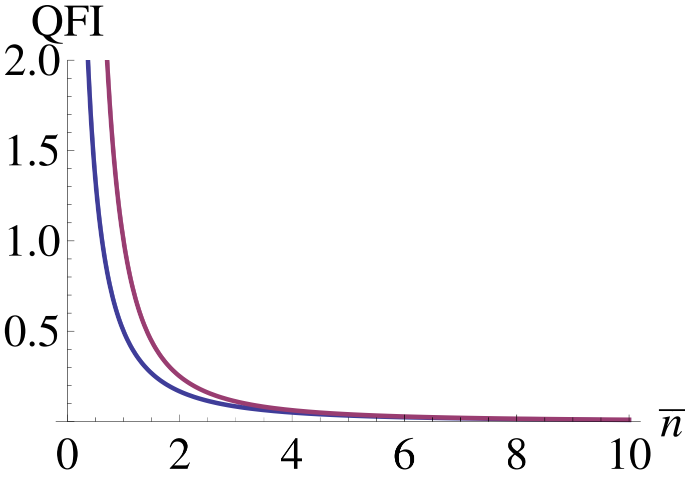

Figure 5.2: Quantum Fisher information $\mathrm{QFI}(\sigma_{\bar{n}})$ associated with the adaptive estimation of the thermal number $\bar{n}$ of a thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}$. Assuming the sub-optimal simulation we find $\mathrm{QFI}(\sigma_{\bar{n}}) = \bar{n}^{-2}$ (upper red line). Compare this with $\mathrm{QFI}_{\bar{n}}^{\infty} = [\bar{n}(\bar{n}+1)]^{-1}$ which was computed in Eq.(5.27) using the asymptotic simulation (lower blue line). This is Fig. 6 from Ref. [8].

As an example consider the additive-noise Gaussian channel $\mathcal{E}_\nu^{\mathrm{add}}$. This channel can be simulated by exploiting a resource state σ_ν whose CM is given by Eq. (5.30)-(5.32) with $\eta = 1$. We may then compute the QFI from the quantum fidelity between gaussian states [82], and by using Eq. (5.3) we find the QCRB $\delta v^2 \geq v^2/n$ [8]. Note that this exactly coincides with the tight achievable bound of Eq. (5.28) which is obtained by simulating the channel via its asymptotic Choi matrix.

Consider now the adaptive estimation of the thermal number $\bar{n}$ of a thermal-loss channel $\mathcal{E}_{\eta,\bar{n}}^{\text{loss}}$ assuming the sub-optimal simulation. Putting $\nu = (1-\eta)(\bar{n}+1/2)$ in Eq. (5.33) we compute the QCRB for $\delta\bar{n}^2$. We do not find the tight achievable bound of Eq. (5.27) but a larger bound given by [8]

$$\delta\bar{n}^2 \geq \bar{n}^2/n\,. \tag{5.34}$$

For comparison, in Fig. 5.2 we plot the QFI for the asymptotic and finite-energy resource state. It is a open problem to find a finite-energy resource that can match the asymptotic bound. Finally, one may easily check that Eq. (5.34) also holds for a noisy amplifier $\mathcal{E}_{\eta,\bar{n}}^{\text{amp}}$ assuming its sub-optimal simulation.

5.5 Quantum channel discrimination

We now move on by considering the scenario of quantum channel discrimination (QCD), in particular we aim at assessing the ultimate performance for discriminating two arbitrary quantum channels acting on a finite-dimensional Hilbert space. Quantum channel discrimination [143–147], together with quantum state discrmination, represents a fundamental tool for the basic formulation of quantum hypothesis testing, a central area in quantum information with many analysis for both discrete and continuous variable systems. If on the one hand, due to the seminal work of Helstrom [55], we know how to bound the error probability affecting the symmetric discrimination of two arbitrary quantum state, on the other, a similar bound is still missing for the discrimination of two arbitrary quantum channels. The main problem in quantum channel discrimination (QCD) is that the strategies involve an optimization over the input state and the output measurement, and this process may also be adaptive in the most general case, so that feedback from the output is used to update the input. The ultimate performance of adaptive QCD is not known because of the extreme difficulty to handle feedback-assistance in quantum protocols. At the same time, it is also known that adaptiveness needs to be considered in QCD. In fact, apart from the cases where two channels are classical [148], co-programmable or teleportation-covariant (see [42] and Sec. 5.2), feedback may greatly improve the discrimination. For instance, Ref. [149] presented two channels which can be perfectly distinguished by using feedback in just two adaptive uses, while they cannot be perfectly discriminated by any number of uses of a block (non-adaptive) protocol, where the channels are probed in an identical and independent fashion, i.e., using multiple copies of the same input state.

Here we derive a universal lower bound for the error probability affecting the discrimination of two arbitrary quantum channels. To do this we design a technique which reduces an adaptive protocol over an arbitrary finite-dimensional quantum channel into a block protocol over multiple copies of the channel's Choi matrix. This is obtained by substituting the standard teleportation protocol with *port-based* teleportation(PBT) [43–45, 150–154] into the simulation of the channel and suitably generalizing the technique of teleportation stretching devised in Sec. 2.5. This reduction clearly applies to adaptive protocols with any task (not just QCD). When applied to QCD, it allows us to bound the ultimate error probability by using the Choi matrices of the channels. As a direct application of this result, we derive interesting bounds on the the ultimate adaptive performance of quantum illumination [51–54, 155–159]. We then go back to adaptive quantum metrology and exploit PBT-stretching to prove a fundamental bound on the parameter estimation that asymptotically follows the Heisenberg scaling. Further applications for quantum and private communications are discussed. These methods and results have been established in [9].

Let us start by considering an adaptive strategy for the binary and symmetric discrimination of two aribitrary equiprobable quantum channels $\{\mathcal{E}_u\} = \{\mathcal{E}_0, \mathcal{E}_1\}$ in a black-box, where $u \in \{0, 1\}$ is binary digit labelling the the channel and having equal priors. An adaptive discrimination protocol $\mathcal{P}_n$ consists of local registers $\mathbf{a}$ and $\mathbf{b}$ prepared initially in a state[1] ρ_0, which are then used to probe the black-box n times with the assistance of a sequence of QOs $\{\Lambda_1, \ldots, \Lambda_n\}$ defining the protocol $\mathcal{P}_n$.

The output state $\rho_n(u)$ of the protocol $\mathcal{P}_n$ is finally detected by an optimal positive-operator valued measure (POVM). For binary discrimination, this is the Helstrom POVM, which leads to the following error probability conditioned on $\mathcal{P}_n$ [55]

$$p(\mathcal{E}_0 \neq \mathcal{E}_1 | \mathcal{P}_n) = \frac{1 - D\left[\rho_n(0), \rho_n(1)\right]}{2}, \tag{5.35}$$

where $D(\rho, \sigma) := ||\rho - \sigma||/2$ is the trace distance. In Eq. (5.35) and in the following, we use the compact notation $\mathcal{E}_0 \neq \mathcal{E}_1$, meaning that, once the input is fixed, we are discriminating between the two output states $\rho_n(0) = \Lambda_n \circ \mathcal{E}_0 \circ \ldots \circ \mathcal{E}_0 \circ \Lambda_1(\rho_0)$ and

[1] We are omitting the superscripts **ab** to simplify the notation and since there is no space for ambiguity

$\rho_n(1) = \Lambda_n \circ \mathcal{E}_1 \circ \ldots \circ \mathcal{E}_1 \circ \Lambda_1(\rho_0)$, which clearly depend on the specific protocol $\mathcal{P}_n$.
By means of an optimization over all discrimination protocols $\mathcal{P}_n$, we define the minimum error probability affecting the n-use adaptive discrimination of $\mathcal{E}_0$ and $\mathcal{E}_1$, i.e., we may write

$$p_n(\mathcal{E}_0 \neq \mathcal{E}_1) := \inf_{\mathcal{P}_n} \; p(\mathcal{E}_0 \neq \mathcal{E}_1 | \mathcal{P}_n). \tag{5.36}$$

This is generally less than the n-copy diamond distance between the two channels $\mathcal{E}_0^{\otimes n}$ and $\mathcal{E}_1^{\otimes n}$

$$p_n(\mathcal{E}_0 \neq \mathcal{E}_1) \leq \frac{1 - \frac{1}{2}||\mathcal{E}_0^{\otimes n} - \mathcal{E}_1^{\otimes n}||_\diamond}{2}. \tag{5.37}$$

The fundamental question is now the following: Can we complete Eq. (5.37) with a lower bound? Up today, this lower has been only proven for co-programmable channels (see Eq. (5.8)), with different program states π_0 and π_1. In this case, we have [42].

$$p_n \geq [1 - D(\pi_0^{\otimes n}, \pi_1^{\otimes n})]/2 \tag{5.38}$$

In general, as we already discussed for parameter estimation, this bound is non-achievable. Remarkably, for jointly teleportation-covariant channels the bound is always achievable and the optimal strategy is non-adaptive. Recall that jointly teleportation-covariant channels are such that $\mathcal{S}$ becomes teleportation and the program state is a Choi matrix $\rho_{\mathcal{E}_u}$. For these channels, Ref. [42] found that Eq. (5.37) holds with an equality and we may write $||\mathcal{E}_0^{\otimes n} - \mathcal{E}_1^{\otimes n}||_\diamond = ||\rho_{\mathcal{E}_0}^{\otimes n} - \rho_{\mathcal{E}_1}^{\otimes n}||$.
The aim of the following sections is to establish a *universal* lower bound for $p_n(\mathcal{E}_0 \neq \mathcal{E}_1)$ which is valid for arbitrary channels. As we will show, this is possible by resorting to a more general simulation of the channels involving multi-copy program states, i.e. simulation of the type $\mathcal{S}(\rho \otimes \pi_u^{\otimes M})$.

5.6 Port-based channel simulation

5.6.1 Port-based teleportation and simulation error

Let us describe port-based teleportation for qudit system of arbitrary finite dimension $d \geq 2$ [43,44]. See Fig. 5.3a, for a graphical description.
Alice and Bob exploit two ensembles of $M \geq 2$ qudits, i.e., Alice has $\mathbf{A} := \{A_1, \ldots, A_M\}$ and Bob has $\mathbf{B} := \{B_1, \ldots, B_M\}$ representing the output "ports". The generic ith pair (A_i, B_i) is initialized in a maximally-entangled state, so that the global resource state

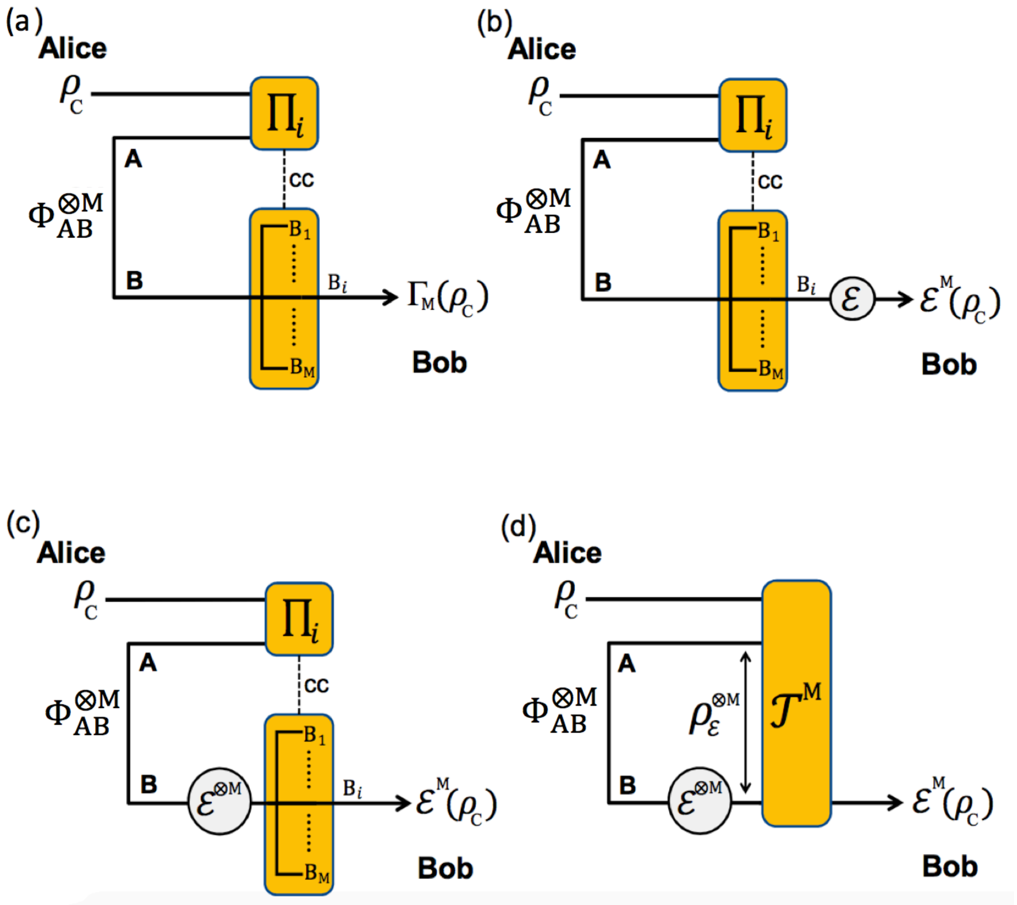

Figure 5.3: From port-based teleportation (PBT) to Choi-simulation of a quantum channel (see also Ref. [43]). **(a)** Schematic representation of the PBT protocol. Alice and Bob share an $M \times M$ qudit state which is given by M maximally-entangled states $\Phi_{\mathbf{AB}}^{\otimes M}$. To teleport an input qubit state ρ_C, Alice applies a suitable POVM $\{\Pi_i\}$ to the input qubit C and her $\mathbf{A}$ qubits. The outcome i is communicated to Bob, who selects the i-th among his $\mathbf{B}$ qubits (tracing all the others). The performance does not depend on the specific "port" i selected and the average output state is given by $\Gamma_M(\rho_C)$ where Γ_M is the PBT channel. The latter reduces to the identity channel in the limit of many ports $M \to \infty$. **(b)** Suppose that Bob applies a quantum channel $\mathcal{E}$ on his teleported output. This produces the output state $\mathcal{E}^M(\rho_C)$ of Eq. (5.54). For large M, one has $\mathcal{E}^M \to \mathcal{E}$ in diamond norm. **(c)** Equivalently, Bob can apply $\mathcal{E}^{\otimes M}$ to all his qubits $\mathbf{B}$ in advance to the CC from Alice. After selection of the port, this will result in the same output as before. **(d)** Now note that Alice's LO and Bob's port selection form a global LOCC $\mathcal{T}^M$ (trace-preserving by averaging over the outcomes). This is applied to a tensor-product state $\rho_{\mathcal{E}}^{\otimes M}$ where $\rho_{\mathcal{E}}$ is the Choi matrix of the original channel $\mathcal{E}$. Thus the approximate channel $\mathcal{E}^M$ is simulated by applying $\mathcal{T}^M$ to $\rho_C \otimes \rho_{\mathcal{E}}^{\otimes M}$ as in Eq. (5.55). This is Fig. 1 from Ref. [9].

reads

$$\Phi_{\mathbf{AB}}^{\otimes M} = \bigotimes_{i=1}^{M} |\Phi\rangle_i\langle\Phi|, \quad |\Phi\rangle_i := d^{-1/2} \sum_k |k\rangle_{A_i} \otimes |k\rangle_{B_i} . \tag{5.39}$$

This resource state may be otimized in a suitable way to increase the performance of the PBT protocol [44]. This is done by acting with an operator on Alice's qudits before detection. This operator unfortunately is non-trace preserving and it cannot be included in our description, where the monotonicity under trace-preserving QOs is crucial. To teleport the state of a qudit C, Alice performs a joint measurement on C and her ensemble $\mathbf{A}$. This is a POVM $\{\Pi_{C\mathbf{A}}^i\}_{i=1}^M$ with M possible outcomes, see Refs. [43, 44] for more details. As soon as Alice communicates the outcome i to Bob, he discards all the ports but the ith one, which contains the teleported state (see Fig. 1a). The scheme is invariant under permutations of the Bell pairs and , therefore, of the ports. For this reason the equiprobable measurement outcomes are independent of the input, and the output is invariant under permutation of the ports. By averaging over the outcomes, we define the teleported state

$$\rho_B^M = \Gamma_M(\rho_C) \ , \tag{5.40}$$

where Γ_M is the corresponding PBT channel explicitly given by the following representation

$$\Gamma_M(\rho_C) = \sum_{i=1}^{M} \mathrm{Tr}_{\mathbf{A}\bar{B}_i C} \left[\Pi_{C\mathbf{A}}^i \left(\rho_C \otimes \Phi_{\mathbf{AB}}^{\otimes M}\right)\right] \ , \tag{5.41}$$

where $\mathrm{Tr}_{\bar{B}_i}$ denotes the trace over all ports $\mathbf{B}$ but B_i In the limit of many ports M, we have that Γ_M approximates an identity channel $\mathcal{I}$ so that Bob's output becomes a perfect replica of Alice's input. More precisely, for any M, we prove that in the diamond norm we have the following error.

Lemma 5.6.1 ([9]) *In arbitrary finite dimension d, the diamond distance between the M-port PBT channel Γ_M and the identity channel $\mathcal{I}$ satisfies*

$$\delta_M := ||\mathcal{I} - \Gamma_M||_\diamond \leq 2d(d-1)M^{-1} \ . \tag{5.42}$$

Proof: As noted in Ref. [160], the channel Γ_M associated with the qudit PBT protocol of Ref. [43] is covariant under unitary transformations, i.e.,

$$\Gamma_M(U\rho U^\dagger) = U\Gamma_M(\rho)U^\dagger, \tag{5.43}$$

for any input state ρ and unitary operator U. Ref. [160] has also shown that, for a channel with such a symmetry, the diamond distance with the identity map is saturated by a maximally entangled state, i.e.,

$$\|\mathcal{I}-\Gamma_M\|_\diamond = \| |\Phi\rangle\langle\Phi| - \mathcal{I}\otimes\Gamma_M\left(|\Phi\rangle\langle\Phi|\right)\| \,, \tag{5.44}$$

where $|\Phi\rangle = d^{-1/2}\sum_{k=1}^{d}|k\rangle|k\rangle$. Here we further show that

$$\| |\Phi\rangle\langle\Phi| - \mathcal{I}\otimes\Gamma_M\left(|\Phi\rangle\langle\Phi|\right)\| = 2[1-f_e(\Gamma_M)] \ , \tag{5.45}$$

where $f_e(\Gamma_M)$ is the entanglement fidelity of the PBT channel Γ_M, i.e. $f_e(\Gamma_M) := \operatorname{Tr}|\Psi\rangle\langle\Psi|(\mathcal{I}_r\otimes\Gamma_M)|\Psi\rangle\langle\Psi|$, where the purification $|\Psi\rangle$ is such that $\rho_C = \operatorname{Tr}_r|\Psi\rangle_{rC}\langle\Psi|$. In order to prove EQ. (5.45), first note that the map $\Lambda_M = \mathcal{I}\otimes\Gamma_M$ is covariant under twirling unitaries of the form $U\otimes U^*$, i.e.,

$$\begin{aligned}&\Lambda_M\left[(U\otimes U^*)\rho(U\otimes U^*)^\dagger\right]\\ &= (U\otimes U^*)\Lambda_M(\rho)(U\otimes U^*)^\dagger,\end{aligned} \tag{5.46}$$

for any input state ρ and unitary operator U. This implies that the state $\Lambda_M(|\Phi\rangle\langle\Phi|)$ is invariant under twirling unitaries, i.e.,

$$(U\otimes U^*)\Lambda_M(|\Phi\rangle\langle\Phi|)(U\otimes U^*)^\dagger = \Lambda_M(|\Phi\rangle\langle\Phi|) \ . \tag{5.47}$$

This is therefore an isotropic state of the form

$$\Lambda_M(|\Phi\rangle\langle\Phi|) = p|\Phi\rangle\langle\Phi| + \frac{1-p}{d^2}\mathbb{I}, \tag{5.48}$$

where $\mathbb{I}$ is the two-qudit identity operator. We may rewrite this state as follows

$$\Lambda_M(|\Phi\rangle\langle\Phi|) = F|\Phi\rangle\langle\Phi| + (1-F)\rho^\perp, \tag{5.49}$$

where $\rho^\perp$ is state with support in the orthogonal complement of Φ, and F is the singlet fraction

$$F := \langle\Phi|\Lambda_M(|\Phi\rangle\langle\Phi|)|\Phi\rangle = p + (1-p)d^{-2}. \tag{5.50}$$

Thanks to the decomposition in Eq. (5.49) and using basic properties of the trace norm, we may then write

$$\begin{aligned}&\| |\Phi\rangle\langle\Phi| - \Lambda_M\left(|\Phi\rangle\langle\Phi|\right)\|\\ &= \|(1-F)|\Phi\rangle\langle\Phi| - (1-F)\rho^\perp\|\\ &= (1-F)\||\Phi\rangle\langle\Phi|\| + (1-F)\|\rho^\perp\|\\ &= 2(1-F)\\ &= 2[1-f_e(\Gamma_M)],\end{aligned} \tag{5.51}$$

where the last step exploits the fact that the singlet fraction F is the channel's entanglement fidelity $f_e(\Gamma_M)$.

Finally, we use the fact that the entanglement fidelity of Γ_M is bounded as [45]

$$f_e(\Gamma_M) \geq 1 - d(d-1)M^{-1}. \tag{5.52}$$

Therefore, combining Eqs. (5.44), (5.45), and (5.52), we derive

$$\|\mathcal{I} - \Gamma_M\|_\diamond \leq 2d(d-1)M^{-1} \quad \blacksquare\ . \tag{5.53}$$

5.6.2 Channel simulation via PBT

Channel simulation through PBT was first shown in Ref. [45] where PBT was introduced as a possible design for a programmable quantum gate array [38]. As depicted in Fig. 5.3b, suppose that Bob applies an arbitrary channel $\mathcal{E}$ to the teleported output, so that Alice's input ρ_C undergoes the action of the following approximate channel

$$\mathcal{E}^M(\rho_C) := \mathcal{E} \circ \Gamma_M(\rho_C). \tag{5.54}$$

Note that the port selection commutes with $\mathcal{E}$, because the POVM acts on a different Hilbert space [45]. Therefore, Bob can equivalently apply $\mathcal{E}$ to each port before Alice's CC, i.e., apply $\mathcal{E}^{\otimes M}$ to his $\mathbf{B}$ qudits before selecting the output port, as shown in Fig. 5.3c. This leads to the following simulation for the approximate channel

$$\mathcal{E}^M(\rho_C) = \mathcal{T}^M(\rho_C \otimes \rho_{\mathcal{E}}^{\otimes M})\ , \tag{5.55}$$

where $\mathcal{T}^M$ is a trace-preserving LOCC and $\rho_{\mathcal{E}}$ is the channel's Choi matrix (see Fig. 5.3d). By construction, the simulation LOCC $\mathcal{T}^M$ is universal, i.e., it does not depend on the channel $\mathcal{E}$. This means that, at fixed M, the channel $\mathcal{E}^M$ is fully determined by the program state $\rho_{\mathcal{E}}$. One can bound the accuracy of the simulation. From Eq. (5.54) and the monotonicity of the diamond norm, we get [9]

$$||\mathcal{E} - \mathcal{E}^M||_\diamond \leq \delta_M, \tag{5.56}$$

where δ_M is the simulation error in Eq. (5.42), with the dimension d being the dimension of the input Hilbert space.

5.7 Port-based teleportation stretching of an adaptive protocol

Channel simulation with port-based teleportation develops similarly to the simulation with standard teleportation and it is at the core of the PBT stretching. The main difference is at the level of the propagation of the error in the simulation which comes form the approximation of the channel at a finite number of copies M of resource state. To achieve the PBT stretching of an adaptive protocol, we first need to replace each channel $\mathcal{E}$ with its M-port approximation $\mathcal{E}^M$ while controlling the propagation of the simulation error δ_M from the channel to the output state. As we have see this is a crucial step also in simulations via standard teleportation. Second, we need to "stretch" the protocol by replacing the approximate channel $\mathcal{E}^M$ with its Choi matrices $\rho_{\mathcal{E}}^{\otimes M}$ and then suitably reorganize all the remaining QOs. Here we describe the technique for a generic task, before specifying it for QCD.

