

This is a repository copy of *Channel Simulation in Quantum Metrology*.

White Rose Research Online URL for this paper:

<https://eprints.whiterose.ac.uk/129756/>

Version: Published Version

Article:

Laurenza, Riccardo, Lupo, Cosmo orcid.org/0000-0002-5227-4009, Spedalieri, Gaetana et al. (2 more authors) (2018) Channel Simulation in Quantum Metrology. *Quantum Measurements and Quantum Metrology*. ISSN 2299-114X

<https://doi.org/10.1515/qmetro-2018-0001>

Reuse

This article is distributed under the terms of the Creative Commons Attribution (CC BY) licence. This licence allows you to distribute, remix, tweak, and build upon the work, even commercially, as long as you credit the authors for the original work. More information and the full terms of the licence here:

<https://creativecommons.org/licenses/>

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.



Review Article

Open Access

Riccardo Laurenza, Cosmo Lupo, Gaetana Spedalieri, Samuel L. Braunstein, and Stefano Pirandola*

Channel Simulation in Quantum Metrology

<https://doi.org/10.1515/qmetro-2018-0001>

Received November 20, 2017; accepted December 23, 2017

Abstract: In this review we discuss how channel simulation can be used to simplify the most general protocols of quantum parameter estimation, where unlimited entanglement and adaptive joint operations may be employed. Whenever the unknown parameter encoded in a quantum channel is completely transferred in an environmental program state simulating the channel, the optimal adaptive estimation cannot beat the standard quantum limit. In this setting, we elucidate the crucial role of quantum teleportation as a primitive operation which allows one to completely reduce adaptive protocols over suitable teleportation-covariant channels and derive matching upper and lower bounds for parameter estimation. For these channels, we may express the quantum Cramér Rao bound directly in terms of their Choi matrices. Our review considers both discrete- and continuous-variable systems, also presenting some new results for bosonic Gaussian channels using an alternative sub-optimal simulation. It is an open problem to design simulations for quantum channels that achieve the Heisenberg limit.

Keywords: quantum metrology, quantum channels

PACS: 03.67.-a, 42.50.-p, 03.65.-w

1 Introduction

Quantum technologies exploit quantum information [1–4] to develop new powerful devices that aim at solving long-standing problems as well as providing completely

novel applications. This is happening in many areas, including quantum communication [5–10], secret key distribution [11–21], sensing (e.g., quantum illumination [22–25]), imaging (e.g., optical resolution [26–28]), and metrology [29–36]. The latter area is particularly active and promising in terms of practical applications. Quantum metrology [29], also known as quantum parameter estimation, deals with the estimation of unknown classical parameters which are encoded in quantum states or quantum transformations, i.e., quantum channels [3]. Here we are interested in the latter scenario of quantum channel estimation. In this setting, we review techniques of channel simulation [37–42] that allow one to simplify the structure of the most general protocols of quantum parameter estimation to a much simpler and treatable version.

To clarify the context, let us formulate the general problem. Suppose that we are given a black-box implementing a quantum channel \mathcal{E}_θ with an unknown classical parameter θ with uniform prior. We are then asked to probe the box n times with the aim of retrieving the best value of θ . Statistically, this means to generate an estimator $\tilde{\theta}$ of θ such that its error variance $\delta\theta^2 = \langle(\tilde{\theta} - \theta)^2\rangle$ is the minimal possible (here the average is assumed over the n probings of the box). It is clear that $\delta\theta^2$, or the standard deviation $\delta\theta$, is expected to decrease as a function of n . Therefore an important crucial question to answer is the following: What is the optimal scaling in n ?

For certain channels the optimal scaling is $\delta\theta \sim n^{-1/2}$, known as the “standard quantum limit” (SQL) because it is also what you would expect with in a completely classical setting. Remarkably, this limit can be beaten for other channels, so that they display a fully quantum behaviour. In fact, it is known that the optimal scaling that is reachable in the quantum setting is $\delta\theta \sim n^{-1}$, also called the “Heisenberg limit” (HL) [34]. In order to understand if a channel \mathcal{E}_θ is limited to the SQL or not, it is essential to adopt the most general quantum protocols of parameter estimation that are allowed by quantum mechanics. These protocols involve the use of unlimited entanglement and are inevitably adaptive, i.e., may involve the use of joint quantum operations where the inputs to the box are optimised as a result of all the previous rounds [41–44]. It is clear that their study is extremely difficult and require

*Corresponding Author: **Stefano Pirandola:** Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK, E-mail: stefano.pirandola@york.ac.uk

Riccardo Laurenza, Cosmo Lupo, Samuel L. Braunstein: Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK

Gaetana Spedalieri: Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK and Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA

some techniques that may reduce their complexity. In this respect, channel simulation is certainly one of the most powerful tools.

Here we review the most important results for channel simulation in quantum metrology, plus we present some new bounds. We start with the discussion of programmable channels [37, 38], which are those channels \mathcal{E} that can be simulated by a program state $\pi_{\mathcal{E}}$ and some joint (trace-preserving) quantum operation or “simulator” \mathcal{S} applied to the input state ρ and the program $\pi_{\mathcal{E}}$, so that $\mathcal{E}(\rho) = \mathcal{S}(\rho \otimes \pi_{\mathcal{E}})$. When a parameter θ labels the channel \mathcal{E}_{θ} , it may happen that the previous simulator \mathcal{S} remains “universal”, i.e., independent on θ , while the program state completely absorbs the label, i.e., it becomes $\pi_{\mathcal{E}_{\theta}}$. If this is the case, one may re-organise an adaptive protocol in a block version and show that the SQL is an upper bound that cannot be beaten [41, 42].

Recently, Ref. [42] adopted a simple criterion to identify these channels at any dimension (finite or infinite). Whenever a quantum channel is teleportation covariant [45], i.e., suitably commuting with teleportation unitaries, it can be simulated by teleporting over its Choi matrix, i.e., the simulator \mathcal{S} is teleportation and the program state $\pi_{\mathcal{E}_{\theta}}$ is the channel’s Choi matrix [42]. Thus for these channels, we have a precise and simple design for their simulation. Furthermore, this design allows one to show that the SQL is asymptotically achievable with a prefactor which is completely determined by the Choi matrix of the channel. Thus, Ref. [42] showed that teleportation-covariance implies the SQL, elucidating how teleportation gives a *no-go* for Heisenberg scaling.

The methodology of Ref. [42] applies to quantum channels of any dimension. As we will explain, the teleportation simulation of bosonic channels [2] needs a careful treatment due to the fact that both the ideal maximally-entangled state and the ideal Bell detection require infinite energy in the setting of continuous-variable systems. Therefore, suitable limits and truncations of the Hilbert spaces need to be considered to avoid divergences [42, 45]. Besides specifying these aspects, we also exploit a different sub-optimal simulation of these channels, where asymptotic maximally-entangled states are not needed, following a recent approach [46].

The paper is structured as follows. In Sec. 2, we review strategies of quantum parameter estimation giving the main definitions. In Sec. 3 we discuss the simulation of programmable channels and their restriction to the SQL. We also discuss potential extensions of this simulation. Then, in Sec. 4, we introduce the specific teleportation design, valid for teleportation-covariant channels, and the teleportation stretching of the parameter estimation proto-

col. We extend these tools to continuous variable systems and bosonic channels in Sec. 5. Then, in Sec. 6, we present some novel bounds based on sub-optimal simulations of Gaussian channels. Finally, Sec. 7 is for conclusions.

2 Protocols of quantum parameter estimation

As already mentioned in the introduction, consider the scenario where we are given a black-box whose input-output physical transformation can be modelled as a quantum channel \mathcal{E}_{θ} encoding an unknown parameter θ with uniform prior distribution (i.e., completely random). The task is to infer θ with an optimal estimator $\tilde{\theta}$, i.e., with minimal error variance $\delta\theta^2$. It is clear that the performance will depend on the specific probing strategy which is adopted. The most basic operations to be done are: (1) Preparing a suitable input state to probe the channel; and (2) detecting the output of the channel by means of a suitable measurement or positive operator-valued measure (POVM). These elementary operations are the only ones that are exploited in block protocols of parameter estimation, which may be “direct” and “assisted”.

