npj | Quantum Information

www.nature.com/npjqi

Corrected: Publisher Correction

ARTICLE OPEN

Fundamental limits to quantum channel discrimination

Stefano Pirandola[1,2], Riccardo Laurenza[3], Cosmo Lupo[4] and Jason L. Pereira[2]

What is the ultimate performance for discriminating two arbitrary quantum channels acting on a finite-dimensional Hilbert space? Here we address this basic question by deriving a general and fundamental lower bound. More precisely, we investigate the symmetric discrimination of two arbitrary qudit channels by means of the most general protocols based on adaptive (feedback-assisted) quantum operations. In this general scenario, we first show how port-based teleportation can be used to simplify these adaptive protocols into a much simpler non-adaptive form, designing a new type of teleportation stretching. Then, we prove that the minimum error probability affecting the channel discrimination cannot beat a bound determined by the Choi matrices of the channels, establishing a general, yet computable formula for quantum hypothesis testing. As a consequence of this bound, we derive ultimate limits and no-go theorems for adaptive quantum illumination and single-photon quantum optical resolution. Finally, we show how the methodology can also be applied to other tasks, such as quantum metrology, quantum communication and secret key generation.

npj Quantum Information (2019)5:50 ; https://doi.org/10.1038/s41534-019-0162-y

INTRODUCTION

Quantum hypothesis testing[1] is a central area in quantum information theory,[2,3] with many studies for both discrete variable (DV)[4] and continuous variable (CV) systems.[5] A number of tools[6–10] have been developed for its basic formulation, known as quantum state discrimination. In particular, since the seminal work of Helstrom in the 70 s,[1] we know how to bound the error probability affecting the symmetric discrimination of two arbitrary quantum states. Remarkably, after about 40 years, a similar bound is still missing for the discrimination of two arbitrary quantum channels. There is a precise motivation for that: The main problem in quantum channel discrimination (QCD)[11–15] is that the strategies involve an optimization over the input states and the output measurements, and this process may be adaptive in the most general case, so that feedback from the output can be used to update the input.

Not only the ultimate performance of adaptive QCD is still unknown due to the difficulty of handling feedback-assistance, but it is also known that adaptiveness needs to be considered in QCD. In fact, apart from the cases where two channels are classical,[16] jointly programmable or teleportation covariant,[17,18] feedback may greatly improve the discrimination. For instance, ref. [19] 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. This suggests that the best discrimination performance is not directly related to the diamond distance,[20] when computed over multiple copies of the quantum channels.

In this work we finally fill this fundamental gap by deriving a universal computable lower bound for the error probability affecting the discrimination of two *arbitrary* quantum channels. To derive this bound we adopt 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 using port-based teleportation (PBT)[21–24] for channel simulation and suitably generalizing the technique of teleportation stretching.[25–27] This reduction is shown for 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, we bound the ultimate adaptive performance of quantum illumination[28–35] and the ultimate adaptive resolution of any single-photon diffraction-limited optical system, setting corresponding no-go theorems for these applications. We then apply our result to adaptive quantum metrology showing an ultimate bound which has an asymptotic Heisenberg scaling. As an example, we also study the adaptive discrimination of amplitude damping channels, which are the most difficult channels to be simulated. Finally, other implications are for the two-way assisted capacities of quantum and private communications.

RESULTS

Adaptive protocols

Let us formulate the most general adaptive protocol over an arbitrary quantum channel $\mathcal{E}$ defined between Hilbert spaces of dimension d (more generally, this can be taken as the dimension of the input space). We first provide a general description and then we specify the protocol to the task of QCD. A general adaptive protocol involves an unconstrained number of quantum systems which may be subject to completely arbitrary quantum operations (QOs). More precisely, we may organize the quantum systems into an input register **a** and an output register **b**, which are prepared in an initial state ρ_0 by applying a QO Λ_0 to some

[1]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, MA 02139, USA; [2]Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, UK; [3]QSTAR, INO-CNR and LENS, Largo Enrico Fermi 2, 50125 Firenze, Italy and [4]Department of Physics and Astronomy, University of Sheffield, Sheffield S3 7RH, UK
Correspondence: Stefano Pirandola (stefano.pirandola@york.ac.uk)

Received: 3 January 2019 Accepted: 13 May 2019
Published online: 05 June 2019

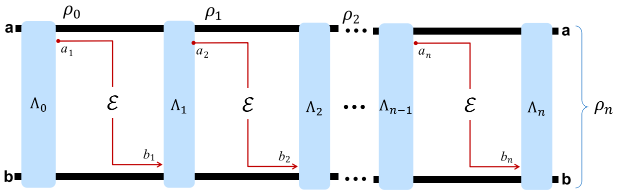

Fig. 1 General structure of an adaptive quantum protocol, where channel uses $\mathcal{E}$ are interleaved by QOs Λ's. See text for more details

fundamental state of **a** and **b**. Then, a system a_1 is picked from the register **a** and sent through the channel $\mathcal{E}$. The corresponding output b_1 is merged with the output register $b_1\mathbf{b}\to\mathbf{b}$. This is followed by another QO Λ_1 applied to **a** and **b**. Then, we send a second system $a_2\in\mathbf{a}$ through $\mathcal{E}$ with the output b_2 being merged again $b_2\mathbf{b}\to\mathbf{b}$ and so on. After n uses, the registers will be in a state ρ_n which depends on $\mathcal{E}$ and the sequence of QOs $\{\Lambda_0, \Lambda_1, \ldots, \Lambda_n\}$ defining the adaptive protocol $\mathcal{P}_n$ with output state ρ_n (see Fig. 1).

In a protocol of quantum communication, the registers belong to remote users and, in absence of entanglement-assistance, the QOs are local operations (LOs) assisted by two-way classical communication (CC), also known as adaptive LOCCs. The output is generated in such a way to approximate some target state.[25] In a protocol of quantum channel estimation, the channel is labelled by a continuous parameter $\mathcal{E}=\mathcal{E}_\theta$ and the QOs include the use of entanglement across the registers. The output state will encode the unknown parameter $\rho_n=\rho_n(\theta)$, which is detected and the outcome processed into an optimal estimator.[17] Here, in a protocol of binary and symmetric QCD, the channel is labelled by a binary digit, i.e., $\mathcal{E}=\mathcal{E}_u$ where $u\in\{0,1\}$ has equal priors. The QOs are generally entangled and they generate an output state encoding the information bit, i.e., $\rho_n=\rho_n(u)$.

The output state $\rho_n(u)$ of an adaptive discrimination 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 conditional error probability

$$p(\mathcal{E}_0\neq\mathcal{E}_1|\mathcal{P}_n)=\frac{1-D[\rho_n(0),\rho_n(1)]}{2}, \tag{1}$$

where $D(\rho,\sigma):=\|\rho-\sigma\|/2$ is the trace distance.[4] The optimization over all discrimination protocols $\mathcal{P}_n$ defines the minimum error probability affecting the n-use adaptive discrimination of $\mathcal{E}_0$ and $\mathcal{E}_1$, i.e., we may write

$$p_n(\mathcal{E}_0\neq\mathcal{E}_1):=\inf_{\mathcal{P}_n} p(\mathcal{E}_0\neq\mathcal{E}_1|\mathcal{P}_n). \tag{2}$$

This is generally less than the n-copy diamond distance between the two channels $\mathcal{E}_0^{\otimes n}$ and $\mathcal{E}_1^{\otimes n}$

$$p_n(\mathcal{E}_0\neq\mathcal{E}_1)\le\frac{1-\frac{1}{2}\|\mathcal{E}_0^{\otimes n}-\mathcal{E}_1^{\otimes n}\|_\diamond}{2}, \tag{3}$$

where[2]

$$\|\mathcal{E}_0^{\otimes n}-\mathcal{E}_1^{\otimes n}\|_\diamond:=\sup_{\rho_{ar}}\|\mathcal{E}_0^{\otimes n}\otimes\mathcal{I}(\rho_{ar})-\mathcal{E}_1^{\otimes n}\otimes\mathcal{I}(\rho_{ar})\|, \tag{4}$$

with $\mathcal{I}$ being an identity map acting on a reference system r. The upper bound in Eq. (3) is achieved by a non-adaptive protocol, where an (optimal) input state ρ_{ar} is prepared and its a-parts transmitted through $\mathcal{E}_u^{\otimes n}$. Note that Eq. (3) is very difficult to compute, which is why we usually compute larger but simpler single-letter upper bounds such as

$$p_n(\mathcal{E}_0\neq\mathcal{E}_1)\le\frac{F(\rho_{\mathcal{E}_0},\rho_{\mathcal{E}_1})^n}{2}, \tag{5}$$

where F is the fidelity between the Choi matrices, $\rho_{\mathcal{E}_0}$ and $\rho_{\mathcal{E}_1}$, of the two channels.