Given an adaptive protocol $\mathcal{P}_n$ over a channel $\mathcal{E}$ with output ρ_n, consider the same protocol over the simulated channel $\mathcal{E}^M$, so that we get the different output ρ_n^M. Later in Sec. 5.7.1, using the "peeling" argument, we bound the output error in terms of the channel simulation error

$$||\rho_n - \rho_n^M|| \leq n||\mathcal{E} - \mathcal{E}^M||_\diamond \leq n\delta_M. \tag{5.57}$$

Once understood that the output state can be closely approximated, let us simplify the adaptive protocol over $\mathcal{E}^M$. Using the simulation in Eq. (5.55), we may replace each channel $\mathcal{E}^M$ with the resource state $\rho_{\mathcal{E}}^{\otimes M}$, iterate the process for all n uses, and collapse all the simulation LOCCs and QOs as shown in Fig. 5.4. As a result, we may write the multi-copy Choi decomposition

$$\rho_n^M = \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM}) \ , \tag{5.58}$$

for a trace-preserving QO $\bar{\Lambda}$. Now, we can combine the two ingredients of Eqs. (5.57) and (5.58), into the following

Lemma 5.7.1 (PBT stretching [9]) *Consider an adaptive quantum protocol (with arbitrary task) over an arbitrary d-dimensional quantum channel $\mathcal{E}$ (which may be unknown and parametrized). After n uses, the output ρ_n of the protocol can be decomposed as follows*

$$||\rho_n - \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM})|| \leq n\delta_M, \tag{5.59}$$

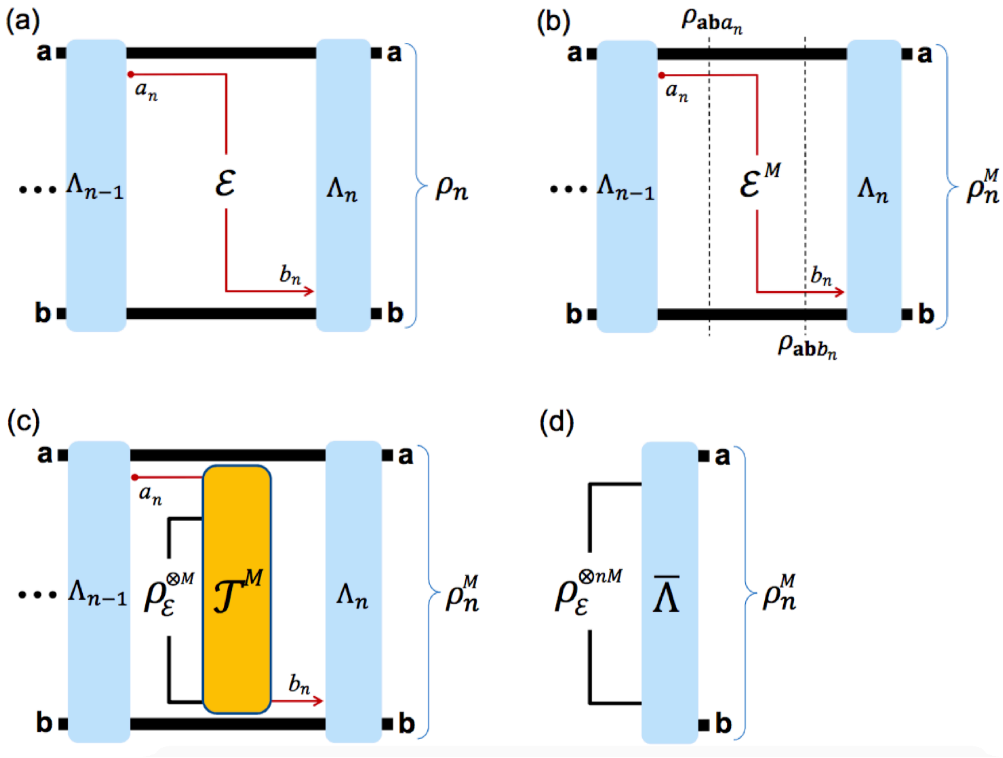

Figure 5.4: Port-based teleportation stretching of a generic adaptive protocol over a quantum channel $\mathcal{E}$. **(a)** We show the last transmission $a_n \to b_n$ through $\mathcal{E}$, which occurs between two adaptive QOs Λ_{n-1} and Λ_n. This last step produces the output state ρ_n. **(b)** In each transmission, we replace $\mathcal{E}$ with its M-port simulation $\mathcal{E}^M$ so that the output of the protocol becomes ρ_n^M which approximates ρ_n for large M. Note that, in the last transmission, the register state $\rho_{\mathbf{ab}a_n}$ undergoes the transformation $\rho_{\mathbf{ab}b_n} = \mathcal{I}_{\mathbf{ab}} \otimes \mathcal{E}^M(\rho_{\mathbf{ab}a_n})$. **(c)** Each propagation through $\mathcal{E}^M$ is replaced by its PBT simulation. For the last transmission, this means that $\rho_{\mathbf{ab}b_n} = \mathcal{I}_{\mathbf{ab}} \otimes \mathcal{T}^M(\rho_{\mathbf{ab}a_n} \otimes \rho_{\mathcal{E}}^{\otimes M})$ where $\mathcal{T}^M$ is the LOCC of the PBT and $\rho_{\mathcal{E}}$ is the Choi matrix of the original channel. **(d)** All the adaptive QOs Λ_i and the simulation LOCCs $\mathcal{T}^M$ are collapsed into a single (trace-preserving) QO $\bar{\Lambda}$. Correspondingly, n instances of $\rho_{\mathcal{E}}^{\otimes M}$ are collected. As a result, the approximate output ρ_n^M is given by $\bar{\Lambda}$ applied to the tensor-product state $\rho_{\mathcal{E}}^{\otimes nM}$ as in Eq. (5.58). This is Fig. 2 from Ref. [9].

where $\bar{\Lambda}$ is a trace-preserving QO, $\rho_{\mathcal{E}}$ is the Choi matrix of $\mathcal{E}$, and δ_M is the M-port simulation error in Eq. (5.42).

In protocols of channel estimation or discrimination, where $\mathcal{E}$ is parametrized, we may write Eq. (5.59) with $\rho_{\mathcal{E}}$ storing the parameter of the channel. In particular, for QCD we have $\{\mathcal{E}_u\}_{u=0,1}$ and the output $\rho_n(u)$ of the adaptive protocol $\mathcal{P}_n$ can be decomposed as follows

$$||\rho_n(u) - \bar{\Lambda}(\rho_{\mathcal{E}_u}^{\otimes nM})|| \leq n\delta_M. \tag{5.60}$$

5.7.1 Propagation of the simulation error

For the sake of completeness, we now give the proof of the first inequality in Eq. (5.57). Consider the adaptive protocol described in the main text. For the n-use output state we may compactly write

$$\rho_n = \Lambda_n \circ \mathcal{E} \circ \Lambda_{n-1} \circ \cdots \circ \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0), \tag{5.61}$$

where Λ's are adaptive QOs and $\mathcal{E}$ is the channel applied to the transmitted signal system. Then, ρ_0 is the preparation state of the registers, obtained by applying the first QO Λ_0 to some fundamental state. Similarly, for the M-port simulation of the protocol, we may write

$$\rho_n^M = \Lambda_n \circ \mathcal{E}^M \circ \Lambda_{n-1} \circ \cdots \circ \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0), \tag{5.62}$$

where $\mathcal{E}^M$ is in the place of $\mathcal{E}$. (Note that the following reasoning applies to a fixed channel $\mathcal{E}$ or, more generally, to classically-parametrized unknown channel $\mathcal{E}_u$).

Consider now two instances ($n = 2$) of the adaptive protocol. We may bound the trace distance between ρ_2 and ρ_2^M using the same "peeling" argument leading to Eq. (2.74)

$$\begin{aligned} \left\|\rho_2 - \rho_2^M\right\| &= ||\Lambda_2 \circ \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0) \\ &- \Lambda_2 \circ \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)|| \\ &\overset{(1)}{\leq} ||\mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0) - \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)|| \\ &\overset{(2)}{\leq} ||\mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0) - \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)|| \\ &+ ||\mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}(\rho_0) - \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)|| \\ &\overset{(3)}{\leq} ||\mathcal{E}(\rho_0) - \mathcal{E}^M(\rho_0)|| \\ &+ ||\mathcal{E}[\Lambda_1 \circ \mathcal{E}^M(\rho_0)] - \mathcal{E}^M[\Lambda_1 \circ \mathcal{E}^M(\rho_0)]|| \\ &\overset{(4)}{\leq} 2||\mathcal{E} - \mathcal{E}^M||_\diamond \,. \end{aligned} \tag{5.63}$$

In (1) we use the monotonicity of the trace distance under completely-positive trace-preserving (CPTP) maps (i.e., quantum channels); in (2) we employ the triangle inequality; in (3) we use the monotonicity with respect to the the CPTP map $\mathcal{E} \circ \Lambda_1$ whereas in (4) we exploit the fact that the diamond norm is an upper bound for the trace norm computed on any input state. Generalizing the result of Eq. (5.63) to arbitrary n, we achieve the first inequality in Eq. (5.57)

5.7.2 A fundamental lower bound for the error probability

We have now all the necessary ingredients to derive the lower bound for the minimum probability of error $p_n(\mathcal{E}_0 \neq \mathcal{E}_1)$ in Eq. (5.37), affecting the symmetric discrimination of two arbitrary finite dimensional quantum channels. Consider an arbitrary protocol $\mathcal{P}_n$, for which we may write Eq. (5.35). Combining Lemma 2 with the triangle inequality leads to

$$\begin{aligned} ||\rho_n(0) - \rho_n(1)|| &\leq 2n\delta_M + ||\bar{\Lambda}(\rho_{\mathcal{E}_0}^{\otimes nM}) - \bar{\Lambda}(\rho_{\mathcal{E}_1}^{\otimes nM})|| \\ &\leq 2n\delta_M + ||\rho_{\mathcal{E}_0}^{\otimes nM} - \rho_{\mathcal{E}_1}^{\otimes nM}||, \end{aligned} \tag{5.64}$$

where we also use the monotonicity of the trace distance under channels. Because $\bar{\Lambda}$ is discarded, the bound does no longer depend on the details of the protocol $\mathcal{P}_n$, which means that it applies to all adaptive protocols. Thus, using Eq. (5.64) in Eqs. (5.35) and (5.36), we get the following.

Theorem 5.7.2 ([9]) *Consider the adaptive discrimination of two channels $\{\mathcal{E}_u\}_{u=0,1}$ in dimension d. After n probings, the minimum error probability satisfies the bound*

$$p_n(\mathcal{E}_0 \neq \mathcal{E}_1) \geq B := \frac{1 - n\delta_M - D(\rho_{\mathcal{E}_0}^{\otimes nM}, \rho_{\mathcal{E}_1}^{\otimes nM})}{2}, \tag{5.65}$$

where M may be chosen to maximize the right hand side.

Let us bound the trace distance in Eq. (5.65) as [83]

$$D^2 \leq 1 - F^{2nM},\ F := \mathrm{Tr}\sqrt{\sqrt{\rho_{\mathcal{E}_1}}\rho_{\mathcal{E}_2}\sqrt{\rho_{\mathcal{E}_1}}}, \tag{5.66}$$

where F is the fidelity between the Choi matrices of the channels. If we also exploit Eq. (5.42), we may write

$$B \geq \frac{1}{2} - \frac{\sqrt{1 - F^{2nM}}}{2} - \frac{d(d-1)n}{M}\,. \tag{5.67}$$

In the previous formula there are terms with opposite monotonicity in M. For this reason, the maximum value of B is achieved at some intermediate value of M.

One possible choice[2] is $M = 4d(d-1)n$, so that $B \geq (1 - 2\sqrt{1 - F^{8d(d-1)n^2}})/4$. In particular, consider two infinitesimally-close channels, so that $F \simeq 1 - \epsilon$ where $\epsilon \simeq 0$ is the infidelity. By expanding in ϵ, we may write [9]

$$B \geq \frac{1}{4} - n\sqrt{2d(d-1)\epsilon} \simeq \frac{\exp(-4n\sqrt{2d(d-1)\epsilon})}{4}. \tag{5.68}$$

Discriminating between two close quantum channels is a problem in many physical scenarios. For instance, this is typical in quantum illumination [51–54, 155–159] (discussed below), quantum optical resolution [48,50] (mentioned below), ideal quantum reading [46,47] and also tests of quantum field theories in non-inertial frames [161], e.g., for detecting effects such as the Unruh or the Hawking radiation.

5.8 Ultimate limit of adaptive quantum illumination

5.8.1 Standard (non-adaptive) protocol

In quantum illumination [51–53, 155], the aim is to determine whether a low-reflectivity object is present or not in a region with thermal noise. We therefore prepare a signal system s and an idler system i in a joint entangled state ρ_{si}. The signal system is sent to probe the target while the idler system is retained for its measurement together with the potential signal reflection from the target. If the object is absent, the "reflected" system is just thermal background noise. If the object is present, then this is composed of the actual reflection of the signal from the target plus thermal background noise. This object can be modelled by a beam splitter, with very small transmissivity $\eta \ll 1$, which combines the each incoming optical mode (signal system) with a thermal mode with b mean number of photons.

In the discrete-variable version of quantum illumination [155], the signal system is prepared in an ensemble of d optical modes, with 1 photon in one of the modes and vacuum in the others. This is the number of modes which are distinguished by the detector in each

[2] In general, by setting $M = xnd(d1)$ for some $x > 2$, we get $B \geq 1/2 - 1/x - 1/2\sqrt{1F^{2xd(d1)^2}}$.

detection process. If we introduce the following $d-$dimensional computational basis

$$|1\rangle := \overbrace{|00\dots01\rangle}^{d}, \tag{5.69}$$

$$|2\rangle := |00\dots10\rangle\,, \tag{5.70}$$

$$\vdots$$

$$|d-1\rangle := |01\dots00\rangle\,, \tag{5.71}$$

$$|d\rangle := |10\dots00\rangle\,, \tag{5.72}$$

then the entangled signal-idler state can be written as

$$\psi_{si} = |\psi\rangle_{si}\,\langle\psi|\,, \quad |\psi\rangle_{si} = d^{-1/2}\sum_{k=1}^{d}|kk\rangle_{si}\ . \tag{5.73}$$

Let us define the d-dimensional identity operator $\mathbb{I}^d := \sum_{k=1}^{d}|k\rangle\,\langle k|$ which projects onto the subspace spanned by the 1-photon states, and the $(d+1)$-dimensional identity operator $\mathbb{I}^{d+1} := \sum_{k=0}^{d}|k\rangle\,\langle k|$ which also includes the vacuum state $|0\rangle := |00\dots00\rangle$. Then, we have the reduced idler state

$$\psi_i := \mathrm{Tr}_s(\psi_{si}) = d^{-1}\mathbb{I}_i^d, \tag{5.74}$$

and we define the thermal state of the environment as [155]

$$\rho^{\mathrm{th}}(b) := (1-db)|0\rangle\langle 0| + b\mathbb{I}^d, \tag{5.75}$$

where b is the mean number of thermal photons per mode. Here $b \ll 1$ and $db \ll 1$, where db is the mean number of thermal photons in each detection event.

The output $(d+1)\times d$ state of the reflected signal and retained idler is given by

$$\begin{aligned} \text{Target absent:} \quad & \sigma = \rho^{\mathrm{th}}(b)\otimes d^{-1}\mathbb{I}_i^d, \\ \text{Target present:} \quad & \rho = (1-\eta)\sigma + \eta\psi_{si}. \end{aligned} \tag{5.76}$$

If the target is probed n times, then we may use the QCB to bound Q the error probability p_{err} in the discrimination of ρ and σ. In the regime of signal-to-noise-ratio $\eta d/b \lesssim 1$, one finds [155]

$$Q = 1 - \frac{\eta^2 d}{8b} + \mathcal{O}(b^2, \eta b)\ , \tag{5.77}$$

which tightens the QCB by a factor d with respect to the unentangled case where $Q \approx 1-\eta^2/(8b)$. From Eq. (5.77), we may write the following bound for the error probability of target detection after n probings [155]

$$p_n(\sigma \neq \rho) \leq \frac{1}{2}\exp\left(-\frac{\eta^2 dn}{8b}\right). \tag{5.78}$$

In particular, for $\eta d/b \simeq 1$, this can be written as

$$p_n(\sigma \neq \rho) \leq \frac{1}{2} \exp\left(-\frac{\eta n}{8}\right). \tag{5.79}$$

5.8.2 Adaptive protocol

The adaptive formulation of the discrete variable protocol of quantum illumination assumes an unlimited quantum computer with two register **a** and **b**, prepared in an arbitrary joint quantum state. In each probing, a system a is picked from the input register **a** and sent to the target. Its reflection a' is stored in the output register **b**. A adaptive quantum operation (QO) is applied to both the update registers before the next transmission and so on. Therefore any probing is interleaved by the application of adaptive QOs Λ's to the registers, defining the adaptive protocol $\mathcal{P}_n$ (see also the main text for this description). After n probings, the state of the registers is $\rho_n(u)$ where $u = 0, 1$ is a bit encoding the absence or presence of the target. This state is optimally measured by an Helstrom POVM. By optimizing over all protocol $\mathcal{P}_n$, we define the minimum error probability p_n for adaptive quantum illumination.

Following the constraints and typical regime of DV quantum illumination, we assume that the signal systems are $(d+1)$-dimensional qudits described by a basis $\{|0\rangle, |1\rangle, \ldots, |d\rangle\}$, where $|i\rangle := |0\cdots 010\cdots 0\rangle$ has one photon in the ith mode. For this reason, the two possible quantum illumination channels, $\mathcal{E}_0$ and $\mathcal{E}_1$, are $(d+1)$-dimensional channels. In particular, consider as their input the maximally-entangled state

$$\Psi_{si} = \frac{1}{d+1} \sum_{k,j=0}^{d} |kk\rangle_{si}\langle jj|, \tag{5.80}$$

which is similar to ψ_{si} in Eq. (5.73) but also includes the vacuum state. Then, we may write the following two $(d+1) \times (d+1)$ dimensional Choi matrices

$$\begin{aligned} \text{Target absent:} \quad & \sigma := \rho_{\mathcal{E}_0} = \rho^{\text{th}}(b) \otimes (d+1)^{-1}\mathbb{I}_i^{d+1}, \\ \text{Target present:} \quad & \rho := \rho_{\mathcal{E}_1} = (1-\eta)\sigma + \eta\Psi_{si}. \end{aligned} \tag{5.81}$$

It is clear that $\mathcal{E}_0$ and $\mathcal{E}_1$ are not jointly teleportation-covariant due to the fact that they have different transmissivities ($\eta_0 = 0$ and $\eta_1 = \eta$).

To bound p_n we apply Theorem 5.7.2 of the main text and, more specifically, Eq. (5.68) of the main text, because $\eta \ll 1$ and, therefore, the fidelity between the Choi matrices can be expanded as $F(\sigma, \rho) \simeq 1 - \epsilon$. Thus, let us start by computing this fidelity. Let us set $x = \sqrt{1 - bd}$ and note that we may write

$$\sqrt{\sigma} = (x|0\rangle_s\langle 0| + \sqrt{b}\mathbb{I}_s^d) \otimes (d+1)^{-1/2}\mathbb{I}_i^{d+1}. \tag{5.82}$$

Then, we may compute

$$\begin{aligned}\Omega^2 :&= \sqrt{\sigma}\rho\sqrt{\sigma}\\ &= \frac{1}{(d+1)^2}\left\{(1-\eta)\left[x^4|0\rangle_s\langle 0| + b^2\mathbb{I}_s^d\right]\otimes\mathbb{I}_i^{d+1}\right.\\ &\left.+\eta\left[x^2|00\rangle_{si}\langle 00| + \sqrt{b}x\sum_{k=1}^{d}(|00\rangle_{si}\langle kk| + |kk\rangle_{si}\langle 00|) + b\sum_{j,k=1}^{d}|kk\rangle_{si}\langle jj|\right]\right\}.\end{aligned} \tag{5.83}$$

One can check that Ω^2 has d^2 degenerate eigenvalues equal to $b^2(d+1)^{-2}$, d degenerate eigenvalues equal to $(1-\eta)x^4(d+1)^{-2}$, and other $d+1$ eigenvalues $\{\lambda_i\}$ given by the diagonalization of the matrix $(d+1)^{-2}\mathbf{M}$ where $\mathbf{M}$ is the matrix with elements

$$M_{1,1} = (1-\eta)x^4 + \eta x^2 \quad , \quad M_{i,i} = b(b+\eta)\ , i \neq 1 \tag{5.84}$$

$$M_{1,j} = M_{j,1} = \eta x\sqrt{b} \quad , \quad M_{i,j} = \eta b\ , i \neq j \tag{5.85}$$

Once we diagonalize Ω^2 we take the square root of its eigenspectrum so as to compute that of Ω. Finally, their sum provides $\mathrm{Tr}\Omega = F(\sigma,\rho)$. We are interested in the regime of low thermal noise $b \ll 1$ and low reflectivity $\eta \ll 1$, thus we may expand at the leading orders in η and b to get

$$F(\sigma,\rho) = 1 - \frac{\eta d + 2b - 2\sqrt{\eta d b}}{2(d+1)} + \mathcal{O}(\eta^2, \eta^{3/2}b^{1/2}, \eta b, b^{3/2}) \tag{5.86}$$

$$= 1 - \frac{\eta d}{2(d+1)} + \mathcal{O}(\eta^2, \sqrt{\eta b}, b). \tag{5.87}$$

In the typical signal-to-noise-ratio $\eta d/b \simeq 1$ of quantum illumination [155], we may directly re-write Eq. (5.86) as $F(\sigma,\rho) \simeq 1-\epsilon$, where

$$\epsilon := \frac{\eta d + 2b - 2\sqrt{d\eta b}}{2(d+1)} \simeq \frac{d\eta}{2(d+1)} < \eta/2. \tag{5.88}$$

By replacing the latter in Eq. (5.68) of the main text (and assuming the correct dimension $d \to d+1$), we get the following lower bound for the minimum error probability p_n of adaptive quantum illumination [9]

$$p_n \geq \frac{1}{4}\exp(-4nd\sqrt{\eta}). \tag{5.89}$$

5.8.3 Single-photon quantum optical resolution

Consider a microscope-type problem where we aim at locating a point in two possible positions, either $s/2$ or $-s/2$, where the separation s is very small. Assume we are limited to use probe states with at most one photon and an output finite-aperture optical system (this makes the optical process to be a qubit-to-qutrit channel, so that the input dimension is $d = 2$). Apart from this, we are allowed to use an arbitrary large quantum computer and arbitrary QOs to manipulate its registers. We may apply Eq. (5.68) with $\epsilon \simeq \eta s^2/16$, where η is a diffraction-related loss parameter. In this way, we find that the error probability affecting the discrimination of the two positions is approximately bounded by $B \gtrsim \frac{1}{4}\exp(-2ns\sqrt{\eta})$ [9].

5.9 Port-based teleportation implies the Heisenberg scaling

As already fully discussed in Sec. 5.2, the adaptive estimation of a noise parameter θ encoded in a teleportation-covariant channel (i.e., such that the parametrized class of channels $\mathcal{E}_\theta$ is jointly-teleportation covariant) is limited to the standard quantum limit (SQL). More generally, the adaptive estimation of a parameter in a quantum channel cannot beat the SQL if the channel has a single-copy simulation, i.e., of the type

$$\mathcal{E}_\theta(\rho) = \mathcal{S}(\rho \otimes \pi_\theta), \tag{5.90}$$

where $\mathcal{S}$ is a (parameter-independent) trace-preserving QO and π_θ is a program state (depending on the parameter). To beat the SQL, the channel should not admit a simulation as in Eq. (5.90) but a multi-copy version

$$\mathcal{E}_\theta(\rho) = \mathcal{S}(\rho \otimes \pi_\theta^{\otimes M}), \tag{5.91}$$

for some $M > 1$. This is approximately the type of simulation that we can achieve by using PBT.

