

Exact solution for the quantum and private capacities of bosonic dephasing channels

Ludovico Lami^{1,*} and Mark M. Wilde^{2,3,†}

¹*Institut für Theoretische Physik und IQST, Universität Ulm, Albert-Einstein-Allee 11, D-89069 Ulm, Germany*

²*Hearne Institute for Theoretical Physics, Department of Physics and Astronomy, and Center for Computation and Technology, Louisiana State University, Baton Rouge, Louisiana 70803, USA*

³*School of Electrical and Computer Engineering, Cornell University, Ithaca, New York 14850, USA*

(Dated: May 13, 2022)

The capacities of noisy quantum channels capture the ultimate rates of information transmission across quantum communication lines, and the quantum capacity plays a key role in determining the overhead of fault-tolerant quantum computation platforms. In the case of bosonic systems, central to many applications, no closed formulas for these capacities were known for bosonic dephasing channels, a key class of non-Gaussian channels modelling, e.g., noise affecting superconducting circuits or fiber-optic communication channels. Here we provide the first exact calculation of the quantum, private, two-way assisted quantum, and secret-key agreement capacities of all bosonic dephasing channels. We prove that they are equal to the relative entropy of the distribution underlying the channel to the uniform distribution. Our result solves a problem that has been open for over a decade, having been posed originally by [Jiang & Chen, *Quantum and Nonlinear Optics* 244, 2010].

I. INTRODUCTION

One of the great promises of quantum information science is that remarkable tasks can be achieved by encoding information into quantum systems [1]. In principle, algorithms executed on quantum computers can factor large integers [2, 3], simulate complex physical dynamics [4, 5], solve unstructured search problems with proven speedups [6–8], and perform linear-algebraic manipulations on large matrices encoded into quantum systems [9, 10]. Additionally, ordinary (“classical”) information can be transmitted securely over quantum channels by means of quantum key distribution [11–13].

However, all of these possibilities are hindered in practice because all quantum systems are subject to decoherence [14, 15]. The most extreme form of decoherence involves a coherent superposition state $|\psi\rangle := \sum_n c_n |n\rangle$ being reduced to an incoherent probabilistic mixture of the states $\{|n\rangle\}_n$, such that the state of the system is $|n\rangle$ with probability $|c_n|^2$. If this happens, then the capabilities of quantum information processing systems are no greater than those of classical systems. Fortunately, with delicate sleight of hand in various experimental platforms or even inherent robustness in some of them, less extreme forms of decoherence can occur. To understand this more nuanced form of decoherence, let us describe the state of the system equivalently in terms of the density operator

$$|\psi\rangle\langle\psi| = \sum_{n,m} c_n c_m^* |n\rangle\langle m|. \quad (1)$$

A simple example of a decoherence process then takes the above density operator to

$$\sum_{n,m} c_n c_m^* e^{-\frac{\gamma}{2}(n-m)^2} |n\rangle\langle m|, \quad (2)$$

in which $\gamma > 0$ is related to the rate or strength of the decoherence. By inspecting the expression for the evolved density operator, we see that this process has the effect of reducing the magnitude of the off-diagonal components of the density matrix, while retaining the magnitude of the diagonal components. In the limit $\gamma \rightarrow \infty$, the decoherence process reduces to the extreme form mentioned above, such that all off-diagonal components are annihilated. We note here that this process is also called dephasing because it reduces or eliminates relative phases. For example, the state $\frac{1}{\sqrt{d}} \sum_n |n\rangle$ is perfectly distinguishable from the state $\frac{1}{\sqrt{d}} \sum_n e^{2\pi i n/d} |n\rangle$, where d is the dimension of the system. If the relative phases (i.e., the off-diagonal elements of the corresponding density matrices) are eliminated, then the states are not distinguishable at all.

Decoherence is a ubiquitous phenomenon affecting all quantum physical systems. In fact, in various platforms for quantum computation, experimentalists employ the T2 time as a phenomenological quantity that roughly measures the time that it takes for a coherent superposition to decohere to a probabilistic mixture [16, 17]. Dephasing noise in some cases is considered to be the dominant source of errors affecting quantum information encoded into superconducting systems [18], as well as other platforms [19, 20] (see also [21–23]). If those systems are employed to carry out quantum computation, then the errors must be amended by means of error-correcting codes, which typically causes expensive overheads in the amount of physical qubits needed. Not only does dephasing affect quantum computers, but it also affects quantum communication systems. Indeed, temperature fluctuations [24] or Kerr nonlinearities [25, 26] in a fiber, imprecision in the path length of a fiber [27], or the lack of a common phase reference between sender and receiver [28, Section II-B] lead to decoherence as well, and this can affect quantum communication and key distribution schemes adversely.

Many of the aforementioned forms of decoherence can be unified under a single model, known as the bosonic dephasing channel [29, 30]. The action of such a channel on the density

* ludovico.lami@gmail.com

† wilde@cornell.edu

operator ρ of a single-mode bosonic system is given by

$$\mathcal{N}_p(\rho) := \int_{-\pi}^{\pi} d\phi p(\phi) e^{-ia^\dagger a \phi} \rho e^{ia^\dagger a \phi}, \quad (3)$$

where p is a probability density function on the interval $[-\pi, \pi]$ and $a^\dagger a$ is the photon number operator. Since each unitary operator $e^{-ia^\dagger a \phi}$ realizes a phase shift of the state ρ , the action of the channel \mathcal{N}_p is to randomize the phase of this state according to the probability density p . To understand this channel a bit more and to relate to the previous discussion, let us consider representing the density operator ρ in the photon number basis as $\rho = \sum_{n,m} \rho_{nm} |n\rangle\langle m|$. Then it is a straightforward calculation to show that

$$\mathcal{N}_p(\rho) = \sum_{n,m} \rho_{nm} (T_p)_{nm} |n\rangle\langle m|, \quad (4)$$

where

$$(T_p)_{nm} := \int_{-\pi}^{\pi} d\phi p(\phi) e^{i\phi(n-m)}. \quad (5)$$

By inspecting (4), we see that the effect of the channel generalizes the action in (2). Thus, the channel preserves diagonal elements of ρ , but reduces the magnitude of the off-diagonal elements, a key signature of decoherence. We note here that multimode versions of the channel in (3) have been defined in [28, Section II-B] and studied further in [31, 32]. As the name suggests, the bosonic dephasing channel can be seen as a generalization to bosonic systems of the qudit dephasing channel [29, 33].

Of primary interest is understanding the information-processing capabilities of the bosonic dephasing channel in (3). We can do so by means of the formalism of quantum Shannon theory [34–38], in which we assume that the channel acts many times to affect multiple quantum systems. Not only does this formalism model dephasing that acts on quantum information encoded in a memory, as in superconducting systems, but also dephasing that affects communication systems. Here, a key quantity of interest is the quantum capacity $Q(\mathcal{N}_p)$ of the bosonic dephasing channel \mathcal{N}_p , which is equal to the largest rate at which quantum information can be faithfully sustained in the presence of dephasing, such that the error probability of decoding correctly decreases to zero as the number of channel uses becomes large [39–44]. The quantum capacity has been traditionally studied with applications to quantum communication in mind; however, recent evidence [45] indicates that it is also relevant for understanding the overhead of fault-tolerant quantum computation, i.e., the fundamental ratio of physical to logical qubits to perform quantum computation indefinitely with little chance of error. The private capacity $P(\mathcal{N}_p)$ is another operational quantity of interest [44, 46], being the largest rate at which private classical information can be faithfully transmitted over many independent uses of the channel \mathcal{N}_p . One can also consider both of these capacities in the scenario in which classical processing or classical communication is allowed for free between every channel use [47, 48], and here we denote the respective quantities by $Q_{\leftrightarrow}(\mathcal{N}_p)$ and $P_{\leftrightarrow}(\mathcal{N}_p)$. The secret-key-agreement capacity $P_{\leftrightarrow}(\mathcal{N}_p)$ is directly related

to the rate at which quantum key distribution is possible over the channel [48], and as such, it is a fundamental limit of experimental interest. Understanding all of these capacities is essential for the forthcoming quantum internet [49, 50], which will consist of various nodes in a network exchanging quantum and private information using the principles of quantum information science.

We note here that while the quantum capacity [29, 30] and the assisted quantum capacity [51] of the bosonic dephasing channel \mathcal{N}_p in (3) have been investigated, neither of them has been calculated so far. The determination of the quantum capacity of this channel, in particular, has been an open problem since [29]. The main difficulty is that \mathcal{N}_p is in general a non-Gaussian channel, which makes the techniques in [52, 53] inapplicable.

One can also study strong converse capacities, which sharpen the interpretation of capacity. In short, the strong converse capacity is the smallest communication rate such that the error probability in decoding necessarily tends to one as the number of channel uses becomes large (see [38] for a detailed account of strong converse capacities). If the usual capacity is equal to the strong converse capacity, then we say that the strong converse property holds for the channel under consideration, and the implication is that the capacity demarcates a very sharp dividing line between achievable and unachievable rates for communication. The strong converse capacities for quantum communication and private communication have been considered in a general context previously in [54, 55]. We let $Q^\dagger(\mathcal{N}_p)$, $P^\dagger(\mathcal{N}_p)$, $Q_{\leftrightarrow}^\dagger(\mathcal{N}_p)$, and $P_{\leftrightarrow}^\dagger(\mathcal{N}_p)$ denote the various strong converse capacities for the communication scenarios mentioned above. By definition, the inequality $Q(\mathcal{N}_p) \leq Q^\dagger(\mathcal{N}_p)$ holds, and similar relations exist between the other capacities and their strong converse counterparts (see, e.g., Eqs. (5.6)–(5.13) of [55]).

II. RESULTS

In this paper, we completely solve all of the aforementioned capacities of the bosonic dephasing channels, finding that they all coincide and are given by the following simple expression:

$$\begin{aligned} \mathcal{C}(\mathcal{N}_p) &:= \log_2(2\pi) - h(p) \\ &= Q(\mathcal{N}_p) = P(\mathcal{N}_p) = Q_{\leftrightarrow}(\mathcal{N}_p) = P_{\leftrightarrow}(\mathcal{N}_p) \\ &= Q^\dagger(\mathcal{N}_p) = P^\dagger(\mathcal{N}_p) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_p) = P_{\leftrightarrow}^\dagger(\mathcal{N}_p), \end{aligned} \quad (6)$$

where

$$h(p) := - \int d\phi p(\phi) \log_2(p(\phi)) \quad (7)$$

is the differential entropy of the probability density p . As discussed in the next section, our result extends to all multimode bosonic dephasing channels, thus closing out the problem in general. We note here that the first expression in (6) can be written in terms of the relative entropy as

$$\log_2(2\pi) - h(p) = D(p||u), \quad (8)$$

where u is the uniform probability density on the interval $[-\pi, \pi]$, and the relative entropy is defined as

$$D(r||s) := \int d\phi r(\phi) \log_2 \left(\frac{r(\phi)}{s(\phi)} \right) \quad (9)$$

for general probability densities r and s . By invoking basic properties of relative entropy, this rewriting indicates that all of the capacities are non-negative for every probability density p and they are equal to zero if and only if the density p is uniform, which represents a complete dephasing of the channel input state.

As Eq. (6) indicates, there is a remarkable simplification of the capacities for bosonic dephasing channels. The ultimate rate of private communication over these channels is no larger than the ultimate rate for quantum communication. Furthermore, unlimited classical communication between the sender and receiver does not enhance the capacities. Finally, the strong converse property holds, meaning that the rate $D(p||u)$ represents a very sharp dividing line between possible and impossible communication rates. As mentioned in the introduction, since dephasing is a prominent source of noise in both quantum communication and computation, we expect our finding to have practical relevance in both scenarios. Based on the recent findings of [45], we expect that $[D(p||u)]^{-1}$ can be related to the ultimate overhead (ratio of physical systems to logical qubits) of fault-tolerant quantum computation with superconducting systems, but further work is needed to demonstrate this definitively.

We prove our main result in Eq. (6) by establishing the following two inequalities:

$$Q(\mathcal{N}_p) \geq D(p||u), \quad (10)$$

$$P_{\leftrightarrow}^{\dagger}(\mathcal{N}_p) \leq D(p||u). \quad (11)$$

Proving (10)–(11) establishes the main result because $Q(\mathcal{N}_p)$ is the smallest among all of the capacities listed and $P_{\leftrightarrow}^{\dagger}(\mathcal{N}_p)$ is the largest. For a precise ordering of the various capacities, see Eqs. (5.6)–(5.13) of [55]. The proofs of the inequalities in (10) and (11) are quite different, and we provide an overview of them in the Methods section [56].

Multimode generalization

We also extend all of our results to all multimode bosonic dephasing channels, an example of which acts simultaneously on a collection of m bosonic modes as

$$\mathcal{N}_p^{(m)}(\rho) := \int_{[-\pi, \pi]^m} d^m \boldsymbol{\phi} p(\boldsymbol{\phi}) e^{-i \sum_j a_j^{\dagger} a_j \phi_j} \rho e^{i \sum_j a_j^{\dagger} a_j \phi_j}, \quad (12)$$

where $\boldsymbol{\phi} := (\phi_1, \dots, \phi_m)$, p is a probability density function on the hypercube $[-\pi, \pi]^m$, and $a_j^{\dagger} a_j$ is the photon number operator acting on the j^{th} mode. The eight capacities listed in (6) are all equal also for the channel $\mathcal{N}_p^{(m)}$, and we denote them by $\mathcal{E}(\mathcal{N}_p^{(m)})$. They are given by the formula

$$\mathcal{E}(\mathcal{N}_p^{(m)}) = m \log_2(2\pi) - h(p), \quad (13)$$

where

$$h(p) = - \int_{[-\pi, \pi]^m} d^m \boldsymbol{\phi} p(\boldsymbol{\phi}) \log_2 p(\boldsymbol{\phi}), \quad (14)$$

constituting a straightforward multimode generalization of (6). As a special case of (12), when p is concentrated on the line $\boldsymbol{\phi} = (\phi, \dots, \phi)$ and $\phi \in [-\pi, \pi]$ is uniformly distributed, one obtains the *completely* dephasing channel considered in [31, 32]. As our result confirms, the quantum and private capacities of this channel (without an energy constraint) are infinite for $m \geq 2$. This divergence is simply an artifact of the model, which requires all entries of $\boldsymbol{\phi}$ to be exactly equal. When this assumption is dropped in favor of an alternative probability density function p , our result yields a finite value of the capacity.