Our question is: Can we complete Eq. (3) with a corresponding lower bound? Up to today this has been only proven for jointly programmable channels, i.e., channels $\mathcal{E}_0$ and $\mathcal{E}_1$ admitting a simulation $\mathcal{E}_u(\rho)=\mathcal{S}(\rho\otimes\pi_u)$ with a trace-preserving QO $\mathcal{S}$ and different program states π_0 and π_1. In this case, we have $p_n\ge[1-D(\pi_0^{\otimes n},\pi_1^{\otimes n})]/2$.[17] In particular, this is true if the channels are jointly teleportation covariant, so that $\mathcal{S}$ becomes teleportation and the program state is a Choi matrix $\rho_{\mathcal{E}_u}$. For these channels, ref. [17] found that Eq. (3) holds with an equality and we may write $\|\mathcal{E}_0^{\otimes n}-\mathcal{E}_1^{\otimes n}\|_\diamond=\|\rho_{\mathcal{E}_0}^{\otimes n}-\rho_{\mathcal{E}_1}^{\otimes n}\|$. More precisely, the question to ask is therefore the following: Can we establish a *universal* lower bound for $p_n(\mathcal{E}_0\neq\mathcal{E}_1)$ which is valid for *arbitrary* channels? As we show here, this is possible by resorting to a more general (multi-program) simulation of the channels, i.e., of the type $\mathcal{S}(\rho\otimes\pi_u^{\otimes M})$.

PBT and simulation of the identity

Let us describe the protocol of PBT with qudits of arbitrary dimension $d\ge 2$. More technical details can be found in the original proposals.[22,23] The parties exploit two ensembles of $M\ge 2$ 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 prepared in a maximally entangled state, so that we have the global state

$$\Phi^{\otimes M}_{\mathbf{AB}}=\otimes_{i=1}^{M}|\Phi\rangle_i\langle\Phi|,\qquad |\Phi\rangle_i:=d^{-1/2}\sum_k|k\rangle_{A_i}\otimes|k\rangle_{B_i}. \tag{6}$$

To teleport the state of a qudit C, Alice performs a joint measurement on C and her ensemble **A**. This is a POVM $\{\Pi^i_{C\mathbf{A}}\}_{i=1}^M$ with M possible outcomes (see refs [22,23] for the details). In the standard protocol considered here, this POVM is a square root measurement (known to be optimal in the qubit case). Once Alice communicates the outcome i to Bob, he discards all the ports but the ith one, which contains the teleported state (see Fig. 2a).

The measurement outcomes are equiprobable and independent of the input, and the output state is invariant under permutation of the ports (this can be understood by the fact that the scheme is invariant under permutation of the Bell states and, therefore, of the ports). Averaging over the outcomes, we define the teleported state $\rho_B^M=\Gamma_M(\rho_C)$, where Γ_M is the corresponding PBT channel. Explicitly, this channel takes the form

$$\Gamma_M(\rho_C)=\sum_{i=1}^{M}\mathrm{Tr}_{\mathbf{A}\bar{B}_iC}[\Pi^i_{C\mathbf{A}}(\rho_C\otimes\Phi^{\otimes M}_{\mathbf{AB}})], \tag{7}$$

where $\mathrm{Tr}_{\bar{B}_i}$ denotes the trace over all ports **B** but B_i.

As shown in ref. [22], the standard protocol gives a depolarizing channel[4] whose probability ξ_M decreases to zero for increasing number of ports M. Therefore, in the limit of many ports $M\gg 1$, the M-port PBT channel Γ_M tends to an identity channel $\mathcal{I}$, so that Bob's output becomes a perfect replica of Alice's input. Here we prove a stronger result in terms of channel uniform convergence.[26,27] In fact, for any M, we show that the simulation error, expressed in terms of the diamond distance between Γ_M and $\mathcal{I}$, is one-to-one with the entanglement fidelity of the PBT channel Γ_M. In turn, this result allows us to write a simple upper bound for this error. Moreover, we can fully characterize the simulation error with an exact analytical expression for qubits (see Methods for the proof, with further details given in Supplementary Section 1).

Lemma 1. In arbitrary (finite) dimension d, the diamond distance between the M-port PBT channel Γ_M and the identity channel $\mathcal{I}$ satisfies

$$\delta_M:=\|\mathcal{I}-\Gamma_M\|_\diamond=2[1-f_e(\Gamma_M)], \tag{8}$$

where $f_e(\Gamma_M):=\langle\Phi|[\mathcal{I}\otimes\Gamma_M(|\Phi\rangle\langle\Phi|)]|\Phi\rangle$ is the entanglement fidelity of Γ_M. This gives the upper bound

$$\delta_M\le 2d(d-1)M^{-1}. \tag{9}$$

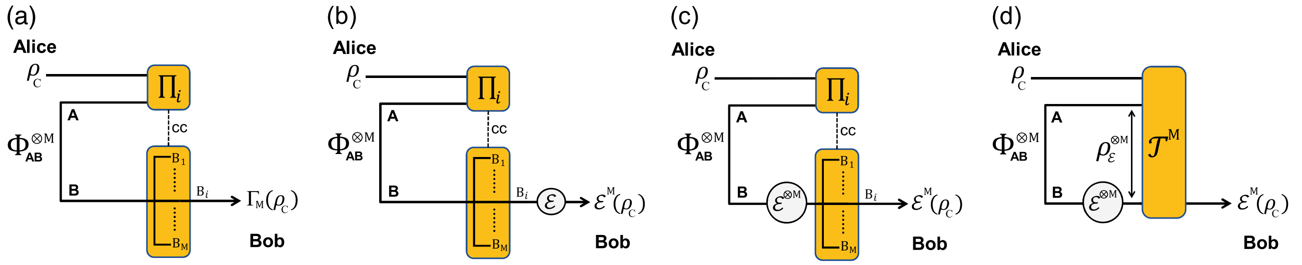

Fig. 2 From port-based teleportation (PBT) to Choi-simulation of a quantum channel (see also ref. [21]). **a** Schematic representation of the PBT protocol. Alice and Bob share an $M \times M$ qudit state which is given by M maximally entangled states $\Phi_{\mathbf{AB}}^{\otimes M}$. To teleport an input qubit state ρ_C, Alice applies a suitable POVM $\{\Pi_i\}$ to the input qubit C and her **A** qubits. The outcome i is communicated to Bob, who selects the i-th among his **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. (12). 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 **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. (13)

More precisely, we can write the exact result

$$\delta_M = \frac{2(d^2-1)}{d^2}\xi_M, \tag{10}$$

where ξ_M is the depolarizing probability of the PBT channel Γ_M. For qubits ($d = 2$), the "PBT number" ξ_M has the closed analytical expression

$$\xi_M = \frac{1}{3}\frac{M+2}{2^{M-1}} + \frac{1}{3}\sum_{s=s_{min}}^{(M-1)/2}\frac{s(s+1)}{2^{M-4}}\begin{pmatrix} M \\ \frac{M-1}{2}-s\end{pmatrix}\frac{(M+2)-\sqrt{(M+2)^2-(2s+1)^2}}{(M+2)^2-(2s+1)^2}, \tag{11}$$

where $s_{min} = 1/2$ for even M and 0 for odd M.