First of all, we may replace the channel $\mathcal{E}_\theta$ with its M-port approximation $\mathcal{E}_\theta^M := \mathcal{E}_\theta \circ \Gamma_M$, where Γ_M is the M-port PBT channel. Using Lemma 5.6.1, the simulation error may be bounded as

$$||\mathcal{E}_\theta - \mathcal{E}_\theta^M||_\diamond \leq \delta_M := ||\mathcal{I} - \Gamma_M||_\diamond \leq 2\beta M^{-1}, \tag{5.92}$$

where we set $\beta := d(d-1)$. By repeating the steps shown in Fig. 5.3, we may write the metrological equivalent of Eq. (5.55). In other words, for any input state ρ_C, we may write the simulation

$$\mathcal{E}_\theta^M(\rho_C) = \mathcal{T}^M(\rho_C \otimes \rho_{\mathcal{E}_\theta}^{\otimes M}), \tag{5.93}$$

where $\mathcal{T}^M$ is a trace-preserving LOCC and $\rho_{\mathcal{E}_\theta}$ is the Choi matrix of $\mathcal{E}_\theta$. Then, we may also repeat the PBT stretching in Fig. 5.4. In this way, the n-use output state $\rho_n = \rho_n(\theta)$

of an adaptive parameter estimation protocol can be decomposed as in Lemma 5.7.1, i.e.,

$$||\rho_n(\theta) - \bar{\Lambda}(\rho_{\mathcal{E}_\theta}^{\otimes nM})|| \leq n\delta_M. \tag{5.94}$$

Using the decomposition in Eq. (5.94), we may write a bound for the optimal quantum Fisher information $\overline{\mathrm{QFI}}_\theta^n := \sup_{\mathcal{P}_n} \mathrm{QFI}_\theta[\mathcal{P}_n]$, where $\mathrm{QFI}_\theta[\mathcal{P}_n]$ is the QFI associated with the protocol $\mathcal{P}_n$. For large n, we obtain the Heisenberg scaling [9]

$$\overline{\mathrm{QFI}}_\theta^n \lesssim n^2 \mathrm{QFI}(\rho_{\mathcal{E}_\theta}), \tag{5.95}$$

where

$$\mathrm{QFI}(\rho_{\mathcal{E}_\theta}) = \frac{4d_B^2(\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_{\theta+d\theta}})}{d\theta^2}. \tag{5.96}$$

In order to prove Eq. (5.95), consider the function

$$q_n(\theta, \delta) = 2\frac{d_B[\rho_n(\theta), \rho_n(\theta+\delta)]}{\delta}. \tag{5.97}$$

We set $u_\theta := \bar{\Lambda}(\rho_{\mathcal{E}_\theta}^{\otimes nM})$ and apply twice the triangular inequality, so that we may write

$$\begin{aligned} d_B[\rho_n(\theta), \rho_n(\theta+\delta)] \leq{}& d_B[\rho_n(\theta), u_\theta] + \\ & d_B[u_\theta, u_{\theta+\delta}] + d_B[u_{\theta+\delta}, \rho_n(\theta+\delta)]. \end{aligned} \tag{5.98}$$

Bounding the Bures distance with the trace distance, we get

$$d_B^2[\rho_n(\theta), u_\theta] \leq \frac{\|\rho_n(\theta) - u_\theta\|}{2} \leq \frac{n\delta_M}{2} \leq \frac{\beta n}{M}. \tag{5.99}$$

Using Eqs. (5.98) and (5.99), we may write

$$q_n(\theta, \delta) \leq 2\frac{d_B[u_\theta, u_{\theta+\delta}]}{\delta} + \frac{4}{\delta}\sqrt{\frac{\beta n}{M}}. \tag{5.100}$$

We may bound d_B in Eq. (5.100) as follows

$$\begin{aligned} d_B[u_\theta, u_{\theta+\delta}] &\overset{(1)}{\leq} d_B[\rho_{\mathcal{E}_\theta}^{\otimes nM}, \rho_{\mathcal{E}_{\theta+\delta}}^{\otimes nM}] \\ &\overset{(2)}{=} \sqrt{2[1 - F(\rho_{\mathcal{E}_\theta}^{\otimes nM}, \rho_{\mathcal{E}_{\theta+\delta}}^{\otimes nM})]} \\ &\overset{(3)}{=} \sqrt{2(1 - F^{nM})} \overset{(4)}{\leq} \sqrt{2nM(1-F)} \\ &\overset{(2)}{=} \sqrt{nM} d_B[\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_{\theta+\delta}}], \end{aligned} \tag{5.101}$$

where: (1) we use the monotonicity of the Bures distance under the CPTP map $\bar{\Lambda}$, (2) we use the standard relation between Bures distance and fidelity, (3) we set $F := F(\rho_{\mathcal{E}_\theta}, \rho_{\mathcal{E}_{\theta+\delta}})$

and exploit the multiplicativity of the fidelity over tensor products, and (4) we use the inequality $F^n \geq 1 - n + nF$. Therefore, from Eq. (5.100), we may derive the inequality

$$q_n(\theta,\delta) \leq 2\sqrt{nM}\frac{d_B[\rho_{\mathcal{E}_\theta},\rho_{\mathcal{E}_{\theta+\delta}}]}{\delta} + \frac{4}{\delta}\sqrt{\frac{\beta n}{M}}. \tag{5.102}$$

Now notice that

$$\lim_{\delta\to 0} 2\frac{d_B[\rho_{\mathcal{E}_\theta},\rho_{\mathcal{E}_{\theta+\delta}}]}{\delta} = \sqrt{\mathrm{QFI}(\rho_{\mathcal{E}_\theta})}. \tag{5.103}$$

This means that for any $\epsilon > 0$, there is $\delta < \delta_\epsilon$ such that

$$q_n(\theta,\delta) \leq \sqrt{nM}\left[\sqrt{\mathrm{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon\right] + \frac{4}{\delta}\sqrt{\frac{\beta n}{M}}. \tag{5.104}$$

Setting $M = n^{1+z}$ (for any $z > 0$) implies

$$\begin{aligned} q_n(\theta,\delta) &\leq \kappa_n(\theta,\delta|\epsilon,z) \qquad (5.105)\\ &:= \sqrt{n^{2+z}}\left[\sqrt{\mathrm{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon\right] + \frac{4}{\delta}\sqrt{\frac{\beta}{n^z}}. \end{aligned}$$

Note that, by definition, $\mathrm{QFI}^n_\theta := \lim_{\delta\to 0} q_n(\theta,\delta)^2$. Then, assume that the limit

$$\lim_{n\to\infty}\lim_{\delta\to 0}\frac{q_n(\theta,\delta)^2}{n^{2+z}} \tag{5.106}$$

exists for any $z > 0$. Then, using Eq. (5.105), which is valid for any n and δ, we may write

$$\begin{aligned} \lim_{n\to\infty}\lim_{\delta\to 0}\frac{q_n(\theta,\delta)}{\sqrt{n^{2+z}}} &\leq \liminf_{n\to\infty,\ \delta\to 0}\frac{\kappa_n(\theta,\delta|\epsilon,z)}{\sqrt{n^{2+z}}} \\ &\leq \sqrt{\mathrm{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon. \qquad (5.107) \end{aligned}$$

The previous inequality leads to

$$\lim_{n\to\infty}\frac{\mathrm{QFI}^n_\theta}{n^{2+z}} \leq \left[\sqrt{\mathrm{QFI}(\rho_{\mathcal{E}_\theta})} + \epsilon\right]^2, \tag{5.108}$$

for any $\epsilon, z > 0$. Now, sending ϵ and z to zero gives the following scaling for large n

$$\mathrm{QFI}^n_\theta \lesssim n^2\mathrm{QFI}(\rho_{\mathcal{E}_\theta})\ . \tag{5.109}$$

Since this upper bound holds for any protocol P (because $\bar{\Lambda}$ disappears), then the asymptotic scaling in Eq. (5.109) may be extended to $\overline{\mathrm{QFI}}^n_\theta$ as in Eq. (5.95). In conclusion we have obtained un upper bound for the quantum Fisher information corresponding to the Heisenberg (quadratic) scaling in the number of uses.

5.10 Port-based teleportation stretching of private communication and single-letter upper bounds

Consider the M-port approximation $\mathcal{E}^M$ of $\mathcal{E}$, as achieved by the PBT simulation with error δ_M. Correspondingly, we have an M-port approximate output state ρ_n^M such that $\left\|\rho_n - \rho_n^M\right\| \leq n\delta_M$ as in Eq. (9) of the main text. Then, we may stretch an adaptive protocol $\mathcal{P}$ over $\mathcal{E}^M$ and write $\rho_n^M = \bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM})$ for a trace-preserving LOCC $\bar{\Lambda}$. Using the triangle inequality, we may write

$$\begin{aligned}\left\|\rho_n^M - \phi_n\right\| &\leq \left\|\rho_n^M - \rho_n\right\| + \left\|\rho_n - \phi_n\right\| \\ &\leq n\delta_M + \epsilon := \gamma. \end{aligned} \tag{5.110}$$

Now consider an entanglement measure E. For instance, E may be the relative entropy of entanglement E_{R} (REE) [36, 87, 88] or the squashed entanglement E_{SE} (SE) [162]. In particular, these measures satisfy a suitable continuity property. For d-dimensional states ρ and σ such that $\|\rho - \sigma\| \leq \gamma$, we may write the Fannes-type inequality

$$|E(\rho) - E(\sigma)| \leq g(\gamma)\log_2 d + h(\gamma), \tag{5.111}$$

where g, h are regular functions going to zero in ϵ'. For the REE and the SE, these functions are

$$\text{REE: } \; g(\gamma) = 4\gamma, \; h(\epsilon) = 2H_2(\gamma), \tag{5.112}$$

$$\text{SE: } \; g(\gamma) = 16\sqrt{\gamma}, \; h(\gamma) = 2H_2(2\sqrt{\gamma}), \tag{5.113}$$

where H_2 is the binary Shannon entropy.

By applying Eq. (5.111) to Eq. (5.110), we get

$$\left|E(\rho_n^M) - E(\phi_n)\right| \leq g(\gamma)\log_2 d + h(\gamma), \tag{5.114}$$

where $E(\phi_n) \geq nR_n$ (normalization) and

$$E(\rho_n^M) = E[\bar{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM})] \leq nM \; E(\rho_{\mathcal{E}}), \tag{5.115}$$

which exploits the monotonicity of E under trace-preserving LOCCs and the subadditivity over tensor-product states. Therefore, we may write

$$R_n \leq M \; E(\rho_{\mathcal{E}}) + \frac{g(n\delta_M + \epsilon)\log_2 d + h(n\delta_M + \epsilon)}{n}. \tag{5.116}$$

Note that for a private state, we may write $\log_2 d \leq cn$ for some constant c. Thus, for any adaptive key generation protocol $\mathcal{P}$ over a d-dimensional quantum channel $\mathcal{E}$, the maximum ϵ-secure key rate that can be generated after n uses is bounded as in Eq. (5.116) where E is an entanglement measure (as the REE or the SE), M is the number of ports, and δ_M is the error of the M-port PBT.

We can find alternate bound by extending the definition of channel's REE to a tripartite version. Consider three finite-dimensional systems a', a and b', and a quantum channel $\mathcal{E} = \mathcal{E}_{a\to b}$ from a to the output system b. Consider a generic input state $\rho_{a'ab'}$ transformed into an output state $\omega_{_{a'bb'}} := \mathcal{E}_{a\to b}(\rho_{a'ab'})$ by the action of this channel. Then, one can define a tripartite version of channel's REE as

$$\tilde{E}_{\mathrm{R}}(\mathcal{E}) := \sup_{\rho_{a'ab'}} E_{\mathrm{R}}(a'|bb')_{\omega} - E_{\mathrm{R}}(a'a|b)_{\rho}, \tag{5.117}$$

which satisfies $K(\mathcal{E}) \leq \tilde{E}_{\mathrm{R}}(\mathcal{E})$ [163]. Moreover, if two channels are close in diamond norm $\|\mathcal{E} - \mathcal{E}'\|_{\diamond} \leq 2\epsilon$, then one may also write the continuity property [163]

$$|\tilde{E}_{\mathrm{R}}(\mathcal{E}) - \tilde{E}_{\mathrm{R}}(\mathcal{E}')| \leq 2\epsilon \log_2 d + f(\epsilon), \tag{5.118}$$

$$f(\epsilon) := (1+\epsilon)\log_2(1+\epsilon) - \epsilon \log_2 \epsilon, \tag{5.119}$$

where d is the dimension of the Hilbert space. Finally, as a straightforward application of the LOCC simulation of a quantum channel $\mathcal{E}$ via a resource state σ, one may write the data-processing upper bound $\tilde{E}_{\mathrm{R}}(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma)$.

In our channel simulation via PBT, we have a multi-copy resource state $\sigma = \rho_{\mathcal{E}}^{\otimes M}$ for the M-port approximation $\mathcal{E}^M$ of the d-dimensional channel $\mathcal{E}$. This means that we may write

$$\tilde{E}_{\mathrm{R}}(\mathcal{E}^M) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}^{\otimes M}) \leq M E_{\mathrm{R}}(\rho_{\mathcal{E}}). \tag{5.120}$$

Then, because we have

$$||\mathcal{E} - \mathcal{E}^M||_{\diamond} \leq ||\mathcal{I} - \Gamma_M||_{\diamond} := \delta_M \leq 2d(d-1)M^{-1}, \tag{5.121}$$

from Eq. (5.118) we may derive

$$\tilde{E}_{\mathrm{R}}(\mathcal{E}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}}^{\otimes M}) + \delta_M \log_2 d + f(\delta_M/2). \tag{5.122}$$

As a result, we may write the upper bound [9]

$$\begin{aligned} K(\mathcal{E}) &\leq E_{\mathrm{R}}(\rho_{\mathcal{E}}^{\otimes M}) + \delta_M \log_2 d + f(\delta_M/2) \\ &\leq M E_{\mathrm{R}}(\rho_{\mathcal{E}}) + \frac{2d(d-1)}{M}\log_2 d + f\left[\frac{d(d-1)}{M}\right] \\ &:= K_{\mathrm{UB}}^{M}(\mathcal{E}). \end{aligned} \tag{5.123}$$

The tightest upper bound is obtained by minimizing $K_{\mathrm{UB}}^{M}(\mathcal{E})$ over M, which is typically a finite value.

Let us apply the bound to channels that are nearly entanglement-breaking, so that $E_{\mathrm{R}}(\rho_{\mathcal{E}}) \ll 1$. In this case, we expect that the optimal value of M is large. It is easy to see that a sub-optimal choice for M is given by

$$\tilde{M} = \sqrt{\frac{2d(d-1)\log_2 d}{E_{\mathrm{R}}(\rho_{\mathcal{E}})}}\,, \tag{5.124}$$

which provides the upper bound [9]

$$\begin{aligned} K(\mathcal{E}) \leq\, & 2\sqrt{2d(d-1)\log_2 d}\sqrt{E_{\mathrm{R}}(\rho_{\mathcal{E}})} \\ & + f\left[\sqrt{\frac{d(d-1)E_{\mathrm{R}}(\rho_{\mathcal{E}})}{2\log_2 d}}\right]. \end{aligned} \tag{5.125}$$

The bound in Eq. (5.125) is particularly interesting for almost entanglement-breaking channels, such that $E_{\mathrm{R}}(\rho_{\mathcal{E}}) \lesssim (\log_2 d)/[8d(d-1)]$.

Chapter 6

Concluding remarks

In this thesis we have first contributed to advance the study of the ultimate bounds on the two-way assisted quantum capacities of quantum channels in both finite and infinite dimensions. In the specific, we have established the ultimate upper bounds for point-to-point quantum communication, entanglement distribution and secret key generation with qubits and bosonic systems. Implicitly, these bounds provide the crucial benchmarks to test quantum repeaters. In fact in order for a quantum repater to be advantageous over point-to-point communications, it must surpass these benchmarks. To derive our results we have designed a general reduction method for adaptive protocols which is summarized in the following.

Summary of the methodology [1, 3]

(1) We have designed an **adaptive-to-block reduction** method which reduces any adaptive protocol for quantum communication, entanglement distribution and key generation to the computation of a single-letter quantity. This is possible by combining the following two main ingredients:

(1.1) Channel's REE. We have extended the notion of relative entropy of entanglement (REE) from states to channels. In particular, we have shown that the two-way capacity $\mathcal{C}(\mathcal{E})$ of any channel $\mathcal{E}$ is upper bounded by a suitably-defined REE bound $E_{\mathrm{R}}^{\bigstar}(\mathcal{E})$.

(1.2) LOCC simulation and teleportation stretching. We have introduced the most general form of simulation of a quantum channel within a quantum/private communication scenario. This is based on arbitrary LOCCs (even asymptotic) and can be used to stretch an arbitrary channel $\mathcal{E}$ into a resource state σ. By exploiting this simulation, we have shown how to reduce an adaptive protocol (achieving an arbitrary task) into a block form, so that its output can be decomposed as $\bar{\Lambda}(\sigma^{\otimes n})$ for a trace-preserving LOCC $\bar{\Lambda}$. This is valid at any dimension (finite or infinite) and can be extended to more complex communication scenarios.

Thus, the insight of our entire reduction method is the combination of (1.1) and (1.2). 'REE+teleportation stretching' allows us to exploit the properties of the REE (monotonicity, subadditivity) and simplify $E_{\mathrm{R}}^{\bigstar}(\mathcal{E})$ into a single-letter quantity so that we may write $\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\sigma)$ for any σ-stretchable channel. This is valid at any dimension.

(2) Teleportation covariance. At any dimension (finite or infinite), we have identified a simple criterion (teleportation covariance) which allows us to find those channels which are stretchable into their Choi matrices (Choi-stretchable channels). For these channels, we may write $\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{R}}(\rho_{\mathcal{E}})$, with the latter being the entanglement flux of the channel.

(3) Tight bounds and two-way capacities. We have shown that the entanglement flux is the tightest upper bound for the two-way capacities of many quantum channels at any dimension, including Pauli, erasure and bosonic Gaussian channels. In particular, we have established the two-way capacities (Q_2, D_2 and K) of the bosonic lossy channel, the quantum-limited amplifier, and the dephasing channel in arbitrary finite dimension, plus the secret key capacity K of the erasure channel in arbitrary finite dimension. All these capacities have extremely simple formulas. For our calculations we have derived a simple formula for the relative entropy between two arbitrary Gaussian states.

(4) Fundamental rate-loss tradeoff. We have finally characterized the rate-loss tradeoff affecting quantum optical communications, so that the rate of repeaterless QKD is restricted to 1.44η bits per channel use at long distances. This rate is achievable with one-way CCs and provides the maximum throughput of a point-to-point QKD protocol.

Future research in this topic should be devoted to the determination of the two-way quantum capacities of those quantum channels that still have a gap between the lower and the upper bound. These are represented for example by the amplitude damping channel, depolarizing channel, the thermal loss channel and the noisy amplifier channel. The approaches could be different, for example one could study the possibility of finding different simulation of the quantum channel relying on other resource states for which the computation of the REE gives an upper bound closer to the (reverse) coherent information. Conversely one can also look for a different definiton of the weak converse upper bound that exploits other entanglement monotones that, once computed on the Choi state of the channel, may provide a bound below the REE.

Our reduction method is very general and it can be applied to any other task whose performance are given in terms of functionals that are monotonic under the action of completely positive trace-preserving operations. This is the case of quantum metrology and quantum channel discrimination. In the former scenario, we have reviewed some results obtained by applying our reduction technique to adaptive protocols for quantum parameter estimation. According to these, the quantum Cramér-Rao bound for programmable teleportation covariant channels is limited by the standard quantum limit (SQL), with the quantum Fisher information computed on the Choi matrix of the channel. As a consequence, in order to check if a channel could beat the SQL and potentially reach the Heisenberg scaling, we need to modify the simulation by using a multi-copy resource state. This modification can be achieved by substituting the standard teleportation with port-based teleportation (PBT) at the core of the channel simulation. By doing this we are then able to show that the Heisenberg scaling directly follows from the PBT scheme. The same PBT-simulation is then exploited in the adaptive discrimination of two arbitrary quantum channels acting on a finite-dimensional Hilbert space. Here we established a general and fundamental lower bound for the error probability affecting the discrimination . This bound is conveniently expressed in terms of the Choi matrices of the channels involved, and for this reason it is computable. In the end we apply our bound in the context of adaptive quantum illumination. It would be interesting to extend our lower bound on the error-probability to bosonic channels but this would require the generalization of the PBT scheme to continuous variables, which is still a subject of study.

Appendix A

Proof of the uniform convergence in the teleportation simulation of bosonic Gaussian channels

The contents of this Appendix are taken from [4].

A.1 Proof of Theorem 2.4.2

Let us start by showing the implication

$$\mathrm{rank}(\mathbf{N}) = 2 \Longrightarrow \lim_{\mu\to\infty} \|\mathcal{G}^{\mu} - \mathcal{G}\|_{\diamond} = 0 \quad \text{Eq. (2.68)}. \tag{A.1.1}$$

Consider an arbitrary single-mode Gaussian channel $\mathcal{G}[\mathbf{T},\mathbf{N},\mathbf{d}]$, so that it transforms the statistical moments as in Eq. (1.67). As we know from Eq. (2.58), for any input state ρ_{Rc}, we may write

$$\mathcal{I}_R \otimes \mathcal{G}^{\mu}(\rho_{Rc}) = \mathcal{I}_R \otimes \mathcal{G}_B \circ \mathcal{T}_{cAB}(\rho_{Rc} \otimes \Phi^{\mu}_{AB}) \tag{A.1.2}$$

$$= \mathcal{I}_R \otimes (\mathcal{G}_c \circ \mathcal{I}^{\mu}_c)(\rho_{Rc}) \tag{A.1.3}$$

$$= \mathcal{I}_R \otimes \mathcal{G}^{\mu}_c(\rho_{Rc}) \tag{A.1.4}$$

where $\mathcal{T}$ is the LOCC of the standard BK protocol and $\mathcal{I}^{\mu}$ is the BK channel, which is locally equivalent to an additive-noise Gaussian channel (B_2 form) with added noise ξ. Therefore, for the Gaussian channel $\mathcal{G}^{\mu}$ we may write the modified transformations

$$\bar{\mathbf{x}} \to \mathbf{T}\bar{\mathbf{x}} + \mathbf{d},\ \ \mathbf{V} \to \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N} + \xi\mathbf{T}\mathbf{T}^T. \tag{A.1.5}$$

As we can see, the transformation of the first moments is identical. The transformation of the second moments is characterized by the modified noise matrix

$$\mathbf{N}^{\xi} = \mathbf{N}+\xi\mathbf{T}\mathbf{T}^{T}. \tag{A.1.6}$$

In other words, we may write $\mathcal{G}^{\mu}[\mathbf{T},\mathbf{N}^{\xi},\mathbf{d}]$.

Because $\mathcal{G}$ and $\mathcal{G}^{\mu}$ have the same displacement, we can set $\mathbf{d}=\mathbf{0}$ without losing generality. Consider the unitary reduction of $\mathcal{G}[\mathbf{T},\mathbf{N},\mathbf{0}]$ into the corresponding canonical form $\mathcal{C}$ by means of two Gaussian unitaries $\hat{U}$ and $\hat{W}$ as in Eq. (1.69). Because $\mathbf{d}=\mathbf{0}$, we may assume that these unitaries are canonical (i.e., with zero displacement), so that they are one-to-one with two symplectic transformations, $\mathbf{S}_A$ and $\mathbf{S}_B$, in the phase space. To simplify the notation define the Gaussian channels

$$\mathcal{U}(\rho) := \hat{U}\rho\hat{U}^{\dagger},\ \ \mathcal{W}(\rho) := \hat{W}\rho\hat{W}^{\dagger}. \tag{A.1.7}$$

Then we may write

$$\mathcal{G} = \mathcal{W}\circ\mathcal{C}\circ\mathcal{U}, \tag{A.1.8}$$

$$\mathcal{G}^{\mu} = \mathcal{W}\circ\mathcal{C}\circ\mathcal{U}\circ\mathcal{I}^{\mu}. \tag{A.1.9}$$

Then notice that we may re-write

$$\mathcal{G}^{\mu} = \mathcal{W}\circ\mathcal{C}^{\mu}\circ\mathcal{U}, \tag{A.1.10}$$

where we have defined

$$\mathcal{C}^{\mu} := \mathcal{C}\circ\mathcal{U}\circ\mathcal{I}^{\mu}\circ\mathcal{U}^{-1}. \tag{A.1.11}$$

In Sec. A.2 we prove the following.