Examples

Let us first discuss some examples of bosonic dephasing channels and how the capacity formula $D(p||u)$ is evaluated for them.

a. Wrapped normal distribution. The most paradigmatic example of a bosonic dephasing channel is that corresponding to a normal distribution $\tilde{p}_{\gamma}(\phi) = (2\pi\gamma)^{-1/2} e^{-\phi^2/(2\gamma)}$ of the angle ϕ over the whole real line. This is the main example studied in [29, 30], which is based on a physical model discussed in those works. Here, $\gamma > 0$ denotes the variance of such a distribution: the larger γ , the larger the uncertainty of the rotation angle in (3), and therefore the stronger the dephasing on the input state. Since values of ϕ that differ modulo 2π can be identified, we obtain as an effective distribution p on $[-\pi, \pi]$ the *wrapped normal distribution*

$$p_{\gamma}(\phi) := \frac{1}{\sqrt{2\pi\gamma}} \sum_{k=-\infty}^{+\infty} e^{-\frac{1}{2\gamma}(\phi+2\pi k)^2}. \quad (15)$$

The matrix $T_{p_{\gamma}}$ obtained by plugging this distribution into (5) has entries $(T_{p_{\gamma}})_{nm} = e^{-\frac{\gamma}{2}(n-m)^2}$. The wrapped normal distribution was first found in connection with Brownian motion on a circle [57], and has been widely studied in the mathematical literature since [58, 59]. Using the expression for its differential entropy from [59, § 3.3], we find that

$$\mathcal{E}(\mathcal{N}_{p_{\gamma}}) = \log_2 \varphi(e^{-\gamma}) + \frac{2}{\ln 2} \sum_{k=1}^{\infty} \frac{(-1)^{k-1} e^{-\frac{\gamma}{2}(k^2+k)}}{k(1-e^{-k\gamma})}, \quad (16)$$

where $\varphi(q) := \prod_{k=1}^{\infty} (1-q^k)$ is the Euler function. In the physically relevant limit $\gamma \ll 1$ (but in practice already for $\gamma \lesssim 1$), p_{γ} and \tilde{p}_{γ} are both concentrated around 0, and their entropies are nearly identical. In this regime

$$\begin{aligned} \mathcal{E}(\mathcal{N}_{p_{\gamma}}) &\approx \frac{1}{2} \log_2 \frac{2\pi}{e\gamma} \\ &\approx \left(0.604 + \frac{1}{2} \log_2 \frac{1}{\gamma} \right) \text{ bits/channel use,} \end{aligned} \quad (17)$$

which demarcates the ultimate limitations on quantum and private communication in the presence of small dephasing noise. In the opposite case $\gamma \gg 1$, resorting to the series expansion for the Euler function, we find that [56]

$$\mathcal{E}(\mathcal{N}_{p_\gamma}) \approx \frac{e^{-\gamma}}{\ln 2}. \quad (18)$$

The above formula generalizes and makes quantitative the claim found in [30, § VI] that the quantum capacity of \mathcal{N}_{p_γ} vanishes exponentially for large γ .

An excellent approximation of the formula in (16) across the whole regime of $\gamma > 0$ is given by the expression

$$\max \left\{ \frac{1}{2} \log_2 \frac{2\pi}{e\gamma}, \frac{2}{\ln 2} e^{-\gamma} - \log_2 (1 + e^{-\gamma}) \right\}, \quad (19)$$

which differs from the true value in (16) by less than 4×10^{-3} .

b. Von Mises distribution. A better analogue of the normal distribution in the case of a circle is the *von Mises distribution*, given by

$$p_\lambda(\phi) := \frac{e^{\frac{1}{\lambda} \cos(\phi)}}{2\pi I_0(1/\lambda)}, \quad (20)$$

where $\lambda > 0$ is a parameter that plays a role analogous to that of γ above, and I_k is a modified Bessel function of the first kind. The matrix T_{p_λ} obtained in (5) has entries $(T_{p_\lambda})_{nm} = \frac{I_{|n-m|(1/\lambda)}}{I_0(1/\lambda)}$. Using the expression for the differential entropy of p_λ from [59, § 3.3], the capacities of the bosonic dephasing channel \mathcal{N}_{p_λ} can be expressed as

$$\mathcal{E}(\mathcal{N}_{p_\lambda}) = \frac{1}{\ln 2} \frac{I_1(1/\lambda)}{\lambda I_0(1/\lambda)} - \log_2 I_0(1/\lambda). \quad (21)$$

c. Wrapped Cauchy distribution. As a final example, we consider the wrapped Cauchy distribution. Recall that the Cauchy probability density function is defined as $\tilde{p}_\kappa(\phi) = \frac{\sqrt{\kappa}}{\pi} \frac{1}{\kappa + \phi^2}$. Although this density is normalized, it does not have a finite mean or variance. Analogous to the wrapped normal distribution, the wrapped Cauchy probability density function is given by

$$p_\kappa(\phi) := \sum_{k=-\infty}^{+\infty} \tilde{p}_\kappa(\phi + 2\pi k) = \frac{1}{2\pi} \frac{\sinh(\sqrt{\kappa})}{\cosh(\sqrt{\kappa}) - \cos \phi}. \quad (22)$$

The corresponding matrix obtained in (5) has exponentially decaying off-diagonal entries $(T_{p_\kappa})_{nm} = e^{-\sqrt{\kappa}|n-m|}$. Since the differential entropy of $p_\kappa(\phi)$ is equal to $\log_2(2\pi(1 - e^{-2\sqrt{\kappa}}))$, the various capacities of \mathcal{N}_{p_κ} evaluate to

$$\mathcal{E}(\mathcal{N}_{p_\kappa}) = \log_2 \frac{1}{1 - e^{-2\sqrt{\kappa}}}. \quad (23)$$

In Figure 1, we plot the capacities given in (16), (21), and (23), respectively for the wrapped normal distribution, the von Mises distribution, and the wrapped Cauchy distribution. The units of the vertical axis are qubits or private bits per channel use, and the horizontal axis is the main parameter governing the various distributions.

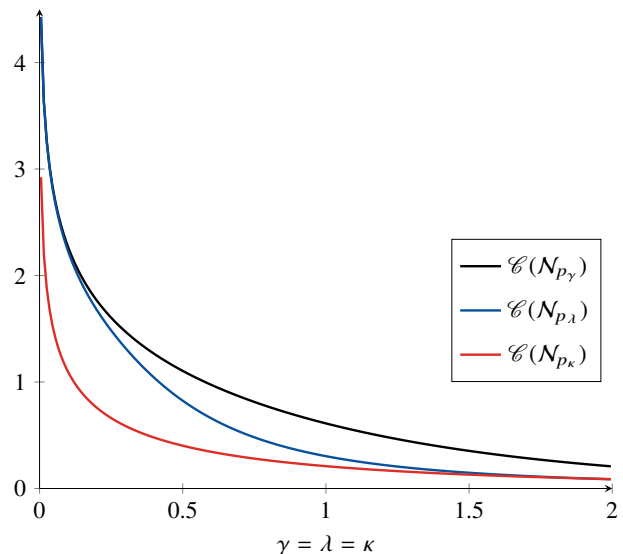


FIG. 1: The capacities of the bosonic dephasing channels associated with the wrapped normal distribution (\mathcal{N}_{p_γ}), the von Mises distribution (\mathcal{N}_{p_λ}), and the wrapped Cauchy distribution (\mathcal{N}_{p_κ}).

III. DISCUSSION

Our main result represents important progress for quantum information theory, solving the capacities of a physically relevant class of non-Gaussian bosonic channels. While for the case of bosonic Gaussian channels many capacities have been solved in prior work [52, 55, 60–64], we are not aware of any other class of non-Gaussian channels that represent relevant models of noise in bosonic systems and whose capacity can be computed to yield a nontrivial value (neither zero nor infinite).

Our formula can be seen as a natural generalization to bosonic systems of that given in [33, 54, 64] for the quantum and private capacities of the qudit dephasing channel. However, the similarity of the final formula should not obscure the fact that the techniques used for its derivation are quite different. In particular, a key technical tool employed here is the Szegő theorem from asymptotic linear algebra [65–67], in addition to a teleportation simulation argument that is rather different from those presented previously.

Going forward from here, it would be interesting to address the capacities of bosonic lossy dephasing channels, in which both loss and dephasing act at the same time. Specifically, such channels are modeled as the serial concatenation $\mathcal{L}_\eta \circ \mathcal{N}_p$, where \mathcal{L}_η is a pure loss channel of transmissivity $\eta \in [0, 1]$. Since the channel \mathcal{L}_η is phase covariant, it does not matter which channel acts first, i.e., $\mathcal{L}_\eta \circ \mathcal{N}_p = \mathcal{N}_p \circ \mathcal{L}_\eta$. This channel is a realistic model for communication and computation, given that both kinds of noises are relevant in these systems. Some preliminary progress on this channel has been reported quite recently in [68]. Our result here, combined with the main result of [61] and a data-processing bottlenecking argument [61, 69], leads to the following upper bound on the quantum and private

capacities of the bosonic lossy dephasing channel:

$$\begin{aligned} Q(\mathcal{L}_\eta \circ \mathcal{N}_p) &\leq P(\mathcal{L}_\eta \circ \mathcal{N}_p) \\ &\leq \min\{P(\mathcal{L}_\eta), P(\mathcal{N}_p)\} \\ &= \min\left\{\left(\log_2(\eta/(1-\eta))\right)_+, D(p\|u)\right\}, \end{aligned} \quad (24)$$

where $x_+ := \max\{x, 0\}$. By the same argument, but invoking the results of [55, 64], the following upper bounds hold for the quantum and private capacities assisted by classical communication:

$$\begin{aligned} Q_{\leftrightarrow}(\mathcal{L}_\eta \circ \mathcal{N}_p) &\leq Q_{\leftrightarrow}^{\dagger}(\mathcal{L}_\eta \circ \mathcal{N}_p), P_{\leftrightarrow}(\mathcal{L}_\eta \circ \mathcal{N}_p) \\ &\leq P_{\leftrightarrow}^{\dagger}(\mathcal{L}_\eta \circ \mathcal{N}_p) \\ &\leq \min\{\log_2(1/(1-\eta)), D(p\|u)\}. \end{aligned} \quad (25)$$

The same data-processing argument can be employed for bosonic dephasing channels composed with other common bosonic Gaussian channels in order to obtain upper bounds on the composed channels' capacities, while using known upper bounds from prior work [55, 64, 70–73].

It also remains open to determine the energy-constrained quantum and private capacities of bosonic dephasing channels, as well as their classical-communication-assisted counterparts, which was the main focus of the recent papers [30, 51]. At the least (and perhaps obviously), the lower bound in (30) is a legitimate lower bound on the energy-constrained quantum capacity of \mathcal{N}_p when the mean photon number of the channel input cannot exceed $d - 1$. Also, it is clear that the energy-constrained classical capacity of \mathcal{N}_p is equal to $g(E) := (E + 1) \log_2(E + 1) - E \log_2 E$, where E is the energy constraint. This identity, which can be proved as in [31, § 3.1] leveraging insights from [74], depends essentially on the fact that Fock states can be perfectly transmitted through any bosonic dephasing channel without losing their purity. Finally, it is an open question to determine the energy-constrained entanglement-assisted classical capacity of bosonic dephasing channels. A formula for the general case is well known [75], but evaluating it and finding an analytical formula is what remains open.

In a forthcoming work [76], we employ a similar approach to establish the ultimate limitations on discrimination and estimation of all bosonic dephasing channels, solving a question posed in part in [77]. In particular, we find that two bosonic dephasing channels \mathcal{N}_{p_1} and \mathcal{N}_{p_2} can be discriminated at a rate equal to functions of their underlying probability densities p_1 and p_2 . For example, in the Stein setting of asymmetric channel discrimination, we show that the rate is given by the relative entropy $D(p_1\|p_2)$, and in the Chernoff setting of symmetric channel discrimination, it is given by the Chernoff information of these densities. If the goal is to estimate which channel is chosen from a parameterized family $\{\mathcal{N}_p\}_p$ of bosonic dephasing channels, then the error achieved in doing so is limited by the Fisher information of the underlying family $\{p(\phi)\}_p$ of probability densities. For all of these results, the rates or error scaling are achieved by transmitting a uniform superposition $\sum_{n=0}^{d-1} |n\rangle / \sqrt{d}$ of photon number states, applying a quantum Fourier transform, and then measuring in the photon number basis. One again needs to take the limit $d \rightarrow \infty$. Upper bounds

on the rates are given by the method of [78], resulting from the observation that bosonic dephasing channels can be realized by applying a common channel on the input and a classical environment state chosen according to the underlying probability density p (for the general multimode case, the common channel is merely to apply the phase shift $e^{-i \sum_j a_j^\dagger a_j \phi_j}$ to the input and then discard the environment system).

IV. METHODS

In this section, we provide a short overview of the techniques used to prove our main result (6). As discussed previously, we only need to justify the inequalities in (10)–(11), which together enforce (6). See [56] for detailed proofs.

To see (10), let us recall that the coherent information of a quantum channel is a lower bound on its quantum capacity [42–44]. Specifically, the following inequality holds for a general channel \mathcal{N} :

$$Q(\mathcal{N}) \geq \sup_{\rho} \{H(\mathcal{N}(\rho)) - H((\text{id} \otimes \mathcal{N})(\psi^\rho))\}, \quad (26)$$

where the von Neumann entropy of a state σ is defined as $H(\sigma) := -\text{Tr}[\sigma \log_2 \sigma]$, the optimization is over every state ρ that can be transmitted into the channel \mathcal{N} , and ψ^ρ is a purification of ρ (such that one recovers ρ after a partial trace). We can apply this lower bound to the bosonic dephasing channel \mathcal{N}_p . For a fixed photon number $d - 1$, let us choose ρ to be the maximally mixed state of dimension d , i.e., $\rho = \tau_d := \frac{1}{d} \sum_{n=0}^{d-1} |n\rangle\langle n|$. This state is purified by the maximally entangled state $\Phi_d := \frac{1}{d} \sum_{n,m=0}^{d-1} |n\rangle\langle m| \otimes |n\rangle\langle m|$. To evaluate the first term in (26), consider from (4) and (5) that the output state is maximally mixed, i.e., $\mathcal{N}_p(\tau_d) = \tau_d$, because the input state τ_d has no off-diagonal elements and the diagonal elements of the matrix T_p in (5) are all equal to one. Thus, we find that $H(\mathcal{N}_p(\tau_d)) = \log_2 d$. For the second term in (26), we again apply (4) and (5) to determine that

$$\begin{aligned} \omega_{p,d} &:= (\mathbb{1} \otimes \mathcal{N}_p)(\Phi_d) \\ &= \frac{1}{d} \sum_{n,m=0}^{d-1} (T_p)_{nm} |n\rangle\langle m| \otimes |n\rangle\langle m|. \end{aligned} \quad (27)$$

As the entropy is invariant under the action of an isometry, and the isometry $|n\rangle \rightarrow |n\rangle |n\rangle$ takes the state

$$\frac{T_d}{d} := \frac{1}{d} \sum_{n,m=0}^{d-1} (T_p)_{nm} |n\rangle\langle m| \quad (28)$$

to $\omega_{p,d}$, we find that the entropy $H(\omega_{p,d})$ reduces to

$$H(\omega_{p,d}) = H(T_d/d). \quad (29)$$

By a straightforward calculation, we then find that

$$\begin{aligned} H(\mathcal{N}_p(\tau_d)) - H(\omega_{p,d}) &= \log_2 d - H(T_d/d) \\ &= \frac{1}{d} \text{Tr}[T_d \log_2 T_d]. \end{aligned} \quad (30)$$

This establishes the value in (30) to be an achievable rate for quantum communication over \mathcal{N}_p . Since this lower bound holds for every photon number $d-1 \in \mathbb{N}$, we can then take the limit $d \rightarrow \infty$ and apply the Szegő theorem [65–67] to conclude that the following value is also an achievable rate:

$$\begin{aligned} & \lim_{d \rightarrow \infty} \frac{1}{d} \text{Tr}[T_d \log_2 T_d] \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} d\phi \, 2\pi p(\phi) \log_2(2\pi p(\phi)) \\ &= D(p||u). \end{aligned} \quad (31)$$

Thus, this establishes the lower bound in (10).