General channel simulation via PBT

Let us discuss how PBT can be used for channel simulation. This was first shown in ref. [21] where PBT was introduced as a possible design for a programmable quantum gate array.[36] As depicted in Fig. 2b, suppose that Bob applies an arbitrary channel $\mathcal{E}$ to the teleported output, so that Alice's input ρ_C is subject to the approximate channel

$$\mathcal{E}^M(\rho_C) := \mathcal{E} \circ \Gamma_M(\rho_C). \tag{12}$$

Note that the port selection commutes with $\mathcal{E}$, because the POVM acts on a different Hilbert space.[21] Therefore, Bob can equivalently apply $\mathcal{E}$ to each port before Alice's CC, i.e., apply $\mathcal{E}^{\otimes M}$ to his **B** qudits before selecting the output port, as shown in Fig. 2c. This leads to the following simulation for the approximate channel

$$\mathcal{E}^M(\rho_C) = \mathcal{T}^M(\rho_C \otimes \rho_{\mathcal{E}}^{\otimes M}), \tag{13}$$

where $\mathcal{T}^M$ is a trace-preserving LOCC and $\rho_{\mathcal{E}}$ is the channel's Choi matrix (see Fig. 2d). 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. (12) and the monotonicity of the diamond norm, we get

$$||\mathcal{E} - \mathcal{E}^M||_\diamond \le \delta_M, \tag{14}$$

where δ_M is the simulation error in Eq. (9), with the dimension d being the one of the input Hilbert space. It is worth to remark that, while the simulation in Eq. (13) relies on a number of copies of the channel's Choi matrix, it can be applied to an arbitrary quantum channel $\mathcal{E}$ without the condition of teleportation covariance.[25]

PBT stretching of an adaptive protocol

Channel simulation is a preliminary tool for the following technique of teleportation stretching, where an arbitrary adaptive protocol is reduced into a simpler block version. There are two main steps. First of all, we 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. This step is crucial also in simulations via standard teleportation[18,26] (see also refs [37–41]). Second, we need to "stretch" the protocol[25] by replacing the various instances of the approximate channel $\mathcal{E}^M$ with a collection of Choi matrices $\rho_{\mathcal{E}}^{\otimes M}$ and then suitably re-organizing all the remaining QOs. Here we describe the technique for a generic task, before specifying it to 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. Using a "peeling" argument (see Methods), we bound the output error in terms of the channel simulation error

$$||\rho_n - \rho_n^M|| \le n||\mathcal{E} - \mathcal{E}^M||_\diamond \le n\delta_M. \tag{15}$$

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. (13), 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. 3. As a result, we may write the multi-copy Choi decomposition

$$\rho_n^M = \overline{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM}), \tag{16}$$

for a trace-preserving QO $\overline{\Lambda}$. Now, we can combine the two ingredients of Eqs. (15) and (16), into the following.

Lemma 2 (PBT stretching). 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

$$||\rho_n - \overline{\Lambda}(\rho_{\mathcal{E}}^{\otimes nM})|| \le n\delta_M, \tag{17}$$

where $\overline{\Lambda}$ 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. (9).

When we apply the lemma to protocols of quantum or private communication, where the QOs Λ_i are LOCCs, then we may write Eq. (17) with $\overline{\Lambda}$ being a LOCC. In protocols of channel estimation or discrimination, where $\mathcal{E}$ is parametrized, we may write Eq. (17) with $\rho_{\mathcal{E}}$ storing the parameter of the channel. In particular, for

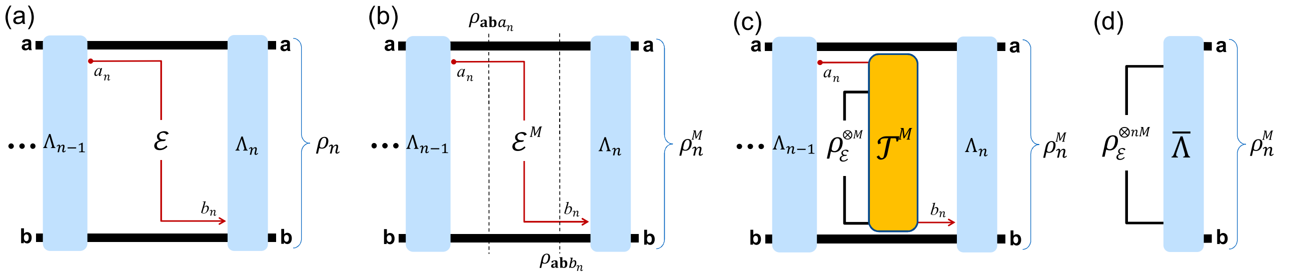

Fig. 3 Port-based teleportation stretching of a generic adaptive protocol over a quantum channel $\mathcal{E}$. This channel is fixed in quantum/private communication, while it is unknown and parametrized in estimation/discrimination problems. **a** We show the last transmission $a_n \to b_n$ through $\mathcal{E}$, 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 $\overline{\Lambda}$. Correspondingly, n instances of $\rho_{\mathcal{E}}^{\otimes M}$ are collected. As a result, the approximate output ρ_n^M is given by $\overline{\Lambda}$ applied to the tensor-product state $\rho_{\mathcal{E}}^{\otimes nM}$ as in Eq. (16)

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

$$||\rho_n(u) - \overline{\Lambda}(\rho_{\mathcal{E}_u}^{\otimes nM})|| \le n\delta_M. \tag{18}$$

Ultimate bound for channel discrimination

We are now ready to show the lower bound for minimum error probability $p_n(\mathcal{E}_0 \ne \mathcal{E}_1)$ in Eq. (3). Consider an arbitrary protocol $\mathcal{P}_n$, for which we may write Eq. (1). Combining Lemma 2 with the triangle inequality leads to

$$\begin{aligned} ||\rho_n(0) - \rho_n(1)|| &\le 2n\delta_M + ||\overline{\Lambda}(\rho_{\mathcal{E}_0}^{\otimes nM}) - \overline{\Lambda}(\rho_{\mathcal{E}_1}^{\otimes nM})|| \\ &\le 2n\delta_M + ||\rho_{\mathcal{E}_0}^{\otimes nM} - \rho_{\mathcal{E}_1}^{\otimes nM}||, \end{aligned} \tag{19}$$

where we also use the monotonicity of the trace distance under channels. Because $\overline{\Lambda}$ is lost, 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. (19) in Eqs. (1) and (2), we get the following.

Theorem 3. 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

$$p_n(\mathcal{E}_0 \ne \mathcal{E}_1) \ge B := \frac{1 - n\delta_M - D(\rho_{\mathcal{E}_0}^{\otimes nM}, \rho_{\mathcal{E}_1}^{\otimes nM})}{2}, \tag{20}$$

where M may be chosen to maximize the right hand side.

Not only this is the first universal bound for adaptive QCD, but also its analytical form is rather surprising. In fact, its tighest value is given by an optimal (finite) number of ports M for the underlying protocol of PBT.