A direct protocol is shown in Fig. 1(top). For each of the n probeings of the channel \mathcal{E}_{θ} , we prepare the same input state σ , so that the total output is a tensor product state $\rho_{\theta}^{\otimes n} = \mathcal{E}_{\theta}(\sigma)^{\otimes n}$, which is then detected by a joint POVM. An assisted protocol is shown in Fig. 1(bottom). In each probing of the channel we use a joint state σ of the input system and an ancillary system. Therefore, the total output state has a slightly different tensor product form $\rho_{\theta}^{\otimes n} = [(\mathcal{E}_{\theta} \otimes I)(\sigma)]^{\otimes n}$. This state is then jointly measured. It is clear that an assisted protocol is a direct protocol over the extended channel $\mathcal{E}_{\theta} \otimes I$.

The most general protocol of quantum parameter estimation involves additional ingredients. Each probing of the channel may in fact be interleaved with joint quantum operations. In this way, unlimited entanglement may be distributed between input and output, and feedback may also be used to adaptively optimise the inputs of the next transmissions [41, 42]. We may think to have a quantum register prepared in some fundamental initial state σ . After a first joint operation, one system is picked from this register and transmitted through the channel. The output becomes again part of the register, which is collectively subject to another joint quantum operation. Then, there is the second probing by transmitting another system of the register through the channel and so on. After n such adaptive probeings, we have an output state ρ_{θ}^n which is subject

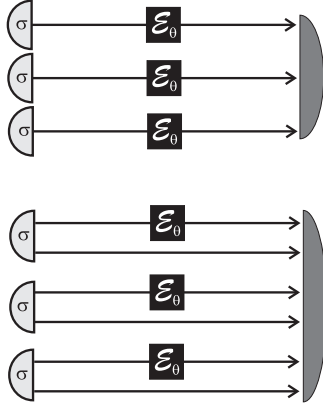


Figure 1: Block protocols for quantum parameter estimation, i.e., the direct protocol (top) and the assisted protocol (bottom). In these protocols, n instances of the quantum channel \mathcal{E}_θ are identically and independently probed with the same input state σ . The resulting output state is a tensor product which is subject to an optimal POVM, whose output is post-processed into an (unbiased) estimator $\hat{\theta}$ of θ .

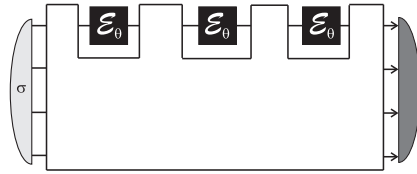


Figure 2: The most general (adaptive) estimation protocol can be represented as a quantum comb, i.e., a quantum circuit board with n slots to plug n instances of the channel \mathcal{E}_θ in. The initial state of the quantum comb is denoted as σ and the output state as ρ_θ^n . The output state is finally detected by a joint POVM whose outcome is classically post-processed to estimate θ .

to a joint POVM. Note that we may assume that the adaptive quantum operations are trace-preserving, because any non-trace preserving process can always be delayed and included in the final POVM by the principle of deferred measurement [1].

An equivalent way to present this adaptive protocol is by resorting to the model of quantum comb [47], as shown in Fig. 2. Indeed, a quantum comb represents a quantum circuit board with n slots to plug in n instances of the quantum channel. The internal structure of the quantum comb is completely generic and includes any possible quantum gate. The initial state σ of the quantum comb is transformed into an output state ρ_θ^n after the action of the comb and the channel. The final state of the comb is then detected by a joint POVM, whose outcome is processed into an estimator $\hat{\theta}$. Note that this strategy includes the previous block protocols as particular cases. It also includes the so-called “sequential” protocols [41], where a state is

transmitted through the entire sequence of n channels before detection.

Suppose that we implement an optimal adaptive protocol, i.e., we implicitly optimise over all possible quantum combs and all possible joint POVMs. The ultimate lower bound for the error variance of any unbiased estimator is the quantum Cramér-Rao bound (QCRB)

$$\delta\theta^2 \geq \frac{1}{\text{QFI}(\rho_\theta^n)}, \quad (1)$$

where QFI denotes the quantum Fisher information [29]

$$\text{QFI}(\rho_\theta^n) = \text{Tr} \left(\mathcal{L}_\theta^2 \rho_\theta^n \right), \quad (2)$$

and \mathcal{L}_θ is the symmetric logarithmic derivative (SLD).

Assuming that the output has spectral decomposition

$$\rho_\theta^n = \sum_j \lambda_j |e_j\rangle \langle e_j|, \quad (3)$$

the expression of the SLD is given by [29, 33]

$$\mathcal{L}_\theta = \sum_{j,k:\lambda_j+\lambda_k>0} \frac{2}{\lambda_j+\lambda_k} \langle e_j | \frac{d\rho_\theta^n}{d\theta} | e_k \rangle |e_j\rangle \langle e_k|. \quad (4)$$

Alternatively, we may express the QFI as [29]

$$\text{QFI}(\rho_\theta^n) = \frac{8[1 - F(\rho_\theta^n, \rho_{\theta+d\theta}^n)]}{d\theta^2}, \quad (5)$$

where $F(\rho, \sigma) := \text{Tr} \sqrt{\sqrt{\sigma} \rho \sqrt{\sigma}}$ is the quantum fidelity [48, 49], which is known to have closed analytical forms, e.g., for two arbitrary Gaussian states [50].

It is important to recall two fundamental properties of the QFI. The first one is its additivity over tensor products. Given any two parametrised states γ_θ and γ'_θ , we may write

$$\text{QFI}(\gamma_\theta \otimes \gamma'_\theta) = \text{QFI}(\gamma_\theta) + \text{QFI}(\gamma'_\theta). \quad (6)$$

The second is its monotonicity under completely-positive and trace preserving (CPTP) maps, i.e., quantum channels. Given a quantum channel Λ , we may write

$$\text{QFI}[\Lambda(\gamma_\theta)] \leq \text{QFI}(\gamma_\theta). \quad (7)$$

Note that, because the output of a block protocol (direct or assisted) is a tensor product state $\rho_\theta^{\otimes n}$ and the additivity of the QFI implies $\text{QFI}(\rho_\theta^{\otimes n}) = n\text{QFI}(\rho_\theta)$, we have that the QCRB associated with this type of protocol becomes

$$\delta\theta^2 \geq \frac{1}{n\text{QFI}(\rho_\theta)}, \quad (8)$$

so that it scales according to the SQL.

By contrast, the output ρ_θ^n of an adaptive protocol is not necessarily a product state. For this reason, the error

variance may behave differently and potentially beat the SQL. Indeed, it is known that $\delta\theta^2$ may scale according to the HL, for instance in the estimation of the phase in a unitary transformation [34]. However, the possibility to express the output state ρ_θ^n as a quantum channel applied to a tensor product, i.e., $\rho_\theta^n = \Lambda(\gamma_\theta^{\otimes n})$, automatically reduces the performance of the protocol back to the SQL, because of the monotonicity and additivity of the QFI. In fact, we may write $\text{QFI}(\rho_\theta^n) \leq \text{QFI}(\gamma_\theta^{\otimes n}) = n\text{QFI}(\gamma_\theta)$. In the following section, we discuss the conditions for this reduction.

3 Programmable channels and protocol reduction

Here we discuss how the most general adaptive protocol for quantum parameter estimation (as the comb in Fig. 2) can be reduced to a block protocol when implemented over programmable channels. This implies that quantum metrology with programmable channels is bounded to the SQL.