To prove the upper bound in (11), we apply a modified teleportation simulation argument. This kind of argument was introduced in [47, Section V], for the specific purpose of finding upper bounds on the quantum capacity assisted by classical communication, and it has been employed in a number of works since then [55, 61, 64, 79, 80]. Since we are interested in bounding the strong converse secret key agreement capacity $P_{\leftrightarrow}^{\dagger}(\mathcal{N}_p)$, we apply reasoning similar to that given in [55]. However, there are some critical differences in our approach here.

To begin, let us again consider the state in (27). As we show in [56], by performing the standard teleportation protocol [81] with the state in (27) as the entangled resource state, rather than the maximally entangled state, we can simulate the action of the channel \mathcal{N}_p on a fixed input state, up to an error that vanishes in the limit as $d \rightarrow \infty$. This key insight demonstrates that the state in (27) is approximately equivalent in a resource-theoretic sense to the channel \mathcal{N}_p . In more detail, we can express this observation in terms of the following equality: for every state ρ ,

$$\lim_{d \rightarrow \infty} \left\| (\text{id} \otimes \mathcal{N}_p)(\rho) - (\text{id} \otimes \mathcal{N}_{p,d})(\rho) \right\|_1 = 0, \quad (32)$$

where $\mathcal{N}_{p,d}(\sigma) := \mathcal{T}(\sigma \otimes \omega_{p,d})$ is the channel resulting from the teleportation simulation. That is, the simulating channel $\mathcal{N}_{p,d}$ is realized by sending in the maximally entangled state Φ_d to \mathcal{N}_p , which generates $\omega_{p,d}$, and then acting on the input state σ and the resource state $\omega_{p,d}$ with the standard teleportation protocol \mathcal{T} . By invoking the main insight from [82, 83] (as used later in [48]), we next note that a protocol for secret key agreement over the channel is equivalent to one for which the goal is to distill a bipartite private state. Such a protocol involves only two parties, and thus the tools of entanglement theory come into play [82, 83].

Now let $\mathcal{P}_{n,\epsilon}$ denote a general, fixed protocol for secret key agreement, involving n uses of the channel \mathcal{N}_p and achieving an error ϵ for generating a bipartite private state of rate $R_{n,\epsilon}$ (where the units of $R_{n,\epsilon}$ are secret key bits per channel use). By using the two aforementioned tools, teleportation simulation and the reduction from secret key agreement to bipartite private distillation, the protocol $\mathcal{P}_{n,\epsilon}$ can be approximately simulated by the action of a single LOCC channel on n copies of the resource state $\omega_{p,d}$. Associated with this simulation are two trace norm errors ϵ and δ_d , the first of which is the error of the original protocol $\mathcal{P}_{n,\epsilon}$ in producing the desired

bipartite private state and the second of which is the error of the simulation. We then invoke Eq. (5.37) of [55] to establish the following inequality, which, for the fixed protocol $\mathcal{P}_{n,\epsilon}$, relates the rate $R_{n,\epsilon}$ at which secret key can be distilled to the aforementioned errors and an entanglement measure called sandwiched Rényi relative entropy of entanglement:

$$R_{n,\epsilon} \leq \tilde{E}_{R,\alpha}(\omega_{p,d}) + \frac{2\alpha}{n(\alpha-1)} \log_2 \left(\frac{1}{1-\delta_d-\epsilon} \right), \quad (33)$$

where $\alpha > 1$ and the sandwiched Rényi relative entropy of entanglement of a general bipartite state ρ is defined as [55]

$$\tilde{E}_{R,\alpha}(\rho) := \inf_{\sigma \in \text{SEP}} \frac{2\alpha}{\alpha-1} \log_2 \left\| \rho^{1/2} \sigma^{(1-\alpha)/2\alpha} \right\|_{2\alpha}, \quad (34)$$

with SEP denoting the set of separable (unentangled) states. By choosing the separable state to be $(\text{id} \otimes \mathcal{N}_p)(\overline{\Phi}_d)$, where $\overline{\Phi}_d := \frac{1}{d} \sum_{n=0}^{d-1} |n\rangle\langle n| \otimes |n\rangle\langle n|$, we find that [56]

$$\tilde{E}_{R,\alpha}(\omega_{p,d}) \leq \frac{1}{\alpha-1} \log_2 \frac{1}{d} \text{Tr}[(T_d)^\alpha]. \quad (35)$$

Thus, we find that the following rate upper bound holds for the secret key agreement protocol $\mathcal{P}_{n,\epsilon}$ for all $d \in \mathbb{N}$:

$$\begin{aligned} R_{n,\epsilon} &\leq \frac{1}{\alpha-1} \log_2 \frac{1}{d} \text{Tr}[(T_d)^\alpha] \\ &\quad + \frac{2\alpha}{n(\alpha-1)} \log_2 \left(\frac{1}{1-\delta_d-\epsilon} \right), \end{aligned} \quad (36)$$

Since this bound holds for all $d \in \mathbb{N}$, we can take the limit $d \rightarrow \infty$ and then arrive at the following upper bound:

$$\begin{aligned} R_{n,\epsilon} &\leq \limsup_{d \rightarrow \infty} \left(\frac{1}{\alpha-1} \log_2 \frac{1}{d} \text{Tr}[(T_d)^\alpha] \right. \\ &\quad \left. + \frac{2\alpha}{n(\alpha-1)} \log_2 \left(\frac{1}{1-\delta_d-\epsilon} \right) \right) \\ &= D_\alpha(p||u) + \frac{2\alpha}{n(\alpha-1)} \log_2 \left(\frac{1}{1-\epsilon} \right). \end{aligned} \quad (37)$$

In the above, we again applied the Szegő theorem [65–67] to conclude that

$$\limsup_{d \rightarrow \infty} \frac{1}{\alpha-1} \log_2 \frac{1}{d} \text{Tr}[(T_d)^\alpha] = D_\alpha(p||u). \quad (38)$$

We also used the fact that $\lim_{d \rightarrow \infty} \delta_d = 0$, which is a consequence of (32). The bound in the last line only depends on the error ϵ of the original protocol $\mathcal{P}_{n,\epsilon}$ and the Rényi relative entropy

$$D_\alpha(p||u) := \frac{1}{\alpha-1} \log_2 \int_{-\pi}^{\pi} d\phi \, p(\phi)^\alpha u(\phi)^{1-\alpha}. \quad (39)$$

As such, it is a uniform upper bound, applying to all n -round secret-key-agreement protocols that generate a private state of rate $R_{n,\epsilon}$ and with error ϵ . Now noting that the n -shot secret key agreement capacity $P_{\leftrightarrow}(\mathcal{N}_p, n, \epsilon)$ is defined as the largest

rate $R_{n,\epsilon}$ that can be achieved by using the channel \mathcal{N}_p n times along with classical communication for free, while allowing for ϵ error, it follows from the uniform bound in (37) that

$$P_{\leftrightarrow}(\mathcal{N}_p, n, \epsilon) \leq D_\alpha(p\|u) + \frac{2\alpha}{n(\alpha-1)} \log_2\left(\frac{1}{1-\epsilon}\right), \quad (40)$$

holding for all $\alpha > 1$. Noting that the strong converse secret-key-agreement capacity is defined as

$$P_{\leftrightarrow}^\dagger(\mathcal{N}_p) := \sup_{\epsilon \in (0,1)} \limsup_{n \rightarrow \infty} P_{\leftrightarrow}(\mathcal{N}_p, n, \epsilon) \quad (41)$$

we take the limit $n \rightarrow \infty$ to find that

$$\begin{aligned} P_{\leftrightarrow}^\dagger(\mathcal{N}_p) &\leq \sup_{\epsilon \in (0,1)} \limsup_{n \rightarrow \infty} \left\{ D_\alpha(p\|u) + \frac{2\alpha}{n(\alpha-1)} \log_2\left(\frac{1}{1-\epsilon}\right) \right\} \\ &= D_\alpha(p\|u). \end{aligned} \quad (42)$$

This upper bound holds for all $\alpha > 1$. Thus, we can finally take the $\alpha \rightarrow 1$ limit, and use a basic property of Rényi relative entropy [84] to conclude the desired upper bound:

$$P_{\leftrightarrow}^\dagger(\mathcal{N}_p) \leq \lim_{\alpha \rightarrow 1} D_\alpha(p\|u) = D(p\|u). \quad (43)$$

This concludes the proof of the capacity formula (6) for the bosonic dephasing channel. The argument required to establish its multimode generalization (13) is very similar [56], with the only substantial technical difference being the application of the *multi-index* Szegő theorem [66, 67].

Acknowledgements. LL is supported by the Alexander von Humboldt Foundation.

-
- [1] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
- [2] P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.
- [3] P. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Review*, 41(2):303–332, 1999.
- [4] S. Lloyd. Universal quantum simulators. *Science*, 273(5278):1073–1078, 1996.
- [5] A. M. Childs, D. Maslov, Y. Nam, N. J. Ross, and Y. Su. Toward the first quantum simulation with quantum speedup. *Proceedings of the National Academy of Sciences of the U.S.A.*, 115(38):9456–9461, 2018.
- [6] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the 28th ACM Symposium on Theory of Computing (STOC)*, pages 212–219, 1996. arXiv:quant-ph/9605043.
- [7] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 79(2):325–328, 1997.
- [8] G. Brassard, P. Høyer, M. Mosca, and A. Tapp. Quantum amplitude amplification and estimation. In *Quantum Computation and Quantum Information: A Millennium Volume*, volume 305 of *Contemporary Mathematics Series*, pages 53–74. AMS, 2002. arXiv:quant-ph/0005055.
- [9] A. W. Harrow, A. Hassidim, and S. Lloyd. Quantum algorithm for linear systems of equations. *Physical Review Letters*, 103(15):150502, 2009.
- [10] A. Gilyén, Y. Su, G. Hao Low, and N. Wiebe. Quantum singular value transformation and beyond: exponential improvements for quantum matrix arithmetics. In *Proceedings of the 51st Annual ACM SIGACT Symposium on Theory of Computing*, pages 193–204, 2019. arXiv:1806.01838.
- [11] C. H. Bennett and G. Brassard. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, pages 175–179, 1984.
- [12] A. K. Ekert. Quantum cryptography based on Bell’s theorem. *Physical Review Letters*, 67:661–663, 1991.
- [13] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev. The security of practical quantum key distribution. *Reviews of Modern Physics*, 81(3):1301–1350, 2009. arXiv:0802.4155.
- [14] H. D. Zeh. On the interpretation of measurement in quantum theory. *Foundations of Physics*, 1(1):69–76, 1970.
- [15] M. Schlosshauer. Decoherence, the measurement problem, and interpretations of quantum mechanics. *Reviews of Modern Physics*, 76:1267–1305, 2005.
- [16] J. J. Bollinger, D. J. Heizen, W. M. Itano, S. L. Gilbert, and D. J. Wineland. A 303-MHz frequency standard based on trapped Be/sup +/ ions. *IEEE Transactions on Instrumentation and Measurement*, 40(2):126–128, 1991.
- [17] P. T. H. Fisk, M. J. Sellars, M. A. Lawn, C. Coles, A. G. Mann, and D. G. Blair. Very high Q microwave spectroscopy on trapped /sup 171/Yb/sup +/ ions: application as a frequency standard. *IEEE Transactions on Instrumentation and Measurement*, 44(2):113–116, 1995.
- [18] F. Brito, D. P. DiVincenzo, R. H. Koch, and M. Steffen. Efficient one- and two-qubit pulsed gates for an oscillator-stabilized Josephson qubit. *New Journal of Physics*, 10(3):033027 (33pp), 2008.
- [19] J. M. Taylor, H.-A. Engel, W. Dür, A. Yacoby, C. M. Marcus, P. Zoller, and M. D. Lukin. Fault-tolerant architecture for quantum computation using electrically controlled semiconductor spins. *Nature Physics*, 1(3):177–183, 2005.
- [20] C. Ospelkaus, C. E. Langer, J. M. Amini, K. R. Brown, D. Leibfried, and D. J. Wineland. Trapped-ion quantum logic gates based on oscillating magnetic fields. *Physical Review Letters*, 101:090502, 2008.
- [21] P. Aliferis and J. Preskill. Fault-tolerant quantum computation