Let us bound the trace distance in Eq. (20) as

$$D^2 \le 1 - F^{2nM}, \quad F := \mathrm{Tr}\sqrt{\sqrt{\rho_{\mathcal{E}_0}}\rho_{\mathcal{E}_1}\sqrt{\rho_{\mathcal{E}_0}}}, \tag{21}$$

where F is the fidelity between the Choi matrices of the channels. This comes from the Fuchs-van de Graaf relations[42] and the multiplicativity of the fidelity over tensor products. Other bounds that can be written are

$$D \le nM||\rho_{\mathcal{E}_0} - \rho_{\mathcal{E}_1}||, \tag{22}$$

from the subadditivity of the trace distance, and

$$D \le \sqrt{nM(\ln\sqrt{2})\min\{S(\rho_{\mathcal{E}_1}||\rho_{\mathcal{E}_0}), S(\rho_{\mathcal{E}_0}||\rho_{\mathcal{E}_1})\}}, \tag{23}$$

from the Pinsker inequality,[43,44] where $S(\rho||\sigma) = \mathrm{Tr}[\rho(\log_2\rho - \log_2\sigma)]$ is the relative entropy.[4]

If we exploit Eqs. (9) and (21) in Eq. (20), we may write the following simplified bound

$$B \ge \frac{1}{2} - \frac{\sqrt{1 - F^{2nM}}}{2} - \frac{d(d-1)n}{M}. \tag{24}$$

In the previous formula there are terms with opposite monotonicity in M, so that the maximum value of the bound B is achieved at some intermediate value of M. Setting $M = xd(d-1)n$ for some $x > 2$, we get

$$B \ge \frac{1}{2} - \frac{1}{x} - \frac{1}{2}\sqrt{1 - F^{2xd(d-1)n^2}}. \tag{25}$$

One good choice is therefore $M = 4d(d-1)n$, so that

$$B \ge (1 - 2\sqrt{1 - F^{8d(d-1)n^2}})/4. \tag{26}$$

In particular, consider two infinitesimally-close channels, so that $F \simeq 1 - \epsilon$ where $\epsilon \simeq 0$ is the infidelity. By expanding in ϵ for any finite n, we may write

$$B \ge \frac{1}{4} - n\sqrt{2d(d-1)\epsilon} \simeq \frac{\exp(-4n\sqrt{2d(d-1)\epsilon})}{4}. \tag{27}$$

For instance, in the case of qubits this becomes $[\exp(-8n\sqrt{\epsilon})]/4$, to be compared with the upper bound $[\exp(-2n\epsilon)]/2$ computed from Eq. (5). Discriminating between two close quantum channels is a problem in many physical scenarios. For instance, this is typical in quantum optical resolution[45–47] (discussed below), quantum illumination[28–35,48,49] (discussed below), ideal quantum reading,[50–54] quantum metrology[55–59] (discussed below), and also tests of quantum field theories in non-inertial frames,[60] e.g., for detecting effects such as the Unruh or the Hawking radiation.

Limits of 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. (27) 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 $B \gtrsim \frac{1}{4}\exp(-2ns\sqrt{\eta})$. This bound establishes a no-go for perfect quantum optical resolution. See Supplementary Section 2 for more mathematical details on this specific application.

Limits of adaptive quantum illumination

Consider the protocol of quantum illumination in the DV setting.[28] Here the problem is to discriminate the presence or not of a target with low reflectivity $\eta \simeq 0$ in a thermal background which has $b \ll 1$ mean thermal photons per optical mode. One assumes that d modes are used in each probing of the target and each of them contains at most one photon. This means that the Hilbert space is $(d+1)$-dimensional with basis $\{|0\rangle, |1\rangle, \ldots, |d\rangle\}$, where $|i\rangle := |0\cdots010\cdots0\rangle$ has one photon in the ith mode. If the target is absent ($u=0$), the receiver detects thermal noise; if the target is present ($u=1$), the receiver measures a mixture of signal and thermal noise.

In the most general (adaptive) version of the protocol, the receiver belongs to a large quantum computer where the $(d+1)$-dimensional signal qudits are picked from an input register, sent to target, and their reflection stored in an output register, with adaptive QOs performed between each probing. After n probings, the state of the registers $\rho_n(u)$ is optimally detected. Assuming the typical regime of quantum illumination,[28] we find that the error probability affecting target detection is approximately bounded by $B \gtrsim \frac{1}{4}\exp(-4nd\sqrt{\eta})$. This bound establishes a no-go for exponential improvement in quantum illumination. Entanglement and adaptiveness can *at most* improve the error exponent with respect to separable probes, for which the error probability is $\lesssim \frac{1}{2}\exp[-n\eta/(8d)]$. See also Supplementary Section 3.

Limits of adaptive quantum metrology

Consider the adaptive estimation of a continuous parameter θ encoded in a quantum channel $\mathcal{E}_\theta$. After n probings, we have a θ-dependent output state $\rho_n(\theta)$ generated by an adaptive quantum estimation protocol $\mathcal{P}_n$. This output state is then measured by a POVM $\mathcal{M}$ providing an optimal unbiased estimator $\tilde{\theta}$ of parameter θ. The minimum error variance $\mathrm{Var}(\tilde{\theta}) := \langle(\tilde{\theta}-\theta)^2\rangle$ must satisfy the quantum Cramer-Rao bound $\mathrm{Var}(\tilde{\theta}) \geq 1/\mathrm{QFI}_\theta(\mathcal{P}_n)$, where $\mathrm{QFI}_\theta(\mathcal{P}_n)$ is the quantum Fisher information[55] associated with $\mathcal{P}_n$. The ultimate precision of adaptive quantum metrology is given by the optimization over all protocols

$$\overline{\mathrm{QFI}}^n_\theta := \sup_{\mathcal{P}_n} \mathrm{QFI}_\theta(\mathcal{P}_n). \tag{28}$$

This quantity can be simplified by PBT stretching. In fact, for any input state ρ_C, we may write the simulation $\mathcal{E}^M_\theta(\rho_C) = \mathcal{T}^M(\rho_C \otimes \rho^{\otimes M}_{\mathcal{E}_\theta})$, which is an immediate extension of Eq. (13). In this way, the output state can be decomposed following Lemma 2, i.e., we may write $||\rho_n(\theta) - \overline{\Lambda}(\rho^{\otimes nM}_{\mathcal{E}_\theta})|| \leq n\delta_M$. Exploiting the latter inequality for large n, we find that the ultimate bound of adaptive quantum metrology takes the form

$$\overline{\mathrm{QFI}}^n_\theta \lesssim n^2 \mathrm{QFI}(\rho_{\mathcal{E}_\theta}), \tag{29}$$

where $\mathrm{QFI}(\rho_{\mathcal{E}_\theta})$ is computed on the channel's Choi matrix. In particular, we see that PBT allows us to write a simple bound in terms of the Choi matrix and implies a general no-go theorem for super-Heisenberg scaling in quantum metrology. See Supplementary Section 4 for a detailed proof of Eq. (29).

Tightening the main formula

Let us note that the formula in Theorem 3 is expressed in terms of the universal error δ_M coming from the PBT simulation of the identity channel (Lemma 1). There are situations where the diamond distance $\Delta_M := ||\mathcal{E} - \mathcal{E}^M||_\diamond$ between a quantum channel $\mathcal{E}$ and its M-port simulation $\mathcal{E}^M$ is exactly computable. In these cases, we can certainly formulate a tighter version of Eq. (20) where δ_M is suitably replaced. In fact, from the peeling argument, we have $||\rho_n - \rho^M_n|| \leq n\Delta_M$, so that a tighter version of Eq. (17) is simply $||\rho_n - \overline{\Lambda}(\rho^{\otimes nM}_{\mathcal{E}})|| \leq n\Delta_M$. Then, for the two possible outputs $\rho_n(0)$ and $\rho_n(1)$ of an adaptive discrimination protocol over $\mathcal{E}_0$ and $\mathcal{E}_1$, we can replace Eq. (19) with

$$||\rho_n(0) - \rho_n(1)|| \leq 2n\overline{\Delta}_M + ||\rho^{\otimes nM}_{\mathcal{E}_0} - \rho^{\otimes nM}_{\mathcal{E}_1}||, \tag{30}$$

where $\overline{\Delta}_M := (||\mathcal{E}_0 - \mathcal{E}^M_0||_\diamond + ||\mathcal{E}_1 - \mathcal{E}^M_1||_\diamond)/2$. It is now easy to check that Eq. (20) becomes the following

$$p_n(\mathcal{E}_0 \neq \mathcal{E}_1) \geq \frac{1 - n\overline{\Delta}_M - D(\rho^{\otimes nM}_{\mathcal{E}_0}, \rho^{\otimes nM}_{\mathcal{E}_1})}{2}. \tag{31}$$

In the following section, we show that $\overline{\Delta}_M$, and therefore the bound in Eq. (31), can be computed for the discrimination of amplitude damping channels.