The original idea of programmability was introduced by Nielsen and Chuang [37] in the context of quantum computation. These authors introduced a model of programmable quantum gate array (PQGA) for the simulation of an arbitrary quantum channel by using a universal unitary and a program state. Assuming finite resources (e.g., a finite number of systems for the program state), the simulation can only be probabilistic. Alternatively, an arbitrary quantum channel can be simulated if we are allowed to use an infinite number of systems (note that this is exactly the limit which needs to be taken in the equivalent formulation of port-based teleportation [51–54] if one wants to achieve perfect fidelity).

Later in 2008, Ref. [38] considered a variant of the PQGA where the simulation is deterministic but can only be applied to a subset of channels, called “programmable” channels. This tool was used in the context of quantum metrology but not immediately applied to adaptive protocols. See also Ref. [39]. It was later called “quantum simulation” in Ref. [40]. The first application to simplify adaptive protocols was presented in Ref. [41] in the context of discrete-variable channels. Later, Ref. [42] considered programmable channels in the context of both discrete- and continuous-variable channels, also identifying the crucial connection with quantum teleportation that we will describe later.

A quantum channel \mathcal{E} is called programmable if there is a “simulator” \mathcal{S} (another quantum channel) and a pro-

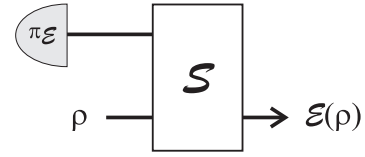


Figure 3: A programmable channel admits a simulation of the form $\mathcal{E}(\rho) = \mathcal{S}(\rho \otimes \pi_{\mathcal{E}})$ where \mathcal{S} is a simulation channel and $\pi_{\mathcal{E}}$ a program state. Channels are co-programmable when they have the same \mathcal{S} , but generally different program states.

gram state $\pi_{\mathcal{E}}$, such that

$$\mathcal{E}(\rho) = \mathcal{S}(\rho \otimes \pi_{\mathcal{E}}). \quad (9)$$

This is also shown in Fig. 3. Without loss of generality, the channel simulator can always be dilated into a unitary U up to introducing extra degrees of freedom in the program state. Then we also say that an ensemble of channels Ω is “co-programmable” if the simulator \mathcal{S} is universal over Ω . In other words, for any $\mathcal{E} \in \Omega$, we may write Eq. (9) with exactly the same \mathcal{S} but generally-different program states $\pi_{\mathcal{E}}$.

Let us now apply these notions to parameter estimation. Assume that the parametrised quantum channel \mathcal{E}_θ spans a family of co-programmable channels, so that we may write the simulation

$$\mathcal{E}_\theta(\rho) = \mathcal{S}(\rho \otimes \pi_{\mathcal{E}_\theta}), \quad \text{for any } \theta. \quad (10)$$

We can then simplify any adaptive protocol over n uses of this channel. In fact, we may replace each instance of the channel with its simulation of Fig. 3, so that the quantum comb in Fig. 2 can be re-organised in the form depicted in Fig. 4. The idea is to replace each use of the channel \mathcal{E}_θ with its program state $\pi_{\mathcal{E}_\theta}$, and then to “stretch” all the program states back in time, while collapsing the simulators \mathcal{S} and the quantum comb (including its initial state σ) into a single quantum channel Λ . In this way, the output of the comb can be decomposed as

$$\rho_\theta^n = \Lambda(\pi_{\mathcal{E}_\theta}^{\otimes n}). \quad (11)$$

Note that the latter decomposition reduces the adaptive protocol into a block protocol up to an overall quantum channel Λ . Because of the properties of the QFI, we know that this is sufficient to restrict the performance of the protocol to the SQL. In fact, using monotonicity and additivity of the QFI, we may write

$$\text{QFI}(\rho_\theta^n) = \text{QFI}[\Lambda(\pi_{\mathcal{E}_\theta}^{\otimes n})] \leq \text{QFI}(\pi_{\mathcal{E}_\theta}^{\otimes n}) = n\text{QFI}(\pi_{\mathcal{E}_\theta}). \quad (12)$$

We have thus obtained that for the estimation of a parameter θ encoded in a programmable channel \mathcal{E}_θ , the QCRB

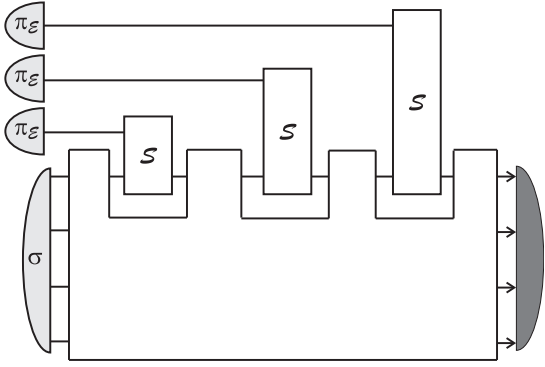


Figure 4: Stretching of a quantum comb. First, suppose we have a quantum comb whose slots are filled by a programmable channel \mathcal{E} . Using the simulation of Fig. 3, we may replace n instances of the quantum channel \mathcal{E} with a collection of n programme states $\pi_{\mathcal{E}}$. The corresponding simulators S can be included in the operations of the quantum comb. In this way, we may collapse the quantum comb (including its initial state σ) and the simulators into a single quantum channel Λ applied to the programme states, so that the output of the comb ρ^n can be decomposed as $\Lambda(\pi_{\mathcal{E}}^{\otimes n})$. In the setting of adaptive parameter estimation, the slots of the comb are filled by a quantum channel \mathcal{E}_θ encoding the unknown classical parameter θ . Assuming that \mathcal{E}_θ spans a family of co-programmable channels, then we may repeat the procedure, and decompose the output state ρ_θ^n as $\Lambda(\pi_{\mathcal{E}_\theta}^{\otimes n})$.

must satisfy the condition $\delta\theta^2 \geq [n\text{QFI}(\pi_{\mathcal{E}_\theta})]^{-1}$. Furthermore, note that this bound is not necessarily achievable. It would be achievable if the program state $\pi_{\mathcal{E}_\theta}$ could be generated by sending some input state through the channel. For instance, this would be the case if $\pi_{\mathcal{E}_\theta}$ were the Choi matrix of the channel, an extra property which is guaranteed if the channel is teleportation-covariant, as explained in the next section.

Before proceeding, we may ask how the channel simulation should be modified in order to cover channels that beat the SQL. One potential idea is to weaken the notion of co-programmability to involve multi-copy program states. For instance, suppose that a quantum channel \mathcal{E}_θ cannot be simulated as in Eq. (10) but as

$$\mathcal{E}_\theta(\rho) = \mathcal{S}(\rho \otimes \pi_{\mathcal{E}_\theta}^{\otimes m}), \quad \text{for any } \theta \text{ and some } m. \quad (13)$$

This leads to the stretching $\rho_\theta^n = \Lambda(\pi_{\mathcal{E}_\theta}^{\otimes mn})$ and therefore to

$$\text{QFI}(\rho_\theta^n) \leq mn\text{QFI}(\pi_{\mathcal{E}_\theta}). \quad (14)$$

We know that the HL $\delta\theta^2 \gtrsim n^{-2}$ cannot be beaten so that we must have $m \leq n$. To get the HL it is sufficient that the condition in Eq. (13) holds asymptotically, i.e., in trace norm limit $\delta_m := \|\mathcal{E}_\theta(\rho) - \mathcal{S}(\rho \otimes \pi_{\mathcal{E}_\theta}^{\otimes m})\| \xrightarrow{m} 0$. Then we may take this limit jointly with the limit in n for the scaling.

4 Teleportation simulation

Teleportation simulation has been used in the past to reduce protocols of quantum communication into entanglement distillation [55–58] and, more recently, to completely simplify protocols of private communication from adaptive to block forms [45], establishing the ultimate limits of QKD in point-to-point lossy communications [45] and also multi-point [59] and repeater-assisted scenarios [60]. More recently, Ref. [42] extended the technique to quantum metrology and quantum channel discrimination.