- against biased noise. *Physical Review A*, 78:052331, 2008.
- [22] P. Aliferis, F. Brito, D. P. DiVincenzo, J. Preskill, M. Steffen, and B. M. Terhal. Fault-tolerant computing with biased-noise superconducting qubits: a case study. *New Journal of Physics*, 11(1):013061, 2009.
- [23] P. Brooks and J. Preskill. Fault-tolerant quantum computation with asymmetric Bacon-Shor codes. *Physical Review A*, 87:032310, 2013.
- [24] K. H. Wanser. Fundamental phase noise limit in optical fibres due to temperature fluctuations. *Electronics Letters*, 28:53–54(1), 1992.
- [25] J. P. Gordon and L. F. Mollenauer. Phase noise in photonic communications systems using linear amplifiers. *Optics Letters*, 15(23):1351–1353, 1990.
- [26] L. Kunz, M. G. A. Paris, and K. Banaszek. Noisy propagation of coherent states in a lossy Kerr medium. *Journal of the Optical Society of America B*, 35(2):214–222, 2018.
- [27] D. Derickson. *Fiber Optic Test and Measurement*. Prentice Hall PTR, 1998. ISBN 978-013534330-2.
- [28] S. D. Bartlett, T. Rudolph, and R. W. Spekkens. Reference frames, superselection rules, and quantum information. *Reviews of Modern Physics*, 79:555–609, 2007.
- [29] L.-Z. Jiang and X.-Y. Chen. Evaluating the quantum capacity of bosonic dephasing channel. In Qihuang Gong, Guang-Can Guo, and Yuen-Ron Shen, editors, *Quantum and Nonlinear Optics*, volume 7846, pages 244–249. International Society for Optics and Photonics, SPIE, 2010.
- [30] A. Arqand, L. Memarzadeh, and S. Mancini. Quantum capacity of a bosonic dephasing channel. *Physical Review A*, 102(4):042413, 2020.
- [31] M. Fanizza, M. Rosati, M. Skotiniotis, J. Calsamiglia, and V. Giovannetti. Squeezing-enhanced communication without a phase reference. *Quantum*, 5:608, 2021.
- [32] Q. Zhuang. Quantum-enabled communication without a phase reference. *Physical Review Letters*, 126(6):060502, 2021.
- [33] I. Devetak and P. W. Shor. The capacity of a quantum channel for simultaneous transmission of classical and quantum information. *Communications in Mathematical Physics*, 256(2):287–303, 2005.
- [34] A. S. Holevo. *Quantum Systems, Channels, Information: A Mathematical Introduction*. Walter de Gruyter, second edition, 2019.
- [35] M. Hayashi. *Quantum Information Theory: Mathematical Foundation*. Springer, second edition, 2017.
- [36] J. Watrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.
- [37] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, second edition, 2017. arXiv:1106.1445.
- [38] S. Khatri and M. M. Wilde. *Principles of Quantum Communication Theory: A Modern Approach*. November 2020. arXiv:2011.04672v1.
- [39] B. Schumacher. Sending entanglement through noisy quantum channels. *Physical Review A*, 54:2614–2628, 1996.
- [40] B. Schumacher and M. A. Nielsen. Quantum data processing and error correction. *Physical Review A*, 54(4):2629–2635, 1996. arXiv:quant-ph/9604022.
- [41] H. Barnum, E. Knill, and M. A. Nielsen. On quantum fidelities and channel capacities. *IEEE Transactions on Information Theory*, 46(4):1317–1329, 2000. arXiv:quant-ph/9809010.
- [42] S. Lloyd. Capacity of the noisy quantum channel. *Physical Review A*, 55(3):1613–1622, 1997. arXiv:quant-ph/9604015.
- [43] P. W. Shor. The quantum channel capacity and coherent information. In *Lecture Notes, MSRI Workshop on Quantum Computation*, 2002.
- [44] I. Devetak. The private classical capacity and quantum capacity of a quantum channel. *IEEE Transactions on Information Theory*, 51(1):44–55, 2005. arXiv:quant-ph/0304127.
- [45] O. Fawzi, A. Müller-Hermes, and A. Shayeghi. A lower bound on the space overhead of fault-tolerant quantum computation. In Mark Braverman, editor, *13th Innovations in Theoretical Computer Science Conference (ITCS 2022)*, volume 215 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 68:1–68:20, Dagstuhl, Germany, 2022. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.
- [46] N. Cai, A. Winter, and R. W. Yeung. Quantum privacy and quantum wiretap channels. *Problems of Information Transmission*, 40(4):318–336, 2004.
- [47] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters. Mixed-state entanglement and quantum error correction. *Physical Review A*, 54(5):3824–3851, 1996. arXiv:quant-ph/9604024.
- [48] M. Takeoka, S. Guha, and M. M. Wilde. The squashed entanglement of a quantum channel. *IEEE Transactions on Information Theory*, 60:4987–4998, 2014. arXiv:1310.0129.
- [49] H. J. Kimble. The quantum internet. *Nature*, 453(7198):1023–1030, 2008.
- [50] S. Wehner, D. Elkouss, and R. Hanson. Quantum internet: A vision for the road ahead. *Science*, 362(6412):eaam9288, 2018.
- [51] A. Arqand, L. Memarzadeh, and S. Mancini. Energy-constrained LOCC-assisted quantum capacity of bosonic dephasing channel. 2021. arXiv:2111.04173.
- [52] A. S. Holevo and R. F. Werner. Evaluating capacities of bosonic Gaussian channels. *Physical Review A*, 63:032312, 2001.
- [53] M. M. Wolf, D. Pérez-García, and G. Giedke. Quantum capacities of bosonic channels. *Physical Review Letters*, 98:130501, 2007.
- [54] M. Tomamichel, M. M. Wilde, and A. Winter. Strong converse rates for quantum communication. *IEEE Transactions on Information Theory*, 63:715–727, 2017. arXiv:1406.2946.
- [55] M. M. Wilde, M. Tomamichel, and M. Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63:1792–1817, 2017. arXiv:1602.08898.
- [56] The supplementary material contains detailed derivations for interested readers.
- [57] G. L. de Haas-Lorentz. *Die Brownsche Bewegung und einige verwandte Erscheinungen*. Die Wissenschaft. Friedr. Vieweg und Sohn, Brunswick, 1913.
- [58] E. Breitenberger. Analogues of the normal distribution on the circle and the sphere. *Biometrika*, 50(1/2):81–88, 1963.
- [59] F. Papadimitriou. *Spatial Entropy and Landscape Analysis*. RaumFragen: Stadt – Region – Landschaft. Springer Fachmedien Wiesbaden, 2022.
- [60] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen. Classical capacity of the lossy bosonic channel: The exact solution. *Physical Review Letters*, 92(2):027902, 2004. arXiv:quant-ph/0308012.
- [61] M. M. Wolf, D. Pérez-García, and G. Giedke. Quantum capacities of bosonic channels. *Physical Review Letters*, 98(13):130501, 2007. arXiv:quant-ph/0606132.
- [62] V. Giovannetti, R. García-Patrón, N. J. Cerf, and A. S. Holevo. Ultimate classical communication rates of quantum optical channels. *Nature Photonics*, 8(10):796–800, 2014.
- [63] V. Giovannetti, S. Lloyd, L. Maccone, and P. W. Shor. Entanglement assisted capacity of the broadband lossy channel. *Physical Review Letters*, 91(4):047901, 2003. arXiv:quant-ph/0304020.

- [64] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi. Fundamental limits of repeaterless quantum communications. *Nature Communications*, 8(1):15043, 2017.
- [65] G. Szegő. Beiträge zur Theorie der Toeplitzschen Formen. *Math. Z.*, 6(3):167–202, 1920.
- [66] S. Serra-Capizzano. Test functions, growth conditions and Toeplitz matrices. *Rend. Circ. Mat. Palermo, Ser. II, Suppl.*, 68:791–795, 2002.
- [67] A. Böttcher and S. M. Grudsky. *Toeplitz matrices, asymptotic linear algebra, and functional analysis*. Birkhäuser Verlag, Basel, 2000.
- [68] P. Leviant, Q. Xu, L. Jiang, and S. Rosenblum. Quantum capacity and codes for the bosonic loss-dephasing channel. 2022. arXiv:2205.00341.
- [69] G. Smith and J. A. Smolin. Additive extensions of a quantum channel. In *2008 IEEE Information Theory Workshop*, pages 368–372, May 2008.
- [70] K. Sharma, M. M. Wilde, S. Adhikari, and M. Takeoka. Bounding the energy-constrained quantum and private capacities of phase-insensitive bosonic Gaussian channels. *New Journal of Physics*, 20(6):063025, 2018.
- [71] M. Rosati, A. Mari, and V. Giovannetti. Narrow bounds for the quantum capacity of thermal attenuators. *Nature Communications*, 9(1):4339, 2018.
- [72] K. Noh, V. V. Albert, and L. Jiang. Quantum capacity bounds of Gaussian thermal loss channels and achievable rates with Gottesman-Kitaev-Preskill codes. *IEEE Transactions on Information Theory*, 65(4):2563–2582, 2019.
- [73] M. Fanizza, F. Kianvash, and V. Giovannetti. Estimating quantum and private capacities of gaussian channels via degradable extensions. *Physical Review Letters*, 127(21):210501, 2021.
- [74] H. P. Yuen and M. Ozawa. Ultimate information carrying limit of quantum systems. *Physical Review Letters*, 70:363–366, 1993.
- [75] A. S. Holevo. Entanglement-assisted capacities of constrained quantum channels. *Theory of Probability and its Applications*, 48(2):243–255, 2004.
- [76] L. Lami and M. M. Wilde. In preparation. 2022.
- [77] M. Rexiti, L. Memarzadeh, and S. Mancini. Discrimination of dephasing channels, 2022. arXiv:2201.00388.
- [78] R. Demkowicz-Dobrzanski and L. Maccone. Using entanglement against noise in quantum metrology. *Physical Review Letters*, 113:250801, 2014.
- [79] J. Niset, J. Fiurasek, and N. J. Cerf. No-go theorem for Gaussian quantum error correction. *Physical Review Letters*, 102(12):120501, 2009. arXiv:0811.3128.
- [80] A. Müller-Hermes. Transposition in quantum information theory. Master’s thesis, Technische Universität München, 2012.
- [81] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13):1895–1899, 1993.
- [82] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. Secure key from bound entanglement. *Physical Review Letters*, 94:160502, 2005.
- [83] K. Horodecki, M. Horodecki, P. Horodecki, and J. Oppenheim. General paradigm for distilling classical key from quantum states. *IEEE Transactions on Information Theory*, 55(4):1898–1929, 2009.
- [84] T. van Erven and P. Harremoës. Rényi divergence and Kullback-Leibler divergence. *IEEE Transactions on Information Theory*, 60(7):3797–3820, 2014.
- [85] M. Reed and B. Simon. *Methods of Modern Mathematical Physics: I: Functional Analysis*. Academic Press, New York, USA, 2nd edition, 1998.
- [86] C. W. Helstrom. *Quantum detection and estimation theory*. Academic press, New York, USA, 1976.
- [87] A. S. Holevo. Investigations in the general theory of statistical decisions. *Trudy Matematicheskogo Instituta imeni V. A. Steklova*, 124:3–140, 1976. (English translation: Proc. Steklov Inst. Math. 124:1–140, 1978).
- [88] A. Uhlmann. The “transition probability” in the state space of a $*$ -algebra. *Reports on Mathematical Physics*, 9(2):273–279, 1976.
- [89] C. A. Fuchs and J. van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Transactions on Information Theory*, 45(4):1216–1227, 1999.
- [90] W. F. Stinespring. Positive functions on C^* -algebras. *Proc. Am. Math. Soc.*, 6(2):211–216, 1955.
- [91] M.-D. Choi. Completely positive linear maps on complex matrices. *Linear Algebra Appl.*, 10(3):285 – 290, 1975.
- [92] K. Kraus. *States, effects and operations: fundamental notions of quantum theory*. Springer, 1983.
- [93] S. Kullback and R. A. Leibler. On information and sufficiency. *Ann. Math. Statist.*, 22(1):79–86, 1951.
- [94] D. Petz. Quasi-entropies for finite quantum systems. *Reports on Mathematical Physics*, 23(1):57–65, 1986.
- [95] Müller-Lennert M., F. Dupuis, O. Szehr, S. Fehr, and M. Tomamichel. On quantum Rényi entropies: A new generalization and some properties. *Journal of Mathematical Physics*, 54(12):122203, 2013.
- [96] M. M. Wilde, A. Winter, and D. Yang. Strong converse for the classical capacity of entanglement-breaking and Hadamard channels via a sandwiched Rényi relative entropy. *Communications in Mathematical Physics*, 331(2):593–622, 2014.
- [97] H. Umegaki. Conditional expectation in an operator algebra. IV. Entropy and information. *Kodai Math. Sem. Rep.*, 14(2):59–85, 1962.
- [98] G. Lindblad. Entropy, information and quantum measurements. *Communications in Mathematical Physics*, 33(4):305–322, 1973.
- [99] F. Hiai and D. Petz. The proper formula for relative entropy and its asymptotics in quantum probability. *Communications in Mathematical Physics*, 143(1):99–114, 1991.
- [100] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. Royal Soc. A*, 461(2053):207–235, 2005.
- [101] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70:1895–1899, 1993.
- [102] Alexander Müller-Hermes. Transposition in quantum information theory. Master’s thesis, Technical University of Munich, September 2012.
- [103] R. A. Horn and C. R. Johnson. *Matrix Analysis*. Cambridge University Press, 1990.
- [104] U. Grenander and G. Szegő. *Toeplitz forms and their applications*. Chelsea Publishing Co., New York, second edition, 1984.
- [105] S. V. Parter. On the distribution of the singular values of Toeplitz matrices. *Linear Algebra Appl.*, 80:115–130, 1986.
- [106] F. Avram. On bilinear forms in Gaussian random variables and Toeplitz matrices. *Probab. Theory Related Fields*, 79(1):37–45, 1988.
- [107] N. L. Zamarashkin and E. E. Tyrtshnikov. Distribution of the eigenvalues and singular numbers of Toeplitz matrices under weakened requirements on the generating function. *Mat. Sb.*, 188(8):83–92, 1997.

- [108] P. Tilli. Locally Toeplitz sequences: spectral properties and applications. *Linear Algebra Appl.*, 278(1-3):91–120, 1998.
- [109] A. Böttcher, S. M. Grudsky, and E. A. Maksimenko. Pushing the envelope of the test functions in the Szegő and Avram-Parter theorems. *Linear Algebra Appl.*, 429(1):346–366, 2008.
- [110] A. Böttcher and S. M. Grudsky. *Spectral properties of banded Toeplitz matrices*. Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2005.
- [111] C. Garoni and S. Serra-Capizzano. *Generalized locally Toeplitz sequences: theory and applications. Vol. I*. Springer, Cham, 2018.
- [112] S. M. Grudsky. Eigenvalues of larger Toeplitz matrices: the asymptotic approach. Lecture notes, 2010.
- [113] J. Åberg. Subspace preservation, subspace locality, and gluing of completely positive maps. *Ann. Phys.*, 313(2):326–367, 2004.
- [114] J. Åberg. Quantifying superposition. 2006. arXiv:quant-ph/0612146.
- [115] T. Baumgratz, M. Cramer, and M. B. Plenio. Quantifying coherence. *Physical Review Letters*, 113:140401, 2014.
- [116] A. Winter and D. Yang. Operational resource theory of coherence. *Physical Review Letters*, 116:120404, 2016.
- [117] E. Chitambar and M.-H. Hsieh. Relating the resource theories of entanglement and quantum coherence. *Physical Review Letters*, 117:020402, 2016.
- [118] B. Regula, K. Fang, X. Wang, and G. Adesso. One-shot coherence distillation. *Physical Review Letters*, 121:010401, 2018.
- [119] K. Fang, X. Wang, L. Lami, B. Regula, and G. Adesso. Probabilistic distillation of quantum coherence. *Physical Review Letters*, 121:070404, 2018.
- [120] L. Lami, B. Regula, and G. Adesso. Generic bound coherence under strictly incoherent operations. *Physical Review Letters*, 122:150402, 2019.
- [121] L. Lami. Completing the Grand Tour of asymptotic quantum coherence manipulation. *IEEE Transactions on Information Theory*, 66(4):2165–2183, 2020.
- [122] A. Streltsov, G. Adesso, and M. B. Plenio. Colloquium: Quantum coherence as a resource. *Reviews of Modern Physics*, 89:041003, 2017.
- [123] C. Lupo, V. Giovannetti, and S. Mancini. Capacities of lossy bosonic memory channels. *Phys. Rev. Lett.*, 104:030501, 2010.
- [124] M. E. Shirokov and A. S. Holevo. On approximation of infinite-dimensional quantum channels. *Probl. Pered. Inform.*, 44(2):3–22, 2008. (English translation: *Problems of Information Transmission* 44(2):73–90, 2008).
- [125] M. E. Shirokov. On the energy-constrained diamond norm and its application in quantum information theory. *Problems of Information Transmission*, 54(1):20–33, 2018.
- [126] E. B. Davies. Quantum stochastic processes. *Communications in Mathematical Physics*, 15(4):277–304, 1969.
- [127] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Transactions on Information Theory*, 45(7):2481–2485, 1999.
- [128] M. M. Wilde. *Quantum Information Theory*. Cambridge University Press, 2nd edition, 2017.
- [129] M. M. Wilde, M. Tomamichel, and M. Berta. Converse bounds for private communication over quantum channels. *IEEE Transactions on Information Theory*, 63(3):1792–1817, 2017.
- [130] K. V. Mardia and P. E. Jupp. *Directional statistics*. Wiley Series in Probability and Statistics. John Wiley & Sons, Ltd., Chichester, 2000.