Discrimination of amplitude damping channels

As an additional example of application of the bound, consider the discrimination between amplitude damping channels. These channels are not teleportation covariant, so that the results from ref. [17] do not apply and no bound is known on the error probability for their adaptive discrimination. Recall that an amplitude damping channel $\mathcal{E}_p$ transforms an input state ρ as follows

$$\mathcal{E}_p(\rho) = \sum\nolimits_{i=0,1} K_i \rho K_i^\dagger, \tag{32}$$

with Kraus operators

$$K_0 := |0\rangle\langle 0| + \sqrt{1-p}|1\rangle\langle 1|, \quad K_1 := \sqrt{p}|0\rangle\langle 1|, \tag{33}$$

where $\{|0\rangle, |1\rangle\}$ is the computational basis and p is the damping probability or rate.

Given two amplitude damping channels, $\mathcal{E}_{p_0}$ and $\mathcal{E}_{p_1}$, first assume a discrimination protocol where these channels are probed by n maximally entangled states and the outputs are optimally measured. The optimal error probability for this (non-adaptive) block protocol is given by $p^{\mathrm{block}}_n = [1 - D(\rho^{\otimes n}_{\mathcal{E}_{p_0}}, \rho^{\otimes n}_{\mathcal{E}_{p_1}})]/2$ and satisfies

$$\frac{1 - \sqrt{1 - F(p_0, p_1)^{2n}}}{2} \leq p^{\mathrm{block}}_n \leq \frac{F(p_0, p_1)^n}{2}, \tag{34}$$

where $F(p_0, p_1) := F(\rho_{\mathcal{E}_{p_0}}, \rho_{\mathcal{E}_{p_1}})$ is the fidelity between the Choi matrices. In particular, we explicitly compute

$$F = \frac{1 + \sqrt{(1-p_0)(1-p_1)} + \sqrt{p_0 p_1}}{2}. \tag{35}$$

It is clear that p^{block}_n in Eq. (34) is an upper bound to ultimate (adaptive) error probability $p_n(\mathcal{E}_{p_0} \neq \mathcal{E}_{p_1})$ for the discrimination of the two channels.

To lowerbound the ultimate probability we employ Eq. (31). In fact, for the M-port simulation $\mathcal{E}^M_p$ of $\mathcal{E}_p$, we compute

$$\Delta_M(p) = ||\mathcal{E}_p - \mathcal{E}^M_p||_\diamond = \xi_M\left(\frac{1-p}{2} + \sqrt{1-p}\right), \tag{36}$$

where ξ_M are the PBT numbers defined in Eq. (11). For any two amplitude damping channels, $\mathcal{E}_{p_0}$ and $\mathcal{E}_{p_1}$, we can then compute $\overline{\Delta}_M(p_0, p_1)$ and use Eq. (31) to bound $p_n(\mathcal{E}_{p_0} \neq \mathcal{E}_{p_1})$. More precisely, we can also exploit Eq. (21) and write the computable lower bound

$$p_n(\mathcal{E}_{p_0} \neq \mathcal{E}_{p_1}) \geq \frac{1 - n\overline{\Delta}_M(p_0, p_1) - \sqrt{1 - F(p_0, p_1)^{2nM}}}{2}. \tag{37}$$

In Fig. 4 we show an example of discrimination between two amplitude damping channels. In particular, we show how large is the gap between the upper bound p^{block}_n of Eq. (34) and the lower

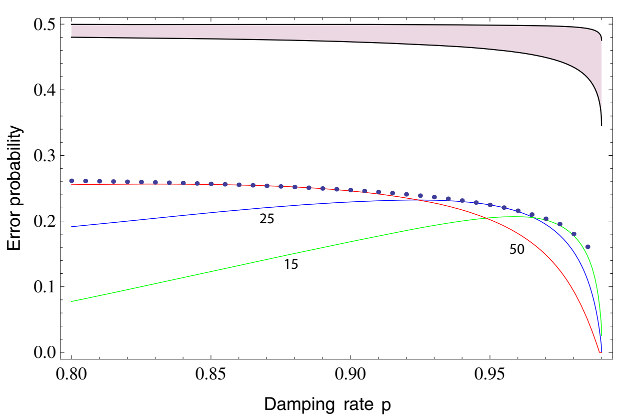

Fig. 4 Error probability in the discrimination of two amplitude damping channels, one with damping rate $p \geq 0.8$ and the other with rate $p + 1\%$. We assume $n = 20$ probings of the unknown channel. The upper dark region identifies the region where the error probability p_n^{block} of Eq. (34) lies. The adaptive error probability $p_n(\mathcal{E}_{p_0} \neq \mathcal{E}_{p_1})$ lies below this dark region and above the dotted points, which represent our lower bound of Eq. (37) optimized over the number of ports M. For comparison, we also plot the lower bound for specific M

bound in Eq. (37) suitably optimized over the number of ports M. It is an open question to find exactly $p_n(\mathcal{E}_{p_0} \neq \mathcal{E}_{p_1})$. At this stage, we do not know if this result may achieved by tightening the upper bound or the lower bound.

DISCUSSION

In this work we have established a general and fundamental lower bound for the error probability affecting the adaptive discrimination of two arbitrary quantum channels acting on a finite-dimensional Hilbert space. This bound is conveniently expressed in terms of the Choi matrices of the channels involved, so that it is very easy to compute. It also applies to many scenarios, including adaptive protocols for quantum-enhance optical resolution and quantum illumination. In order to derive our result, we have employed port-based teleportation as a tool for channel simulation, and developed a methodology which simplifies adaptive protocols performed over an arbitrary finite-dimensional channel. This technique can be applied to many other scenarios. For instance, in quantum metrology we are able to prove that adaptive protocols of quantum channel estimation are limited by a bound simply expressed in terms of the Choi matrix of the channel and following the Heisenberg scaling in the number of probings. Not only this shows that our bound is asymptotically tight but also draws an unexpected connection between port-based teleportation and quantum metrology. Further potential applications are in quantum and private communications, which are briefly discussed in our Supplementary Section 5.