Lemma A.1.1 *Consider a Gaussian channel $\mathcal{G}$ with $\tau := \det\mathbf{T}\neq 1$ and $\mathrm{rank}(\mathbf{N})=2$. Then $\mathcal{C}$ and $\mathcal{C}^{\mu}$ have the same unitary dilation but different environmental states ρ_e and ρ_e^{μ}, i.e., for any input state ρ we may write*

$$\mathcal{C}(\rho)=\mathcal{D}(\rho\otimes\rho_e),\ \ \ \mathcal{C}^{\mu}(\rho)=\mathcal{D}(\rho\otimes\rho_e^{\mu}), \tag{A.1.12}$$

where $\mathcal{D}(\rho_{ce}) := \mathrm{Tr}_e\left(\hat{U}_{ce}\rho_{cae}\hat{U}_{ce}^{\dagger}\right)$ with $\hat{U}_{ce}$ unitary. Furthermore

$$\lim_{\mu\to\infty} F(\rho_e^{\mu},\rho_e) = 1. \tag{A.1.13}$$

Using this lemma in Eqs. (A.1.8) and (A.1.10) leads to

$$\mathcal{G}(\rho) = \mathcal{W} \circ \mathcal{D}[\mathcal{U}(\rho) \otimes \rho_e], \tag{A.1.14}$$

$$\mathcal{G}^\mu(\rho) = \mathcal{W} \circ \mathcal{D}[\mathcal{U}(\rho) \otimes \rho_e^\mu] \ . \tag{A.1.15}$$

Clearly these relations can be extended to the presence of a reference system R, so that for any input ρ_{Rc}, we may write

$$\mathcal{I}_R \otimes \mathcal{G}_c(\rho_{Rc}) = \mathcal{I}_R \otimes \mathcal{W} \circ \mathcal{D}[\mathcal{U}(\rho_{Rc}) \otimes \rho_e], \tag{A.1.16}$$

$$\mathcal{I}_R \otimes \mathcal{G}_c^\mu(\rho_{Rc}) = \mathcal{I}_R \otimes \mathcal{W} \circ \mathcal{D}[\mathcal{U}(\rho_{Rc}) \otimes \rho_e^\mu]. \tag{A.1.17}$$

As a result for any ρ_{Rc}, we may bound the trace distance as follows

$$\begin{aligned}
&\|\mathcal{I}_R \otimes \mathcal{G}_c^\mu(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{G}_a(\rho_{Rc})\| && \text{(A.1.18)}\\
&= \|\mathcal{I}_R \otimes \mathcal{W} \circ \mathcal{D}[\mathcal{U}(\rho_{Rc}) \otimes \rho_e^\mu] - \mathcal{I}_R \otimes \mathcal{W} \circ \mathcal{D}[\mathcal{U}(\rho_{Rc}) \otimes \rho_e]\| && \text{(A.1.19)}\\
&\overset{(1)}{\leq} \|\mathcal{U}(\rho_{Rc}) \otimes \rho_e^\mu - \mathcal{U}(\rho_{Rc}) \otimes \rho_e\| && \text{(A.1.20)}\\
&\overset{(2)}{=} \|\rho_e^\mu - \rho_e\| \overset{(3)}{\leq} 2\sqrt{1 - F(\rho_e^\mu, \rho_e)^2}, && \text{(A.1.21)}
\end{aligned}$$

where we use: (1) the monotonicity under CPTP maps (including the partial trace) (2) multiplicity over tensor products; and (3) one of the Fuchs-van der Graaf relations. As we can see the upper-bound in Eq. (A.1.21) does not depend on the input state ρ_{Rc}. Therefore, we may extend the result to the supremum and write

$$\begin{aligned}
\|\mathcal{G}^\mu - \mathcal{G}\|_\diamond &:= \sup_{\rho_{Rc}} \|\mathcal{I}_R \otimes \mathcal{G}_c^\mu(\rho_{Rc}) - \mathcal{I}_R \otimes \mathcal{G}_c(\rho_{Rc})\| \\
&\leq 2\sqrt{1 - F(\rho_e^\mu, \rho_e)^2}.
\end{aligned} \tag{A.1.22}$$

Now, using Eq. (A.1.13), we obtain

$$\lim_{\mu \to \infty} \|\mathcal{G}^\mu - \mathcal{G}\|_\diamond = 0, \tag{A.1.23}$$

proving the result for $\tau := \det \mathbf{T} \neq 1$ and $\text{rank}(\mathbf{N}) = 2$, i.e.,

$$\left.\begin{aligned} \tau := \det \mathbf{T} \neq 1 \\ \text{rank}(\mathbf{N}) = 2 \end{aligned}\right\} \Longrightarrow \text{Eq. (2.68)}. \tag{A.1.24}$$

Let us now remove the assumption $\tau := \det \mathbf{T} \neq 1$. Note that the Gaussian channels with $\tau = 1$ and $\text{rank}(\mathbf{N}) = 2$ are those $\tilde{\mathcal{G}}$ unitarily equivalent to the B_2 form $\mathcal{C}[1, 2, \xi']$

with added noise $\xi' \geq 0$. In this case, we dilate the form in the asymptotic single-mode representation described in Sec. 1.3.1.1. In other words, we may write

$$\tilde{\mathcal{G}} = \mathcal{W} \circ \mathcal{C}[1, 2, \xi'] \circ \mathcal{U} \tag{A.1.25}$$

$$= \mathcal{W} \circ \lim_{\tau \to 1} \mathcal{C}[\tau, 2, \bar{n}_{\xi',\tau}] \circ \mathcal{U} \tag{A.1.26}$$

$$= \lim_{\tau \to 1} \ \mathcal{W} \circ \mathcal{C}[\tau, 2, \bar{n}_{\xi',\tau}] \circ \mathcal{U} \tag{A.1.27}$$

where $\bar{n}_{\xi',\tau} := [\xi'(1-\tau)^{-1} - 1]/2$ and it is easy to check the commutation of the limit. Let us call $\mathcal{B}_\tau$ the beam-splitter dilation associated with the attenuator C form $\mathcal{C}[\tau, 2, \bar{n}]$, and call $\rho_e(\bar{n})$ the corresponding thermal state of the environment. Then, we may write the approximation

$$\tilde{\mathcal{G}} = \lim_{\tau \to 1} \ \tilde{\mathcal{G}}^\tau, \tag{A.1.28}$$

$$\tilde{\mathcal{G}}^\tau(\rho) := \mathcal{W} \circ \mathcal{B}_\tau[\mathcal{U}(\rho) \otimes \rho_e(\bar{n}_{\xi',\tau})]. \tag{A.1.29}$$

Similarly, for the teleportation-simulated channel, we may write

$$\tilde{\mathcal{G}}^\mu = \lim_{\tau \to 1} \ \tilde{\mathcal{G}}^{\mu,\tau}, \tag{A.1.30}$$

$$\tilde{\mathcal{G}}^{\mu,\tau}(\rho) := \mathcal{W} \circ \mathcal{B}_\tau[\mathcal{U}(\rho) \otimes \rho_e^\mu(\bar{n}_{\xi',\tau})], \tag{A.1.31}$$

where $\rho_e^\mu(\bar{n}_{\xi',\tau})$ is a modified environmental state.

We can now exploit the triangle inequality. For any input ρ and any $\tau < 1$, we may write

$$\begin{aligned}\left\|\tilde{\mathcal{G}}^\mu(\rho) - \tilde{\mathcal{G}}(\rho)\right\| \leq{}& \left\|\tilde{\mathcal{G}}^\mu(\rho) - \tilde{\mathcal{G}}^{\mu,\tau}(\rho)\right\| \\ &+ \left\|\tilde{\mathcal{G}}^{\mu,\tau}(\rho) - \tilde{\mathcal{G}}^\tau(\rho)\right\| + \left\|\tilde{\mathcal{G}}^\tau(\rho) - \tilde{\mathcal{G}}(\rho)\right\|.\end{aligned} \tag{A.1.32}$$

By taking the limit for $\tau \to 1$ and using Eqs. (A.1.28) and (A.1.30), we find

$$\left\|\tilde{\mathcal{G}}^\mu(\rho) - \tilde{\mathcal{G}}(\rho)\right\| \leq \lim_{\tau \to 1} \left\|\tilde{\mathcal{G}}^{\mu,\tau}(\rho) - \tilde{\mathcal{G}}^\tau(\rho)\right\| \ . \tag{A.1.33}$$

Repeating previous arguments, from Eqs. (A.1.29) and (A.1.31), we easily derive

$$\left\|\tilde{\mathcal{G}}^{\mu,\tau}(\rho) - \tilde{\mathcal{G}}^\tau(\rho)\right\| \leq 2\sqrt{1 - F[\rho_e^\mu(\bar{n}_{\xi',\tau}), \rho_e(\bar{n}_{\xi',\tau})]^2}, \tag{A.1.34}$$

so that

$$\left\|\tilde{\mathcal{G}}^\mu(\rho) - \tilde{\mathcal{G}}(\rho)\right\| \leq \lim_{\tau \to 1} \ 2\sqrt{1 - F[\rho_e^\mu(\bar{n}_{\xi',\tau}), \rho_e(\bar{n}_{\xi',\tau})]^2}. \tag{A.1.35}$$

The previous inequality holds for any input state and can be easily extended to the presence of a reference system R, so that we may write

$$\left\|\tilde{\mathcal{G}}^\mu - \tilde{\mathcal{G}}\right\|_\diamond \leq \lim_{\tau \to 1} \ 2\sqrt{1 - F[\rho_e^\mu(\bar{n}_{\xi',\tau}), \rho_e(\bar{n}_{\xi',\tau})]^2}. \tag{A.1.36}$$

One can easily check (see Appendix A.3), that the previous inequality leads to uniform convergence

$$\lim_{\mu\to\infty}\left\|\tilde{\mathcal{G}}^{\mu}-\tilde{\mathcal{G}}\right\|_{\diamond}=0\ , \tag{A.1.37}$$

completing the proof of the implication in Eq. (A.1.1).

Let us now show the opposite implication

$$\mathrm{rank}(\mathbf{N})=2\Longleftarrow\text{Eq. (2.68)}, \tag{A.1.38}$$

or, equivalently,

$$\mathrm{rank}(\mathbf{N})<2\Longrightarrow\text{No uniform convergence.} \tag{A.1.39}$$

Note that Gaussian channels with $\mathrm{rank}(\mathbf{N})<2$ are the identity channel $B_2(Id)$, having zero rank, and the B_1 form, having unit rank. We already know that there is no uniform convergence in the teleportation simulation of the identity channel and this property trivially extends to the teleportation simulation $\mathcal{U}_G^{\mu}=\mathcal{U}_G\circ\mathcal{I}^{\mu}$ of any Gaussian unitary $\mathcal{U}_G$. In fact, it is easy to check that

$$\left\|\mathcal{U}_G^{\mu}-\mathcal{U}_G\right\|_{\diamond}=\left\|\mathcal{I}^{\mu}-\mathcal{I}\right\|_{\diamond}=2\ , \tag{A.1.40}$$

due to invariance under unitaries. For the B_1 form $\tilde{\mathcal{C}}=\mathcal{C}[1,1,0]$, we now explicitly show that there is no uniform convergence in its teleportation simulation. Let us consider the simulation $\tilde{\mathcal{C}}^{\mu}$ by means of a μ-energy BK protocol and consider an input TMSV state $\Phi_{Rc}^{\tilde{\mu}}$ with diverging energy $\tilde{\mu}$. We have the two output states

$$\rho_{Rc}^{\tilde{\mu}}:=\mathcal{I}_R\otimes\tilde{\mathcal{C}}_c(\Phi_{Rc}^{\tilde{\mu}}),\ \rho_{Rc}^{\mu,\tilde{\mu}}:=\mathcal{I}_R\otimes\tilde{\mathcal{C}}_c^{\mu}(\Phi_{Rc}^{\tilde{\mu}}). \tag{A.1.41}$$

In particular, note that $\rho_{Rc}^{\mu,\tilde{\mu}}$ is a Gaussian state with CM

$$\mathbf{V}^{\mu,\tilde{\mu}}=\begin{pmatrix}\tilde{\mu} & 0 & \sqrt{\tilde{\mu}^2-1} & 0\\ 0 & \tilde{\mu} & 0 & -\sqrt{\tilde{\mu}^2-1}\\ \sqrt{\tilde{\mu}^2-1} & 0 & \tilde{\mu}+\xi & 0\\ 0 & -\sqrt{\tilde{\mu}^2-1} & 0 & \tilde{\mu}+\xi+1\end{pmatrix}, \tag{A.1.42}$$

where ξ is the added noise associated with the BK protocol and depends on μ according to $\xi=2(\mu-\sqrt{\mu^2-1})$. Using the Fuchs-van de Graaf inequalities [83], already introduce in Eq. (1.118) we may write

$$\left\|\rho_{Rc}^{\mu,\tilde{\mu}}-\rho_{Rc}^{\tilde{\mu}}\right\|\geq 2\left[1-F\left(\rho_{Rc}^{\mu,\tilde{\mu}},\rho_{Rc}^{\tilde{\mu}}\right)\right]. \tag{A.1.43}$$

Then, by computing the fidelity [82] and expanding in $\tilde{\mu}$, we obtain

$$F\left(\rho_{Rc}^{\mu,\tilde{\mu}}, \rho_{Rc}^{\tilde{\mu}}\right) \simeq O(\tilde{\mu}^{-1/4}), \tag{A.1.44}$$

so that

$$\lim_{\tilde{\mu}\to\infty} \left\|\rho_{Rc}^{\mu,\tilde{\mu}} - \rho_{Rc}^{\tilde{\mu}}\right\| = 2, \tag{A.1.45}$$

which clearly implies $\left\|\tilde{\mathcal{C}}^{\mu} - \tilde{\mathcal{C}}\right\|_{\diamond} = 2$. Then, we may extend the result to any Gaussian channel which is unitarily equivalent to the B_1 form. Consider Eqs. (A.1.8) and (A.1.10) with $\tilde{\mathcal{C}} = \mathcal{C}[1,1,0]$, i.e,

$$\mathcal{G} = \mathcal{W} \circ \tilde{\mathcal{C}} \circ \mathcal{U}, \;\; \mathcal{G}^{\mu} = \mathcal{W} \circ \tilde{\mathcal{C}}^{\mu} \circ \mathcal{U}, \tag{A.1.46}$$

where

$$\tilde{\mathcal{C}}^{\mu} := \tilde{\mathcal{C}} \circ \mathcal{U} \circ \mathcal{I}^{\mu} \circ \mathcal{U}^{-1}. \tag{A.1.47}$$

Assume the input state $\Psi_{Rc}^{\tilde{\mu}} := \mathcal{I}_R \otimes \mathcal{U}^{-1}(\Phi_{Rc}^{\tilde{\mu}})$, so that we have the two output states

$$\rho_{Rc}^{\tilde{\mu}} := \mathcal{I}_R \otimes \mathcal{G}_c(\Psi_{Rc}^{\tilde{\mu}}) = \mathcal{I}_R \otimes \mathcal{W} \circ \tilde{\mathcal{C}}(\Phi_{Rc}^{\tilde{\mu}}), \tag{A.1.48}$$

$$\rho_{Rc}^{\mu,\tilde{\mu}} := \mathcal{I}_R \otimes \mathcal{G}_c^{\mu}(\Psi_{Rc}^{\tilde{\mu}}) = \mathcal{I}_R \otimes \mathcal{W} \circ \tilde{\mathcal{C}}^{\mu}(\Phi_{Rc}^{\tilde{\mu}}). \tag{A.1.49}$$

Because the fidelity is invariant under unitaries, we may neglect $\mathcal{U}_B$ and write

$$F\left(\rho_{Rc}^{\mu,\tilde{\mu}}, \rho_{Rc}^{\tilde{\mu}}\right) = F\left[\mathcal{I}_R \otimes \tilde{\mathcal{C}}^{\mu}(\Phi_{Rc}^{\tilde{\mu}}), \mathcal{I}_R \otimes \tilde{\mathcal{C}}(\Phi_{Rc}^{\tilde{\mu}})\right]. \tag{A.1.50}$$

Let us derive the CM $\tilde{\mathbf{V}}^{\mu,\tilde{\mu}}$ of the state $\mathcal{I}_R \otimes \tilde{\mathcal{C}}^{\mu}(\Phi_{Ra}^{\tilde{\mu}})$. Starting from the CM $\mathbf{V}^{\mu}$ of the TMSV in Eq. (1.43) and applying Eq. (A.1.47), we easily see that this CM is given by

$$\tilde{\mathbf{V}}^{\mu,\tilde{\mu}} = \mathbf{V}^{\mu} + \mathbf{0} \oplus \left[\xi \mathbf{S}_A \mathbf{S}_A^T + \mathrm{diag}(0,1)\right], \tag{A.1.51}$$

where $\mathbf{0}$ is the 2×2 zero matrix, and $\mathbf{S}_A$ is the symplectic matrix associated with the Gaussian unitary $\mathcal{U}$ (which can be taken to be canonical without losing generality). Let us set

$$\mathbf{S}_A = \begin{pmatrix} a & c \\ d & b \end{pmatrix}, \tag{A.1.52}$$

where the elements are real values such that $\det \mathbf{S}_A = +1$ (because $\mathbf{S}_A$ is symplectic). Then, we may compute the fidelity and expand it at the leading order in $\tilde{\mu}$, finding

$$F\left[\mathcal{I}_R \otimes \tilde{\mathcal{C}}^{\mu}(\Phi_{Rc}^{\tilde{\mu}}), \mathcal{I}_R \otimes \tilde{\mathcal{C}}(\Phi_{Rc}^{\tilde{\mu}})\right]^4$$

$$\simeq \gamma \tilde{\mu}^{-1} + O(\tilde{\mu}^{-3/2}), \tag{A.1.53}$$

$$\gamma := \frac{a^2 + c^2 + 2\xi}{2\xi(a^2 + c^2 + \xi)^2} > 0. \tag{A.1.54}$$

Clearly, this implies $\|\mathcal{G}^\mu - \mathcal{G}\|_\diamond = 2$ for any Gaussian channel unitarily equivalent to the B_1 form. ■

Note that the rank of the noise matrix $\mathbf{N}$ is indeed a fundamental quantity in the previous proof. Given a single-mode Gaussian channel $\mathcal{G}[\mathbf{T}, \mathbf{N}, \mathbf{d}]$, consider its teleportation simulation $\mathcal{G}^\mu[\mathbf{T}, \mathbf{N}^\xi, \mathbf{d}]$. For all channels with $\mathrm{rank}(\mathbf{N}) = 2$, we may write

$$\mathrm{rank}(\mathbf{N}^\xi) = \mathrm{rank}(\mathbf{N}) \text{ for any } \xi. \tag{A.1.55}$$

This means that $\mathcal{G}^\mu$ may have the same canonical form and, therefore, the same unitary dilation as $\mathcal{G}$. By contrast, for Gaussian channels with $\mathrm{rank}(\mathbf{N}) < 2$, such as the identity channel or the B_1 form, we can see that we have $\mathrm{rank}(\mathbf{N}^\xi) > \mathrm{rank}(\mathbf{N})$ for $\xi \neq 0$, so that the canonical form changes its class because of the teleportation simulation. As a result, the dilation changes and the data-processing bound in Eqs. (A.1.18)-(A.1.21) cannot be applied.

A.2 Proof of Lemma A.1.1

Consider the canonical forms $\mathcal{C}$ with $\tau := \det \mathbf{T} \neq 1$ and $\mathrm{rank}(\mathbf{N}) = 2$. These correspond to A_2, $C(\mathrm{Att})$, $C(\mathrm{Amp})$, and D. Given $\mathcal{C}$, consider the variant

$$\mathcal{C}^\mu := \mathcal{C} \circ \mathcal{U} \circ \mathcal{I}^\mu \circ \mathcal{U}^{-1}, \tag{A.2.56}$$

where $\mathcal{U}$ is a canonical Gaussian unitary with associated symplectic matrix $\mathbf{S}_A$, and $\mathcal{I}^\mu$ is the BK teleportation channel, which is locally (point-wise) equivalent to an additive-noise Gaussian channel (B_2 form) with added noise

$$\xi = 2[\mu - \sqrt{\mu^2 - 1}]. \tag{A.2.57}$$

Note that we may use the Bloch-Messiah decomposition [164, 165]

$$\mathbf{S}_A = \mathbf{O}_1 \mathbf{S}_q \mathbf{O}_2, \tag{A.2.58}$$

where $\mathbf{O}$'s are symplectic orthogonal matrices, while $\mathbf{S}_q = \mathrm{diag}(r, r^{-1})$ for $r > 0$ is a squeezing matrix. Here we show that $\mathcal{C}$ and $\mathcal{C}^\mu$ have the same unitary dilation with different environmental states ρ_e and ρ_e^μ, whose fidelity $F(\rho_e^\mu, \rho_e) \overset{\mu\to\infty}{\to} 1$. Let us start with the form C.

A.2.1 Lossy channel $C(\mathbf{Att})$ and amplifier $C(\mathbf{Amp})$

Consider the canonical C form $\mathcal{C}(\tau > 0, 2, \bar{n})$ representing either a thermal-loss channel ($0 < \tau < 1$) or a noisy quantum amplifier ($\tau > 1$). Their action on the input covariance matrix (CM) $\mathbf{V}$ is given by

$$\mathbf{V} \to \tau\mathbf{V} + |1-\tau|\omega\mathbf{I} \ , \tag{A.2.59}$$

where $\omega := 2\bar{n} + 1 \geq 1$. From Eq. (A.2.56), we may write

$$\begin{aligned}\mathbf{V} &\to \tau(\mathbf{V} + \xi\mathbf{S}_A\mathbf{S}_A^T) + |1-\tau|\omega\mathbf{I} \\ &= \tau\mathbf{V} + |1-\tau|\tilde{\mathbf{W}},\end{aligned} \tag{A.2.60}$$

where we have set

$$\tilde{\mathbf{W}} := \omega\mathbf{I} + \gamma\mathbf{S}_A\mathbf{S}_A^T, \quad \gamma := \frac{\xi\tau}{|1-\tau|} \geq 0. \tag{A.2.61}$$

According to Eqs. (A.2.60) and (A.2.61), we may represent $\mathcal{C}^\mu(\tau > 0, 2, \bar{n})$ with the same two-mode symplectic matrix $\mathbf{M}(C)$ of the original C form, but replacing the thermal state $\rho_e(\bar{n})$ with a zero-mean Gaussian state ρ_e^μ whose CM can be written as $\tilde{\mathbf{W}}$. To check this is indeed the case, we need to verify that $\tilde{\mathbf{W}}$ is a bona fide CM (see Eq. (1.56)). It is certainly positive definite, so we just need to check that its symplectic eigenvalue is greater than 1. Note that we may apply the orthogonal symplectic $\mathbf{O}_1$ so that

$$\mathbf{W} : = \mathbf{O}_1^T\tilde{\mathbf{W}}\mathbf{O}_1 = \omega\mathbf{I} + \gamma\mathbf{S}_q^2 \ . \tag{A.2.62}$$

The symplectic eigenvalue is equal to

$$\begin{aligned}\nu &= \sqrt{\det\mathbf{W}} = \sqrt{\omega^2 + \gamma^2 + \gamma\omega\left(r^2 + 1/r^2\right)} \\ &\geq \omega + \gamma \geq 1 \ .\end{aligned} \tag{A.2.63}$$

Finally we compute the fidelity between the environmental states, finding

$$\begin{aligned}F(\rho_e^\mu, \rho_e) = \sqrt{2r}\,\Big[&\sqrt{\left(\gamma r^2\omega + \omega^2 + 1\right)\left(\gamma\omega + r^2\left(\omega^2+1\right)\right)} \\ &- \sqrt{\left(\omega^2-1\right)\left(\gamma\omega + \gamma r^4\omega + r^2\left(\gamma^2+\omega^2-1\right)\right)}\Big]^{-1/2},\end{aligned} \tag{A.2.64}$$

which goes to 1 for $\mu \to \infty$ (so that $\xi \to 0$ and $\gamma \to 0$). This is true for any finite value of the squeezing $r > 0$ and the thermal variance ω.

A.2.2 Conjugate of the amplifier D

Let us consider the D form $\mathcal{C}(\tau < 0, 2, \bar{n})$ which transforms the input as follows

$$\mathbf{V} \to -\tau \mathbf{Z}\mathbf{V}\mathbf{Z} + (1-\tau)\omega \mathbf{I}. \tag{A.2.65}$$

Then, the action of $\mathcal{C}^{\mu}(\tau < 0, 2, \bar{n})$ can be written as

$$\begin{aligned}\mathbf{V} &\to -\tau \mathbf{Z}(\mathbf{V} + \xi \mathbf{S}_A \mathbf{S}_A^T)\mathbf{Z} + (1-\tau)\omega \mathbf{I} \\ &= -\tau \mathbf{Z}\mathbf{V}\mathbf{Z} + (1-\tau)\left(\omega \mathbf{I} - \kappa \mathbf{Z}\mathbf{S}_A \mathbf{S}_A^T \mathbf{Z}\right) \\ &= -\tau \mathbf{Z}\mathbf{V}\mathbf{Z} + (1-\tau)\tilde{\mathbf{W}}\end{aligned} \tag{A.2.66}$$

where $\kappa := \xi\tau/(1-\tau) \leq 0$. Using the Bloch-Messiah decomposition of Eq. (A.2.58) and $\mathbf{Z}\mathbf{S}_q^2\mathbf{Z} = \mathbf{S}_q^2$, we may write

$$\begin{aligned}\tilde{\mathbf{W}} &= \omega \mathbf{I} - \kappa \mathbf{Z}\mathbf{O}_1 \mathbf{S}_q^2 \mathbf{O}_1^T \mathbf{Z} \\ &= \omega \mathbf{I} - \kappa (\mathbf{Z}\mathbf{O}_1\mathbf{Z})\mathbf{S}_q^2 (\mathbf{Z}\mathbf{O}_1^T \mathbf{Z}).\end{aligned} \tag{A.2.67}$$

Thus, we may represent $\mathcal{C}^{\mu}(\tau < 0, 2, \bar{n})$ with the same two-mode symplectic matrix $\mathbf{M}(D)$ as the original D form, but replacing the thermal state $\rho_e(\bar{n})$ with a zero-mean Gaussian state ρ_e^{μ} whose CM can be written as $\tilde{\mathbf{W}}$ in Eq. (A.2.67). To check this is indeed the case, we need to verify that $\tilde{\mathbf{W}}$ is a bona fide CM. First notice that the matrix $\mathbf{\Sigma} := \mathbf{Z}\mathbf{O}_1\mathbf{Z}$ is orthogonal and symplectic. We may therefore apply the symplectic $\mathbf{\Sigma}^T$ and write

$$\mathbf{W} = \mathbf{\Sigma}^T \tilde{\mathbf{W}} \mathbf{\Sigma} = \omega \mathbf{I} - \kappa \mathbf{S}_q^2 \ .$$

Because $\kappa \leq 0$, this is positive definite and it has symplectic eigenvalue

$$\begin{aligned}\nu &= \sqrt{\omega^2 + \kappa^2 - \omega\kappa(r^2 + 1/r^2)} \\ &\geq \omega - \kappa \geq 1 \ .\end{aligned} \tag{A.2.68}$$

Finally we compute the fidelity between the environmental states, finding

$$\begin{aligned}F(\rho_e^{\mu}, \rho_e) = \sqrt{2}r \Big[&\sqrt{(-\kappa r^2\omega + \omega^2 + 1)\left(-\kappa\omega + r^2\left(\omega^2 + 1\right)\right)} \\ &- \sqrt{(1-\omega^2)\left(\kappa\omega + \kappa r^4\omega - r^2\left(\kappa^2 + \omega^2 - 1\right)\right)}\Big]^{-1/2},\end{aligned} \tag{A.2.69}$$

which goes to 1 for large μ (so that $\xi \to 0$ and $\kappa \to 0$). This is true for any finite value of the squeezing $r > 0$ and the thermal variance ω.