Supplemental Material

I. PRELIMINARIES, NOTATION, AND DEFINITIONS

A. Quantum states and channels

An arbitrary quantum system is mathematically representable by a separable complex Hilbert space \mathcal{H} . We start by reviewing a few basic concepts from the theory of operators acting on a Hilbert space \mathcal{H} . An operator $X : \mathcal{H} \rightarrow \mathcal{H}$ acting on \mathcal{H} is **bounded** if its **operator norm** $\|X\|_\infty := \sup_{|\psi\rangle \in \mathcal{H}, \|\psi\rangle\| \leq 1} \|X|\psi\rangle\|$ is finite, i.e., if $\|X\|_\infty < \infty$. The Banach space of bounded operators acting on \mathcal{H} equipped with the norm $\|\cdot\|_\infty$ will be sometimes denoted by $\mathcal{B}(\mathcal{H})$. A bounded operator $X \in \mathcal{B}(\mathcal{H})$ is **positive semi-definite** if $\langle \psi | X | \psi \rangle \geq 0$ for all $|\psi\rangle \in \mathcal{H}$. The set of positive semi-definite bounded operators forms a cone, denoted here by $\mathcal{B}_+(\mathcal{H})$.

A bounded operator T such that the series defining $\text{Tr}|T| = \text{Tr}\sqrt{T^\dagger T} =: \|T\|_1 < \infty$ converges is said to be of **trace class**. Trace class operators acting on \mathcal{H} form another Banach space, denoted by $\mathcal{T}(\mathcal{H})$, once they are equipped with the trace norm $\|\cdot\|_1$. We denote the cone of positive semi-definite trace class operators by $\mathcal{T}_+(\mathcal{H})$. Since trace class operators are compact, the spectral theorem applies [85, Theorem VI.16]. This means that every $T \in \mathcal{T}(\mathcal{H})$ can be decomposed as $T = \sum_{k=0}^{\infty} t_k |e_k\rangle\langle f_k|$, where $\|T\|_1 = \sum_k |t_k| < \infty$, $\{|e_k\rangle\}_k$ and $\{|f_k\rangle\}_k$ are orthonormal bases of \mathcal{H} , and the series converges absolutely in trace norm.

Quantum states of a system A are described by **density operators**, i.e., positive semi-definite trace class operators with trace 1, on \mathcal{H}_A . The distance between two density operators ρ, σ acting on the same Hilbert space can be measured in two different but compatible ways, either with the **trace distance** $\frac{1}{2}\|\rho - \sigma\|_1$, endowed with a direct operational interpretation via the Helstrom–Holevo theorem for state discrimination [86, 87] or with the **fidelity** $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1^2$ [88]. Two fundamental relations known as the Fuchs–van de Graaf inequalities establish the essential equivalence of these two distance measures. They can be stated as [89]

$$1 - \sqrt{F(\rho, \sigma)} \leq \frac{1}{2} \|\rho - \sigma\|_1 \leq 1 - F(\rho, \sigma). \quad (\text{S1})$$

Physical transformations between states of a system A and states of a system B are represented mathematically as **quantum channels**, i.e., completely positive trace-preserving maps $\Lambda : \mathcal{T}(\mathcal{H}_A) \rightarrow \mathcal{T}(\mathcal{H}_B)$ [90–92]. A linear map $\Lambda : \mathcal{T}(\mathcal{H}_A) \rightarrow \mathcal{T}(\mathcal{H}_B)$ is

- (i) positive if $\Lambda(\mathcal{T}_+(\mathcal{H}_A)) \subseteq \mathcal{T}_+(\mathcal{H}_B)$;
- (ii) completely positive, if $\text{id}_N \otimes \Lambda : \mathcal{T}(\mathbb{C}^N \otimes \mathcal{H}_A) \rightarrow \mathcal{T}(\mathbb{C}^N \otimes \mathcal{H}_B)$ is a positive map for all $N \in \mathbb{N}$, where id_N represents the identity channel acting on the space of $N \times N$ complex matrices;
- (iii) trace preserving, if $\text{Tr} \Lambda(X) = \text{Tr} X$ holds for all trace class X .

B. Entropies and relative entropies

Let p, q be two probability density functions defined on the same measurable space \mathcal{X} with measure μ . For some $\alpha \in (0, 1) \cup (1, \infty)$, define their **α -Rényi divergence** by [84]

$$D_\alpha(p||q) := \frac{1}{\alpha - 1} \log_2 \int_{\mathcal{X}} d\mu(x) p(x)^\alpha q(x)^{1-\alpha}. \quad (\text{S2})$$

This definition can be extended to $\alpha \in \{0, 1, \infty\}$ [84, Definition 3] by taking suitable limits. For our purposes, it suffices to consider the **Kullback–Leibler** divergence [93] obtained by taking the limit $\alpha \rightarrow 1^-$ in (S2). It is defined as

$$D_1(p||q) = D(p||q) := \int_{\mathcal{X}} d\mu(x) p(x) \log_2 \frac{p(x)}{q(x)}. \quad (\text{S3})$$

The following technical result is important for this paper.

Lemma S1 [84, Theorems 3 and 5]. *For all fixed p, q , the α -Rényi divergence is monotonically non-decreasing in α . Moreover, $\lim_{\alpha \rightarrow 1^-} D_\alpha(p||q) = D(p||q)$, and if $D_{\alpha_0}(p||q) < \infty$ for some $\alpha_0 > 1$ (and therefore $D_\alpha(p||q) < \infty$ for all $0 < \alpha \leq \alpha_0$) then also*

$$\lim_{\alpha \rightarrow 1^+} D_\alpha(p||q) = D(p||q). \quad (\text{S4})$$

As a special case of the above formalism, one can define the *differential entropy* of a probability density function p on \mathcal{X} by setting

$$h(p) := - \int_{\mathcal{X}} d\mu(x) p(x) \log_2 p(x), \quad (\text{S5})$$

whenever the integral is well defined.

We now consider entropies and relative entropies between quantum states. For the sake of simplicity we assume throughout this subsection that all quantum systems are finite dimensional. Indeed, in this paper we shall not consider entropies and relative entropies of infinite-dimensional states.

The most immediate way to extend (S2) to the case of two quantum states ρ, σ is to define the *Petz–Rényi entropy* [94]

$$D_\alpha(\rho\|\sigma) := \frac{1}{\alpha-1} \log_2 \text{Tr} \rho^\alpha \sigma^{1-\alpha}, \quad (\text{S6})$$

where as usual $\alpha \in (0, 1) \cup (1, \infty)$, and we convene to set $D_\alpha(\rho\|\sigma) = +\infty$ whenever $\alpha > 1$ and $\text{supp} \rho \not\subseteq \text{supp} \sigma$, where $\text{supp} X$ denotes the *support* of X , i.e., the orthogonal complement of its kernel. Although (S6) is a sensible definition, it is often helpful to consider an alternative quantity. The *sandwiched α -Rényi relative entropy* is defined as [95, 96]

$$\tilde{D}_\alpha(\rho\|\sigma) := \frac{2\alpha}{\alpha-1} \log_2 \left\| \sigma^{\frac{1-\alpha}{2\alpha}} \rho^{\frac{1}{2}} \right\|_{2\alpha}. \quad (\text{S7})$$

Here, for $\beta > 0$ we define the corresponding *Schatten norm* of a matrix X as

$$\|X\|_\beta := \left(\text{Tr} \left[|X|^\beta \right] \right)^{1/\beta}, \quad (\text{S8})$$

where $|X| := \sqrt{X^\dagger X}$. As before, it is understood that $\tilde{D}_\alpha(\rho\|\sigma) = +\infty$ when $\alpha > 1$ and $\text{supp} \rho \not\subseteq \text{supp} \sigma$. Importantly, when $[\rho, \sigma] = 0$, i.e., ρ and σ commute, (S6) and (S7) coincide, and are equal to the α -Rényi divergence between the spectra of ρ and σ . Namely,

$$[\rho, \sigma] = 0 \implies \tilde{D}_\alpha(\rho\|\sigma) = D_\alpha(\rho\|\sigma). \quad (\text{S9})$$

Taking the limit for $\alpha \rightarrow 1$ of either (S6) or (S7) yields the (Umegaki) *relative entropy*, given by [97–99]

$$D(\rho\|\sigma) := \lim_{\alpha \rightarrow 1} \tilde{D}_\alpha(\rho\|\sigma) = \lim_{\alpha \rightarrow 1} D_\alpha(\rho\|\sigma) = \text{Tr} \left[\rho (\log_2 \rho - \log_2 \sigma) \right]. \quad (\text{S10})$$

The final quantity we need to define is the simplest of all, namely, the (von Neumann) *entropy* of a density matrix ρ :

$$S(\rho) := - \text{Tr} \left[\rho \log_2 \rho \right]. \quad (\text{S11})$$

C. Continuous-variable systems

A single-mode continuous-variable system is mathematically modelled by the Hilbert space $\mathcal{H}_1 := L^2(\mathbb{R})$, which comprises all square-integrable complex-valued functions over \mathbb{R} . The operators x and $p := -i \frac{d}{dx}$ satisfy the *canonical commutation relation* $[x, p] = i\mathbb{1}$, where $\mathbb{1}$ denotes the identity operator (in this case, acting on \mathcal{H}_1). Introducing the *annihilation* and *creation operators*

$$a := \frac{x + ip}{\sqrt{2}}, \quad a^\dagger := \frac{x - ip}{\sqrt{2}}, \quad (\text{S12})$$

this can be recast in the form

$$[a, a^\dagger] = \mathbb{1}. \quad (\text{S13})$$

Creation operators map the *vacuum state* $|0\rangle$ to the *Fock states*

$$|k\rangle := \frac{(a^\dagger)^k}{\sqrt{k!}} |0\rangle. \quad (\text{S14})$$

Fock states are eigenvectors of the *photon number* operator $a^\dagger a$, which satisfies

$$a^\dagger a |k\rangle = k |k\rangle. \quad (\text{S15})$$

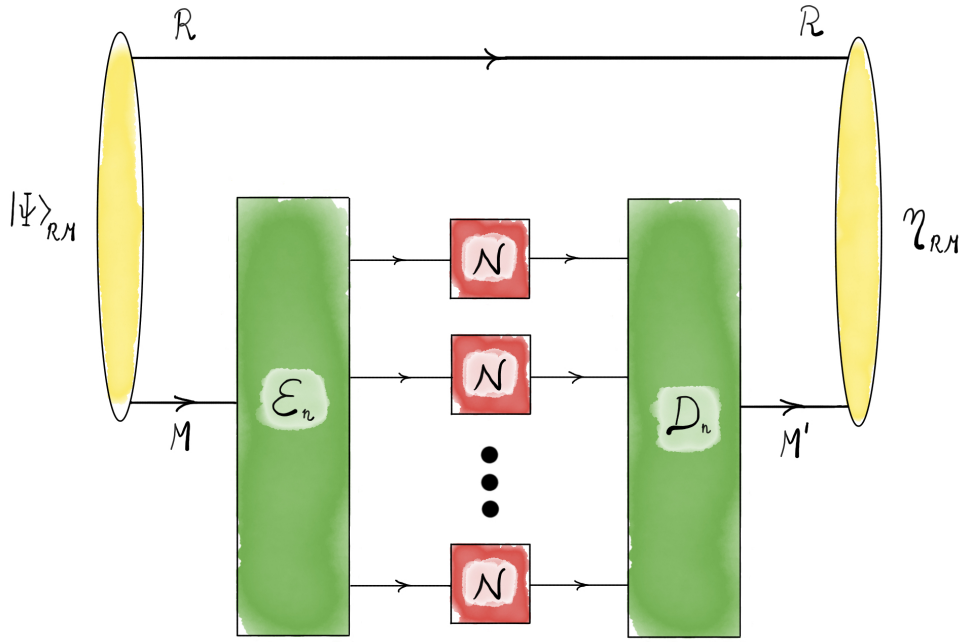


FIG. S2: A depiction of a quantum communication protocol that uses the channel n times.

D. Unassisted capacities of quantum channels

In this section, we briefly define the quantum and private capacities of a quantum channel. We begin with the quantum capacity. An $(|M|, \epsilon)$ code for quantum communication over the channel $\mathcal{N}_{A \rightarrow B}$ consists of an encoding channel $\mathcal{E}_{M \rightarrow A}$ and a decoding channel $\mathcal{D}_{B \rightarrow M'}$ such that the channel fidelity of the coding scheme and the identity channel id_M is not smaller than $1 - \epsilon$:

$$F(\text{id}_M, \mathcal{D}_{B \rightarrow M'} \circ \mathcal{N}_{A \rightarrow B} \circ \mathcal{E}_{M \rightarrow A}) \geq 1 - \epsilon \quad (\text{S16})$$

where the channel fidelity of channels \mathcal{N}_1 and \mathcal{N}_2 is defined as

$$F(\mathcal{N}_1, \mathcal{N}_2) := \inf_{\rho} F((\text{id} \otimes \mathcal{N}_1)(\rho), (\text{id} \otimes \mathcal{N}_2)(\rho)), \quad (\text{S17})$$

with the optimization over every bipartite state ρ and the reference system allowed to be arbitrarily large. See Figure S2 for a depiction of a quantum communication protocol that uses the channel n times.