METHODS

Simulation error in diamond norm (proof of Lemma 1)

It is easy to check that the channel Γ_M associated with the qudit PBT protocol of ref. [21] is covariant under unitary transformations, i.e.,

$$\Gamma_M(U\rho U^\dagger) = U\Gamma_M(\rho)U^\dagger, \tag{38}$$

for any input state ρ and unitary operator U. As discussed in ref. [61], for a channel with such a symmetry, the diamond distance with the identity map is saturated by a maximally entangled state, i.e.,

$$\|\mathcal{I} - \Gamma_M\|_\diamond = \||\Phi\rangle\langle\Phi| - \mathcal{I} \otimes \Gamma_M(|\Phi\rangle\langle\Phi|)\|, \tag{39}$$

where $|\Phi\rangle = d^{-1/2}\sum_{k=1}^{d}|k\rangle|k\rangle$. Here we first show that

$$\||\Phi\rangle\langle\Phi| - \mathcal{I} \otimes \Gamma_M(|\Phi\rangle\langle\Phi|)\| = 2[1 - f_e(\Gamma_M)]. \tag{40}$$

In fact, note that the map $\Lambda_M = \mathcal{I} \otimes \Gamma_M$ is covariant under twirling unitaries of the form $U \otimes U^*$, i.e.,

$$\Lambda_M\left[(U \otimes U^*)\rho(U \otimes U^*)^\dagger\right] = (U \otimes U^*)\Lambda_M(\rho)(U \otimes U^*)^\dagger, \tag{41}$$

for any input state ρ and unitary operator U. This implies that the quantum state $\Lambda_M(|\Phi\rangle\langle\Phi|)$ is invariant under twirling unitaries, i.e.,

$$(U \otimes U^*)\Lambda_M(|\Phi\rangle\langle\Phi|)(U \otimes U^*)^\dagger = \Lambda_M(|\Phi\rangle\langle\Phi|). \tag{42}$$

This is therefore an isotropic state of the form

$$\Lambda_M(|\Phi\rangle\langle\Phi|) = (1-p)|\Phi\rangle\langle\Phi| + \frac{p}{d^2}\mathbb{I}, \tag{43}$$

where $\mathbb{I}$ is the two-qudit identity operator.

We may rewrite this state as follows

$$\Lambda_M(|\Phi\rangle\langle\Phi|) = F|\Phi\rangle\langle\Phi| + (1-F)\rho^\perp, \tag{44}$$

where $\rho^\perp$ is state with support in the orthogonal complement of Φ, and F is the singlet fraction

$$F := \langle\Phi|\Lambda_M(|\Phi\rangle\langle\Phi|)|\Phi\rangle = 1 - p + pd^{-2}. \tag{45}$$

Thanks to the decomposition in Eq. (44) and using basic properties of the trace norm,[4] we may then write

$$\begin{aligned} &\||\Phi\rangle\langle\Phi| - \Lambda_M(|\Phi\rangle\langle\Phi|)\| \\ &= \|(1-F)|\Phi\rangle\langle\Phi| - (1-F)\rho^\perp\| \\ &= (1-F)\||\Phi\rangle\langle\Phi|\| + (1-F)\|\rho^\perp\| \\ &= 2(1-F) \\ &= 2[1 - f_e(\Gamma_M)], \end{aligned} \tag{46}$$

where the last step exploits the fact that the singlet fraction F is the channel's entanglement fidelity $f_e(\Gamma_M)$. This completes the proof of Eq. (40).

Therefore, combining Eqs. (39) and (40), we obtain

$$\|\mathcal{I} - \Gamma_M\|_\diamond = 2[1 - f_e(\Gamma_M)], \tag{47}$$

which is Eq. (8) of the main text. Then, we know that the entanglement fidelity of Γ_M is bounded as[21]

$$f_e(\Gamma_M) \geq 1 - d(d-1)M^{-1}. \tag{48}$$

Therefore, using Eq. (48) in Eq. (47), we derive the following upper bound

$$\|\mathcal{I} - \Gamma_M\|_\diamond \leq 2d(d-1)M^{-1}, \tag{49}$$

which is Eq. (9) of the main text.

Let us now prove Eq. (10). It is known[22] that implementing the standard PBT protocol over the resource state of Eq. (6) leads to a PBT channel Γ_M, which is a qudit depolarizing channel. Its isotropic Choi matrix ρ_{Γ_M}, given in Eq. (43), can be written in the form

$$\rho_{\Gamma_M} = \left(1 - \frac{d^2-1}{d^2}\xi_M\right)|\Phi\rangle^0\langle\Phi| + \sum_{i=1}^{d^2-1}\frac{\xi_M}{d^2}|\Phi\rangle^i\langle\Phi|, \tag{50}$$

where ξ_M is the probability p of depolarizing, $|\Phi\rangle^0\langle\Phi|$ is the projector onto the initial maximally entangled state of two qudits (one system of which was sent through the channel), and $|\Phi\rangle^i\langle\Phi|$ are the projectors onto the other $d^2 - 1$ maximally entangled states of two qudits (generalized Bell states). Since the Choi matrix of the identity channel is $\rho_{\mathcal{I}} = |\Phi\rangle^0\langle\Phi|$, it is easy to compute

$$\begin{aligned} |\rho_{\mathcal{I}} - \rho_{\Gamma_M}| &:= \sqrt{(\rho_{\mathcal{I}} - \rho_{\Gamma_M})(\rho_{\mathcal{I}} - \rho_{\Gamma_M})^\dagger} \\ &= \tfrac{d^2-1}{d^2}\xi_M|\Phi\rangle^0\langle\Phi| + \sum_{i=1}^{d^2-1}\tfrac{\xi_M}{d^2}|\Phi\rangle^i\langle\Phi|. \end{aligned} \tag{51}$$

From the previous equation, we derive

$$\mathrm{Tr}_2|\rho_{\mathcal{I}} - \rho_{\Gamma_M}| = \frac{2(d^2-1)}{d^3}\xi_M\sum_{j=0}^{d-1}|j\rangle\langle j|, \tag{52}$$

where we have used $\mathrm{Tr}_2|\Phi\rangle^i\langle\Phi| = d^{-1}\sum_{j=0}^{d-1}|j\rangle\langle j|$ in the qudit computational basis $\{|j\rangle\}$ and we have summed over the d^2 generalized Bell states. It is clear that Eq. (52) is a diagonal matrix with equal non-zero elements, i.e., it is a scalar. As a result, we can apply Proposition 1 of ref. [62] over the Hermitian operator $\rho_{\mathcal{I}} - \rho_{\Gamma_M}$, and write

$$\|\mathcal{I} - \Gamma_M\|_{\diamond} = \|\rho_{\mathcal{I}} - \rho_{\Gamma_M}\| = \mathrm{Tr}|\rho_{\mathcal{I}} - \rho_{\Gamma_M}| = \tfrac{2(d^2-1)}{d^2}\xi_M. \tag{53}$$

The final step of the proof is to compute the explicit expression of ξ_M for qubits, which is the formula given in Eq. (11). Because this derivation is technically involved, it is reported in Supplementary Section 1.

Propagation of the simulation error

For the sake of completeness, we provide the proof of the first inequality in Eq. (15) (this kind of proof already appeared in refs [25,26]). Consider the adaptive protocol described in the main text. For the n-use output state we may compactly write

$$\rho_n = \Lambda_n \circ \mathcal{E} \circ \Lambda_{n-1} \circ \cdots \circ \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0), \tag{54}$$

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

$$\rho_n^M = \Lambda_n \circ \mathcal{E}^M \circ \Lambda_{n-1} \circ \cdots \circ \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0), \tag{55}$$

where $\mathcal{E}^M$ is in the place of $\mathcal{E}$.

Consider now two instances ($n = 2$) of the adaptive protocol. We may bound the trace distance between ρ_2 and ρ_2^M using a "peeling" argument[17,18,25–27]

$$\begin{aligned}\|\rho_2 - \rho_2^M\| &= \|\Lambda_2 \circ \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0) - \Lambda_2 \circ \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)\| \\ &\overset{(1)}{\leq} \|\mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0) - \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)\| \\ &\overset{(2)}{\leq} \|\mathcal{E} \circ \Lambda_1 \circ \mathcal{E}(\rho_0) - \mathcal{E} \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)\| \\ &\quad + \|\mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}(\rho_0) - \mathcal{E}^M \circ \Lambda_1 \circ \mathcal{E}^M(\rho_0)\| \\ &\overset{(3)}{\leq} \|\mathcal{E}(\rho_0) - \mathcal{E}^M(\rho_0)\| \\ &\quad + \|\mathcal{E}[\Lambda_1 \circ \mathcal{E}^M(\rho_0)] - \mathcal{E}^M[\Lambda_1 \circ \mathcal{E}^M(\rho_0)]\| \\ &\overset{(4)}{\leq} 2\|\mathcal{E} - \mathcal{E}^M\|_{\diamond}.\end{aligned} \tag{56}$$

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. (56) to arbitrary n, we achieve the first inequality in Eq. (15). Note that the previous reasoning can also be applied to a classically-parametrized unknown channel.