Let us start with discrete-variable systems and, in particular, qubits (arguments can be easily generalised to any finite dimension). We first recall the basic ingredients of teleportation and then we discuss how these can be modified to implement a tool of channel simulation. The standard qubit teleportation protocol [5, 61] can be broken down in three steps:

- (1) **Resource.** A maximally-entangled state $|\Phi_+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ is prepared for qubits A (Alice) and B (Bob).
- (2) **Bell detection.** Alice performs a Bell detection on qubit A and an input qubit a (in an arbitrary state ρ). Recall that the Bell detection has four outcomes $\alpha \in \{0, 1, 2, 3\}$ with POVM elements $|\Phi_\alpha\rangle\langle\Phi_\alpha|$ where $|\Phi_\alpha\rangle = (I \otimes \sigma_\alpha)|\Phi_+\rangle$ and σ_α are the four Pauli unitaries [1]

$$\begin{aligned} \sigma_0 = I &:= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_1 = X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (15) \\ \sigma_2 = Y &:= \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}, \quad \sigma_3 = Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \end{aligned} \quad (16)$$

- (3) **Pauli corrections.** Finally, depending on the output of the Bell measurement α , the conditional Pauli unitary σ_α^{-1} is applied on the qubit B , retrieving the input state ρ .

The standard teleportation protocol simulates the identity channel. A modification of the protocol is to employ a resource state which is not maximally-entangled but an arbitrary bipartite state. In this way teleportation implements not the identity but simulates a noisy channel from the input qubit a to the output qubit B . Suppose that we choose the resource state to be the Choi matrix of a quantum channel \mathcal{E} , i.e.,

$$\xi_{\mathcal{E}} = (\mathcal{E} \otimes I)(\Phi_+). \quad (17)$$

By teleporting over this state can we simulate channel \mathcal{E} ?

The answer is *yes* for so-called teleportation-covariant channels [45, 57, 58]. By definition a quantum channel \mathcal{E}

is teleportation-covariant if, for any random teleportation unitary U (corresponding to a Pauli operator in the qubit case), we may write

$$\mathcal{E}(U\rho U^\dagger) = V\mathcal{E}(\rho)V^\dagger, \quad (18)$$

for some other unitary V [45]. This property is a sufficient condition to ensure that the channel \mathcal{E} can be simulated by teleporting over its Choi matrix or Choi-Jamiolkowski (CJ) state $\xi_{\mathcal{E}}^{\text{CJ}}$ (this is also known as teleportation-simulable or Choi-stretchable channel [45]). In other words, we may write the simulation [42, 45]

$$\mathcal{E}(\rho) = \mathcal{T}(\rho \otimes \xi_{\mathcal{E}}^{\text{CJ}}), \quad (19)$$

where \mathcal{T} is teleportation. See Fig. 5 for a visual proof of Eq. (19). This is clearly a powerful design but only holds for the teleportation-covariant subset of programmable channels.

In the setting of quantum parameter estimation, we are interested in joint teleportation-covariance, where a parametrised quantum channel \mathcal{E}_θ satisfies Eq. (18) with a θ -independent set of output unitaries, i.e., [42]

$$\mathcal{E}_\theta(U\rho U^\dagger) = V\mathcal{E}_\theta(\rho)V^\dagger, \quad \text{for any } \theta. \quad (20)$$

This is exactly the situation when θ is a noise parameter, i.e., a parameter that can be uniquely associated to an environment dilating the quantum channel.

If Eq. (20) holds, then we can write $\mathcal{E}_\theta(\rho) = \mathcal{T}(\rho \otimes \xi_{\mathcal{E}_\theta}^{\text{CJ}})$ and repeat the stretching of a quantum comb as before. In this way, we may decompose the output state of an adaptive parameter estimation protocol as [42]

$$\rho_\theta^n = \Lambda \left[(\xi_{\mathcal{E}_\theta}^{\text{CJ}})^{\otimes n} \right], \quad (21)$$

for some quantum channel Λ . As a result, we get

$$\text{QFI}(\rho_\theta^n) \leq n\text{QFI}(\xi_{\mathcal{E}_\theta}^{\text{CJ}}). \quad (22)$$

This means that the estimation of a noise parameter of a teleportation-covariant channel is limited to the SQL with a pre-factor given by its Choi matrix, i.e., the QCRB reads [42]

$$\delta\theta^2 \geq [n\text{QFI}(\xi_{\mathcal{E}_\theta}^{\text{CJ}})]^{-1}. \quad (23)$$

The teleportation simulation not only allows us to compute explicitly the upper bound, but also yields a matching lower bound. As a matter of fact, an optimal strategy that saturates the bound employs a block (assisted) estimation protocol where the maximally-entangled state Φ_+ is used at the input of the channel in an identical and independent way. This strategy provides a QFI exactly equal to $n\text{QFI}(\xi_{\mathcal{E}_\theta}^{\text{CJ}})$. As a result, the QCRB in Eq. (23) is asymptotically achievable for large n .

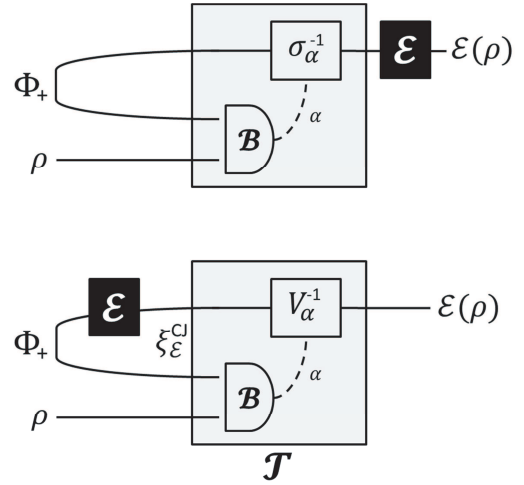


Figure 5: (Top) Consider a qubit teleportation protocol where an input state ρ is teleported to the input of a quantum channel \mathcal{E} . This is achieved by applying a Bell detection \mathcal{B} to the input ρ and a maximally-entangled state Φ_+ , followed by the classical communication of the outcome α which triggers a conditional Pauli correction σ_α^{-1} . (Bottom) Assume that \mathcal{E} is teleportation covariant as in Eq. (18). The Pauli corrections can be pushed at the output of the channel where they become generally-different unitary corrections V_α^{-1} (depending on the channel these may again be Pauli operators or not). Now the application of the channel \mathcal{E} on Φ_+ creates the Choi matrix $\xi_{\mathcal{E}}^{\text{CJ}} = (\mathcal{E} \otimes I)(\Phi_+)$ as a resource state for the next teleportation protocol \mathcal{T} . As a result the channel \mathcal{E} is simulated by teleporting over its Choi matrix as in Eq. (19). We also say that a teleportation-covariant channel \mathcal{E} is a Choi-stretchable channel [45].

Let us compute the QCRB for specific examples. It is known that erasure, dephasing and depolarizing channels are teleportation-covariant [45]. More precisely, these channels satisfy the condition of joint teleportation covariance of Eq. (20) with θ being their channel-defining probability parameter p . Recall that an erasure channel is represented by [1]

$$\mathcal{E}_p^{\text{erase}}(\rho) = (1-p)\rho + p|e\rangle\langle e|, \quad (24)$$

where $|e\rangle$ is an orthogonal erasure state and p is the erasure probability. A dephasing channel is defined as [1]

$$\mathcal{E}_p^{\text{phase}}(\rho) = (1-p)\rho + pZ\rho Z^\dagger, \quad (25)$$

where p is the probability of phase flip. Finally, a depolarizing channel with probability p is defined as [1]

$$\mathcal{E}_p^{\text{depol}}(\rho) = (1-p)\rho + p\pi, \quad (26)$$

where π is the maximally-mixed state.