A.2.3 Canonical form A_2

The A_2 form $\mathcal{C}(0,1,\bar{n})$ transforms the input CM as

$$\mathbf{V} \to \mathbf{\Pi V \Pi} + \omega \mathbf{I} \ , \tag{A.2.70}$$

where

$$\mathbf{\Pi} := \frac{\mathbf{I}+\mathbf{Z}}{2} = \mathrm{diag}(1,0). \tag{A.2.71}$$

The action of the variant $\mathcal{C}^{\mu}(0,1,\bar{n})$ is given by

$$\mathbf{V} \to \mathbf{\Pi}(\mathbf{V} + \xi \mathbf{S_A S_A^T})\mathbf{\Pi} + \omega \mathbf{I} = \mathbf{\Pi V \Pi} + \tilde{\mathbf{W}} \ , \tag{A.2.72}$$

where

$$\tilde{\mathbf{W}} := \omega \mathbf{I} {+} \xi \mathbf{\Pi S_A S_A^T \Pi}. \tag{A.2.73}$$

Thus, we may represent $\mathcal{C}^{\mu}(0,1,\bar{n})$ with the same two-mode symplectic matrix $\mathbf{M}(A_2)$ of the original A_2 form, but replacing the thermal state $\rho_e(\bar{n})$ with a zero-mean Gaussian state ρ_e^{μ} whose CM can be written as $\tilde{\mathbf{W}}$ in Eq. (A.2.73). To check this is indeed the case, we need to verify that $\tilde{\mathbf{W}}$ is a bona fide CM. $\tilde{\mathbf{W}}$ is clearly positive definite. To derive its symplectic eigenvalue, let us set

$$\mathbf{S}_A = \begin{pmatrix} a & c \\ d & b \end{pmatrix}, \tag{A.2.74}$$

where the real entries must satisfy $\det \mathbf{S}_A = ab - cd = 1$. Then we get

$$\tilde{\mathbf{W}} = \begin{pmatrix} \xi(a^2+c^2)+\omega & 0 \\ 0 & \omega \end{pmatrix}, \tag{A.2.75}$$

with symplectic eigenvalue

$$\nu = \sqrt{[\xi(a^2+c^2)+\omega]\omega} \geq \omega \geq 1 \ . \tag{A.2.76}$$

Finally we compute the fidelity between the environmental states, yielding

$$\begin{aligned} F(\rho_e^{\mu}, \rho_e) = \sqrt{2} \Big[& \sqrt{(\omega^2+1)\left(\xi\omega\left(a^2+c^2\right)+\omega^2+1\right)} \\ & - \sqrt{(\omega^2-1)\left(\xi\omega\left(a^2+c^2\right)+\omega^2-1\right)} \Big]^{-1/2}, \end{aligned} \tag{A.2.77}$$

which clearly goes to 1 for large μ (i.e., for $\xi \to 0$). This is true for any finite value of the real parameters a and c, and the thermal variance ω.

A.3 Asymptotic results for the B_2 form

Consider the B_2 form $\mathcal{C}[1, 2, \xi']$ with added noise ξ'. This can be expressed as an asymptotic C form $\mathcal{C}(0 < \tau < 1, 2, \bar{n})$ with $\tau \to 1$ and thermal variance

$$\omega = \xi'/(1 - \tau). \tag{A.3.78}$$

The channel $\mathcal{C}[1, 2, \xi']$ and its simulation $\mathcal{C}^\mu[1, 2, \xi']$ [according to Eq. (A.2.56)] have the same (asymptotic) unitary dilation but different environmental states ρ_e and ρ_e^μ. These are the states associated with $\mathcal{C}(0 < \tau < 1, 2, \bar{n}_{\xi',\tau})$ and $\mathcal{C}^\mu(0 < \tau < 1, 2, \bar{n}_{\xi',\tau})$ where $\bar{n}_{\xi',\tau} := [\xi'(1 - \tau)^{-1} - 1]/2$. Using Eq. (A.3.78) in Eq. (A.2.64) and taking the limit for $\tau \to 1$, we may write

$$F(\rho_e^\mu, \rho_e) = 2\sqrt{\frac{r\xi'\sqrt{\xi\xi' + r^4\xi\xi' + r^2(\xi^2 + \xi'^2)}}{2\xi\xi'(1 + r^4) + r^2(\xi^2 + 4\xi'^2)}} + O(\tau - 1), \tag{A.3.79}$$

where ξ is defined in Eq. (A.2.57) and r is a squeezing parameter associated with the input canonical unitary $\mathcal{U}_A$. Then, the limit in $\xi \to 0$ (i.e., $\mu \to \infty$) provides

$$F(\rho_e^\mu, \rho_e) = 1 + O(\xi) + O(\tau - 1)\ . \tag{A.3.80}$$

Similarly, we may write the expansion

$$2\sqrt{1 - F(\rho_e^\mu, \rho_e)^2} = O(\xi) + O(\tau - 1). \tag{A.3.81}$$

Appendix B

Fundamental limits to quantum and secure communication through quantum channels

The contents of this Appendix have been published as Supplementary Notes of [1], where I contributed by deriving the analytical formulas of the upper bounds on the two-way quantum capacities for the discrete variable channels. Specifically Eqs. (B.1.19), (B.1.29), (B.1.33), (B.1.35), (B.1.44), (B.1.51), (B.1.57) and (B.1.88). The other derivations presented here were done by my co-authors as specified in the "Authors contributions "of [1].

B.1 Ultimate limits in qubit communications

Consider an arbitrary discrete variable channel $\mathcal{E}$ in dimension d, we can easily derive its Choi matrix $\rho_{\mathcal{E}} = I \otimes \mathcal{E}(\Phi)$ from the maximally-entangled state

$$\Phi = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |ii\rangle, \tag{B.1.1}$$

where $\{|0\rangle, \ldots, |i\rangle, \ldots, |d-1\rangle\}$ is the computational basis of the qudit. We write the spectral decomposition

$$\rho_{\mathcal{E}} = \sum_k p_k |\varphi_k\rangle\langle\varphi_k|, \tag{B.1.2}$$

where $\mathbf{p} = \{p_k\}$ are the eigenvalues of the Choi matrix. The von Neumann entropy is simply equal to the Shannon entropy of the previous eigenvalues, i.e.,

$$S(\rho_{\mathcal{E}}) = H(\mathbf{p}) := -\sum_k p_k \log_2 p_k. \tag{B.1.3}$$

From the Choi matrix we may compute the coherent and reverse coherent information of the channel. In particular, for unital channels, these quantities coincide and are given by the simple formula in Eq. (2.17), i.e.,

$$I_{\mathrm{C}}(\mathcal{E}) = I_{\mathrm{RC}}(\mathcal{E}) = \log_2 d - S(\rho_{\mathcal{E}}) = \log_2 d - H(\mathbf{p}). \tag{B.1.4}$$

To compute the entanglement flux of the channel (upper bound), recall that we have

$$\mathbf{\Phi}(\mathcal{E}) := E_{\mathrm{R}}(\rho_{\mathcal{E}}) \leq S(\rho_{\mathcal{E}}||\tilde{\sigma}_s) \ , \tag{B.1.5}$$

for some suitable separable state $\tilde{\sigma}_s$. Let us write its spectral decomposition

$$\tilde{\sigma}_s = \sum_k s_k |\lambda_k\rangle\langle\lambda_k|, \tag{B.1.6}$$

where $|\lambda_k\rangle$ (s_k) are the orthogonal eigenstates (eigenvalues) of $\tilde{\sigma}_s$. We may then write

$$S(\rho_{\mathcal{E}}||\tilde{\sigma}_s) = -S(\rho_{\mathcal{E}}) - \mathrm{Tr}\left(\rho_{\mathcal{E}} \log_2 \tilde{\sigma}_s\right) = -H(\mathbf{p}) - \sum_k \langle\lambda_k|\rho_{\mathcal{E}}|\lambda_k\rangle \log_2 s_k \ . \tag{B.1.7}$$

The separable state $\tilde{\sigma}_s$ may be constructed by applying the channel $I \otimes \mathcal{E}$ to the input separable state

$$\sigma_s = \frac{1}{d} \sum_{i=0}^{d-1} |ii\rangle \langle ii| \, , \tag{B.1.8}$$

so that we have the output

$$\tilde{\sigma}_s = \frac{1}{d} \sum_{i=0}^{d-1} |i\rangle\langle i| \otimes \mathcal{E}(|i\rangle\langle i|). \tag{B.1.9}$$

This specific choice will be optimal in some cases and suboptimal in others.

B.1.1 Erasure channel in arbitrary finite dimension

Consider a qudit in arbitrary dimension d with computational basis $\{|i\rangle\}$ (results can be easily specified to the case of a qubit $d = 2$). The erasure channel replaces an incoming qudit state ρ with an orthogonal erasure state $|e\rangle$ with some probability p. In other words, we have the action

$$\mathcal{E}_{\text{erase}}(\rho) = (1-p)\rho + p|e\rangle\langle e| \ . \tag{B.1.10}$$

The simplicity of this channel relies in the fact that the input states either are perfectly transmitted or they are lost (while in other quantum channels, the input states are all transmitted into generally-different outputs). This feature allows one to apply simple reasonings such as those in ref. [89] which determined the Q_2 of this channel (more precisely, the Q_2 of the qubit erasure channel, but the extension to arbitrary d is trivial).

It is easy to see that this channel is teleportation-covariant (and therefore Choi-stretchable). In fact, any input unitary U applied to the state ρ is mapped into an output augmented unitary $U \oplus I$, i.e., we may write

$$\mathcal{E}_{\text{erase}}(U\rho U^{\dagger}) = (U \oplus I)\mathcal{E}_{\text{erase}}(\rho)(U \oplus I)^{\dagger}. \tag{B.1.11}$$

Let us write the Kraus decomposition of this channel

$$\mathcal{E}_{\text{erase}}(\rho) = A\rho A^{\dagger} + \sum_{i=0}^{d-1} A_i \rho A_i^{\dagger}, \tag{B.1.12}$$

where $A := \sqrt{1-p}I$ (with I being the $d \times d$ identity) and $A_i := \sqrt{p}|e\rangle\langle i|$. We then compute its Choi matrix

$$\rho_{\mathcal{E}_{\text{erase}}} = (1-p)\Phi + \frac{p}{d}(I \otimes |e\rangle\langle e|). \tag{B.1.13}$$

Note that $\text{Tr}[\Phi(I \otimes |e\rangle\langle e|)] = 0$, so that Eq. (B.1.13) is the spectral decomposition of $\rho_{\mathcal{E}}$ over two orthogonal subspaces, where Φ has eigenvalue $1-p$, and $I \otimes |e\rangle\langle e|$ is degenerate with d eigenvalues equal to p/d. Therefore, it is easy to compute the von Neumann entropy, which is

$$S\left(\rho_{\mathcal{E}_{\text{erase}}}\right) = -(1-p)\log_2(1-p) - p\log_2\left(\frac{p}{d}\right). \tag{B.1.14}$$

To compute the entanglement flux of the channel, we consider the separable state $\tilde{\sigma}_s$ in Eq. (B.1.9), which here becomes

$$\tilde{\sigma}_s = \frac{1}{d}\sum_{i=0}^{d-1}\left[(1-p)|ii\rangle\langle ii| + p|i,e\rangle\langle i,e|\right]. \tag{B.1.15}$$

We have now all the elements to be used in Eq. (B.1.7), which provides

$$\mathbf{\Phi}(\mathcal{E}_{\text{erase}}) \leq S(\rho_{\mathcal{E}_{\text{erase}}}||\tilde{\sigma}_s) = (1-p)\log_2 d. \tag{B.1.16}$$

For the lower bound, one can easily check that the coherent and reverse coherent information of this channel are not sufficient to reach the upper bound, since we get

$$I_{\text{C}}(\mathcal{E}_{\text{erase}}) = (1-2p)\log_2 d, \quad I_{\text{RC}}(\mathcal{E}_{\text{erase}}) = (1-p)\log_2 d - H_2(p), \tag{B.1.17}$$

where the extra term $H_2(p)$ is the binary Shannon entropy. Note that these quantities are achievable rates for one-way entanglement distribution but not necessarily the optimal rates. Indeed it is easy to find a strategy based on one-way backward CCs which reaches $(1-p)\log_2 d$. This follows the same reasoning of ref. [89].

Alice can send halves of EPR states to Bob in large n uses of the channel. A fraction $1-p$ will be perfectly distributed. The identification of these good cases can be done by Bob performing a dichotomic POVM $\{|e\rangle\langle e|, I-|e\rangle\langle e|\}$ on each received system and communicating to Alice which instances were perfectly transmitted. At that point Alice and Bob possess $n(1-p)$ EPR states with $\log_2 d$ ebits each. On average this gives a rate of $(1-p)\log_2 d$ ebits per channel use. Thus, one may write

$$D_1(\rho_{\mathcal{E}_{\text{erase}}}) \geq (1-p)\log_2 d\ , \tag{B.1.18}$$

whose combination with Eq. (B.1.16) provides

$$\mathcal{C}(\mathcal{E}_{\text{erase}}) = D_2(\mathcal{E}_{\text{erase}}) = Q_2(\mathcal{E}_{\text{erase}}) = K(\mathcal{E}_{\text{erase}}) = \mathbf{\Phi}(\mathcal{E}_{\text{erase}}) = (1-p)\log_2 d. \tag{B.1.19}$$

Since the two-way quantum capacity of the erasure channel is already known [89], our novel result regards the determination of its secret key capacity

$$K(\mathcal{E}_{\text{erase}}) = (1-p)\log_2 d. \tag{B.1.20}$$

It is clear that, for qubits, we have $K(\mathcal{E}_{\text{erase}}) = 1-p$.

Qubit Pauli channels

Consider a Pauli channel $\mathcal{P}$ acting on a qubit state ρ. The Kraus representation of this channel is

$$\mathcal{P}(\rho) = \sum_{k=0}^{3} p_k P_k \rho P_k^\dagger = p_0\rho + p_1 X\rho X + p_2 Y\rho Y + p_3 Z\rho Z, \tag{B.1.21}$$

where $\mathbf{p} := \{p_k\}$ is a probability distribution and $P_k \in \{I, X, Y, Z\}$ are Pauli operators, with I the identity and

$$X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ Y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{B.1.22}$$

It is easy to check that a Pauli channel is teleportation-covariant and, therefore, Choi-stretchable. Teleportation covariance simply comes from the fact that the Pauli operators (qubit teleportation unitaries) either commute or anticommute with the other Pauli operators (Kraus operators of the channel). For a Pauli channel we can also write the stronger condition

$$[\rho_{\mathcal{P}}, P_k^* \otimes P_k] = 0 \quad \text{for any } k, \tag{B.1.23}$$

i.e., its Choi matrix is invariant under twirling operations restricted to the generators of the Pauli group. In fact, the Choi matrix of a Pauli channel is Bell-diagonal, i.e., it has spectral decomposition

$$\rho_{\mathcal{P}} = \sum_{k=0}^{3} p_k \Phi_k, \tag{B.1.24}$$

where the eigenvalues p_k are the channel probabilities, and the eigenvectors Φ_k are the four Bell states

$$\left\{ \frac{|00\rangle \pm |11\rangle}{\sqrt{2}}, \frac{|10\rangle \pm |01\rangle}{\sqrt{2}} \right\}. \tag{B.1.25}$$

It is clear that $S(\rho_{\mathcal{P}}) = H(\mathbf{p})$. Then, using the separable state $\tilde{\sigma}_s$ as in Eq. (B.1.9), we derive the following upper bound for the entanglement flux of this channel

$$\mathbf{\Phi}(\mathcal{P}) \leq 1 - H(\mathbf{p}) + H_2(p_1 + p_2). \tag{B.1.26}$$

Since a Pauli channel is unital, its (reverse) coherent information is just given by $I_{(\mathrm{R})\mathrm{C}}(\mathcal{P}) = 1 - H(\mathbf{p})$. Therefore, the two-way capacity of a Pauli channel with arbitrary distribution $\mathbf{p} := \{p_k\}$ must satisfy

$$1 - H(\mathbf{p}) \leq \mathcal{C}(\mathcal{P}) \leq 1 - H(\mathbf{p}) + H_2(p_1 + p_2). \tag{B.1.27}$$

Latter result can be made stronger by exploiting the fact that $\rho_{\mathcal{P}}$ is Bell-diagonal. For any such a state we can compute the REE by using the formula of Ref. [36]. In fact, let us set $p_{\max} := \max\{p_k\}$, then we may write

$$E_{\mathrm{R}}(\rho_{\mathcal{P}}) = \begin{cases} 1 - H_2(p_{\max}) & \text{if } p_{\max} \geq \frac{1}{2} \\ 0 & \text{otherwise.} \end{cases} \tag{B.1.28}$$

Thus, we have the tighter upper bound

$$1 - H(\mathbf{p}) \leq \mathcal{C}(\mathcal{P}) \leq \mathbf{\Phi}(\mathcal{P}) = \begin{cases} 1 - H_2(p_{\max}) & \text{if } p_{\max} \geq \frac{1}{2} \\ 0 & \text{otherwise.} \end{cases}. \tag{B.1.29}$$

In the following subsections, we specialize this result to depolarising and dephasing channels.

Qubit depolarising channel

This is a Pauli channel with probability distribution

$$\mathbf{p} = \left\{ 1 - \frac{3p}{4}, \frac{p}{4}, \frac{p}{4}, \frac{p}{4} \right\}, \tag{B.1.30}$$

so that we have

$$\mathcal{P}_{\text{depol}}(\rho) = \left(1 - \frac{3p}{4}\right)\rho + \frac{p}{4}(X\rho X + Y\rho Y + Z\rho Z) = (1-p)\rho + p\frac{I}{2} \ . \tag{B.1.31}$$

Let us set

$$\kappa(p) := 1 - H_2\left(\frac{3p}{4}\right). \tag{B.1.32}$$

Then, from Eq. (B.1.29), we derive the following bounds for the two-way capacity of the depolarising channel

$$\kappa(p) - \frac{3p}{4}\log_2 3 \leq \mathcal{C}(\mathcal{P}_{\text{depol}}) \leq \kappa(p), \tag{B.1.33}$$

for $p \leq 2/3$, while $\mathcal{C}(\mathcal{P}_{\text{depol}}) = 0$ otherwise.

Qubit dephasing channel

This is a Pauli channel with probability distribution $\mathbf{p} = \{1-p, 0, 0, p\}$, so that we have

$$\mathcal{P}_{\text{deph}}(\rho) = (1-p)\rho + pZ\rho Z. \tag{B.1.34}$$

It is easy to see that $H(\mathbf{p}) = H_2(p_{\max}) = H_2(p)$, so that Eq. (B.1.29) leads to

$$\mathcal{C}(\mathcal{P}_{\text{deph}}) = D_2(\mathcal{P}_{\text{deph}}) = Q_2(\mathcal{P}_{\text{deph}}) = K(\mathcal{P}_{\text{deph}}) = \mathbf{\Phi}(\mathcal{P}_{\text{deph}}) = 1 - H_2(p), \tag{B.1.35}$$

which also coincides with the unassisted quantum capacity of this channel $Q(\mathcal{P}_{\text{deph}})$ [70].

B.1.2 Pauli channels in arbitrary finite dimension

Let us now consider Pauli channels $\mathcal{P}_d$ in arbitrary dimension $d \geq 2$. These qudit channels are also called “Weyl channels” and they have Kraus representation

$$\mathcal{P}_d(\rho) = \sum_{a,b=0}^{d-1} p_{ab}(X^a Z^b)\rho(X^a Z^b)^\dagger, \tag{B.1.36}$$

where p_{ab} is a probability distribution for $a, b \in \mathbb{Z}_d := \{0, 1, \ldots, d-1\}$. Here X and Z are generalized Pauli operators whose action on the computational basis $\{|j\rangle\}$ is given by

$$X|j\rangle = |j \oplus 1\rangle \ , \ Z|j\rangle = \omega^j |j\rangle \ , \tag{B.1.37}$$

where $\oplus$ is the modulo d addition and

$$\omega := \exp(i2\pi/d). \tag{B.1.38}$$

These operators satisfy the generalized commutation relation

$$Z^b X^a = \omega^{ab} X^a Z^b. \tag{B.1.39}$$

Not only for $d = 2$ (qubits) but also at any $d \geq 2$ a Pauli channel is teleportation-covariant. The channel's Choi matrix $\rho_{\mathcal{P}_d}$ is Bell-diagonal with eigenvalues $\{p_{ab}\}$, so that we may write its von Neumann entropy in terms of the Shannon entropy as follows

$$S(\rho_{\mathcal{P}_d}) = H(\{p_{ab}\}). \tag{B.1.40}$$

Note that the Choi matrix can also be written as

$$\rho_{\mathcal{P}_d} = \frac{1}{d}\sum_{a,b,j,k}^{d-1} p_{ab}(I \otimes X^a Z^b)|jj\rangle\langle kk|(I \otimes X^a Z^b)^\dagger = \frac{1}{d}\sum_{a,b,j,k}^{d-1} p_{ab}\, \omega^{b(j-k)}|j, j \oplus a\rangle\langle k, k \oplus a|. \tag{B.1.41}$$

Then, let us consider a separable state $\tilde{\sigma}_s$ which is constructed as in Eq. (B.1.9). This state can be re-written as

$$\tilde{\sigma}_s = \frac{1}{d}\sum_{a,b,i=0}^{d-1} p_{ab}|i, i \oplus a\rangle\langle i, i \oplus a|. \tag{B.1.42}$$

By applying Eq. (B.1.7), we find

$$\mathbf{\Phi}(\mathcal{P}_d) \leq \log_2 d - H(\{p_{ab}\}) + H(\{p_a\}), \tag{B.1.43}$$

where $p_a := \sum_{b=0}^{d-1} p_{ab}$. Since the d-dimensional Pauli channel is unital, we may also write $I_{(\mathrm{R})\mathrm{C}}(\mathcal{P}_d) = \log_2 d - H(\{p_{ab}\})$, so that we derive the following bounds for its two-way capacity

$$\log_2 d - H(\{p_{ab}\}) \leq \mathcal{C}(\mathcal{P}_d) \leq \log_2 d - H(\{p_{ab}\}) + H(\{p_a\}), \tag{B.1.44}$$

which generalizes Eq. (B.1.27) to arbitrary dimension d. In the following two subsections, we consider the specific cases of the depolarising and dephasing channels in arbitrary finite dimension d.

B.1.3 Depolarising channel in arbitrary finite dimension

Consider a depolarising channel acting on a qudit with dimension $d \geq 2$. This channel can be written as

$$\mathcal{P}_{d\text{-depol}}(\rho) = (1-p)\rho + p\frac{I}{d} = A\rho A^\dagger + \sum_{i,j=0}^{d-1} A_{ij}\rho A_{ij}^\dagger, \tag{B.1.45}$$

where $A = \sqrt{1-p}I$ and $A_{ij} = \sqrt{p/d}|i\rangle\langle j|$. Its Choi matrix is the isotropic state

$$\rho_{\mathcal{P}_{d\text{-depol}}} = (1-p)|\Phi\rangle\langle\Phi| + \frac{p}{d^2} I \otimes I, \tag{B.1.46}$$

satisfying the twirling condition

$$\left[\rho_{\mathcal{P}_{d\text{-depol}}}, U^* \otimes U\right] = 0, \tag{B.1.47}$$

for any qudit unitary U.

The REE of an isotropic state can be evaluated exactly by using the formula of ref. [166]. Thus we can exactly compute the entanglement flux of the d-dimensional depolarising channel. Let us set

$$f := \frac{d^2-1}{d^2}p, \quad \kappa(d,p) := \log_2 d - H_2(f) - f\log_2(d-1). \tag{B.1.48}$$

Then, we may write the following expression

$$\mathbf{\Phi}(\mathcal{P}_{d\text{-depol}}) = E_{\mathrm{R}}\left(\rho_{\mathcal{P}_{d\text{-depol}}}\right) = \begin{cases} \kappa(d,p) & \text{if } p \leq \frac{d}{d+1}, \\ 0 & \text{otherwise.} \end{cases} \tag{B.1.49}$$

Because the depolarising channel is unital, we may use Eq. (B.1.4) to compute its (reverse) coherent information. We specifically find

$$I_{(\mathrm{R})\mathrm{C}}(\mathcal{P}_{d\text{-depol}}) = \log_2 d - H_2(f) - f\log_2(d^2-1) = \kappa(d,p) - f\log_2(d+1). \tag{B.1.50}$$

Thus, the two-way capacity of this channel must satisfy the bounds

$$\kappa(d,p) - f\log_2(d+1) \leq \mathcal{C}(\mathcal{P}_{d\text{-depol}}) \leq \kappa(d,p), \tag{B.1.51}$$

for $p \leq d/(d+1)$, while zero otherwise.