PBT simulation of amplitude damping channels

Here we show the result in Eq. (36) for $\Delta_M(p) = \|\mathcal{E}_p - \mathcal{E}_p^M\|_{\diamond}$, which is the error associated with the M-port simulation of an arbitrary amplitude damping channel $\mathcal{E}_p$. From ref. [22], we know that the PBT channel Γ^M is a depolarizing channel. In the qubit computational basis $\{|i,j\rangle\}_{i,j=0,1}$, it has the following Choi matrix

$$\rho_{\Gamma^M} = \begin{pmatrix} \frac{1}{2} - \frac{\xi_M}{4} & 0 & 0 & \frac{1}{2} - \frac{\xi_M}{2} \\ 0 & \frac{\xi_M}{4} & 0 & 0 \\ 0 & 0 & \frac{\xi_M}{4} & 0 \\ \frac{1}{2} - \frac{\xi_M}{2} & 0 & 0 & \frac{1}{2} - \frac{\xi_M}{4} \end{pmatrix}, \tag{57}$$

where ξ_M are the PBT numbers of Eq. (11). Note that these take decreasing positive values, for instance

$$\begin{aligned}\xi_2 &= \tfrac{6-\sqrt{3}}{6} \simeq 0.71, \\ \xi_3 &= 1/2, \\ \xi_4 &= \tfrac{13-2\sqrt{2}-2\sqrt{5}}{16}, \\ \xi_5 &= \tfrac{35-4\sqrt{6}-4\sqrt{10}}{48}, \\ \xi_6 &= \tfrac{70-15\sqrt{3}-5\sqrt{7}-3\sqrt{15}}{96} \simeq 0.2.\end{aligned} \tag{58}$$

By applying the Kraus operators K_0 and K_1 of $\mathcal{E}_p$ locally to ρ_{Γ^M} we obtain the Choi matrix of the M-port simulation $\mathcal{E}_p^M$, which is

$$\rho_{\mathcal{E}_p^M} = \begin{pmatrix} x & 0 & 0 & y \\ 0 & (1-p)\xi_M & 0 & 0 \\ 0 & 0 & w & 0 \\ y & 0 & 0 & z \end{pmatrix}, \tag{59}$$

where $x := \frac{1}{2} - (1-p)\frac{\xi_M}{4}$, $y := \sqrt{1-p}\left(\frac{1}{2} - \frac{\xi_M}{2}\right)$, $z := \left(\frac{1}{2} - \frac{\xi_M}{4}\right)(1-p)$, and $w := \left(\frac{1}{2} - \frac{\xi_M}{4}\right)p + \frac{\xi_M}{4}$. This has to be compared with the Choi matrix of $\mathcal{E}_p$, which is

$$\rho_{\mathcal{E}_p} = \begin{pmatrix} \frac{1}{2} & 0 & 0 & \frac{\sqrt{1-p}}{2} \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \frac{p}{2} & 0 \\ \frac{\sqrt{1-p}}{2} & 0 & 0 & \frac{1-p}{2} \end{pmatrix}. \tag{60}$$

Now, consider the Hermitian matrix $J = \rho_{\mathcal{E}_p^M} - \rho_{\mathcal{E}_p}$. If the matrix $\phi = \mathrm{Tr}_2\sqrt{J^{\dagger}J} = \mathrm{Tr}_2\sqrt{JJ^{\dagger}}$ is scalar (i.e., both of its eigenvalues are equal), then the trace distance between the Choi matrices $\|J\|$ is equal to the diamond distance between the channels $\Delta_M(p)$ [62, Proposition 1]. After simple algebra we indeed find

$$\phi = \frac{\xi_M}{8}[2(1-p) + a_- + a_+]\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \tag{61}$$

where $a_{\pm} = \sqrt{1-p}\sqrt{5 \pm 4\sqrt{1-p} - p}$. Because ϕ is scalar, the condition above is met and the expression of $\Delta_M(p)$ is twice the (degenerate) eigenvalue of ϕ, i.e.,

$$\Delta_M(p) = \frac{\xi_M}{4}[2(1-p) + a_- + a_+], \tag{62}$$

which simplifies to Eq. (36).

DATA AVAILABILITY

The data sets generated in this study are available from the corresponding author upon reasonable request.

CODE AVAILABILITY

The code used to generate data will be made available to the interested reader upon reasonable request.

ACKNOWLEDGEMENTS

This work has been supported by the EPSRC via the 'UK Quantum Communications Hub' (EP/M013472/1) and by the European Commission via 'Continuous Variable Quantum Communications' (CiViQ, Project ID: 820466). The authors would like to thank Satoshi Ishizaka, Sam Braunstein, Seth Lloyd, Gaetana Spedalieri, and Zhi-Wei Wang for feedback.

AUTHOR CONTRIBUTIONS

All authors contributed to prove the main theoretical results of the work. S.P. developed the basic idea and methodology, steered the research project, wrote the main manuscript and Supplementary Sections 4 and 5. R.L. wrote Supplementary Section 3. C.L wrote Supplementary Sections 2 and 4. J.P. contributed to refine Lemma 1 and to study the PBT simulation of amplitude damping channels, besides writing Supplementary Section 1.

ADDITIONAL INFORMATION

Supplementary information accompanies the paper on the *npj Quantum Information* website (https://doi.org/10.1038/s41534-019-0162-y).