The one-shot quantum capacity $Q_{\epsilon}(\mathcal{N}_{A \rightarrow B})$ of the channel $\mathcal{N}_{A \rightarrow B}$ is defined as

$$Q_{\epsilon}(\mathcal{N}) := \sup_{\mathcal{E}, \mathcal{D}} \{\log_2 |M| : \exists (M, \epsilon) \text{ quantum communication protocol for } \mathcal{N}_{A \rightarrow B}\}, \quad (\text{S18})$$

where the optimization is over every encoding channel \mathcal{E} and decoding channel \mathcal{D} . The (asymptotic) quantum capacity of $\mathcal{N}_{A \rightarrow B}$ is then defined as

$$Q(\mathcal{N}) := \inf_{\epsilon \in (0,1)} \liminf_{n \rightarrow \infty} \frac{1}{n} Q_{\epsilon}(\mathcal{N}^{\otimes n}). \quad (\text{S19})$$

The strong converse quantum capacity of $\mathcal{N}_{A \rightarrow B}$ is defined as

$$Q^{\dagger}(\mathcal{N}) := \sup_{\epsilon \in (0,1)} \limsup_{n \rightarrow \infty} \frac{1}{n} Q_{\epsilon}(\mathcal{N}^{\otimes n}). \quad (\text{S20})$$

The quantum capacity is equal to the regularized coherent information of the channel [39–44]:

$$Q(\mathcal{N}) = \lim_{n \rightarrow \infty} \frac{1}{n} Q^{(1)}(\mathcal{N}^{\otimes n}) = \sup_{n \in \mathbb{N}_+} \frac{1}{n} Q^{(1)}(\mathcal{N}^{\otimes n}), \quad (\text{S21})$$

$$Q^{(1)}(\mathcal{N}) := \sup_{|\Psi\rangle_{AA'}} I_{\text{coh}}(A \rangle B)_V,$$

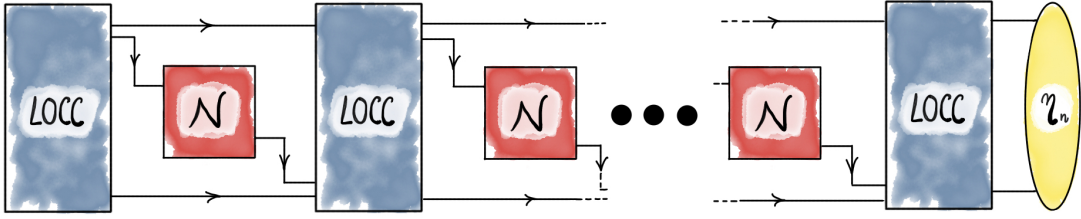


FIG. S3: An LOCC-assisted protocol that involves n uses of the quantum channel \mathcal{N} .

where

$$\begin{aligned} v_{AB} &:= (\text{id}_A \otimes \mathcal{N}_{A' \rightarrow B})(\Psi_{AA'}), \\ I_{\text{coh}}(A)B)_\rho &:= S(\rho_B) - S(\rho_{AB}). \end{aligned} \quad (\text{S22})$$

This gives us a method for evaluating the quantum capacity of particular channels of interest, including the bosonic dephasing channels.

Let us now recall basic definitions related to private capacity. Let $\mathcal{U}_{A \rightarrow BE}^N$ be an isometric channel extending the channel $\mathcal{N}_{A \rightarrow B}$ [90]. An $(|M|, \epsilon)$ code for private communication over the channel $\mathcal{N}_{A \rightarrow B}$ consists of a set $\{\rho_A^m\}_m$ of encoding states and a decoder, specified as a positive operator-valued measure $\{\Lambda_B^m\}_m$. It achieves an error ϵ if there exists a state σ_E of the environment, such that the following inequality holds for every message m :

$$F\left(\sum_{m'} |m'\rangle\langle m'| \otimes \text{Tr}_B[\Lambda_B^{m'} \mathcal{U}_{A \rightarrow BE}^N(\rho_A^m)], |m\rangle\langle m| \otimes \sigma_E\right) \geq 1 - \epsilon. \quad (\text{S23})$$

The one-shot private capacity $P_\epsilon(\mathcal{N}_{A \rightarrow B})$ of the channel $\mathcal{N}_{A \rightarrow B}$ is defined as

$$P_\epsilon(\mathcal{N}) := \sup_{\{\rho_A^m\}_m, \{\Lambda_B^m\}_m} \{\log_2 |M| : \exists (M, \epsilon) \text{ private communication protocol for } \mathcal{N}_{A \rightarrow B}\}, \quad (\text{S24})$$

where the optimization is over every set $\{\rho_A^m\}_m$ of encoding states and decoding POVM $\{\Lambda_B^m\}_m$. The (asymptotic) private capacity of $\mathcal{N}_{A \rightarrow B}$ is then defined as

$$P(\mathcal{N}) := \inf_{\epsilon \in (0,1)} \liminf_{n \rightarrow \infty} \frac{1}{n} P_\epsilon(\mathcal{N}^{\otimes n}). \quad (\text{S25})$$

The strong converse private capacity of $\mathcal{N}_{A \rightarrow B}$ is defined as

$$P^\dagger(\mathcal{N}) := \sup_{\epsilon \in (0,1)} \limsup_{n \rightarrow \infty} \frac{1}{n} P_\epsilon(\mathcal{N}^{\otimes n}). \quad (\text{S26})$$

The following inequalities are direct consequences of the definitions:

$$\begin{aligned} Q(\mathcal{N}) &\leq Q^\dagger(\mathcal{N}), \\ P(\mathcal{N}) &\leq P^\dagger(\mathcal{N}). \end{aligned} \quad (\text{S27})$$

Less trivially, we also have that [100]

$$Q(\mathcal{N}) \leq P(\mathcal{N}). \quad (\text{S28})$$

E. Two-way assisted capacities of quantum channels

In this section, we define the quantum and private capacities when the channel of interest is assisted by local operations and classical communication. We begin with the LOCC-assisted quantum capacity.

An $(n, |M|, \epsilon)$ protocol \mathcal{P} for LOCC-assisted quantum communication consists of a separable state $\sigma_{A'_1 A_1 B'_1}$, the set $\{\mathcal{L}_{A'_{i-1} B_{i-1} B'_{i-1} \rightarrow A'_i A_i B'_i}\}_{i=2}^n$ of LOCC channels, and the LOCC channel $\mathcal{L}_{A'_n B_n B'_n \rightarrow M_A M_B}^{(n)}$. (See [38] for the definition of an LOCC channel.) The final state of the protocol is

$$\eta_{M_A M_B} := (\mathcal{L}_{A'_n B_n B'_n \rightarrow M_A M_B}^{(n)} \circ \mathcal{N}_{A_n \rightarrow B_n} \circ \mathcal{L}_{A'_{n-1} B_{n-1} B'_{n-1} \rightarrow A'_n A_n B'_n}^{(n-1)} \circ \dots \circ \mathcal{L}_{A'_1 B_1 B'_1 \rightarrow A'_2 A_2 B'_2}^{(1)} \circ \mathcal{N}_{A_1 \rightarrow B_1})(\sigma_{A'_1 A_1 B'_1}), \quad (\text{S29})$$

satisfying

$$F(\eta_{M_A M_B}, \Phi_{M_A M_A}) \geq 1 - \epsilon, \quad (\text{S30})$$

where $\Phi_{M_A M_A}$ is a maximally entangled state of Schmidt rank $|M|$. Such a protocol is depicted in Figure S3. We note here that it suffices for such a protocol to generate the maximally entangled state $\Phi_{M_A M_B}$ because entanglement and quantum communication are equivalent communication resource when classical communication is freely available, due to the teleportation protocol [101].

The n -shot LOCC-assisted quantum capacity of the channel $\mathcal{N}_{A \rightarrow B}$ is defined as

$$Q_{\leftrightarrow, n, \epsilon}(\mathcal{N}) := \sup_{\mathcal{P}} \left\{ \frac{1}{n} \log_2 |M| : \exists(|M|, \epsilon) \text{ LOCC-assisted q. comm. protocol } \mathcal{P} \text{ for } \mathcal{N}_{A \rightarrow B} \right\}, \quad (\text{S31})$$

where the optimization is over every LOCC-assisted quantum communication protocol \mathcal{P} . The (asymptotic) LOCC-assisted quantum capacity of $\mathcal{N}_{A \rightarrow B}$ is then defined as

$$Q_{\leftrightarrow}(\mathcal{N}) := \inf_{\epsilon \in (0,1)} \liminf_{n \rightarrow \infty} Q_{\leftrightarrow, n, \epsilon}(\mathcal{N}). \quad (\text{S32})$$

The strong converse LOCC-assisted quantum capacity of $\mathcal{N}_{A \rightarrow B}$ is defined as

$$Q_{\leftrightarrow}^{\dagger}(\mathcal{N}) := \sup_{\epsilon \in (0,1)} \limsup_{n \rightarrow \infty} Q_{\leftrightarrow, n, \epsilon}(\mathcal{N}). \quad (\text{S33})$$

An $(n, |M|, \epsilon)$ protocol \mathcal{K} for secret key agreement over a quantum channel is defined essentially the same as an LOCC-assisted protocol for quantum communication, except that the target final state of the protocol is more general. That is, the final step of the protocol is an LOCC channel $\mathcal{L}_{A'_n B_n B'_n \rightarrow M_A M_B S_A S_B}^{(n)}$, where S_A and S_B are extra systems of the sender Alice and the receiver Bob. Let us then denote the final state of the protocol by $\eta_{M_A M_B S_A S_B}$. Such a protocol satisfies

$$F(\eta_{M_A M_B S_A S_B}, \gamma_{M_A M_B S_A S_B}) \geq 1 - \epsilon, \quad (\text{S34})$$

where $\gamma_{M_A M_B S_A S_B}$ is a private state of dimension $|M|$ [82, 83], having the form

$$\gamma_{M_A M_B S_A S_B} := U_{M_A M_B S_A S_B} (\Phi_{M_A M_B} \otimes \theta_{S_A S_B}) U_{M_A M_B S_A S_B}^{\dagger}. \quad (\text{S35})$$

In the above, $U_{M_A M_B S_A S_B}$ is a twisting unitary of the form

$$U_{M_A M_B S_A S_B} = \sum_{i,j} |i\rangle\langle i|_{M_A} \otimes |j\rangle\langle j|_{M_B} \otimes U_{S_A S_B}^{i,j}, \quad (\text{S36})$$

with each $U_{S_A S_B}^{i,j}$ a unitary. Also, $\Phi_{M_A M_B}$ is a maximally entangled state of Schmidt rank $|M|$ and $\theta_{S_A S_B}$ is an arbitrary state. The fact that such a protocol is equivalent to the more familiar notion of secret key agreement, involving three parties generating a tripartite secret key state of the form $\frac{1}{|M|} \sum_{m=0}^{|M|-1} |m\rangle\langle m|_{M_A} \otimes |m\rangle\langle m|_{M_B} \otimes \sigma_E$, is the main contribution of [82, 83] (see [38] for another presentation).

The n -shot secret-key-agreement capacity of the channel $\mathcal{N}_{A \rightarrow B}$ is defined as

$$P_{\leftrightarrow, n, \epsilon}(\mathcal{N}) := \sup_{\mathcal{K}} \left\{ \frac{1}{n} \log_2 |M| : \exists(|M|, \epsilon) \text{ secret-key-agreement protocol } \mathcal{K} \text{ for } \mathcal{N}_{A \rightarrow B} \right\}, \quad (\text{S37})$$

where the optimization is over every secret key agreement protocol \mathcal{K} . The (asymptotic) secret key agreement capacity of $\mathcal{N}_{A \rightarrow B}$ is then defined as

$$P_{\leftrightarrow}(\mathcal{N}) := \inf_{\epsilon \in (0,1)} \liminf_{n \rightarrow \infty} P_{\leftrightarrow, n, \epsilon}(\mathcal{N}). \quad (\text{S38})$$

The strong converse secret key agreement capacity of $\mathcal{N}_{A \rightarrow B}$ is defined as

$$P_{\leftrightarrow}^{\dagger}(\mathcal{N}) := \sup_{\epsilon \in (0,1)} \limsup_{n \rightarrow \infty} P_{\leftrightarrow, n, \epsilon}(\mathcal{N}). \quad (\text{S39})$$

The following inequalities are direct consequences of the definitions:

$$\begin{aligned} Q_{\leftrightarrow}(\mathcal{N}) &\leq Q_{\leftrightarrow}^{\dagger}(\mathcal{N}) \\ P_{\leftrightarrow}(\mathcal{N}) &\leq P_{\leftrightarrow}^{\dagger}(\mathcal{N}). \end{aligned} \quad (\text{S40})$$

Due to the fact that a more general target state is allowed in secret key agreement, the following inequalities hold

$$\begin{aligned} Q_{\leftrightarrow}(\mathcal{N}) &\leq P_{\leftrightarrow}(\mathcal{N}) \\ Q_{\leftrightarrow}^{\dagger}(\mathcal{N}) &\leq P_{\leftrightarrow}^{\dagger}(\mathcal{N}). \end{aligned} \quad (\text{S41})$$

Finally, due to the fact that classical communication can only enhance capacities, the following inequalities hold:

$$\begin{aligned} Q(\mathcal{N}) &\leq Q_{\leftrightarrow}(\mathcal{N}) \\ Q^{\dagger}(\mathcal{N}) &\leq Q_{\leftrightarrow}^{\dagger}(\mathcal{N}) \\ P(\mathcal{N}) &\leq P_{\leftrightarrow}(\mathcal{N}) \\ P^{\dagger}(\mathcal{N}) &\leq P_{\leftrightarrow}^{\dagger}(\mathcal{N}). \end{aligned} \quad (\text{S42})$$

Thus, to establish the collapse of all of the capacities discussed in this section and the previous one, for the case of bosonic dephasing channels, it suffices to prove the lower bound on $Q(\mathcal{N})$ and the upper bound on $P_{\leftrightarrow}^{\dagger}(\mathcal{N})$.

F. Teleportation simulation

The d -dimensional quantum teleportation protocol [101] takes as input a d -dimensional quantum state $\rho_{A'}$ of a system A' , a d -dimensional maximally entangled state

$$\Phi_d^{AB} := |\Phi_d\rangle\langle\Phi_d|_{AB}, \quad |\Phi_d\rangle_{AB} := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A |k\rangle_B, \quad (\text{S43})$$

and by using only local operations and one-way classical communication from Alice to Bob reproduces the exact same state ρ on the system B . To define it rigorously, for $x, z \in \{0, \dots, d-1\}$ let us introduce the unitary matrices

$$X(x) := \sum_{k=0}^{d-1} |k \oplus x\rangle\langle k|, \quad Z(z) := \sum_{k=0}^{d-1} e^{\frac{2\pi i}{d} z k} |k\rangle\langle k|, \quad U(x, z) := X(x)Z(z), \quad (\text{S44})$$

where \oplus denotes sum modulo d . Then the teleportation channel $\mathcal{T}_{A'AB \rightarrow B}^{(d)}$ is given by

$$\mathcal{T}_{A'AB \rightarrow B}^{(d)}(X_{A'AB}) := \sum_{x, z=0}^{d-1} U(x, z)_B \text{Tr}_{AA'} \left[X_{A'AB} U(x, z)_{A'} \Phi_d^{AA'} U(x, z)_{A'}^{\dagger} \right] U(x, z)_B^{\dagger}. \quad (\text{S45})$$

The effectiveness of the standard quantum teleportation protocol is expressed by the identity

$$\mathcal{T}_{A'AB \rightarrow B}^{(d)}(\rho_{A'} \otimes \Phi_d^{AB}) = \rho_B, \quad (\text{S46})$$

meaning that the same operator ρ is written in the registers A' and B on the left-hand and on the right-hand side, respectively.

Some channels can be simulated by the action of the standard teleportation protocol on their Choi states [47], in the sense that

$$\mathcal{T}_{A'AB \rightarrow B}^{(d)}(\rho_{A'} \otimes \Phi_N^{AB}) = \mathcal{N}(\rho_{A'}), \quad (\text{S47})$$

where Φ_N^{AB} is the Choi state of the channel \mathcal{N} . For example, this is the case for all Pauli channels. More generally, other channels can be simulated approximately by the action of the teleportation protocol on their Choi states. This concept was introduced in [47] for the explicit purpose of obtaining upper bounds on the LOCC-assisted quantum capacity of a channel in terms of an entanglement measure evaluated on the Choi state. The idea was rediscovered in [102] for the same purpose, and more recently the same idea was used to bound the secret-key-agreement capacity [64] and the strong converse secret-key-agreement capacity [55]. Here we make use of this concept in order to obtain upper bounds on the strong converse secret key agreement capacity of all bosonic dephasing channels. As discussed earlier, it suffices to consider establishing an upper bound on this latter capacity because it is the largest among all the capacities that we consider in this paper.