For each family of these channels \mathcal{E}_p (i.e., erasure, dephasing or depolarizing), we compute the Choi matrix $\xi_{\mathcal{E}_p}^{\text{CJ}}$ and the associated QFI, finding $\text{QFI}(\xi_{\mathcal{E}_p}^{\text{CJ}}) = [p(1-p)]^{-1}$

for each of the families. Then, using Eq. (23), we find that the adaptive estimation of p is bounded by the following asymptotically-achievable QCRB [42]

$$\delta p^2 \geq p(1-p)n^{-1}. \quad (27)$$

5 Extension to continuous variables

5.1 Teleportation simulation of bosonic channels

In this section we consider bosonic channels and their teleportation simulation. We start by reviewing the teleportation of bosonic states *à la* Vaidman [6] and then *à la* Braunstein and Kimble [7]. We then discuss how the latter protocol can be modified to simulate bosonic channels and, in particular, bosonic Gaussian channels [42, 45, 62, 63]. The optimal simulation of bosonic channels is asymptotic and requires a careful treatment of the simulation error by introducing a suitable energy-bounded diamond norm. We therefore follow the formalism developed in Refs. [42, 45] which rigorously accounts for these aspects (see also Ref. [64]).

Consider a bosonic mode with quadrature operators \hat{q}, \hat{p} satisfying the commutation relation $[\hat{q}, \hat{p}] = i$ (we put $\hbar = 1$). A bosonic channel is a CPTP map between an input and an output mode. Vaidman's teleportation protocol [6] considers an ideal (infinite-energy) EPR state Φ_{EPR} of modes A (Alice) and B (Bob). An input mode a , prepared in some finite-energy state ρ , is then mixed in a balanced beam-splitter with mode A and the two output modes “ \pm ” are homodyned with outcomes q_- and p_+ . This detection realises the ideal continuous-variable Bell detection \mathcal{B} (which projects on displaced EPR states). The complex variable $\alpha = q_- + ip_+$ is then sent to Bob, who applies a displacement [2] $D(-\alpha)$ on his mode B , thus retrieving the input state ρ .

The Braunstein-Kimble protocol [7] removes the singularities from the previous description, therefore allowing for a realistic and practical implementation of the idea [65]. The main point is to use a two-mode squeezed vacuum (TMSV) state Φ_μ as resource for teleportation. This is a two-mode Gaussian state [2] with zero mean and μ -dependent covariance matrix. Its parameter μ quantifies both the amount of two-mode squeezing (or entanglement) between modes A and B , and the variance of the thermal noise in each individual mode. The ideal EPR state can be defined by taking the limit for infinite squeezing,

i.e., we may define the asymptotic state $\Phi_{\text{EPR}} := \lim_\mu \Phi_\mu$ in terms of a diverging sequence of TMSV states. Similarly, the same relaxation can be done for the Bell detection. One may consider a sequence of Gaussian POVMs [2] \mathcal{B}_μ which are (quasi-)projections on displaced TMSV states $\Phi_{\mu,\alpha} := D(\alpha)\Phi_\mu D(-\alpha)$. The ideal case is obtained by taking the limit of $\mu \rightarrow \infty$, i.e., the ideal Bell detection is formally defined as $\mathcal{B} := \lim_\mu \mathcal{B}_\mu$.

It is clear that, using a realistic Braunstein-Kimble protocol with finite squeezing μ (for both resource and Bell detection), we cannot achieve perfect teleportation fidelity. However, we may asymptotically approximate perfect teleportation for large values of μ for any energy-bounded alphabet at the input [7, 66]. In other words, consider the compact set of energy-constrained single-mode bosonic states $\mathcal{D}_N^1 := \{\rho : \text{Tr}(\rho \hat{N}) \leq N\}$ where \hat{N} is the photon number operator. For any input $\rho \in \mathcal{D}_N^1$, we write the output of the Braunstein-Kimble μ -protocol \mathcal{T}_μ as $\rho_\mu := \mathcal{E}_\mu^{\text{BK}}(\rho)$, where $\mathcal{E}_\mu^{\text{BK}}$ is an associated teleportation channel. In the limit of large μ , one has

$$\|\rho_\mu - \rho\| \xrightarrow{\mu} 0, \quad (28)$$

for any finite N . This result may be extended to the presence of an ancillary system and mapped into a corresponding convergence in energy-bounded diamond distance.

Let us define the set of energy-constrained bipartite states

$$\mathcal{D}_N := \{\rho_{ra} : \text{Tr}(\hat{N}_{ra}\rho_{ra}) \leq N\}, \quad (29)$$

where r is an arbitrary ancillary multi-mode system and \hat{N}_{ra} is the total number operator. One can check that \mathcal{D}_N is a compact set [67]. Then, for two bosonic channels, \mathcal{E}_1 and \mathcal{E}_2 , we may define the energy-bounded diamond distance as [42, 45]

$$\|\mathcal{E}_1 - \mathcal{E}_2\|_{\diamond N} := \sup_{\rho_{ra} \in \mathcal{D}_N} \|\mathcal{J}_r \otimes \mathcal{E}_1(\rho_{ra}) - \mathcal{J}_r \otimes \mathcal{E}_2(\rho_{ra})\|. \quad (30)$$

(See Ref. [68] for a slightly different definition of energy-constrained diamond norm). For any energy constraint N , consider the distance between the Braunstein-Kimble channel $\mathcal{E}_\mu^{\text{BK}}$ and the identity channel \mathcal{J} associated with perfect teleportation (*à la* Vaidman). From the point-wise trace-norm limit in Eq. (28) and the compactness of \mathcal{D}_N , we derive the vanishing simulation error

$$\delta(\mu, N) := \left\| \mathcal{E}_\mu^{\text{BK}} - \mathcal{J} \right\|_{\diamond N} \xrightarrow{\mu} 0, \quad \text{for any finite } N. \quad (31)$$

Here it is important to remark that the latter convergence to zero is not guaranteed if we consider unconstrained alphabets, i.e., we remove $N < +\infty$. It is in fact easy to construct a sequence of input states with diverging energy N such that the joint limit of the error simulation $\delta(\mu, N)$ in N and

μ is not defined. For this counter-example see discussions in Ref. [64].

Consider now a teleportation-covariant bosonic channel. This means that the channel must satisfy the property [45]

$$\mathcal{E}[D(\alpha)\rho D(-\alpha)] = D(\tilde{\alpha})\mathcal{E}(\rho)D(-\tilde{\alpha}) \quad (32)$$

where the output amplitudes $\tilde{\alpha}$ are functions of the input ones α . This is certainly the case for single-mode Gaussian channels [2]. Because of this property, we may write the continuous-variable version of the simulation in Eq. (19). In fact, by simulating \mathcal{E} with a finite-squeezing Braunstein-Kimble protocol \mathcal{T}_μ , we generate the approximated channel

$$\mathcal{E}_\mu(\rho) = \mathcal{T}_\mu(\rho \otimes \xi_\mathcal{E}^\mu), \quad (33)$$

where \mathcal{T}_μ is based on a finite-squeezing Bell detection \mathcal{B}_μ and $\xi_\mathcal{E}^\mu$ is generated by a TMSV state Φ_μ as

$$\xi_\mathcal{E}^\mu := (\mathcal{E} \otimes I)(\Phi_\mu). \quad (34)$$

The latter defines the asymptotic Choi matrix in the limit $\xi_\mathcal{E}^{\text{CJ}} := \lim_\mu \xi_\mathcal{E}^\mu$. Note that we may write the composition $\mathcal{E}_\mu = \mathcal{E} \circ \mathcal{E}_\mu^{\text{BK}}$. Therefore, for any bounded alphabet with energy N , we have the channel simulation error [42, 45]

$$\|\mathcal{E}_\mu - \mathcal{E}\|_{\diamond N} \leq \|\mathcal{E}_\mu^{\text{BK}} - \mathcal{J}\|_{\diamond N} := \delta(\mu, N). \quad (35)$$

5.2 Teleportation stretching of a comb in continuous variables

Assume now that the quantum channel \mathcal{E} fills n slots of a quantum comb with output ρ^n . Then, assume to replace \mathcal{E} with its imperfect simulation \mathcal{E}_μ so that the output is ρ_μ^n . We may bound the simulation error on the output state $\|\rho_\mu^n - \rho^n\|$ in terms of the channel simulation error. In fact, by adopting a peeling argument [42, 45] based on basic properties of the trace distance (i.e., its monotonicity under CPTP maps and the triangle inequality), we may write [45]

$$\|\rho_\mu^n - \rho^n\| \leq n \|\mathcal{E}_\mu - \mathcal{E}\|_{\diamond N} \leq n\delta(\mu, N). \quad (36)$$

Then, we also observe that we may stretch the approximated channel \mathcal{E}_μ by using the teleportation simulation of Eq. (33). Therefore, for the simulated output we may write the decomposition [45]

$$\rho_\mu^n = \Lambda_\mu \left[(\xi_\mathcal{E}^\mu)^{\otimes n} \right], \quad (37)$$

where Λ_μ is a global quantum channel associated with the quantum comb and also the teleportation protocol \mathcal{T}_μ .