B.1.4 Dephasing channel in arbitrary finite dimension

Consider a generalized dephasing channel affecting a qudit in arbitrary dimension $d \geq 2$. This channel has Kraus representation [167]

$$\mathcal{P}_{d\text{-deph}}(\rho) = \sum_{i=0}^{d-1} P_i Z^i \rho (Z^\dagger)^i, \quad , \tag{B.1.52}$$

where Z is the generalized Pauli (phase-flip) operator defined in Eq. (B.1.37), and P_i is the probability of i phase flips.

The channel's Choi matrix is

$$\rho_{\mathcal{P}_{d\text{-deph}}} = \sum_{mjl} \frac{P_m}{d} \exp\left[\frac{2i\pi}{d}(j-l)m\right] |jj\rangle\langle ll|. \tag{B.1.53}$$

By diagonalizing, we find d non-zero eigenvalues $\mathbf{P} := \{P_0, \ldots, P_{d-1}\}$, so that the Von Neumann entropy is given by

$$S(\rho_{\mathcal{P}_{d\text{-deph}}}) = H(\mathbf{P}). \tag{B.1.54}$$

The separable state $\tilde{\sigma}_s$ in Eq. (B.1.9) turns out to be diagonal in the computational basis and takes the form

$$\tilde{\sigma}_s = \sum_{i=0}^{d-1} \frac{1}{d} |ii\rangle\langle ii| \ . \tag{B.1.55}$$

Thus, using Eq. (B.1.7), we find

$$\mathbf{\Phi}(\mathcal{P}_{d\text{-deph}}) \leq S(\rho_{\mathcal{P}_{d\text{-deph}}} || \tilde{\sigma}_s) = \log_2 d - H(\mathbf{P}). \tag{B.1.56}$$

Since this channel is unital, from Eq. (B.1.4) we have that its (reverse) coherent information is $I_{(\mathrm{R})\mathrm{C}}(\mathcal{P}_{d\text{-deph}}) = \log_2 d - H(\mathbf{P})$, so that lower and upper bounds coincide. This means that this channel is distillable and its two-way capacity is equal to

$$C(\mathcal{P}_{d\text{-deph}}) = D_2(\mathcal{P}_{d\text{-deph}}) = Q_2(\mathcal{P}_{d\text{-deph}}) = K(\mathcal{P}_{d\text{-deph}}) = \Phi(\mathcal{P}_{d\text{-deph}}) = \log_2 d - H(\mathbf{P}). \tag{B.1.57}$$

B.1.5 Amplitude damping channel

The amplitude damping channel describes the process of energy dissipation through spontaneous emission in a two-level system. Its application to an input qubit state is defined by the Kraus representation

$$\mathcal{E}_{\mathrm{damp}}(\rho) = \textstyle\sum_{i=0,1} A_i \rho A_i^{\dagger}, \tag{B.1.58}$$

where

$$A_0 := |0\rangle\langle 0| + \sqrt{1-p}\, |1\rangle\langle 1|\,, \quad A_1 := \sqrt{p}\, |0\rangle\langle 1|\,, \tag{B.1.59}$$

and p is the probability of damping. This channel is not teleportation-covariant. In fact, because we have

$$|0\rangle\langle 0| \rightarrow |0\rangle\langle 0|\,, \quad |1\rangle\langle 1| \rightarrow p\,|0\rangle\langle 0| + (1-p)\,|1\rangle\langle 1|\,, \tag{B.1.60}$$

there is no unitary U able to realize $U\mathcal{E}_{\mathrm{damp}}(|0\rangle\langle 0|)U^{\dagger} = \mathcal{E}_{\mathrm{damp}}(X\,|0\rangle\langle 0|\,X)$ for Pauli operator X.

The amplitude damping channel can be decomposed as

$$\mathcal{E}_{\mathrm{damp}} = \mathcal{E}_{\mathrm{CV}\rightarrow\mathrm{DV}} \circ \mathcal{E}_{\eta(p)} \circ \mathcal{E}_{\mathrm{DV}\rightarrow\mathrm{CV}}, \tag{B.1.61}$$

where $\mathcal{E}_{\mathrm{DV}\to\mathrm{CV}}$ is an identity mapping from the original qubit (e.g. a spin) to a single-rail qubit, which is the subspace of a bosonic mode spanned by the vacuum and the single photon states; then, $\mathcal{E}_{\eta(p)}$ is a lossy channel with transmissivity $\eta(p) := 1 - p$; finally, $\mathcal{E}_{\mathrm{CV}\to\mathrm{DV}}$ is an identity mapping from the single-rail qubit to the original qubit. Note that the two mappings can be performed via perfect hybrid teleportation and the middle lossy channel preserves the 2-dimensional effective Hilbert space of the system.

Thanks to this decomposition, we can include $\mathcal{E}_{\mathrm{DV}\to\mathrm{CV}}$ in Alice's LOs and $\mathcal{E}_{\mathrm{CV}\to\mathrm{DV}}$ into Bob's LOs. The middle lossy channel $\mathcal{E}_{\eta(p)}$ can therefore be stretched into its asymptotic Choi matrix $\rho_{\mathcal{E}_{\eta(p)}}$. Overall, this means that the amplitude damping channel can be stretched into the asymptotic resource state $\sigma = \rho_{\mathcal{E}_{\eta(p)}}$ by means of an asymptotic simulation. By applying teleportation stretching, we therefore reduce the output of an adaptive protocol to the form

$$\rho^n_{\mathbf{ab}} := \rho_{\mathbf{ab}}(\mathcal{E}^{\otimes n}_{\mathrm{damp}}) = \bar{\Lambda}\left(\rho^{\otimes n}_{\mathcal{E}_{\eta(p)}}\right), \tag{B.1.62}$$

where both $\bar{\Lambda}$ and $\rho_{\mathcal{E}_{\eta(p)}}$ are intended as asymptotic limits. Thus, our reduction method provides the upper bound

$$\mathcal{C}(\mathcal{E}_{\mathrm{damp}}) \leq \mathbf{\Phi}\left[\mathcal{E}_{\eta(p)}\right] = -\log_2 p. \tag{B.1.63}$$

We can combine the latter result with the fact that we cannot exceed the logarithm of the dimension of the input Hilbert space (see this simple "dimensionality bound" in the main text, in the discussion just before Proposition 5). This leads to

$$\mathcal{C}(\mathcal{E}_{\mathrm{damp}}) \leq \min\{1, -\log_2 p\}. \tag{B.1.64}$$

The best lower bound is given by optimizing the reverse coherent information over the input states $\rho_u = \mathrm{diag}(1-u, u)$ for $0 \leq u \leq 1$. In fact, we have [32]

$$I_{\mathrm{RC}}(p) := \max_u I_{\mathrm{RC}}(\mathcal{E}_{\mathrm{damp}}, \rho_u) = \max_u \{H_2(u) - H_2(up)\}. \tag{B.1.65}$$

This is an achievable lower bound for entanglement distribution assisted by a final round of backward CCs. Note that this is strictly higher than the $Q_1 = Q$ of the channel, which is given by [32]

$$Q_1(\mathcal{E}_{\mathrm{damp}}) = \max_u \{H_2[u(1-p)] - H_2(up)\}. \tag{B.1.66}$$

Thus, in total, we may write

$$I_{\mathrm{RC}}(p) \leq \mathcal{C}(\mathcal{E}_{\mathrm{damp}}) \leq \min\{1, -\log_2 p\}. \tag{B.1.67}$$

An alternative upper bound for the two-way capacity of a quantum channel is its squashed entanglement, i.e., we may write [168]

$$\mathcal{C}(\mathcal{E}) \leq E_{\mathrm{sq}}(\mathcal{E}). \tag{B.1.68}$$

The squashed entanglement of an arbitrary channel $\mathcal{E}$, from system A to system B, is defined as [168]

$$E_{\mathrm{sq}}(\mathcal{E}) := \frac{1}{2} \max_{\rho_A} \inf_{V_{C\to EF}} [S(B|E)_\omega + S(B|F)_\omega], \tag{B.1.69}$$

where ρ_A is an arbitrary input state, and ω is the global output state

$$\omega_{BEF} := V_{C\to EF}[U^{\mathcal{E}}_{A\to BC}(\rho_A)], \tag{B.1.70}$$

with $U^{\mathcal{E}}_{A\to BC}$ being an isometric extension of $\mathcal{E}$ and $V_{C\to EF}$ being an arbitrary "squashing isometry".

In Eq. (B.1.69), the terms in the brackets are conditional von Neumann entropies computed over ω_{BEF}, i.e.,

$$S(B|E)_\omega = S(BE)_\omega - S(E)_\omega, \quad S(B|F)_\omega = S(BF)_\omega - S(F)_\omega. \tag{B.1.71}$$

Then note that the most general input state reads

$$\rho_A = \begin{pmatrix} 1-\gamma & c^* \\ c & \gamma \end{pmatrix}, \tag{B.1.72}$$

where $\gamma \in [0,1]$ is the population of the excited state $|1\rangle$, while the off-diagonal term $|c| \leq \sqrt{(1-\gamma)\gamma}$ accounts for coherence. Thus, the maximization in Eq. (B.1.69) is mapped into a maximization over parameters γ and c.

Let us compute the squashed entanglement of the amplitude damping channel $\mathcal{E}_{\mathrm{damp}}$. Recall that its action is described by Eq. (B.1.58) with Kraus operators as in Eq. (B.1.59). In the computational basis $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$, the unitary dilation of $\mathcal{E}_{\mathrm{damp}}$ is therefore given by the following matrix

$$U_p = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & \sqrt{1-p} & \sqrt{p} & \\ 0 & -\sqrt{p} & \sqrt{1-p} & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \tag{B.1.73}$$

so that we may write

$$\mathcal{E}_{\mathrm{damp}}(\rho_A) = \mathrm{Tr}_C[U_p(\rho_A \otimes |0\rangle\langle 0|_C)U_p^\dagger], \tag{B.1.74}$$

where C is an environmental qubit prepared in the fundamental state $|0\rangle$. It is clear that Eq. (B.1.74) expresses the isometric extension of the channel, i.e., it corresponds to $\mathcal{E}_{\text{damp}}(\rho_A) = \text{Tr}_C[U^{\text{damp}}_{A\to BC}(\rho_A)]$.

As a squashing channel we consider another amplitude damping channel but with damping probability equal to 1/2, so that its unitary dilation is $V = U_{1/2}$. In other words, we consider the squashing isometry $V_{C\to EF} = \left[U^{\text{damp}}_{C\to EF}\right]_{p=1/2}$ (so that we are more precisely deriving an upper bound of the squashed entanglement of the channel). Let us derive the global output state ω_{BEF} step-by-step.

The state of systems B and C at the output of the dilation U_p is given by

$$\rho_{BC} := U_p(\rho_A \otimes |0\rangle\langle 0|_C)U_p^\dagger = \begin{pmatrix} 1-\gamma & \sqrt{p}c^* & \sqrt{1-p}c^* & 0 \\ c\sqrt{p} & p\gamma & \sqrt{1-p}\sqrt{p}\gamma & 0 \\ c\sqrt{1-p} & \sqrt{1-p}\sqrt{p}\gamma & (1-p)\gamma & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}. \tag{B.1.75}$$

Now the system C is sent through the squashing amplitude damping channel with probability 1/2. At the output of the dilation $U_{1/2}$ we have the final output state

$$\omega_{BEF} = (I_B \otimes U_{1/2})\rho_{BC} \otimes |0\rangle\langle 0|_F (I_B \otimes U_{1/2})^\dagger$$

$$= \begin{pmatrix} 1-\gamma & \frac{\sqrt{p}c^*}{\sqrt{2}} & \frac{\sqrt{p}c^*}{\sqrt{2}} & 0 & \sqrt{1-p}c^* & 0 & 0 & 0 \\ \frac{c\sqrt{p}}{\sqrt{2}} & \frac{p\gamma}{2} & \frac{p\gamma}{2} & 0 & \frac{\sqrt{(1-p)p\gamma}}{\sqrt{2}} & 0 & 0 & 0 \\ \frac{c\sqrt{p}}{\sqrt{2}} & \frac{p\gamma}{2} & \frac{p\gamma}{2} & 0 & \frac{\sqrt{(1-p)p\gamma}}{\sqrt{2}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ c\sqrt{1-p} & \frac{\sqrt{(1-p)p\gamma}}{\sqrt{2}} & \frac{\sqrt{(1-p)p\gamma}}{\sqrt{2}} & 0 & \gamma - p\gamma & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}. \tag{B.1.76}$$

We now proceed with the calculation of the entropies in Eq. (B.1.71), which are obtained from the eigenvalues of the reduced states ρ_{BE}, ρ_{BF}, ρ_E and ρ_F. We obtain

$$\rho_E = \rho_F = \begin{pmatrix} 1 - \frac{p\gamma}{2} & \frac{\sqrt{p}c^*}{\sqrt{2}} \\ \frac{c\sqrt{p}}{\sqrt{2}} & \frac{p\gamma}{2} \end{pmatrix}, \tag{B.1.77}$$

with eigenvalues

$$\lambda_{1,2} = \frac{1}{2}\left(1 \pm \sqrt{2|c|^2 p + (p\gamma - 1)^2}\right). \tag{B.1.78}$$

The eigenvalues of ρ_{BE} and ρ_{BF} are too complicated to be reported here but it is easy to check that, exactly as for $\lambda_{1,2}$ in previous Eq. (B.1.78), their dependence on c is just through the modulus $|c|$, so that we can choose c to be real without losing generality. Because c is real, we also have that the entropic functional $\digamma(\rho) = S(B|E)_\omega + S(B|F)_\omega$ computed over the input state ρ is exactly the same as that computed over the state $Z\rho Z$, with Z being the phase-flip Pauli operator. Using the latter observation, together with the concavity of the conditional quantum entropy, one simply has

$$\digamma(\rho) = \frac{\digamma(\rho) + \digamma(Z\rho Z)}{2} \leq \digamma\left(\frac{\rho + Z\rho Z}{2}\right) = \digamma(\bar{\rho}), \tag{B.1.79}$$

where $\bar{\rho}$ is diagonal. This means that we may reduce the maximization to diagonal input states ($c = 0$).

As a result, we may just consider

$$\rho_E = \rho_F = \begin{pmatrix} 1 - \frac{p\gamma}{2} & 0 \\ 0 & \frac{p\gamma}{2} \end{pmatrix}, \tag{B.1.80}$$

with eigenvalues

$$\lambda_1 = \frac{p\gamma}{2},\ \lambda_2 = 1 - \frac{p\gamma}{2}, \tag{B.1.81}$$

and

$$\rho_{BE} = \rho_{BF} = \begin{pmatrix} \frac{1}{2}(p-2)\gamma + 1 & 0 & 0 & 0 \\ 0 & \frac{p\gamma}{2} & \frac{\sqrt{(1-p)p\gamma}}{\sqrt{2}} & 0 \\ 0 & \frac{\sqrt{(1-p)p\gamma}}{\sqrt{2}} & \gamma - p\gamma & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \tag{B.1.82}$$

with eigenvalues

$$\nu_1 = \frac{\gamma}{2}(2 - p),\ \nu_2 = 1 - \nu_1,\ \nu_3 = \nu_4 = 0. \tag{B.1.83}$$

From the previous eigenvalues, we compute the conditional quantum entropies in Eq. (B.1.71). Thus, we find that the squashed entanglement of the amplitude damping channel must satisfy the bound

$$E_{\mathrm{sq}}(\mathcal{E}_{\mathrm{damp}}) \leq \max_{\gamma} \left\{ H_2(\nu_1) - H_2(\lambda_1) \right\}, \tag{B.1.84}$$

where H_2 is the binary Shannon entropy of Eq. (2.12). In particular, the function $H_2(\nu_1) - H_2(\lambda_1)$ is concave and symmetric in γ, so that the maximum is reached for $\gamma = 1/2$, which corresponds to a maximally mixed state at the input. This reduces Eq. (B.1.84) to the simple bound

$$E_{\mathrm{sq}}(\mathcal{E}_{\mathrm{damp}}) \leq H_2\left(\frac{1}{2} - \frac{p}{4}\right) - H_2\left(1 - \frac{p}{4}\right). \tag{B.1.85}$$

If we choose a squashing amplitude damping channel with generic probability of damping η and we repeat the calculation from the beginning we obtain the following bound for the squashed entanglement

$$E_{\mathrm{sq}}(\mathcal{E}_{\mathrm{damp}}) \leq \frac{1}{2} \max_{\gamma} \min_{\eta} \left\{ H_2(\gamma - p\gamma\eta) + H_2\left[\gamma(1 - p + p\eta)\right] - H_2\left[p\gamma(1-\eta)\right] - H_2(p\gamma\eta) \right\}. \tag{B.1.86}$$

The minimum of the function inside the curly bracket is for $\eta = 1/2$, so our choice of a balanced amplitude damping channel as a squashing channel is now justified. Note that the sub-optimal choice $\eta = 0$ corresponds to use the identity as squashing channel; correspondingly, the right hand side of Eq. (B.1.86) becomes half of the entanglement-assisted classical capacity C_{A} of the amplitude damping channel, i.e.,

$$E_{\mathrm{sq}}(\mathcal{E}_{\mathrm{damp}}) \leq \frac{1}{2} C_{\mathrm{A}}(\mathcal{E}_{\mathrm{damp}}) = \frac{1}{2} \max_{\gamma} \left\{ H_2(\gamma) + H_2\left[\gamma(1-p)\right] - H_2(p\gamma) \right\}. \tag{B.1.87}$$

In conclusion, combining the lower bound of Eq. (B.1.65) and the upper bound of Eq. (B.1.85), we find that the two-way capacity of the amplitude damping channel is within the sandwich

$$\max_{u} \{ H_2(u) - H_2(up) \} \leq \mathcal{C}(\mathcal{E}_{\mathrm{damp}}) \leq H_2\left(\frac{1}{2} - \frac{p}{4}\right) - H_2\left(1 - \frac{p}{4}\right). \tag{B.1.88}$$

Note that, for high damping ($p \simeq 1$), the upper bound in Eq. (B.1.88) provides the scaling of $\lesssim 0.793(1-p)$ bits per channel use, while Eq. (B.1.64) provides the scaling of $\lesssim 1.44(1-p)$ bits per channel use.

B.2 Ultimate limits in bosonic communications

B.2.1 Relative entropy between Gaussian states

Before giving the results for the two-way capacities for quantum and secure communication through for bosonic Gaussian channel, we provide a fundamental tools for their derivation. Namely we provide a simple formula for the relative entropy between two arbitrary Gaussian states $\rho_1(u_1, V_1)$ and $\rho_2(u_2, V_2)$ directly in terms of their statistical moments. Our formula improves and thus supersedes previous expressions [169, 170]. We have the following

Theorem B.2.1 ([1], Theorem 7) *For two arbitrary multimode Gaussian states, $\rho_1(u_1, V_1)$ and $\rho_2(u_2, V_2)$, the entropic functional*

$$\Sigma := -\mathrm{Tr}\left(\rho_1 \log_2 \rho_2\right) \tag{B.2.89}$$

is given by

$$\Sigma(V_1, V_2, \delta) = \frac{\ln\det\left(V_2 + \frac{i\mathbf{\Omega}}{2}\right) + \mathrm{Tr}(V_1 G_2) + \delta^T G_2 \delta}{2\ln 2}, \tag{B.2.90}$$

where $\delta := u_1 - u_2$ and $G_i := G(V_i) = 2i\mathbf{\Omega}\coth^{-1}(2V_i i\mathbf{\Omega})$. As a consequence, the von Neumann entropy of a Gaussian state $\rho(u, V)$ is equal to

$$S(\rho) := -\mathrm{Tr}\left(\rho \log_2 \rho\right) = \Sigma(V, V, 0)\ , \tag{B.2.91}$$

and the relative entropy of two Gaussian states $\rho_1(u_1, V_1)$ and $\rho_2(u_2, V_2)$ is given by

$$\begin{aligned} S(\rho_1||\rho_2) &:= \mathrm{Tr}\left[\rho_1(\log_2 \rho_1 - \log_2 \rho_2)\right] \\ &= -S(\rho_1) - \mathrm{Tr}\left(\rho_1 \log_2 \rho_2\right) \\ &= -\Sigma(V_1, V_1, 0) + \Sigma(V_1, V_2, \delta)\ . \end{aligned} \tag{B.2.92}$$

Proof: The starting point is the use of the Gibbs-exponential form for Gaussian states [82]. Start with zero-mean Gaussian states, this can be written as $\rho_i = Z_i^{-1}\exp[-\hat{x}^T G_i \hat{x}/2]$, where $G_i = g(V_i)$ is the Gibbs-matrix and $Z_i = \det\left(V_i + i\Omega/2\right)^{1/2}$ is the normalization factor (with $i = 1, 2$). Then, replacing into the definition of Σ given in Eq. (B.2.89), we find

$$\begin{aligned} (2\ln 2)\Sigma &= 2\ln Z_2 + \mathrm{Tr}\left(\rho_1 \hat{x}^T G_2 \hat{x}\right) \\ &= \ln\det\left(V_2 + i\Omega/2\right) \\ &+ \sum_{jk} \mathrm{Tr}\left(\rho_1 \hat{x}_j \hat{x}_k\right) G_{2jk}\ . \end{aligned} \tag{B.2.93}$$

Using the commutator $\langle[\hat{x}_j, \hat{x}_k]\rangle = i\Omega_{jk}$ and the anticommutator $\langle\{\hat{x}_j, \hat{x}_k\}\rangle = 2V_{jk}$, we derive

$$\begin{aligned} \sum_{jk} \mathrm{Tr}\left(\rho_1 \hat{x}_j \hat{x}_k\right) G_{2jk} &= \mathrm{Tr}\left[\left(V_1 + \frac{i\Omega}{2}\right)^T G_2\right] \\ &= \mathrm{Tr}\left(V_1 G_2\right), \end{aligned} \tag{B.2.94}$$

where we also exploit the fact that $\mathrm{Tr}(\Omega G) = 0$, because Ω is antisymmetric and G is symmetric (as V).

Let us now extend the formula to non-zero mean values (with difference $\delta = u_1 - u_2$). This means to perform the replacement $\hat{x} \to \hat{x} - u_2$, so that

$$\begin{aligned}\mathrm{Tr}\,(\rho_1 \hat{x}_j \hat{x}_k) &\to \mathrm{Tr}\,[\rho_1(\hat{x}_j - u_{2j})(\hat{x}_k - u_{2k})] \\ &= \mathrm{Tr}\,[\rho_1(\hat{x}_j - u_{1j} + \delta_j)(\hat{x}_k - u_{1k} + \delta_k)] \\ &= \mathrm{Tr}\,[\rho_1(\hat{x}_j - u_{1j})(\hat{x}_k - u_{1k})] + \delta_j \delta_k \ . \end{aligned} \tag{B.2.95}$$

By replacing this expression in Eq. (B.2.94), we get

$$\sum_{jk} \mathrm{Tr}\,(\rho_1 \hat{x}_j \hat{x}_k)\, G_{2jk} \to \mathrm{Tr}\,(V_1 G_2) + \delta^T G_2 \delta \ . \tag{B.2.96}$$

Thus, by combining Eqs. (B.2.93) and (B.2.96), we achieve Eq. (B.2.90). The other Eqs. (B.2.91) and (B.2.92) are immediate consequences. This completes the proof of Theorem B.2.1. ■

As discussed in ref. [82], the Gibbs-matrix G becomes singular for a pure state or, more generally, for a mixed state containing vacuum contributions (i.e., with some of the symplectic eigenvalues equal to 1/2). In this case the Gibbs-exponential form must be used carefully by making a suitable limit. Since Σ is basis independent, we can perform the calculations in the basis in which V_2, and therefore G_2, is diagonal. In this basis

$$\Sigma = \frac{1}{2} \sum_{k=1}^{n} \sum_{\pm} \alpha_k^{\pm} \log_2(v_{2k} \pm 1/2) \ , \tag{B.2.97}$$

where $\{v_{2k}\}$ is the symplectic spectrum of V_2, and

$$\alpha_k^{\pm} = 1 \pm [(V_1)_{k,k} + (V_1)_{k+n,k+n}] \ . \tag{B.2.98}$$

Now, if $v_{2k} = 1/2$ for some k, then its contribution to the sum in Eq. (B.2.97) is either zero or infinity.