G. Bosonic dephasing channel

Definition S2. Let p be a probability density function on the interval $[-\pi, \pi]$. The associated **bosonic dephasing channel** is the quantum channel $\mathcal{N}_p : \mathcal{T}(\mathcal{H}_1) \rightarrow \mathcal{T}(\mathcal{H}_1)$ acting on a single-mode system and given by

$$\mathcal{N}_p(\rho) := \int_{-\pi}^{\pi} d\phi p(\phi) e^{-ia^\dagger a \phi} \rho e^{ia^\dagger a \phi}, \quad (\text{S48})$$

where $a^\dagger a$ is the photon number operator.

The action of the bosonic dephasing channel can be easily described by representing the input operator in the Fock basis. By means of this representation the Hilbert space of a single-mode system, \mathcal{H}_1 , becomes equivalent to that of square-summable complex-valued sequences, denoted $\ell^2(\mathbb{N})$. Operators on \mathcal{H}_1 are represented by **infinite matrices**, i.e., operators $S : \ell^2(\mathbb{N}) \rightarrow \ell^2(\mathbb{N})$. Given two such operators S, T , which we formally write $S = \sum_{h,k} S_{hk} |h\rangle\langle k|$ and $T = \sum_{h,k} T_{hk} |h\rangle\langle k|$, their **Hadamard product** is defined by

$$S \circ T := \sum_{h,k} S_{hk} T_{hk} |h\rangle\langle k|. \quad (\text{S49})$$

One of the fundamental facts concerning the Hadamard product is the *Schur product theorem* [103, Theorem 7.5.3]: it states that if $S \geq 0$ and $T \geq 0$ are positive semi-definite, then also $S \circ T \geq 0$ is such. The theorem is usually stated for matrices, but is immediately generalisable to the operator case as a consequence of the remark below.

Remark S3. Let $T : \ell^2(\mathbb{N}) \rightarrow \ell^2(\mathbb{N})$ be an infinite matrix. Then $T \geq 0$ if and only if $T^{(d)} \geq 0$ for all $d \in \mathbb{N}_+$, where $T^{(d)}$ is the $d \times d$ top left corner of T . This follows from the fact that the linear span of the basis vectors $|k\rangle$, $k \in \mathbb{N}$, is dense in $\ell^2(\mathbb{N})$.

Given an infinite matrix T which represents a bounded operator $T : \ell^2(\mathbb{N}) \rightarrow \ell^2(\mathbb{N})$, we can define the associated **Hadamard channel** as

$$\begin{aligned} \mathcal{L}_T : \mathcal{T}(\ell^2(\mathbb{N})) &\longrightarrow \mathcal{T}(\ell^2(\mathbb{N})) \\ S &\longmapsto S \circ T. \end{aligned} \quad (\text{S50})$$

The following is then easily established.

Lemma S4. Let $T : \ell^2(\mathbb{N}) \rightarrow \ell^2(\mathbb{N})$ be a bounded operator represented by an infinite matrix. Then the Hadamard channel (S50) is a completely positive and trace preserving map, i.e., a quantum channel, if and only if

- (i) $T \geq 0$ as an operator; and
- (ii) $T_{kk} = 1$ for all $k \in \mathbb{N}$.

Proof. The two conditions are clearly necessary. In fact, if $T_{kk} \neq 1$ for some $k \in \mathbb{N}_+$, then $\text{Tr}[T \circ |k\rangle\langle k|] = T_{kk} \neq 1 = \text{Tr}|k\rangle\langle k|$; i.e., \mathcal{L}_T is not trace preserving. Also, if $T \not\geq 0$ then by Remark S3 there exists $d \in \mathbb{N}_+$ and some $|\psi\rangle \in \mathbb{C}^d$ such that $\langle \psi | T^{(d)} | \psi \rangle < 0$. Rewriting $\langle \psi | T^{(d)} | \psi \rangle = \sum_{h,k=0}^{d-1} \psi_h^* \psi_k T_{hk} = d \langle + | (T \circ \psi) | + \rangle$, where $\psi := |\psi\rangle\langle \psi|$ and $|+\rangle := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle$, shows that in this case \mathcal{L}_T would not even be positive, let alone completely positive.

Vice versa, conditions (i)–(ii) are sufficient. In fact, on the one hand, by (ii), for an arbitrary X , we have that $\text{Tr} \mathcal{L}_T(X) = \sum_k T_{kk} X_{kk} = \text{Tr} X$, i.e., \mathcal{L}_T is trace preserving. On the other hand, if $T \geq 0$ then for all $d \in \mathbb{N}_+$ and for all positive semi-definite bipartite operators $X \geq 0$ acting on $\mathbb{C}^d \otimes \ell^2(\mathbb{N})$ we have that $(I \otimes \mathcal{L}_T)(X) = d(|+\rangle\langle +| \otimes T) \circ X \geq 0$, where $|+\rangle$ is defined above, and the last inequality follows by the Schur product theorem. Since d is arbitrary, this proves that \mathcal{L}_T is completely positive. \square

The theory of Hadamard channels we just sketched out is relevant here due to the following simple observation.

Lemma S5. When both the input and the output density operators are represented in the Fock basis, the bosonic dephasing channel \mathcal{N}_p acts as the Hadamard channel

$$\mathcal{N}_p(\rho) = \rho \circ T_p, \quad (\text{S51})$$

$$(T_p)_{hk} := \int_{-\pi}^{\pi} d\phi p(\phi) e^{-i\phi(h-k)}. \quad (\text{S52})$$

Proof. Due to (S15), we have that $\mathcal{N}_p(\rho) = \sum_{h,k} \rho_{hk} \int_{-\pi}^{\pi} d\phi p(\phi) e^{-i\phi(h-k)} |h\rangle\langle k| = \rho \circ T_p$. \square

II. CAPACITIES OF BOSONIC DEPHASING CHANNELS

A. Infinite Toeplitz matrices and theorems of Szegő and Avram–Parter type

Observe that the expression for $(T_p)_{hk}$ only depends on the difference $h - k$. Matrices with this property are named after the mathematician Otto Toeplitz. Formally, a **Toeplitz matrix** of size $d \in \mathbb{N}_+$ is a matrix of the form

$$T = \begin{pmatrix} a_0 & a_{-1} & a_{-2} & \dots & a_{-d+1} \\ a_1 & a_0 & a_{-1} & \dots & a_{-d+2} \\ a_2 & a_1 & a_0 & \dots & a_{-d+3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{d-1} & a_{d-2} & a_{d-3} & \dots & a_0 \end{pmatrix}, \quad (\text{S53})$$

where $a_0, \dots, a_{d-1} \in \mathbb{C}$. Alternatively, it can be defined to have entries

$$T_{hk} = a_{h-k}. \quad (\text{S54})$$

This definition can be formally extended to the case of **infinite Toeplitz matrices**, simply by letting $h, k \in \mathbb{N}$ run over all non-negative integers. Note that the top left corners $T^{(d)} := \sum_{h,k=0}^{d-1} T_{hk} |h\rangle\langle k|$ of an infinite Toeplitz matrix are Toeplitz matrices.

In applications one often encounters the case in which the numbers a_k are the Fourier coefficients of an absolutely integrable function $a : [-\pi, \pi] \rightarrow \mathbb{C}$, i.e.

$$a_k = \int_{-\pi}^{+\pi} \frac{d\phi}{2\pi} a(\phi) e^{-ik\phi}. \quad (\text{S55})$$

In this paper, we will consider mainly non-negative functions $a : [-\pi, \pi] \rightarrow \mathbb{R}_+$.

A result due to Szegő [65, 104] states that the spectrum of the $d \times d$ top left corners $T^{(d)}$ of an infinite Toeplitz matrix converges to the generating function $a : [-\pi, \pi] \rightarrow \mathbb{R}$ (for now assumed to be real-valued), in the sense that

$$\lim_{d \rightarrow \infty} \frac{1}{d} \text{Tr} F(T^{(d)}) = \lim_{d \rightarrow \infty} \frac{1}{d} \sum_{j=1}^d F(\lambda_j(T^{(d)})) = \int_{-\pi}^{\pi} \frac{d\phi}{2\pi} F(a(\phi)) \quad (\text{S56})$$

whenever a and $F : \mathbb{R} \rightarrow \mathbb{R}$ are sufficiently well behaved. Here, $\lambda_j(T^{(d)})$ denotes the j^{th} eigenvalue of the matrix $T^{(d)}$. The scope and extension of Szegő's result has been expanded over the years by relaxing the conditions to be imposed on a and F so that (S56) holds. At the same time, an analogous class of results, initially conceived by Parter [105] and Avram [106], has been developed to deal with the case of complex-valued generating functions $a : [-\pi, \pi] \rightarrow \mathbb{C}$. Results of the Avram–Parter type generalize (S56) by stating that

$$\lim_{d \rightarrow \infty} \frac{1}{d} \text{Tr} F(|T^{(d)}|) = \lim_{d \rightarrow \infty} \frac{1}{d} \sum_{j=1}^d F(s_j(T^{(d)})) = \int_{-\pi}^{\pi} \frac{d\phi}{2\pi} F(|a(\phi)|), \quad (\text{S57})$$

where $s_j(T^{(d)})$ is now the j^{th} singular value of the matrix $T^{(d)}$. Both Szegő's and Avram–Parter's result have been generalized in successive steps, by Zamarashkin and Tyrtshnikov [107], Tilli [108], Serra-Capizzano [66], Böttcher, Grudsky, and Maksimenko [109], and others. For a detailed account of these developments, we refer the reader to the textbooks [67, 110, 111] and especially to the lecture notes by Grudsky [112]. Here we will just need the following lemma, extracted from the work of Serra-Capizzano.

Lemma S6 (Serra-Capizzano [66]). *If $a : [-\pi, \pi] \rightarrow \mathbb{R}_+$ is such that*

$$\int_{-\pi}^{+\pi} \frac{d\phi}{2\pi} a(\phi)^\alpha < \infty \quad (\text{S58})$$

for some $\alpha \geq 1$, and moreover $F : \mathbb{R}_+ \rightarrow \mathbb{R}$ is continuous and satisfies

$$F(x) = O(x^\alpha) \quad (x \rightarrow \infty), \quad (\text{S59})$$

then (S56) holds.

Proof. The original result by Serra-Capizzano [66, Theorem 2] states that the identity (S57) involving singular values holds. However, under the stronger hypotheses that we are making here it can be seen that (S56) and (S57) are actually equivalent. Since a takes on values in \mathbb{R}_+ , we only need to check that for each d the singular values and the eigenvalues of $T^{(d)}$ coincide. To this end, it suffices to note that $T^{(d)}$ is a positive semi-definite operator, simply because

$$\begin{aligned} \sum_{h,k=0}^{d-1} \psi_h^* \psi_k T_{hk} &= \sum_{h,k=0}^{d-1} \psi_h^* \psi_k \int_{-\pi}^{+\pi} \frac{d\phi}{2\pi} a(\phi) e^{-i(h-k)\phi} \\ &= \int_{-\pi}^{+\pi} \frac{d\phi}{2\pi} a(\phi) \sum_{h,k=0}^{d-1} \psi_h^* \psi_k e^{-i(h-k)\phi} \\ &= \int_{-\pi}^{+\pi} \frac{d\phi}{2\pi} a(\phi) \left| \sum_{k=0}^{d-1} \psi_k e^{ik\phi} \right|^2 \\ &\geq 0 \end{aligned} \tag{S60}$$

for every $|\psi\rangle \in \mathbb{C}^d$. This can also be seen as a simple consequence of (the easy direction of) Bochner's theorem. \square

B. Proof of main result

Before stating and proving our main result, let us fix some terminology. For an infinite matrix τ that is also a density operator on $\ell^2(\mathbb{N})$, the associated *maximally correlated state* $\Omega[\tau]$ on $\ell^2(\mathbb{N}) \otimes \ell^2(\mathbb{N})$ is defined by

$$\Omega[\tau] := \sum_{h,k=0}^{\infty} \tau_{hk} |h\rangle\langle k| \otimes |h\rangle\langle k|. \tag{S61}$$

Maximally correlated states appear naturally in connecting coherence theory [113–121] (see also the review article [122]) with entanglement theory. When seen in this latter context, they are useful because they represent a particularly simple class of entangled states.

Also, recall that the Rényi entropy of a probability density defined on the interval $[-\pi, \pi]$ need not be finite; that is, it can be equal to $-\infty$. It is always bound from above by 2π , due to the non-negativity of relative entropy. Indeed, $h(p) \leq \log_2 2\pi$ for every probability density p defined on $[-\pi, \pi]$ because $\log_2 2\pi - h(p) = D(p||u) \geq 0$, where u is the uniform probability density on $[-\pi, \pi]$. However, as an example, if we take the probability density to be $p(x) = |x|^{-\frac{1}{\alpha}}/\mathcal{N}$ for $\alpha > 1$, where \mathcal{N} is a normalization factor, then the Rényi entropy $h_\alpha(p)$ diverges to $-\infty$. Note that the condition $h_\alpha(p) > -\infty$ is equivalent to the condition $\int_{-\pi}^{+\pi} d\phi p(\phi)^\alpha < \infty$.

Theorem S7. *Let $p : [-\pi, +\pi] \rightarrow \mathbb{R}_+$ be a probability density function with the property that one of its Rényi entropies is finite for some $\alpha_0 > 1$, i.e.*

$$\int_{-\pi}^{+\pi} d\phi p(\phi)^{\alpha_0} < \infty. \tag{S62}$$

Then the two-way assisted quantum capacity, the unassisted quantum capacity, the private capacity, the secret-key capacity, and all of the corresponding strong converse capacities of the associated bosonic dephasing channel \mathcal{N}_p coincide, and are given by the expression

$$\begin{aligned} Q(\mathcal{N}_p) &= Q^\dagger(\mathcal{N}_p) = P(\mathcal{N}_p) = P^\dagger(\mathcal{N}_p) = Q_{\leftrightarrow}(\mathcal{N}_p) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_p) = K(\mathcal{N}_p) = P_{\leftrightarrow}^\dagger(\mathcal{N}_p) \\ &= D(p||u) = \log_2(2\pi) - h(p) \\ &= \log_2(2\pi) - \int_{-\pi}^{\pi} d\phi p(\phi) \log_2 \frac{1}{p(\phi)}. \end{aligned} \tag{S63}$$

Here, $D(p||u)$ denotes the Kullback–Leibler divergence between p and the uniform probability density u over $[-\pi, \pi]$, and $h(p)$ is the differential entropy of p .

Remark S8. The condition on the Rényi entropy of p is of a purely technical nature. We expect it to be obeyed in all cases of practical interest. For example, it holds true provided that p is bounded on $[-\pi, \pi]$.