Thus, combining Eqs. (36) and (37), we may write [45]

$$\left\| \rho^n - \Lambda_\mu(\xi_\mathcal{E}^{\mu \otimes n}) \right\| \leq n\delta(\mu, N), \quad (38)$$

which goes to zero for large μ and finite N (and n). The latter Eq. (38) represents the rigorous stretching of an adaptive protocol (quantum comb) performed over a teleportation-covariant bosonic channel.

As discussed in Ref. [64] in relation to the use of channel simulation in quantum/private communications, other approaches that neglect the energy constraint on the input alphabet and do not explicitly describe the propagation of the simulation error from the channels to the output state may be affected by technical issues and divergences in the results.

5.3 Teleportation stretching of adaptive metrology in continuous variables

To apply the methodology to adaptive parameter estimation, we need joint teleportation covariance for the family of channels \mathcal{E}_θ 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]

$$\left\| \rho_\theta^n - \Lambda_\mu(\xi_{\mathcal{E}_\theta}^{\mu \otimes n}) \right\| \leq n\delta(\mu, N), \quad (39)$$

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, we may write

$$\text{QFI}(\rho_\theta^n) = \frac{4d_B^2(\rho_\theta^n, \rho_{\theta+d\theta}^n)}{d\theta^2}, \quad (40)$$

where

$$\begin{aligned} d_B(\rho, \sigma) &:= \sqrt{2[1 - F(\rho, \sigma)]} \\ &\leq \sqrt{2D(\rho, \sigma)} = \sqrt{\|\rho - \sigma\|}. \end{aligned} \quad (41)$$

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]

$$d_B(\rho_\theta^n, \rho_{\theta+d\theta}^n) \leq \sqrt{2[1 - (F_\theta^\mu)^n] + 2\sqrt{n\delta(\mu, N)}}, \quad (42)$$

where $F_\theta^\mu := F(\xi_{\mathcal{E}_\theta}^\mu, \xi_{\mathcal{E}_{\theta+d\theta}}^\mu)$. For any finite n and N , we may take the limit for large μ and write

$$d_B(\rho_\theta^n, \rho_{\theta+d\theta}^n) \leq \lim_\mu \sqrt{2[1 - (F_\theta^\mu)^n]} = \sqrt{2[1 - (F_\theta^\infty)^n]}, \quad (43)$$

where $F_\theta^\infty := \lim_\mu F_\theta^\mu$. In other words, we have

$$\text{QFI}(\rho_\theta^n) \leq \frac{8[1 - (F_\theta^\infty)^n]}{d\theta^2}. \quad (44)$$

It is easy to check [42] that the upper bound is additive, so that

$$\text{QFI}(\rho_\theta^n) \leq n \frac{8[1 - F_\theta^\infty]}{d\theta^2} := n\text{QFI}_\theta^\infty. \quad (45)$$

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 $\xi_{\mathcal{E}_\theta}^{\mu \otimes n}$. By making an optimal measurement, we achieve

$$\text{QFI}(\xi_{\mathcal{E}_\theta}^{\mu \otimes n}) = n \frac{8[1 - F_\theta^\mu]}{d\theta^2}, \quad (46)$$

whose limit for large μ coincides with the upper bound in Eq. (45). Because, this protocol uses independent probing states, the QCRB is achievable for large n .

In conclusion, Eq. (45) 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}_θ (so that the family is jointly tele-covariant) is limited to the SQL. In fact, it satisfies the asymptotically achievable QCRB [42]

$$\delta\theta^2 \geq (n\text{QFI}_\theta^\infty)^{-1}, \quad (47)$$

where QFI_θ^∞ is related to the asymptotic Choi matrix of the channel $\xi_{\mathcal{E}_\theta}^{\text{CJ}}$ according to the limit in Eq. (45).

5.4 Results for bosonic Gaussian channels

Consider a single bosonic mode with quadrature operators $\hat{\mathbf{x}} = (\hat{q}, \hat{p})^T$. A Gaussian state is completely characterised by its mean value $\bar{\mathbf{x}}$ and covariance matrix (CM) \mathbf{V} [2]. A single-mode Gaussian channel transforms these statistical moments as follows

$$\bar{\mathbf{x}} \rightarrow \mathbf{T}\bar{\mathbf{x}} + \mathbf{d}, \quad \mathbf{V} \rightarrow \mathbf{T}\mathbf{V}\mathbf{T}^T + \mathbf{N}, \quad (48)$$

where \mathbf{d} is a displacement vector, \mathbf{T} and $\mathbf{N} = \mathbf{N}^T$ are 2×2 real matrices satisfying the conditions $\mathbf{N} = \mathbf{N}^T \geq 0$ and $\det \mathbf{N} \geq (\det \mathbf{T} - 1)^2/4$ [2, 69]. Phase-insensitive Gaussian channels have diagonal matrices

$$\mathbf{T} = \sqrt{\eta} \mathbf{I}, \quad \mathbf{N} = \nu \mathbf{I} \quad (49)$$

where $\eta \in \mathbb{R}$ is a transmissivity parameter (loss or amplification), while $\nu \geq 0$ represents noise [2]. Typically, they

also have $\mathbf{d} = \mathbf{0}$, i.e., they do not add displacements to the input.

One of the most important is the thermal-loss channel $\mathcal{E}_{\eta, \bar{n}}^{\text{loss}}$, which is defined by transmissivity $\eta \in [0, 1]$ and noise $\nu = (1 - \eta)(\bar{n} + 1/2)$ with thermal number \bar{n} . This channel can be realised by a beam-splitter (of transmissivity η) mixing the input with an environmental thermal mode with \bar{n} mean number of photons. It is clearly teleportation-covariant. More strongly, it is jointly teleportation-covariant in the thermal number \bar{n} . Therefore, consider the adaptive estimation of parameter $\bar{n} > 0$ (e.g., this can be related to a measurement of temperature). By using Eq. (47) one computes [42] $\text{QFI}_{\bar{n}}^\infty = [\bar{n}(\bar{n} + 1)]^{-1}$ and therefore the QCRB

$$\delta\bar{n}^2 \geq \frac{\bar{n}(\bar{n} + 1)}{n}. \quad (50)$$

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 $\mathcal{E}_{\eta, \bar{n}}^{\text{amp}}$ 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. (50). Finally, consider an additive-noise Gaussian channel $\mathcal{E}_\nu^{\text{add}}$ 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] $\text{QFI}_\nu^\infty = \nu^{-2}$ and therefore the QCRB

$$\delta\nu^2 \geq \nu^2/n. \quad (51)$$

6 Sub-optimal simulation of bosonic Gaussian channels

Here we present an alternative simulation for single-mode bosonic Gaussian channels which does not need to consider the limit of an asymptotic Choi matrix (but still requires the limit of an ideal Bell detection). Consider a two-mode Gaussian state with zero mean and generic CM

$$\mathbf{V}_{AB} = \begin{pmatrix} \mathbf{A} & \mathbf{C} \\ \mathbf{C}^T & \mathbf{B} \end{pmatrix}. \quad (52)$$

By teleporting over this Gaussian resource using a Braunstein-Kimble protocol with gain g we obtain a Gaussian teleportation channel such that [46] $\bar{\mathbf{x}} \rightarrow g\bar{\mathbf{x}}$ and

$$\mathbf{V} \rightarrow g^2\mathbf{V} + g^2\mathbf{Z}\mathbf{A}\mathbf{Z} + \mathbf{B} - g(\mathbf{Z}\mathbf{C} + \mathbf{C}^T\mathbf{Z}), \quad (53)$$

where $\mathbf{Z} = \text{diag}(1, -1)$. Therefore, a phase-insensitive Gaussian channel $\mathcal{E}_{\eta, \nu}$ with parameters η and ν [see Eqs. (48) and (49) with $\mathbf{d} = \mathbf{0}$] can be simulated by using the gain $g = \sqrt{\eta}$ and using a CM \mathbf{V}_{AB} with the choice

$$\mathbf{A} = a\mathbf{I}, \mathbf{B} = b\mathbf{I}, \mathbf{C} = c\mathbf{Z}, \quad (54)$$

so that $\nu = ag^2 - 2cg + b$ [46].