B.2.2 Fundamental rate-loss scaling in quantum optical communications

Coherent and reverse coherent information of a Gaussian channel

Here we discuss the computation of the (reverse) coherent information for the most important single-mode Gaussian channels, i.e., the thermal-loss channel, the amplifier channel and the additive-noise Gaussian channel. Compactly, their action on input quadratures is given by

$$\hat{x} \to \sqrt{\eta}\hat{x} + \sqrt{|1-\eta|}\hat{x}_E + z, \tag{B.2.99}$$

where $\eta \geq 0$ is the transmission (or gain), E is the environmental mode in a thermal state with $\bar{n}$ mean photons, and z is a classical Gaussian variable with CM $\xi I \geq 0$. The Choi matrix $\rho_{\mathcal{E}}$ of this Gaussian channel $\mathcal{E} = \mathcal{E}(\eta, \bar{n}, \xi)$ is defined as an asymptotic limit. At the input we consider a sequence of TMSV states Φ^{μ} with CM as in Eq. (1.43). Then, at the output, we get a sequence of finite-energy Gaussian states

$$\rho_{\mathcal{E}}^{\mu} := \mathcal{I} \otimes \mathcal{E}(\Phi^{\mu}), \tag{B.2.100}$$

whose limit defines $\rho_{\mathcal{E}} := \lim_{\mu} \rho_{\mathcal{E}}^{\mu}$. The quasi-Choi matrices $\rho_{\mathcal{E}}^{\mu}$ are zero-mean Gaussian states with CM

$$\begin{aligned} V^{\mu}(\eta, \bar{n}, \xi) &= \left(\begin{array}{cc} \mu \mathbf{I} & \gamma \mathbf{Z} \\ \gamma \mathbf{Z} & \beta \mathbf{I} \end{array} \right) , \\ \beta :&= \eta\mu + |1-\eta| \left(\bar{n} + \frac{1}{2} \right) + \xi \ , \\ \gamma :&= \sqrt{\eta(\mu^2 - 1/4)} \ . \end{aligned} \tag{B.2.101}$$

Let us consider the symplectic eigenvalues of the output CM in Eq. (B.2.101), which are given by

$$\nu_{\pm} = \sqrt{\frac{\Delta \pm \sqrt{\Delta^2 - 4 \det V^{\mu}}}{2}}, \quad \Delta := \mu^2 + \beta^2 - 2\gamma^2. \tag{B.2.102}$$

Using the formula of the von Neumann entropy for Gaussian states and the definitions of the coherent information I_{C} and reverse coherent information I_{RC}, we may write

$$I_{\mathrm{C}}(\mathcal{E}, \Phi^{\mu}) = I(A\rangle B)_{\rho_{\mathcal{E}}^{\mu}} = s(\beta) - s(\nu_-) - s(\nu_+) \ , \tag{B.2.103}$$

$$I_{\mathrm{RC}}(\mathcal{E}, \Phi^{\mu}) = I(A\langle B)_{\rho_{\mathcal{E}}^{\mu}} = s(\mu) - s(\nu_-) - s(\nu_+) \ , \tag{B.2.104}$$

where function $s(x) := (x + 1/2)\log_2(x + 1/2) - (x - 1/2)\log_2(x - 1/2)$. It is easy to see that these quantities are continuous and increasing in μ, for any fixed values of η, $\bar{n}$ and ξ. For instance, for the lossy channel ($0 \leq \eta \leq 1$, $\bar{n} = \xi = 0$), we simply have

$$I(A\rangle B)_{\rho_{\mathcal{E}}^{\mu}} = s\left[\frac{1-\eta}{2} + \eta\mu\right] - s\left[\frac{\eta}{2} + (1-\eta)\mu\right] \ , \tag{B.2.105}$$

$$I(A\langle B)_{\rho_{\mathcal{E}}^{\mu}} = s(\mu) - s\left[\frac{\eta}{2} + (1-\eta)\mu\right] . \tag{B.2.106}$$

Thus, the limit for $\mu \to +\infty$ in the expressions of Eq. (B.2.104) is regular and finite. The asymptotic values represent the coherent and reverse coherent information of the considered Gaussian channels, i.e., we have

$$I_{\mathrm{C}}(\mathcal{E}) = I(A\rangle B)_{\rho_{\mathcal{E}}} := \lim_{\mu} I(A\rangle B)_{\rho_{\mathcal{E}}^{\mu}} \ , \tag{B.2.107}$$

$$I_{\mathrm{RC}}(\mathcal{E}) = I(A\langle B)_{\rho_{\mathcal{E}}} := \lim_{\mu} I(A\langle B)_{\rho_{\mathcal{E}}^{\mu}}, \tag{B.2.108}$$

as already defined in Eqs. (2.29) and (2.30). Correspondingly, the hashing inequality can be safely extended to the limit, i.e., from

$$\max\{I(A\rangle B)_{\rho_{\mathcal{E}}^{\mu}}, I(A\langle B)_{\rho_{\mathcal{E}}^{\mu}}\} \leq D_1(\rho_{\mathcal{E}}^{\mu}), \tag{B.2.109}$$

we may write

$$\max\{I_{\mathrm{C}}(\mathcal{E}), I_{\mathrm{RC}}(\mathcal{E})\} \leq D_1(\rho_{\mathcal{E}}) := \lim_{\mu} D_1(\rho_{\mathcal{E}}^{\mu}). \tag{B.2.110}$$

For the thermal-loss channel, the best lower bound is the reverse coherent information, given by [33]

$$I_{\mathrm{RC}}(\eta, \bar{n}) = -\log_2(1-\eta) - h(\bar{n}), \tag{B.2.111}$$

where $h(x) := (x+1)\log_2(x+1) - x\log_2 x$ is the entropic function. In particular, for a lossy channel ($\bar{n} = 0$), one has

$$I_{\mathrm{RC}}(\eta) = -\log_2(1-\eta)\,. \tag{B.2.112}$$

For the amplifier channel, the best lower bound is given by the coherent information, which is equal to [33, 62]

$$I_{\mathrm{C}}(\eta, \bar{n}) = \log_2\left(\frac{\eta}{\eta-1}\right) - h(\bar{n}), \tag{B.2.113}$$

and becomes

$$I_{\mathrm{C}}(\eta) = \log_2\left(\frac{\eta}{\eta-1}\right), \tag{B.2.114}$$

for the quantum-limited amplifier ($\bar{n} = 0$). The coherent information and reverse coherent information of the additive-noise Gaussian channel coincide. We have [62]

$$I_{\mathrm{C}}(\xi) = I_{\mathrm{RC}}(\xi) = -\log_2 \xi - \frac{1}{\ln 2}. \tag{B.2.115}$$

B.2.3 Entanglement flux of a Gaussian channel

Here we discuss how to compute the entanglement flux of a single-mode Gaussian channel (in canonical form). We provide the general recipe and then we go into details of the specific channels in the next subsections. The entanglement flux of a Gaussian channel $\mathcal{E}$ satisfies

$$\Phi(\mathcal{E}) \leq \liminf_{\mu\to+\infty} S(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s}) \ , \tag{B.2.116}$$

where $\rho^{\mu}_{\mathcal{E}}$ is a sequence of quasi-Choi matrices as defined in Eq. (B.2.100) with CMs as in Eq. (B.2.101), while $\tilde{\sigma}^{\mu}_{s}$ is a suitable sequence of separable Gaussian states.

For any μ, we choose a separable Gaussian state $\tilde{\sigma}^{\mu}_{s}$ with CM $\tilde{V}^{\mu}(\eta,\bar{n},\xi)$ as in Eq. (B.2.101) but with the replacement

$$\gamma \to \sqrt{(\mu-1/2)(\beta-1/2)}, \tag{B.2.117}$$

for the off-diagonal term. At fixed marginals μ and β, this is the most-correlated separable Gaussian state that we can build according to Eqs. (2.110) and (2.111); it has maximum (non-Gaussian) discord [103] and minimizes the relative entropy $S(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s})$ as long as $\rho^{\mu}_{\mathcal{E}}$ is an entangled state. In the specific case where the channel $\mathcal{E}$ is entanglement-breaking, then $\rho^{\mu}_{\mathcal{E}}$ becomes separable and we can trivially pick $\tilde{\sigma}^{\mu}_{s} = \rho^{\mu}_{\mathcal{E}}$, which gives $S(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s}) = 0$. In general, we are left with the analytical calculation of the relative entropy $S(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s})$ between two Gaussian states. This can be done in terms of their statistical moments according to our formula for the REE between two arbitrary multimode Gaussian states, which is given in the "Methods" section of our paper. For $S(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s})$ we find regular expressions with a well-defined limit, so that we can put $\liminf_{\mu} = \lim_{\mu}$ in Eq. (B.2.116). We provide full algebraic details below for the various Gaussian channels.

B.2.4 Entanglement flux of a thermal-loss channel

Consider a thermal-loss channel $\mathcal{E}_{\text{loss}}(\eta,\bar{n})$ with transmissivity $0 \leq \eta \leq 1$ and thermal number $\bar{n}$, so that thermal noise has variance $\omega = \bar{n}+1/2$. For $\bar{n} \geq \eta(1-\eta)^{-1}$, this channel is entanglement-breaking and we have $\Phi(\eta,\bar{n}) = 0$. For $\bar{n} < \eta(1-\eta)^{-1}$ we compute the relative entropy $S^{\mu} := S\left(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s}\right)$ from the CMs $V^{\mu}(\eta \leq 1,\bar{n},0)$ and $\tilde{V}^{\mu}(\eta \leq 1,\bar{n},0)$ of the zero-mean Gaussian states $\rho^{\mu}_{\mathcal{E}}$ and $\tilde{\sigma}^{\mu}_{s}$. Using our formula for the relative entropy between Gaussian states, we get

$$S^{\mu} = -S_1 + \frac{\Delta}{2\ln 2} + \frac{1}{2}\log_2\left\{\frac{2\mu-1}{4}[2\omega-1+2\eta(\mu-\omega)]\right\}, \tag{B.2.118}$$

where S_1 is the contribution of the von Neumann entropy, while the other two terms come from the entropic functional $\Sigma(V^{\mu},\tilde{V}^{\mu},0)$. The term Δ is analytical but too cumbersome to be reported here. By expanding for large μ, we may write

$$\Delta \to 2\left[1-2\omega\coth^{-1}\left(\frac{1+\eta}{\eta-1}\right)\right]+O(\mu^{-1}) \ , \tag{B.2.119}$$

$$S_1 \to h(\bar{n})+\log_2\left[e(1-\eta)\mu\right]+O(\mu^{-1}), \tag{B.2.120}$$

and

$$\frac{1}{2}\log_2\left\{\frac{2\mu-1}{4}[2\omega-1+2\eta(\mu-\omega)]\right\}\to\log_2\mu\sqrt{\eta}+O(\mu^{-1}) \ . \tag{B.2.121}$$

Taking the limit $S^{\infty}=\liminf_{\mu} S^{\mu}=\lim_{\mu} S^{\mu}$, we get

$$S^{\infty}=-\log_2\left[(1-\eta)\eta^{\bar{n}}\right]-h(\bar{n}) \ . \tag{B.2.122}$$

As a result, by replacing in Eq. (B.2.116), we find that the entanglement flux of a thermal-loss channel $\mathcal{E}_{\text{loss}}(\eta,\bar{n})$ satisfies

$$\mathbf{\Phi}(\eta,\bar{n})\leq\mathbf{\Phi}_{\text{loss}}(\eta,\bar{n}):=\begin{cases}-\log_2\left[(1-\eta)\eta^{\bar{n}}\right]-h(\bar{n}) & \text{for } \bar{n}<\frac{\eta}{1-\eta},\\ \\ 0 \quad \text{otherwise.}\end{cases} \tag{B.2.123}$$

The thermal bound in Eq. (B.2.123) is clearly tighter than previous bounds based on the squashed entanglement, such as the “Takeoka-Guha-Wilde” (TGW) thermal bound [106]

$$K_{\text{TGW}}=\log_2\left[\frac{(1-\eta)\bar{n}+1+\eta}{(1-\eta)\bar{n}+1-\eta}\right] \ , \tag{B.2.124}$$

and its improved version [100]. However, Φ_{loss} does not generally coincide with the achievable lower-bound [33] given by the reverse coherent information of the channel in Eq. (B.2.111). Thus, the generic two-way capacity of the thermal-loss channel satisfies the sandwich relation

$$-\log_2(1-\eta)-h(\bar{n})\leq\mathcal{C}_{\text{loss}}(\eta,\bar{n})\leq\mathbf{\Phi}_{\text{loss}}(\eta,\bar{n}). \tag{B.2.125}$$

It is easy to check that, for a lossy channel ($\bar{n}=0$), the bounds Eq. (B.2.125) coincide, therefore establishing

$$\mathcal{C}_{\text{loss}}(\eta)=-\log_2(1-\eta) \ . \tag{B.2.126}$$

Full calculation details for the lossy channel

For the sake of completeness, we provide the specific details of the computation of the relative entropy S^{μ} for the specific case of a lossy channel. After some algebra, we achieve

$$S^{\mu}=\log_2\left[\left(\mu-\frac{1}{2}\right)\sqrt{\eta}\right]-s\left[(1-\eta)\mu+\frac{\eta}{2}\right]+\frac{\Delta}{2\ln 2} \ , \tag{B.2.127}$$

where

$$\begin{aligned}\Delta :=& \frac{c-(2\mu-1)(1-\eta)a}{b}\coth^{-1}\left[\frac{(1-\eta)(1-2\mu)-a}{2}\right]\\ &-\frac{c+(2\mu-1)(1-\eta)a}{b}\coth^{-1}\left[\frac{(1-\eta)(1-2\mu)+a}{2}\right],\end{aligned} \tag{B.2.128}$$

and

$$a := \sqrt{1-(6-\eta)\eta+4\mu[1+(4-\eta)\eta+(1-\eta)^2\mu]}, \tag{B.2.129}$$

$$b := \sqrt{8\mu+(2\mu-1)[4\eta+(2\mu-1)(1-\eta)^2]}, \tag{B.2.130}$$

$$c := 2\eta(2\mu-1)\left(2\sqrt{4\mu^2-1}-1-2\mu\right)-\eta^2(2\mu-1)^2-(1+2\mu)^2. \tag{B.2.131}$$

We now insert the expression of Δ in Eq. (B.2.127) and we take the limit for $\mu \to +\infty$. This limit is defined (i.e., $\liminf_\mu = \lim_\mu$) and we get

$$S^\infty = \lim_{\mu\to+\infty} S^\mu = -\log_2(1-\eta)\ . \tag{B.2.132}$$

We can show this limit step-by-step. First note that, for large ν, we have

$$s(\nu) \to \log_2 e\nu + O(\nu^{-1})\ . \tag{B.2.133}$$

Thus, in the limit of $\mu \to +\infty$, the first two terms in the RHS of Eq. (B.2.127) become

$$\log_2\left[\left(\mu-\frac{1}{2}\right)\sqrt{\eta}\right] \to \log_2\left(\mu\sqrt{\eta}\right)+O(\mu^{-1}), \tag{B.2.134}$$

$$-s\left[(1-\eta)\mu+\frac{\eta}{2}\right] \to -\log_2[e(1-\eta)\mu]+O(\mu^{-1}). \tag{B.2.135}$$

Then, it is easy to show that, for $\mu \to +\infty$, we have

$$\begin{aligned}\Delta \to& \left[-4(1-\eta)\mu+O(\mu^0)\right]\coth^{-1}\left[-2(1-\eta)\mu+O(\mu^0)\right]\\ &-\left[-2+O(\mu^{-1})\right]\coth^{-1}\left[\frac{1+\eta}{1-\eta}+O(\mu^{-1})\right]\\ &\to 2-\ln\eta+O(\mu^{-1})\ .\end{aligned} \tag{B.2.136}$$

In conclusion, by using Eqs. (B.2.134), (B.2.135) and (B.2.136) into Eq. (B.2.127), we obtain the final result in Eq. (B.2.132).

B.2.5 Entanglement flux of a quantum amplifier

Consider an amplifier channel $\mathcal{E}_{\text{amp}}(\eta,\bar{n})$ with gain $\eta > 1$ and thermal number $\bar{n}$, so that thermal noise has variance $\omega = \bar{n}+1/2$. For $\bar{n} \geq (\eta-1)^{-1}$ this channel is entanglement breaking and therefore $\mathbf{\Phi}(\eta,\bar{n})=0$. For $\bar{n}<(\eta-1)^{-1}$ we compute the relative entropy $S^{\mu}:=S\left(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s}\right)$ from the CMs $V^{\mu}(\eta>1,\bar{n},0)$ and $\tilde{V}^{\mu}(\eta>1,\bar{n},0)$ of the zero-mean Gaussian states $\rho^{\mu}_{\mathcal{E}}$ and $\tilde{\sigma}^{\mu}_{s}$. Up to terms $O(\mu^{-1})$, we get

$$S(\rho^{\mu}_{\mathcal{E}})\rightarrow h(\bar{n})+\log_2 e(\eta-1)\mu,\quad -\operatorname{Tr}\left(\rho^{\mu}_{\mathcal{E}}\log_2\tilde{\sigma}^{\mu}_{s}\right)\rightarrow\frac{\ln(\eta\mu^2)+2+4\omega\coth^{-1}\left(\frac{\eta+1}{\eta-1}\right)}{2\ln 2}. \tag{B.2.137}$$

For large μ we therefore obtain

$$S^{\infty}=\log_2\left(\frac{\eta^{\bar{n}+1}}{\eta-1}\right)-h(\bar{n}). \tag{B.2.138}$$

Thus we find

$$\mathbf{\Phi}(\eta,\bar{n})\leq\mathbf{\Phi}_{\text{amp}}(\eta,\bar{n}):=\begin{cases}\log_2\left(\frac{\eta^{\bar{n}+1}}{\eta-1}\right)-h(\bar{n})\ \text{ for }\bar{n}<(\eta-1)^{-1},\\ \\ 0\quad\text{otherwise.}\end{cases} \tag{B.2.139}$$

In general, $\mathbf{\Phi}_{\text{amp}}(\eta,\bar{n})$ does not coincide with the best known lower bound which is given by the coherent information of the channel in Eq. (B.2.113). Thus, the two-way capacity of a quantum amplifier channel satisfies

$$\log_2\left(\frac{\eta}{\eta-1}\right)-h(\bar{n})\leq\mathcal{C}_{\text{amp}}(\eta,\bar{n})\leq\mathbf{\Phi}_{\text{amp}}(\eta,\bar{n}). \tag{B.2.140}$$

It is easy to check that, for the quantum-limited amplifier ($\bar{n}=0$), the previous upper and lower bounds coincide, thus determining its two-way capacity

$$\mathcal{C}_{\text{amp}}(\eta)=\log_2\left(\frac{\eta}{\eta-1}\right). \tag{B.2.141}$$

Thus, $\mathcal{C}_{\text{amp}}(\eta)$ turns out to coincide with the unassisted quantum capacity $Q_{\text{amp}}(\eta)$ [62, 122].

B.2.6 Entanglement flux of an additive-noise Gaussian channel

Consider an additive-noise Gaussian channel $\mathcal{E}_{\text{add}}(\xi)$ with noise variance $\xi\geq 0$. For $\xi\geq 1$ this channel is entanglement breaking and therefore we have $\mathbf{\Phi}(\xi)=0$. For $\xi<1$ we compute the relative entropy $S^{\mu}:=S\left(\rho^{\mu}_{\mathcal{E}}||\tilde{\sigma}^{\mu}_{s}\right)$ from the CMs $V^{\mu}(1,0,\xi)$ and $\tilde{V}^{\mu}(1,0,\xi)$ of the zero-mean Gaussian states $\rho^{\mu}_{\mathcal{E}}$ and $\tilde{\sigma}^{\mu}_{s}$. Discarding terms $O(\mu^{-1})$, we get

$$S(\rho^{\mu}_{\mathcal{E}})\rightarrow\log_2(e^2\xi\mu),\quad -\operatorname{Tr}\left(\rho^{\mu}_{\mathcal{E}}\log_2\tilde{\sigma}^{\mu}_{s}\right)\rightarrow\frac{\ln\left[\frac{(2\mu-1)(2\xi+2\mu-1)}{4}\right]+2(1+\xi)}{2\ln 2}. \tag{B.2.142}$$

which leads to

$$S^{\infty} = \liminf_{\mu} S^{\mu} = \lim_{\mu} S^{\mu} = \frac{\xi - 1}{\ln 2} - \log_2 \xi \ . \tag{B.2.143}$$

Thus we find

$$\mathbf{\Phi}(\xi) \leq \mathbf{\Phi}_{\text{add}}(\xi) := \begin{cases} \frac{\xi-1}{\ln 2} - \log_2 \xi & \text{for } \xi < 1, \\ \\ 0 \quad \text{otherwise.} \end{cases} \tag{B.2.144}$$

The best lower bound is its coherent information $I_{\mathrm{C}}(\xi)$ of Eq. (B.2.115), so that the two-way capacity satisfies

$$-1/\ln 2 - \log_2 \xi \leq \mathcal{C}_{\text{add}}(\xi) \leq \mathbf{\Phi}_{\text{add}}(\xi) \ . \tag{B.2.145}$$

B.2.7 Secondary canonical forms

For the conjugate of the amplifier it is easy to check that this channel is always entanglement-breaking, so that it has zero flux and, therefore, zero two-way capacity $\mathcal{C} = 0$. The A_2-form, which is a 'half' depolarising channel, is also an entanglement-breaking channel, so that $\mathbf{\Phi} = \mathcal{C} = 0$. Finally, for the "pathological" B_1-form, we find the trivial bound $\mathbf{\Phi} = +\infty$.

References

[1] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, "Fundamental limits of repeaterless quantum communications," *Nature Communications*, vol. 8, p. 15043, 2017.

[2] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi *arXiv:1510.08863v1*, 2015.

[3] S. Pirandola, S. L. Braunstein, R. Laurenza, C. Ottaviani, T. P. W. Cope, G. Spedalieri, and L. Banchi, "Theory of channel simulation and bounds for private communication," *Quantum Science and Technology*, vol. 3, no. 3, p. 035009, 2018.

[4] S. Pirandola, R. Laurenza, and S. L. Braunstein, "Teleportation simulation of bosonic gaussian channels: strong and uniform convergence," *The European Physical Journal D*, vol. 72, no. 9, p. 162, 2018.

[5] R. Laurenza, S. L. Braunstein, and S. Pirandola, "Finite-resource teleportation stretching for continuous-variable systems," *Scientific Reports*, vol. 8, no. 1, p. 15267, 2018.

[6] R. Laurenza, S. Tserkis, S. L. Braunstein, T. C. Ralph, and S. Pirandola, "Tight finite-resource bounds for private communication over gaussian channels," *arXiv:1808.00608*, 2018.

[7] R. Laurenza and S. Pirandola, "General bounds for sender-receiver capacities in multipoint quantum communications," *Phys. Rev. A*, vol. 96, p. 032318, 2017.

[8] R. Laurenza, C. Lupo, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Channel simulation in quantum metrology," *Quantum Meas. Quantum Metrol*, vol. 5, pp. 1–12, 2018.

[9] S. Pirandola, R. Laurenza, and C. Lupo, “Fundamental limits to quantum channel discrimination,” *arXiv:1803.02834*, 2018.

[10] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information.* Cambridge University Press, Cambridge, 2000.

[11] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, “Gaussian quantum information,” *Rev. Mod. Phys.*, vol. 84, pp. 621–669, May 2012.

[12] M. Hayashi, *Quantum Information Theory - An introduction.* Springer, 2006.

[13] S. L. Braunstein and P. van Loock, “Quantum information with continuous variables,” *Rev. Mod. Phys.*, vol. 77, pp. 513–577, Jun 2005.

[14] D. P. Divincenzo, “Quantum computation,” *Science*, p. 255, 1995.

[15] D. Abbott, C. R. Doering, C. M. Caves, D. M. Lidar, H. E. Brandt, A. R. Hamilton, D. K. Ferry, J. Gea-Banacloche, S. M. Bezrukov, and L. B. Kish, “Dreams versus reality: Plenary debate session on quantum computing,” *Quantum Information Processing*, vol. 2, pp. 449–472, Dec 2003.

[16] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, “Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels,” *Physical review letters*, vol. 70, no. 13, p. 1895, 1993.

[17] S. L. Braunstein and S. Pirandola, “Unite to build a quantum internet,” *Nature*, vol. 532, pp. 169–171, 2016.

[18] L. Vaidman, “Teleportation of quantum states,” *Phys. Rev. A*, vol. 49, pp. 1473–1476, 1994.

[19] S. L. Braunstein and H. J. Kimble, “Teleportation of continuous quantum variables,” *Phys. Rev. Lett.*, vol. 80, pp. 869–872, Jan 1998.

[20] S. L. Braunstein, G. M. D’Ariano, G. J. Milburn, and M. F. Sacchi, “Universal teleportation with a twist,” *Phys. Rev. Lett.*, vol. 84, pp. 3486–3489, Apr 2000.

[21] C. H. Bennett and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,” 01 1984.

[22] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Rev. Mod. Phys.*, vol. 74, pp. 145–195, 2002.

[23] H. J. Kimble, "The quantum internet," *Nature*, vol. 453, pp. 1023–1030, 06 2008.

[24] S. Bäuml, K. Azuma, G. Kato, and D. Elkouss, "Linear programs for entanglement and key distribution in the quantum internet," *arXiv:1809.03120*, 2018.

[25] H.-P. Breuer and F. Petruccione, *The Theory of Open Quantum Systems.* Oxford University, New York, 01 2006.

[26] H.-J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum repeaters: The role of imperfect local operations in quantum communication," *Phys. Rev. Lett.*, vol. 81, pp. 5932–5935, 1998.

[27] S. Pirandola, "Capacities of repeater-assisted quantum communications," *arXiv:1601.00966*, 2016.

[28] C. H. Bennett, I. Devetak, P. W. Shor, and J. A. Smolin, "Inequalities and separations among assisted capacities of quantum channels," *Phys. Rev. Lett.*, vol. 96, p. 150502, 2006.