Competing interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

REFERENCES

1. Helstrom, C. W. *Quantum Detection and Estimation Theory*. (Academic, New York, 1976).
2. Watrous, J. *The theory of quantum information* (Cambridge Univ. Press, Cambridge, 2018).
3. Holevo, A. *Quantum Systems, Channels, Information: A Mathematical Introduction* (De Gruyter, Berlin, 2012).
4. Nielsen, M. A. & Chuang, I. L. *Quantum computation and quantum information* (Cambridge Univ. Press, Cambridge, 2010).
5. Weedbrook, C. et al. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621 (2012).
6. Audenaert, K. M. R. et al. Discriminating states: the quantum Chernoff Bound. *Phys. Rev. Lett.* **98**, 160501 (2007).
7. Calsamiglia, J., Munoz-Tapia, R., Masanes, L., Acin, A. & Bagan, E. The quantum Chernoff bound as a measure of distinguishability between density matrices: application to qubit and Gaussian states. *Phys. Rev. A* **77**, 032311 (2008).
8. Pirandola, S. & Lloyd, S. Computable bounds for the discrimination of Gaussian states. *Phys. Rev. A* **78**, 012331 (2008).
9. Audenaert, K. M. R., Nussbaum, M., Szkola, A. & Verstraete, F. Asymptotic error rates in quantum hypothesis testing. *Commun. Math. Phys.* **279**, 251 (2008).
10. Spedalieri, G. & Braunstein, S. L. Asymmetric quantum hypothesis testing with Gaussian states. *Phys. Rev. A* **90**, 052307 (2014).
11. Acin, A. Statistical distinguishability between unitary operations. *Phys. Rev. Lett.* **87**, 177901 (2001).
12. Sacchi, M. Entanglement can enhance the distinguishability of entanglement-breaking channels. *Phys. Rev. A* **72**, 014305 (2005).
13. Wang, G. & Ying, M. Unambiguous discrimination among quantum operations. *Phys. Rev. A* **73**, 042301 (2006).
14. Childs, A., Preskill, J. & Renes, J. Quantum information and precision measurement. *J. Mod. Opt.* **47**, 155 (2000).
15. Invernizzi, C., Paris, M. G. A. & Pirandola, S. Optimal detection of losses by thermal probes. *Phys. Rev. A* **84**, 022334 (2011).
16. Hayashi, M. Discrimination of two channels by adaptive methods and its application to quantum system. *IEEE Trans. Inf. Theory* **55**, 3807 (2009).
17. Pirandola, S. & Lupo, C. Ultimate precision of adaptive noise estimation. *Phys. Rev. Lett.* **118**, 100502 (2017).
18. Pirandola, S., Bardhan, B. R., Gehring, T., Weedbrook, C. & Lloyd, S. Advances in photonic quantum sensing. *Nat. Photon.* **12**, 724–733 (2018).
19. Harrow, A. W., Hassidim, A., Leung, D. W. & Watrous, J. Adaptive versus non-adaptive strategies for quantum channel discrimination. *Phys. Rev. A* **81**, 032339 (2010).
20. Paulsen, V. I. *Completely Bounded Maps and Operator Algebras* (Cambridge Univ. Press, Cambridge, 2002).
21. Ishizaka, S. & Hiroshima, T. Asymptotic teleportation scheme as a universal programmable quantum processor. *Phys. Rev. Lett.* **101**, 240501 (2008).
22. Ishizaka, S. & Hiroshima, T. Quantum teleportation scheme by selecting one of multiple output ports. *Phys. Rev. A* **79**, 042306 (2009).
23. Ishizaka, S. Some remarks on port-based teleportation. Preprint at https://arxiv.org/abs/1506.01555 (2015).
24. Wang, Z.-W. & Braunstein, S. L. Higher-dimensional performance of port-based teleportation. *Sci. Rep.* **6**, 33004 (2016).
25. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017). Preprint at https://arxiv.org/abs/1510.08863 (2015).
26. Pirandola, S. et al. Theory of channel simulation and bounds for private communication. *Quantum Sci. Technol.* **3**, 035009 (2018).
27. Pirandola, S., Laurenza, R. & Braunstein, S. L. Teleportation simulation of bosonic Gaussian channels: strong and uniform convergence. *Eur. Phys. J. D.* **72**, 162 (2018).
28. Lloyd, S. Enhanced sensitivity of photodetection via quantum illumination. *Science* **321**, 1463 (2008).
29. Tan, S.-H. et al. Quantum illumination with Gaussian states. *Phys. Rev. Lett.* **101**, 253601 (2008).
30. Shapiro, J. H. & Lloyd, S. Quantum illumination versus coherent-state target detection. *New J. Phys.* **11**, 063045 (2009).
31. Zhang, Z., Tengner, M., Zhong, T., Wong, F. N. C. & Shapiro, J. H. Entanglement's benefit survives an entanglement-breaking channel. *Phys. Rev. Lett.* **111**, 010501 (2013).
32. Lopaeva, E. D. et al. Experimental realization of quantum illumination. *Phys. Rev. Lett.* **110**, 153603 (2013).
33. Zhang, Z., Mouradian, S., Wong, F. N. C. & Shapiro, J. H. Entanglement-enhanced sensing in a lossy and noisy environment. *Phys. Rev. Lett.* **114**, 110506 (2015).
34. Barzanjeh, S. et al. Microwave quantum illumination. *Phys. Rev. Lett.* **114**, 080503 (2015).
35. Weedbrook, C., Pirandola, S., Thompson, J., Vedral, V. & Gu, M. How discord underlies the noise resilience of quantum illumination. *New J. Phys.* **18**, 043027 (2016).
36. Nielsen, M. A. & Chuang, I. L. Programmable quantum gate arrays. *Phys. Rev. Lett.* **79**, 321 (1997).
37. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys.* **2**, 51 (2019). Preprint at https://arxiv.org/abs/1601.00966 (2016).
38. Laurenza, R. & Pirandola, S. General bounds for sender-receiver capacities in multipoint quantum communications. *Phys. Rev. A* **96**, 032318 (2017).
39. Laurenza, R., Braunstein, S. L. & Pirandola, S. Finite-resource teleportation stretching for continuous-variable systems. *Sci. Rep.* **8**, 15267 (2018). Preprint at https://arxiv.org/abs/1706.06065 (2017).
40. Cope, T. P. W., Hetzel, L., Banchi, L. & Pirandola, S. Simulation of non-Pauli channels. *Phys. Rev. A* **96**, 022323 (2017).
41. Cope, T. P. W. & Pirandola, S. Adaptive estimation and discrimination of Holevo-Werner channels. *Quantum Meas. Quantum Metrol.* **4**, 44–52 (2017).
42. Fuchs, C. A. & van de Graaf, J. Cryptographic distinguishability measures for quantum mechanical states. *IEEE Trans. Inf. Theory* **45**, 1216 (1999).
43. Pinsker, M. S *Information and Information Stability of Random Variables and Processes*. (Holden Day, San Francisco, 1964).
44. Carlen, E. A. & Lieb, E. H. Bounds for entanglement via an extension of strong subadditivity of entropy. *Lett. Math. Phys.* **101**, 1–11 (2012).
45. Tsang, M., Nair, R. & Lu, X.-M. Quantum theory of superresolution for two incoherent optical point sources. *Phys. Rev. X* **6**, 031033 (2016).
46. Lupo, C. & Pirandola, S. Ultimate precision bound of quantum and subwavelength imaging. *Phys. Rev. Lett.* **117**, 190802 (2016).
47. Nair, R. & Tsang, M. Far-field superresolution of thermal electromagnetic sources at the quantum limit. *Phys. Rev. Lett.* **117**, 190801 (2016).
48. Cooney, T., Mosonyi, M. & Wilde, M. M. Strong converse exponents for a quantum channel discrimination problem and quantum-feedback-assisted communication. *Comm. Math. Phys.* **344**, 797–829 (2016).
49. De Palma, G. & Borregaard, J. The minimum error probability of quantum illumination. *Phys. Rev. A* **98**, 012101 (2018).
50. Pirandola, S. Quantum reading of a classical digital memory. *Phys. Rev. Lett.* **106**, 090504 (2011).
51. Pirandola, S., Lupo, C., Giovannetti, V., Mancini, S. & Braunstein, S. L. Quantum reading capacity. *New J. Phys.* **13**, 113012 (2011).
52. Dall'Arno, M. et al. Experimental implementation of unambiguous quantum reading. *Phys. Rev. A* **85**, 012308 (2012).
53. Dall'Arno, M., Bisio, A. & D'Ariano, G. M. Ideal quantum reading of optical memories. *Int. J. Quant. Inf.* **10**, 1241010 (2012).
54. Spedalieri, G. Cryptographic aspects of quantum reading. *Entropy* **17**, 2218–2227 (2015).
55. Braunstein, S. L. & Caves, C. M. Statistical distance and the geometry of quantum states. *Phys. Rev. Lett.* **72**, 3439 (1994).
56. Braunstein, S. L., Caves, C. M. & Milburn, G. J. Generalized uncertainty relations: theory, examples, and Lorentz invariance. *Ann. Phys.* **247**, 135–173 (1996).
57. Paris, M. G. A. Quantum estimation for quantum technology. *Int. J. Quant. Inf.* **7**, 125–137 (2009).
58. Giovannetti, V., Lloyd, S. & Maccone, L. Advances in quantum metrology. *Nat. Photon.* **5**, 222 (2011).
59. Braun, D. et al. Quantum enhanced measurements without entanglement. *Rev. Mod. Phys.* **90**, 035006 (2018).
60. Doukas, J., Adesso, G., Pirandola, S. & Dragan, A. Discriminating quantum field theories in non-inertial frames. *Class. Quantum Grav.* **32**, 035013 (2015).
61. Majenz, C. *Entropy in Quantum Information Theory, Communication and Cryptography*. PhD thesis, University of Copenhagen. (2017).
62. Nechita, I. et al. Almost all quantum channels are equidistant. *J. Math. Phys.* **59**, 052201 (2018).