We are interested in finding a finite-energy resource state σ_ν that can simulate a phase-insensitive Gaussian channel $\mathcal{E}_{\eta, \nu}$ according to

$$\mathcal{E}_{\eta, \nu}(\rho) = \mathcal{T}_\eta(\rho \otimes \sigma_\nu), \quad (55)$$

where \mathcal{T}_η is the Braunstein-Kimble protocol with ideal Bell detection and gain $g = \sqrt{\eta}$. More precisely, we may write $\mathcal{T}_\eta = \lim_{\mu} \mathcal{T}_\mu^\eta$, where \mathcal{T}_μ^η is the Braunstein-Kimble μ -protocol with gain $g = \sqrt{\eta}$. A possible choice for σ_ν is a Gaussian state with zero mean and CM

$$\mathbf{V}(\sigma_\nu) = \begin{pmatrix} a\mathbf{I} & c\mathbf{Z} \\ c\mathbf{Z} & b\mathbf{I} \end{pmatrix}, \quad (56)$$

with the following elements

$$a = \frac{1}{2} \cosh 2r, \quad b = \frac{|1 - \eta|}{2} + \frac{\eta}{2} \cosh 2r, \quad c = \frac{\sqrt{\eta}}{2} \sinh 2r, \quad (57)$$

where

$$r = -\frac{1}{2} \ln \left[\frac{2\nu - |1 - \eta|}{2\eta} \right]. \quad (58)$$

It is worth remarking that there exist many finite-energy resource states that can simulate a given channel. A different family of resource states has been obtained in Ref. [46] to characterise the teleportation fidelity. This family of resource states has also been exploited in quantum communication [70] to derive weak converse upper bounds for the secret key capacity of phase-insensitive Gaussian channels. These bounds closely approximate the ideal and tightest bounds obtained for infinite energy [45]. In what follows we use the sub-optimal simulation of Eq. (55) with the finite-energy resource state specified by Eqs. (56)-(58). It is the first time that this finite-resource approach is used in quantum metrology.

Note that the form of the simulation in Eq. (55) is such that the noise parameter ν only appears in the resource state σ_ν or, in other words, the teleportation LOCC \mathcal{T}_η 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

$$\delta\nu^2 \geq \frac{1}{n\text{QFI}(\sigma_\nu)}. \quad (59)$$

As an example consider the additive-noise Gaussian channel $\mathcal{E}_\nu^{\text{add}}$. This channel can be simulated by exploiting a resource state σ_ν whose CM is given by Eq. (56)-(58) with $\eta = 1$ (see also Refs. [71, 72]). We may then compute the QFI from the quantum fidelity [50], and find the QCRB $\delta\nu^2 \geq \nu^2/n$. Note that this exactly coincides with the tight achievable bound of Eq. (51) 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. (59) we compute the QCRB for $\delta\bar{n}^2$. We do not find the tight achievable bound of Eq. (50) but a larger bound given by

$$\delta\bar{n}^2 \geq \bar{n}^2/n. \quad (60)$$

For comparison, in Fig. 6 we plot the QFI for the asymptotic and finite-energy resource state. It is an open problem to find a finite-energy resource that can match the asymptotic bound. Finally, one may easily check that Eq. (60) also holds for a noisy amplifier $\mathcal{E}_{\eta, \bar{n}}^{\text{amp}}$ assuming its sub-optimal simulation.

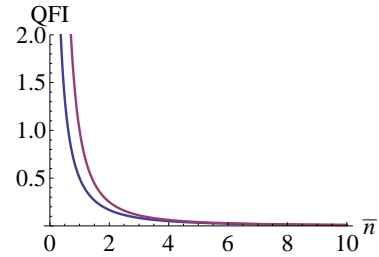


Figure 6: Quantum Fisher information $\text{QFI}(\sigma_{\bar{n}})$ associated with the adaptive estimation of the thermal number \bar{n} of a thermal-loss channel $\mathcal{E}_{\eta, \bar{n}}$. Assuming the sub-optimal simulation we find $\text{QFI}(\sigma_{\bar{n}}) = \bar{n}^{-2}$ (upper red line). Compare this with $\text{QFI}_{\bar{n}}^{\infty} = [\bar{n}(\bar{n} + 1)]^{-1}$ which is computed using the asymptotic simulation (lower blue line).

7 Conclusions

Channel simulation is a powerful tool for completely simplifying protocols of adaptive parameter estimation, for instance represented as a quantum comb. This technique

allows one to compute the ultimate precision in estimating noise parameters that are encoded in discrete- or continuous-variable channels. The tool easily applies to any programmable channel whose unknown parameter is encoded in its program (environmental) state. One can then reduce an adaptive protocol and show that the QCRB is limited to the SQL.

When a programmable channel is teleportation-covariant (such as an erasure, a Pauli or a Gaussian channel), we can exploit a precise design for its simulation which is based on a simple modification of the teleportation protocol. In this way, we may show that the QCRB is limited to the SQL with the QFI being computed on the Choi matrix of the channel (in an asymptotic fashion for bosonic Gaussian channels). Furthermore, the QCRB is shown to be achievable by a block (i.e., non-adaptive) protocol based on entanglement-assistance.

As a consequence of the previous results, a quantum channel able to beat the SQL and potentially reach the Heisenberg scaling must be necessarily non-programmable in the sense discussed in this review, i.e., it cannot be perfectly simulated by means of a single-copy program state. A potential approach to cover this type of channel is therefore considering an extended definition of multi-programmability where the simulation is achieved by using a multi-copy resource state.

In conclusion, we have reviewed the state-of-the-art in the theory of channel simulation within the context of quantum parameter estimation. The reader interested in similar applications in quantum channel discrimination may consult Ref. [42] and a forthcoming review paper [73]. The reader interested in applications to quantum and private communications (e.g., for establishing two-way capacities) may consult Ref. [64] and also one of the founding papers [45].

Acknowledgement: This work has been supported by the Innovation Fund Denmark (Qubiz project), the European Union (MSCA-IF-2016), and the EPSRC via the ‘UK Quantum Communications Hub’ (EP/M013472/1). S. P. thanks R. Demkowicz-Dobrzański, S. Lloyd, L. Maccone, J. Kolodyński, D. Braun, and G. Adesso for feedback on these topics.