[29] D. Leung and G. Smith, "Continuity of quantum channel capacities," *Communications in Mathematical Physics*, vol. 292, no. 1, pp. 201–215, 2009.

[30] G. Smith, "Quantum channel capacities," *2010 IEEE Information Theory Workshop*, pp. 1–5, 2010.

[31] L. Gyongyosi, S. Imre, and H. V. Nguyen, "A survey on quantum channel capacities," *IEEE Communications Surveys Tutorials*, vol. 20, no. 2, pp. 1149–1205, 2018.

[32] R. García-Patrón, S. Pirandola, S. Lloyd, and J. H. Shapiro, "Reverse coherent information," *Phys. Rev. Lett.*, vol. 102, p. 210501, 2009.

[33] S. Pirandola, R. García-Patrón, S. L. Braunstein, and S. Lloyd, "Direct and reverse secret-key capacities of a quantum channel," *Phys. Rev. Lett.*, vol. 102, p. 050503, 2009.

[34] M. Christandl, A. Ekert, M. Horodecki, P. Horodecki, J. Oppenheim, and R. Renner, "Unifying classical and quantum key distillation," in *Theory of Cryptography* (S. P. Vadhan, ed.), (Berlin, Heidelberg), pp. 456–478, Springer Berlin Heidelberg, 2007.

[35] M. B. Plenio and S. Virmani, "An introduction to entanglement measures," *Quant. Inf. Comput.*, vol. 7, pp. 1–51, 2007.

[36] V. Vedral, M. B. Plenio, M. A. Rippin, and P. L. Knight, "Quantifying entanglement," *Phys. Rev. Lett.*, vol. 78, pp. 2275–2279, Mar 1997.

[37] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, "Mixed-state entanglement and quantum error correction," *Phys. Rev. A*, vol. 54, pp. 3824–3851, 1996.

[38] M. A. Nielsen and I. L. Chuang, "Programmable quantum gate arrays," *Phys. Rev. Lett.*, vol. 79, pp. 321–324, 1997.

[39] D. Leung and W. Matthews, "On the power of ppt-preserving and non-signalling codes," *IEEE Transactions on Information Theory*, vol. 61, no. 8, pp. 4486–4499, 2015.

[40] V. Giovannetti, S. Lloyd, and L. Maccone, "Quantum metrology," *Phys. Rev. Lett.*, vol. 96, p. 010401, 2006.

[41] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology," *Nature Photonics*, vol. 5, pp. 222 EP –, 2011.

[42] S. Pirandola and C. Lupo, "Ultimate precision of adaptive noise estimation," *Phys. Rev. Lett.*, vol. 118, p. 100502, 2017.

[43] S. Ishizaka and T. Hiroshima, "Quantum teleportation scheme by selecting one of multiple output ports," *Phys. Rev. A*, vol. 79, p. 042306, 2009.

[44] S. Ishizaka, "Some remarks on port-based teleportation," *arXiv: 1506.01555*, 2015.

[45] S. Ishizaka and T. Hiroshima, "Asymptotic teleportation scheme as a universal programmable quantum processor," *Phys. Rev. Lett.*, vol. 101, p. 240501, 2008.

[46] S. Pirandola, "Quantum reading of a classical digital memory," *Phys. Rev. Lett.*, vol. 106, p. 090504, 2011.

[47] S. Pirandola, C. Lupo, V. Giovannetti, S. Mancini, and S. L. Braunstein, "Quantum reading capacity," *New Journal of Physics*, vol. 13, no. 11, p. 113012, 2011.

[48] C. Lupo and S. Pirandola, “Ultimate precision bound of quantum and subwavelength imaging,” *Phys. Rev. Lett.*, vol. 117, p. 190802, 2016.

[49] Y. Kuznetsova, A. Neumann, and S. R. J. Brueck, “Imaging interferometric microscopy–approaching the linear systems limits of optical resolution,” *Opt. Express*, vol. 15, no. 11, pp. 6651–6663, 2007.

[50] M. Tsang, R. Nair, and X.-M. Lu, “Quantum theory of superresolution for two incoherent optical point sources,” *Phys. Rev. X*, vol. 6, p. 031033, 2016.

[51] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, “Quantum illumination with gaussian states,” *Phys. Rev. Lett.*, vol. 101, p. 253601, Dec 2008.

[52] J. H. Shapiro and S. Lloyd, “Quantum illumination versus coherent-state target detection,” *New Journal of Physics*, vol. 11, no. 6, p. 063045, 2009.

[53] Z. Zhang, M. Tengner, T. Zhong, F. N. C. Wong, and J. H. Shapiro, “Entanglement’s benefit survives an entanglement-breaking channel,” *Phys. Rev. Lett.*, vol. 111, p. 010501, 2013.

[54] E. D. Lopaeva, I. Ruo Berchera, I. P. Degiovanni, S. Olivares, G. Brida, and M. Genovese, “Experimental realization of quantum illumination,” *Phys. Rev. Lett.*, vol. 110, p. 153603, 2013.

[55] C. W. Helstrom, “Quantum detection and estimation theory,” *Journal of Statistical Physics*, vol. 1, no. 2, pp. 231–252, 1969.

[56] R. Simon, N. Mukunda, and B. Dutta, “Quantum-noise matrix for multimode systems: U (n) invariance, squeezing, and normal forms,” *Physical Review A*, vol. 49, no. 3, p. 1567, 1994.

[57] R. Simon, “Peres-horodecki separability criterion for continuous variable systems,” *Phys. Rev. Lett.*, vol. 84, pp. 2726–2729, Mar 2000.

[58] J. Williamson, “On the algebraic problem concerning the normal forms of linear dynamical systems,” *American Journal of Mathematics*, vol. 58, no. 1, pp. 141–163, 1936.

[59] V. I. Arnold, *Mathematical Methods of Classical Mechanics.* Springer-Verlag, New York, 1978.

[60] A. Serafini, F. Illuminati, and S. D. Siena, “Symplectic invariants, entropic measures and correlations of gaussian states,” *Journal of Physics B: Atomic, Molecular and Optical Physics*, vol. 37, no. 2, p. L21, 2004.

[61] A. S. Holevo, M. Sohma, and O. Hirota, “Capacity of quantum gaussian channels,” *Phys. Rev. A*, vol. 59, pp. 1820–1828, Mar 1999.

[62] A. S. Holevo and R. F. Werner, “Evaluating capacities of bosonic gaussian channels,” *Phys. Rev. A*, vol. 63, p. 032312, 2001.

[63] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, “Quantum channels and memory effects,” *Rev. Mod. Phys.*, vol. 86, pp. 1203–1259, Dec 2014.

[64] G. Lindblad, “Completely positive maps and entropy inequalities,” *Comm. Math. Phys.*, vol. 40, no. 2, pp. 147–151, 1975.

[65] K. Kraus, *States, Effects and Operations*, vol. 190. Springer-Verlag, Berlin, 1983.

[66] W. F. Stinespring, “Positive functions on c*-algebras,” *Proceedings of the American Mathematical Society*, vol. 6, no. 2, pp. 211–216, 1955.

[67] K. Kraus, “General state changes in quantum theory,” *Annals of Physics*, vol. 64, no. 2, pp. 311 – 335, 1971.

[68] F. Caruso and V. Giovannetti, “Degradability of bosonic gaussian channels,” *Phys. Rev. A*, vol. 74, p. 062307, Dec 2006.

[69] F. Caruso, V. Giovannetti, and A. S. Holevo, “One-mode bosonic gaussian channels: a full weak-degradability classification,” *New Journal of Physics*, vol. 8, no. 12, p. 310, 2006.

[70] I. Devetak and P. W. Shor, “The capacity of a quantum channel for simultaneous transmission of classical and quantum information,” *Communications in Mathematical Physics*, vol. 256, no. 2, pp. 287–303, 2005.

[71] A. S. Holevo, “One-mode quantum gaussian channels: Structure and quantum capacity,” *Problems of Information Transmission*, vol. 43, pp. 1–11, Mar 2007.

[72] S. Pirandola, S. L. Braunstein, and S. Lloyd, "Characterization of collective gaussian attacks and security of coherent-state quantum cryptography," *Phys. Rev. Lett.*, vol. 101, p. 200504, Nov 2008.

[73] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130502, 2012.

[74] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, pp. 397 EP –, 05 2015.

[75] C. Ottaviani, G. Spedalieri, S. L. Braunstein, and S. Pirandola, "Continuous-variable quantum cryptography with an untrusted relay: Detailed security analysis of the symmetric configuration," *Phys. Rev. A*, vol. 91, p. 022320, Feb 2015.

[76] R. F. Werner, "All teleportation and dense coding schemes," *Journal of Physics A: Mathematical and General*, vol. 34, no. 35, p. 7081, 2001.

[77] S. Popescu, "Bell's inequalities versus teleportation: What is nonlocality?," *Phys. Rev. Lett.*, vol. 72, pp. 797–799, Feb 1994.

[78] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, "Advances in quantum teleportation," *Nature Photonics*, vol. 9, pp. 641 EP –, 09 2015.

[79] M. E. Shirokov, "On the energy-constrained diamond norm and its application in quantum information theory," *Problems of Information Transmission*, vol. 54, pp. 20–33, Jan 2018.

[80] A. Winter, "Energy-constrained diamond norm with applications to the uniform continuity of continuous variable channel capacities," *arXiv:1712.10267*, 2017.

[81] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, and G. Adesso, "Optimal continuous variable quantum teleportation with limited resources," *Phys. Rev. Lett.*, vol. 119, p. 120503, 2017.

[82] L. Banchi, S. L. Braunstein, and S. Pirandola, "Quantum fidelity for arbitrary gaussian states," *Phys. Rev. Lett.*, vol. 115, p. 260501, Dec 2015.

[83] C. A. Fuchs and J. van de Graaf, “Cryptographic distinguishability measures for quantum-mechanical states,” *IEEE Transactions on Information Theory*, vol. 45, no. 4, pp. 1216–1227, 1999.

[84] M. Horodecki, P. Horodecki, and R. Horodecki, “General teleportation channel, singlet fraction, and quasidistillation,” *Phys. Rev. A*, vol. 60, pp. 1888–1898, 1999.

[85] S. Albeverio, S.-M. Fei, and W.-L. Yang, “Optimal teleportation based on bell measurements,” *Phys. Rev. A*, vol. 66, p. 012301, 2002.

[86] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, “Parameter estimation of quantum channels,” *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5172–5185, 2008.

[87] V. Vedral and M. B. Plenio, “Entanglement measures and purification procedures,” *Phys. Rev. A*, vol. 57, pp. 1619–1633, Mar 1998.

[88] V. Vedral, “The role of relative entropy in quantum information theory,” *Rev. Mod. Phys.*, vol. 74, pp. 197–234, Mar 2002.

[89] C. H. Bennett, D. P. DiVincenzo, and J. A. Smolin, “Capacities of quantum erasure channels,” *Phys. Rev. Lett.*, vol. 78, pp. 3217–3220, 1997.

[90] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, “Secure key from bound entanglement,” *Phys. Rev. Lett.*, vol. 94, p. 160502, 2005.

[91] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim, “General paradigm for distilling classical key from quantum states,” *IEEE Transactions on Information Theory*, vol. 55, pp. 1898–1929, April 2009.

[92] M. Christandl, N. Schuch, and A. Winter, “Entanglement of the antisymmetric state,” *Communications in Mathematical Physics*, vol. 311, no. 2, pp. 397–422, 2012.

[93] I. Devetak and A. Winter, “Distillation of secret key and entanglement from quantum states,” *Proceedings of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, vol. 461, no. 2053, pp. 207–235, 2005.

[94] B. Schumacher and M. A. Nielsen, “Quantum data processing and error correction,” *Phys. Rev. A*, vol. 54, pp. 2629–2635, 1996.

[95] S. Lloyd, “Capacity of the noisy quantum channel,” *Phys. Rev. A*, vol. 55, pp. 1613–1622, 1997.

[96] A. Winter, “Tight uniform continuity bounds for quantum entropies: Conditional entropy, relative entropy distance and energy constraints,” *Communications in Mathematical Physics*, vol. 347, no. 1, pp. 291–313, 2016.

[97] A. S. Holevo, *Quantum systems, channels, information: a mathematical introduction*, vol. 16. Walter de Gruyter, 2013.

[98] M. J. Donald and M. Horodecki, “Continuity of relative entropy of entanglement,” *Physics Letters A*, vol. 264, no. 4, pp. 257 – 260, 1999.

[99] B. Synak-Radtke and M. Horodecki, “On asymptotic continuity of functions of quantum states,” *Journal of Physics A: Mathematical and General*, vol. 39, no. 26, p. L423, 2006.

[100] K. Goodenough, D. Elkouss, and S. Wehner, “Assessing the performance of quantum repeaters for all phase-insensitive gaussian bosonic channels,” *New Journal of Physics*, vol. 18, no. 6, p. 063005, 2016.

[101] S. Bose, “Quantum communication through an unmodulated spin chain,” *Phys. Rev. Lett.*, vol. 91, p. 207901, 2003.

[102] S. Bose, A. Bayat, P. Sodano, L. Banchi, and P. Verrucchi, *Spin Chains as Data Buses, Logic Buses and Entanglers*, pp. 1–37. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014.

[103] S. Pirandola, G. Spedalieri, S. L. Braunstein, N. J. Cerf, and S. Lloyd, “Optimality of gaussian discord,” *Phys. Rev. Lett.*, vol. 113, p. 140405, 2014.

[104] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, “The classical-quantum boundary for correlations: Discord and related measures,” *Rev. Mod. Phys.*, vol. 84, pp. 1655–1707, 2012.

[105] S. Pirandola, “Quantum discord as a resource for quantum cryptography,” *Scientific Reports*, vol. 4, pp. 6956 EP –, 11 2014.

[106] M. Takeoka, S. Guha, and M. M. Wilde, “Fundamental rate-loss tradeoff for optical quantum key distribution,” *Nature Communications*, vol. 5, pp. 5235 EP –, 2014.

[107] N. Hosseinidehaj and R. Malaney, "Gaussian entanglement distribution via satellite," *Phys. Rev. A*, vol. 91, p. 022304, 2015.

[108] G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental satellite quantum communications," *Phys. Rev. Lett.*, vol. 115, p. 040502, 2015.

[109] D. Dequal, G. Vallone, D. Bacco, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental single-photon exchange along a space link of 7000 km," *Phys. Rev. A*, vol. 93, p. 010301, 2016.

[110] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Phys. Rev. Lett.*, vol. 93, p. 170504, 2004.

[111] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Gehring, C. S. Jacobsen, and U. L. Andersen, "High-rate measurement-device-independent quantum cryptography," *Nature Photonics*, vol. 9, pp. 397 EP –, 05 2015.

[112] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, pp. 238 EP –, 01 2003.

[113] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, "Continuous-variable quantum cryptography using two-way quantum communication," *Nature Physics*, vol. 4, pp. 726 EP –, 07 2008.

[114] C. Ottaviani and S. Pirandola, "General immunity and superadditivity of two-way gaussian quantum cryptography," *Scientific Reports*, vol. 6, pp. 22225 EP –, 03 2016.

[115] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, vol. 81, pp. 1301–1350, 2009.

[116] S. L. Braunstein and S. Pirandola, "Side-channel-free quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130502, 2012.

[117] H.-K. Lo, M. Curty, and B. Qi, "Measurement-device-independent quantum key distribution," *Phys. Rev. Lett.*, vol. 108, p. 130503, 2012.

[118] V. C. Usenko and R. Filip, "Feasibility of continuous-variable quantum key distribution with noisy coherent states," *Phys. Rev. A*, vol. 81, p. 022318, 2010.

[119] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, "Quantum cryptography approaching the classical limit," *Phys. Rev. Lett.*, vol. 105, p. 110501, 2010.

[120] C. Weedbrook, S. Pirandola, and T. C. Ralph, "Continuous-variable quantum key distribution using thermal states," *Phys. Rev. A*, vol. 86, p. 022318, 2012.

[121] C. Weedbrook, C. Ottaviani, and S. Pirandola, "Two-way quantum cryptography at different wavelengths," *Phys. Rev. A*, vol. 89, p. 012309, 2014.

[122] M. M. Wolf, D. Pérez-García, and G. Giedke, "Quantum capacities of bosonic channels," *Phys. Rev. Lett.*, vol. 98, p. 130501, 2007.

[123] P. Liuzzo-Scorpo and G. Adesso, "Optimal secure quantum teleportation of coherent states of light," *Proc. SPIE 10358, Quantum Photonic Devices*, vol. 103580V, 2017.

[124] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, and G. Adesso, "Erratum: Optimal continuous variable quantum teleportation with limited resources [phys. rev. lett. 119, 120503 (2017)]," *Phys. Rev. Lett.*, vol. 120, p. 029904, 2018.

[125] J. D. S. Tserkis and T. C. Ralph, "Simulation of gaussian channels via teleportation and error correction of gaussian states," *arXiv:1803.03516*, 2018.

[126] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, "Unconditional quantum teleportation," *Science*, vol. 282, no. 5389, pp. 706–709, 1998.

[127] S. Pirandola and S. Mancini, "Quantum teleportation with continuous variables: A survey," *Laser Physics*, vol. 16, no. 10, pp. 1418–1438, 2006.

[128] J. Fiurášek, "Improving the fidelity of continuous-variable teleportation via local operations," *Phys. Rev. A*, vol. 66, p. 012304, Jul 2002.

[129] M. B. Plenio, "Logarithmic negativity: A full entanglement monotone that is not convex," *Phys. Rev. Lett.*, vol. 95, p. 090503, 2005.

[130] A. Mari, *Private communications.*

[131] S. Guha, J. H. Shapiro, and B. I. Erkmen, "Classical capacity of bosonic broadcast communication and a minimum output entropy conjecture," *Phys. Rev. A*, vol. 76, p. 032303, 2007.

[132] F. Dupuis, P. Hayden, and K. Li, "A father protocol for quantum broadcast channels," *IEEE Transactions on Information Theory*, vol. 56, no. 6, pp. 2946–2956, 2010.

[133] J. Yard, P. Hayden, and I. Devetak, "Quantum broadcast channels," *IEEE Transactions on Information Theory*, vol. 57, no. 10, pp. 7147–7162, 2011.

[134] J. Yard, P. Hayden, and I. Devetak, "Capacity theorems for quantum multiple-access channels: classical-quantum and quantum-quantum capacity regions," *IEEE Transactions on Information Theory*, vol. 54, pp. 3091–3113, July 2008.

[135] J. Majer, J. M. Chow, J. M. Gambetta, J. Koch, B. R. Johnson, J. A. Schreier, L. Frunzio, D. I. Schuster, A. A. Houck, A. Wallraff, A. Blais, M. H. Devoret, S. M. Girvin, and R. J. Schoelkopf, "Coupling superconducting qubits via a cavity bus," *Nature*, vol. 449, pp. 443 EP –, 2007.

[136] G. K. Brennen, D. Song, and C. J. Williams, "Quantum-computer architecture using nonlocal interactions," *Phys. Rev. A*, vol. 67, p. 050302, 2003.

[137] M. Takeoka, K. P. Seshadreesan, and M. M. Wilde, "Unconstrained distillation capacities of a pure-loss bosonic broadcast channel," in *2016 IEEE International Symposium on Information Theory (ISIT)*, pp. 2484–2488, July 2016.

[138] V. Giovannetti, S. Lloyd, and L. Maccone, "Advances in quantum metrology," *Nature Photonics*, vol. 5, pp. 222 EP –, 2011.

[139] S. L. Braunstein and C. M. Caves, "Statistical distance and the geometry of quantum states," *Phys. Rev. Lett.*, vol. 72, pp. 3439–3443, 1994.

[140] M. G. A. Paris, "Quantum estimation for quantum technology," vol. 7, 2008.

[141] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, "Parameter estimation of quantum channels," *IEEE Transactions on Information Theory*, vol. 54, no. 11, pp. 5172–5185, 2008.

[142] R. Demkowicz-Dobrzański and L. Maccone, “Using entanglement against noise in quantum metrology,” *Phys. Rev. Lett.*, vol. 113, p. 250801, 2014.

[143] A. Acín, “Statistical distinguishability between unitary operations,” *Phys. Rev. Lett.*, vol. 87, p. 177901, 2001.

[144] M. F. Sacchi, “Entanglement can enhance the distinguishability of entanglement-breaking channels,” *Phys. Rev. A*, vol. 72, p. 014305, 2005.

[145] G. Wang and M. Ying, “Unambiguous discrimination among quantum operations,” *Phys. Rev. A*, vol. 73, p. 042301, 2006.

[146] A. M. Childs, J. Preskill, and J. Renes, “Quantum information and precision measurement,” *Journal of Modern Optics*, vol. 47, no. 2-3, pp. 155–176, 2000.

[147] C. Invernizzi, M. G. A. Paris, and S. Pirandola, “Optimal detection of losses by thermal probes,” *Phys. Rev. A*, vol. 84, p. 022334, 2011.

[148] M. Hayashi, “Discrimination of two channels by adaptive methods and its application to quantum system,” *IEEE Transactions on Information Theory*, vol. 55, pp. 3807–3820, Aug 2009.

[149] A. W. Harrow, A. Hassidim, D. W. Leung, and J. Watrous, “Adaptive versus non-adaptive strategies for quantum channel discrimination,” *Phys. Rev. A*, vol. 81, p. 032339, Mar 2010.

[150] Z.-W. Wang and S. L. Braunstein, “Higher-dimensional performance of port-based teleportation,” *Scientific Reports*, vol. 6, pp. 33004 EP –, 09 2016.

[151] S. Beigi and R. König, “Simplified instantaneous non-local quantum computation with applications to position-based cryptography,” *New Journal of Physics*, vol. 13, no. 9, p. 093036, 2011.

[152] S. Strelchuk, M. Horodecki, and J. Oppenheim, “Generalized teleportation and entanglement recycling,” *Phys. Rev. Lett.*, vol. 110, p. 010505, 2013.

[153] M. Studziński, S. Strelchuk, M. Mozrzymas, and M. Horodecki, “Port-based teleportation in arbitrary dimension,” *Scientific Reports*, vol. 7, no. 1, p. 10871, 2017.

[154] M. Mozrzymas, M. Studziński, S. Strelchuk, and M. Horodecki, “Optimal port-based teleportation,” *New Journal of Physics*, vol. 20, no. 5, p. 053006, 2018.

[155] S. Lloyd, "Enhanced sensitivity of photodetection via quantum illumination," *Science*, vol. 321, no. 5895, pp. 1463–1465, 2008.

[156] Z. Zhang, S. Mouradian, F. N. C. Wong, and J. H. Shapiro, "Entanglement-enhanced sensing in a lossy and noisy environment," *Phys. Rev. Lett.*, vol. 114, p. 110506, 2015.

[157] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, "Microwave quantum illumination," *Phys. Rev. Lett.*, vol. 114, p. 080503, 2015.

[158] C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, and M. Gu, "How discord underlies the noise resilience of quantum illumination," *New Journal of Physics*, vol. 18, no. 4, p. 043027, 2016.

[159] G. De Palma and J. Borregaard, "Minimum error probability of quantum illumination," *Phys. Rev. A*, vol. 98, p. 012101, 2018.

[160] C. Majenz, *Entropy in Quantum Information Theory - Communication and Cryptography.* PhD thesis, University of Copenhagen, 2017.

[161] J. Doukas, G. Adesso, S. Pirandola, and A. Dragan, "Discriminating quantum field theories in non-inertial frames," *Classical and Quantum Gravity*, vol. 32, no. 3, p. 035013, 2015.

[162] M. C. Selwyn, *The Structure of Bipartite Quantum States Insights from Group Theory and Cryptography This dissertation is submitted for the degree of Doctor of Philosophy.* PhD thesis, 2006.

[163] E. Kaur and M. M. Wilde, "Amortized entanglement of a quantum channel and approximately teleportation-simulable channels," *Journal of Physics A: Mathematical and Theoretical*, vol. 51, no. 3, p. 035303, 2018.

[164] C. Bloch and A. Messiah, "The canonical form of an antisymmetric tensor and its application to the theory of superconductivity," vol. 39, pp. 95–106, 1962.

[165] S. L. Braunstein, "Squeezing as an irreducible resource," *Phys. Rev. A*, vol. 71, p. 055801, 2005.

[166] B. Synak-Radtke, K. Horodecki, and M. Horodecki, "Bounds on localizable information via semidefinite programming," *Journal of Mathematical Physics*, vol. 46, no. 8, p. 082107, 2005.

[167] S. Pirandola, S. Mancini, S. L. Braunstein, and D. Vitali, “Minimal qudit code for a qubit in the phase-damping channel,” *Phys. Rev. A*, vol. 77, p. 032309, Mar 2008.

[168] M. Takeoka, S. Guha, and M. M. Wilde, “The squashed entanglement of a quantum channel,” *IEEE Transactions on Information Theory*, vol. 60, no. 8, pp. 4987–4998, 2014.

[169] X.-y. Chen, “Gaussian relative entropy of entanglement,” *Phys. Rev. A*, vol. 71, p. 062320, 2005.

[170] S. Scheel and D.-G. Welsch, “Entanglement generation and degradation by passive optical devices,” *Phys. Rev. A*, vol. 64, p. 063811, 2001.