References

- [1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
- [2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* **84**, 621

- (2012).
- [3] F. Caruso, V. Giovannetti, C. Lupo, and S. Mancini, *Rev. Mod. Phys.* **86**, 1203 (2014).
- [4] U. L. Andersen, J. S. Neergaard-Nielsen, P. van Loock, and A. Furusawa, *Nature Phys.* **11**, 713 (2015).
- [5] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, *Phys. Rev. Lett.* **70**, 1895 (1993).
- [6] L. Vaidman, *Phys. Rev. A* **49**, 1473 (1994).
- [7] S. L. Braunstein and H. J. Kimble, *Phys. Rev. Lett.* **80**, 869 (1998).
- [8] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, *Nat. Photon.* **9**, 641 (2015).
- [9] H. J. Kimble, *Nature* **453**, 1023 (2008).
- [10] S. Pirandola and S. L. Braunstein, *Nature* **532**, 169 (2016).
- [11] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
- [12] E. Diamanti and A. Leverrier, *Entropy* **17**, 6072 (2015).
- [13] V. C. Usenko and R. Filip, *Entropy* **18**, 20 (2016).
- [14] C. H. Bennett and G. Brassard. *Quantum Cryptography: Public Key Distribution and Coin Tossing*, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175-179 (1984).
- [15] A.K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991).
- [16] M. Lucamarini and S. Mancini, *Phys. Rev. Lett.* **94**, 140501 (2005).
- [17] S. L. Braunstein, and S. Pirandola, *Phys. Rev. Lett.* **108**, 130502 (2012).
- [18] F. Grosshans, G. Van Ache, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Nature* **421**, 238 (2003).
- [19] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, *Phys. Rev. Lett.* **93**, 170504 (2004).
- [20] S. Pirandola, S. Mancini, S. Lloyd, and S. L. Braunstein, *Nat. Phys.* **4**, 726 (2008).
- [21] S. Pirandola, C. Ottaviani, G. Spedalieri, C. Weedbrook, S. L. Braunstein, S. Lloyd, T. Ghering, C.S. Jacobsen, and U. L. Andersen, *Nat. Photon.* **9**, 397 (2015).
- [22] S. Lloyd, *Science* **321**, 1463 (2008).
- [23] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, *Phys. Rev. Lett.* **101**, 253601 (2008).
- [24] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, *Phys. Rev. Lett.* **114**, 080503 (2015).
- [25] C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, and M. Gu, *New J. Phys.* **18**, 043027 (2016).
- [26] M. Tsang, R. Nair, and X. Lu, *Phys. Rev. X* **6**, 031033 (2016).
- [27] C. Lupo and S. Pirandola, *Phys. Rev. Lett.* **117**, 190802 (2016).
- [28] R. Nair, and M. Tsang, *Phys. Rev. Lett.* **117**, 190801 (2016).
- [29] S. L. Braunstein and C. M. Caves, *Phys. Rev. Lett.* **72**, 3439 (1994).
- [30] P. Kok, S. L. Braunstein, and J. P. Dowling, *J. Op. B* **6**, 8 (2004).
- [31] V. Giovannetti, S. Lloyd, and L. Maccone, *Science* **306**, 1330 (2004).
- [32] H. M. Wiseman and G. J. Milburn, *Quantum Measurement and Control* (Cambridge University Press, 2010).
- [33] M. G. A. Paris, *Int. J. Quant. Inf.* **7**, 125 (2009).
- [34] V. Giovannetti, S. Lloyd, and L. Maccone, *Nature Photon.* **5**, 222 (2011).
- [35] G. Toth and I. Apellaniz, *J. Phys. A: Math. Theor.* **47**, 424006 (2014).
- [36] D. Braun, G. Adesso, F. Benatti, R. Floreanini, U. Marzolino, M. W. Mitchell, and S. Pirandola, *Quantum enhanced measurements*

- without entanglement*, arXiv:1701.05152 (2017).
- [37] M. A. Nielsen and Isaac L. Chuang, *Phys. Rev. Lett.* **79**, 321 (1997).
- [38] Z. Ji, G. Wang, R. Duan, Y. Feng, and M. Ying, *IEEE Trans. Info. Theory* **54**, 5172 (2008).
- [39] K. Matsumoto, *On metric of quantum channel spaces*, arXiv:1006.0300v1 (2010).
- [40] J. Kolodyński and R. Demkowicz-Dobrzański, *New J. Phys.* **15** 073043 (2013).
- [41] R. Demkowicz-Dobrzański and L. Maccone, *Phys. Rev. Lett.* **113**, 250801 (2014).
- [42] S. Pirandola, and C. Lupo, *Phys. Rev. Lett.* **118**, 100502 (2017); *ibidem* **119**, 129901 (2017).
- [43] R. Demkowicz-Dobrzański, J. Czajkowski, and P. Sekatski, *Phys. Rev. X* **7**, 041009 (2017).
- [44] S. Zhou, M. Zhang, J. Preskill, and L. Jiang, *Achieving the Heisenberg limit in quantum metrology using quantum error correction*, arXiv:1706.02445 (2017).
- [45] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Nat. Commun.* **8**, 15043 (2017).
- [46] P. Liuzzo-Scorpo, A. Mari, V. Giovannetti, and G. Adesso, *Phys. Rev. Lett.* **119**, 120503 (2017).
- [47] G. Chiribella, G. M. D'Ariano, and P. Perinotti, *Phys. Rev. Lett.* **101**, 060401 (2008).
- [48] A. Uhlmann, *Rep. Math. Phys.* **9**, 273 (1976).
- [49] R. Jozsa, *Journal of Modern Optics* **41**, 2315 (1994).
- [50] L. Banchi, S. L. Braunstein, and S. Pirandola, *Phys. Rev. Lett.* **115**, 260501 (2015).
- [51] S. Ishizaka and T. Hiroshima, *Phys. Rev. Lett.* **101**, 240501 (2008).
- [52] S. Ishizaka and T. Hiroshima, *Phys. Rev. A* **79**, 042306 (2009).
- [53] S. Ishizaka, *Some remarks on port-based teleportation*, arXiv:1506.01555 (2015).
- [54] W. Zhi-Wei and S. L. Braunstein, *Sci. Rep.* **6**, 33004 (2016).
- [55] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, W. K. Wootters, *Phys. Rev. A* **54**, 3824 (1996).
- [56] M. M. Wolf, *Notes on Quantum Channels and Operations* (2012).
- [57] A. Muller-Hermes, *Transposition in quantum information theory* (Master's thesis, Technical University of Munich, 2012).
- [58] D. Leung and W. Matthews, *IEEE Trans. Info. Theory* **61**, 4486 (2015).
- [59] R. Laurenza and S. Pirandola, *Phys. Rev. A* **96**, 032318 (2017).
- [60] S. Pirandola, *Capacities of repeater-assisted quantum communications*, arXiv:1601.00966 (2016).
- [61] S. Pirandola and S. Mancini, *Laser Physics* **16**, 1418 (2006).
- [62] G. Giedke and J. I. Cirac, *Phys. Rev. A* **66**, 032316 (2002).
- [63] J. Niset, J. Fiurasek, and N. J. Cerf, *Phys. Rev. Lett.* **102**, 120501 (2009).
- [64] 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*, arXiv:1711.09909 (2017).
- [65] A. Furusawa, J. L. Sørensen, S. L. Braunstein, C. A. Fuchs, H. J. Kimble, and E. S. Polzik, *Science* **282**, 706 (1998).
- [66] S. L. Braunstein, G. M. D'Ariano, G. J. Milburn, and M. F. Sacchi, *Phys. Rev. Lett.* **84**, 3486 (2000).
- [67] A. S. Holevo, *Probab. Theory Appli.* **48**, 243 (2004).
- [68] M. E. Shirokov, *Energy-constrained diamond norms and their use in quantum information theory*, arXiv:1706.00361 (2017).
- [69] F. Caruso, V. Giovannetti, A. S. Holevo, *New J. Phys.* **8**, 310 (2006).
- [70] R. Laurenza, S. L. Braunstein, and S. Pirandola, arXiv:1706.06065 (2017).
- [71] M. Ban, M. Sasaki, and M. Takeoka, *J. Phys. A* **35**, L401 (2002).
- [72] A. Christ, C. Lupo, and C. Silberhorn, *New J. Phys.* **14**, 083007 (2012).
- [73] S. Pirandola, B. R. Bardhan, T. Gehring, C. Weedbrook, and S. Lloyd, *Advances in quantum sensing*, in preparation (2017).