Remark S9. By using Hölder's inequality, it can be easily verified that if (S100) holds for $\alpha_0 \geq 1$ then it holds for all α such that $1 \leq \alpha \leq \alpha_0$.

Proof of Theorem S7. The smallest of all eight quantities is the unassisted quantum capacity $Q(\mathcal{N}_p)$, and the largest is $P_{\leftrightarrow}^{\dagger}(\mathcal{N}_p)$. Therefore, it suffices to prove that

$$Q(\mathcal{N}_p) \geq D(p||u), \quad P_{\leftrightarrow}^{\dagger}(\mathcal{N}_p) \leq D(p||u). \quad (\text{S64})$$

Note that it is elementary to verify that

$$D(p||u) = \int_{-\pi}^{+\pi} d\phi p(\phi) \log_2 \frac{p(\phi)}{1/(2\pi)} = \log_2(2\pi) - \int_{-\pi}^{+\pi} d\phi p(\phi) \log_2 \frac{1}{p(\phi)} = \log_2(2\pi) - h(p), \quad (\text{S65})$$

where the differential entropy $h(p)$ is defined by (S5).

To bound $Q(\mathcal{N}_p)$ from below, we need an ansatz for a state $|\Psi\rangle_{AA'}$ to plug into (S21). Letting A and A' be single-mode systems, we can consider the maximally entangled state $|\Phi_d\rangle_{AA'} := \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle_A |k\rangle_{A'}$ locally supported on the subspace spanned by first d Fock states $|k\rangle$ (see (S14)), where $k \in \{0, \dots, d-1\}$. Let us also define the truncated matrix

$$T_p^{(d)} := \Pi_d T \Pi_d = \sum_{h,k=0}^{d-1} T_{hk} |h\rangle\langle k|, \quad (\text{S66})$$

where

$$\Pi_d := \sum_{k=0}^{d-1} |k\rangle\langle k|. \quad (\text{S67})$$

Then note that

$$\begin{aligned} \omega_{p,d} &:= (I \otimes \mathcal{N}_p)(\Phi_d) \\ &= \frac{1}{d} \sum_{h,k=0}^{d-1} (I \otimes \mathcal{N}_p)(|hh\rangle\langle kk|) \\ &= \frac{1}{d} \sum_{h,k=0}^{d-1} (T_p)_{hk} |hh\rangle\langle kk| \\ &= \frac{1}{d} \Omega[T_p^{(d)}]. \end{aligned} \quad (\text{S68})$$

Consider that

$$\begin{aligned} Q(\mathcal{N}_p) &\stackrel{(i)}{=} \limsup_{d \rightarrow \infty} I_{\text{coh}}(A)B \left(I \otimes \mathcal{N}_p^{A' \rightarrow B} \right) (\Phi_d^{AA'}) \\ &\stackrel{(ii)}{=} \limsup_{d \rightarrow \infty} I_{\text{coh}}(A)B \omega_{p,d} \\ &\stackrel{(iii)}{=} \limsup_{d \rightarrow \infty} \left(\log_2 d - S(T_p^{(d)}/d) \right) \\ &\stackrel{(iv)}{=} \limsup_{d \rightarrow \infty} \left(\log_2 d + \frac{1}{d} \text{Tr} T_p^{(d)} \left(-\log_2 d + \log_2 T_p^{(d)} \right) \right) \\ &= \limsup_{d \rightarrow \infty} \frac{1}{d} \text{Tr} T_p^{(d)} \log_2 T_p^{(d)} \\ &\stackrel{(v)}{=} \int_{-\pi}^{\pi} \frac{d\phi}{2\pi} (2\pi p(\phi)) \log_2 (2\pi p(\phi)) \\ &= \log_2(2\pi) - \int_{-\pi}^{\pi} d\phi p(\phi) \log_2 \frac{1}{p(\phi)}. \end{aligned} \quad (\text{S69})$$

Here: (i) follows from the LSD theorem (S21); in (ii) we introduced the state $\omega_{p,d}$ defined by (S61); (iii) comes from (S22), due to the fact that $S(\Omega[\tau]) = S(\tau)$ on the one hand, and

$$\text{Tr}_A \omega_{p,d}^{AB} = \text{Tr}_A (I \otimes \mathcal{N}_p^{A' \rightarrow B})(\Phi_d^{AA'})$$

$$\begin{aligned}
&= \frac{1}{d} \text{Tr}_A \sum_{h,k=0}^{d-1} (T_p)_{hk} |h\rangle\langle k|_A \otimes |h\rangle\langle k|_B \\
&= \frac{1}{d} \sum_{h,k=0}^{d-1} (T_p)_{hk} \delta_{hk} |h\rangle\langle k|_B \\
&= \frac{1}{d} \sum_{k=0}^{d-1} |k\rangle\langle k|_B \\
&= \frac{\mathbb{1}_B}{d}
\end{aligned} \tag{S70}$$

and therefore $S(\text{Tr}_A(I \otimes \mathcal{N}_p^{A' \rightarrow B})(\Phi_d^{AA'})) = \log_2 d$ on the other; in (iv) we simply substituted the definition (S11) of von Neumann entropy; and finally in (v) we employed Lemma S6 with the choice $a(\phi) = 2\pi p(\phi)$. This is possible due to our assumption that (S100) holds for some $\alpha > 1$. Note that $F(x) = x \log_2 x$ satisfies $|F(x)| < x^\alpha$ for all $\alpha > 1$ and for all sufficiently large $x \in \mathbb{R}_+$. This concludes the proof of the lower bound on $Q(\mathcal{N}_p)$ in (S64). We remark in passing that the Szegő theorem has been applied before, although with an entirely different scope, in the context of quantum information theory [123].

We now establish the upper bound on $P_{\leftrightarrow}^{\dagger}(\mathcal{N}_p)$ in (S64). We claim that there is a sequence of LOCC protocols that can simulate \mathcal{N}_p using $\omega_{p,d}$ defined by (S68) as a resource state and with error vanishing as $d \rightarrow \infty$. To see why this is the case, let ρ be an arbitrary input state, and consider the d -dimensional teleportation protocol (S45) on ρ that uses $\omega_{p,d}$ as a resource. In formula, let us define

$$\mathcal{N}_{p,d}^{A' \rightarrow B}(\rho_{A'}) := \mathcal{T}_{A'AB \rightarrow B}^{(d)}(\rho_{A'} \otimes \omega_{p,d}^{AB}). \tag{S71}$$

We see that

$$\begin{aligned}
&\mathcal{N}_{p,d}^{A' \rightarrow B}(\rho_{A'}) \\
&\stackrel{\text{(vi)}}{=} \sum_{x,z=0}^{d-1} X(x)_B Z(z)_B \text{Tr}_{AA'} \left[\rho_{A'} \otimes \omega_{p,d}^{AB} X(x)_{A'} Z(z)_{A'} \Phi_d^{AA'} Z(z)_{A'}^{\dagger} X(x)_{A'}^{\dagger} \right] Z(z)_B^{\dagger} X(x)_B^{\dagger} \\
&\stackrel{\text{(vii)}}{=} \sum_{x,z=0}^{d-1} \sum_{h,k=0}^{d-1} \frac{1}{d} (T_p)_{hk} X(x)_B Z(z)_B \\
&\quad \text{Tr}_{AA'} \left[\rho_{A'} \otimes |hh\rangle\langle kk|_{AB} X(x)_{A'} Z(z)_{A'} \Phi_d^{AA'} Z(z)_{A'}^{\dagger} X(x)_{A'}^{\dagger} \right] Z(z)_B^{\dagger} X(x)_B^{\dagger} \\
&\stackrel{\text{(viii)}}{=} \sum_{x,z=0}^{d-1} \sum_{h,k=0}^{d-1} \frac{1}{d} (T_p)_{hk} X(x)_B Z(z)_B \\
&\quad \left(\text{Tr}_{AA'} \left[\rho_{A'} \otimes |h\rangle\langle k|_A Z(z)_A^{\dagger} X(x)_A^{\dagger} \Phi_d^{AA'} X(x)_A^* Z(z)_A^* \right] |h\rangle\langle k|_B \right) Z(z)_B^{\dagger} X(x)_B^{\dagger} \\
&\stackrel{\text{(ix)}}{=} \sum_{x,z=0}^{d-1} \sum_{h,k=0}^{d-1} \frac{1}{d} (T_p)_{hk} X(x)_B Z(z)_B \\
&\quad \left(e^{\frac{2\pi i}{d} z(k-h)} \text{Tr}_{AA'} \left[\rho_{A'} \otimes |h \oplus x\rangle\langle k \oplus x|_A \Phi_d^{AA'} \right] |h\rangle\langle k|_B \right) Z(z)_B^{\dagger} X(x)_B^{\dagger} \\
&\stackrel{\text{(x)}}{=} \sum_{x,z=0}^{d-1} \sum_{h,k=0}^{d-1} \frac{1}{d^2} (T_p)_{hk} X(x)_B Z(z)_B \left(e^{\frac{2\pi i}{d} z(k-h)} \rho_{h \oplus x, k \oplus x} |h\rangle\langle k|_B \right) Z(z)_B^{\dagger} X(x)_B^{\dagger} \\
&\stackrel{\text{(xi)}}{=} \sum_{x,z=0}^{d-1} \sum_{h,k=0}^{d-1} \frac{1}{d^2} (T_p)_{hk} \rho_{h \oplus x, k \oplus x} |h \oplus x\rangle\langle k \oplus x|_B \\
&= \sum_{x=0}^{d-1} \sum_{h,k=0}^{d-1} \frac{1}{d} (T_p)_{hk} \rho_{h \oplus x, k \oplus x} |h \oplus x\rangle\langle k \oplus x|_B \\
&\stackrel{\text{(xii)}}{=} \sum_{h,k=0}^{d-1} \left(\frac{1}{d} \sum_{x=0}^{d-1} (T_p)_{h \oplus x, k \oplus x} \right) \rho_{hk} |h\rangle\langle k|_B.
\end{aligned} \tag{S72}$$

In the above derivation, (vi) follows from (S45), (vii) from (S68), (viii) from the formula

$$M \otimes \mathbb{1} |\Phi_d\rangle = \mathbb{1} \otimes M^\top |\Phi_d\rangle, \quad (\text{S73})$$

valid for the maximally entangled state (S43) in any finite dimension, (ix) and (xi) from (S44), (x) from the identity

$$\text{Tr} \left[M_A \otimes N_{A'} \Phi_d^{AA'} \right] = \frac{1}{d} \text{Tr} [MN^\top], \quad (\text{S74})$$

and finally (xii) by a simple change of variable $h \oplus x \mapsto h, k \oplus x \mapsto k$, once one observes that

$$\sum_{x=0}^{d-1} (T_p)_{hk} \mapsto \sum_{x=0}^{d-1} (T_p)_{h \oplus x, k \oplus x} = \sum_{x=0}^{d-1} (T_p)_{h \ominus (-x'), k \ominus (-x')} = \sum_{x'=0}^{d-1} (T_p)_{h \oplus x', k \oplus x'}, \quad (\text{S75})$$

where $x' := -x$.

The calculation in (S72) shows that

$$\langle h | \mathcal{N}_{p,d}(\rho) | k \rangle = \left(\frac{1}{d} \sum_{x=0}^{d-1} (T_p)_{h \oplus x, k \oplus x} \right) \rho_{hk}. \quad (\text{S76})$$

We now want to argue that for fixed $h, k \in \mathbb{N}$ the above quantity converges to $(T_p)_{hk} \rho_{hk} = \langle h | \mathcal{N}_p(\rho) | k \rangle$ as $d \rightarrow \infty$. To this end, note that if $d \geq h, k$ we have that $(T_p)_{h \oplus x, k \oplus x} = T_{hk}$ provided that either $x \leq \min\{d-1-h, d-1-k\} = \min\{d-h, d-k\} - 1$ or $x \geq \max\{d-h, d-k\}$. Therefore, $(T_p)_{h \oplus x, k \oplus x} \neq T_{hk}$ for at most $|h-k|$ values of x , out of the d possible ones. We can estimate the remainder terms pretty straightforwardly using the inequality $|(T_p)_{hk}| \leq 1$, valid for all $h, k \in \mathbb{N}$. Doing so yields

$$\begin{aligned} \left| (T_p)_{hk} - \frac{1}{d} \sum_{x=0}^{d-1} (T_p)_{h \oplus x, k \oplus x} \right| &\leq \left| (T_p)_{hk} - \frac{d-|h-k|}{d} (T_p)_{hk} \right| + \frac{|h-k|}{d} \\ &\leq \frac{2|h-k|}{d} \xrightarrow{d \rightarrow \infty} 0. \end{aligned} \quad (\text{S77})$$

Thus, for all fixed $h, k \in \mathbb{N}$,

$$\langle h | \mathcal{N}_{p,d}(\rho) | k \rangle \xrightarrow{d \rightarrow \infty} \langle h | \mathcal{N}_p(\rho) | k \rangle \quad \forall \rho, \quad (\text{S78})$$

as claimed. We now argue that this implies the stronger fact that

$$\lim_{d \rightarrow \infty} \left\| ((\mathcal{N}_{p,d} - \mathcal{N}_p)_{A \rightarrow B} \otimes I_E) (\rho_{A'E}) \right\|_1 = 0 \quad \forall \rho_{A'E}, \quad (\text{S79})$$

where it is understood that $\rho_{A'E}$ is an arbitrary, but fixed state of a bipartite system $A'E$, with the quantum system E arbitrary. The above identity is usually expressed in words by saying that $\mathcal{N}_{p,d}$ converges to \mathcal{N}_p in the *topology of strong convergence* [124, 125]. The arguments that allow to deduce (S79) from (S78) are standard:

(a) Since the linear span of the Fock states $\{|k\rangle\}_{k \in \mathbb{N}}$ is dense in \mathcal{H}_1 and moreover the operators $\mathcal{N}_{p,d}(\rho), \mathcal{N}_p(\rho)$ are uniformly bounded in trace norm — since they are states, they all have trace norm 1 — we see that (S78) actually holds also when $|h\rangle, |k\rangle$ are replaced by any two fixed vectors $|\psi\rangle, |\phi\rangle \in \mathcal{H}_1$. In formula,

$$\langle \psi | \mathcal{N}_{p,d}(\rho) | \phi \rangle \xrightarrow{d \rightarrow \infty} \langle \psi | \mathcal{N}_p(\rho) | \phi \rangle \quad \forall \rho, \quad \forall |\psi\rangle, |\phi\rangle \in \mathcal{H}_1. \quad (\text{S80})$$

(b) Therefore, by definition $\mathcal{N}_{p,d}(\rho)$ converges to $\mathcal{N}_p(\rho)$ in the *weak operator topology*. Since the latter object is also a quantum state, an old result due to Davies [126, Lemma 4.3], which can also be seen as an elementary consequence of the ‘gentle measurement lemma’ [127, Lemma 9] (see also [128, Lemmata 9.4.1 and 9.4.2]), states that in fact there is trace norm convergence, i.e.

$$\lim_{d \rightarrow \infty} \left\| (\mathcal{N}_{p,d} - \mathcal{N}_p) (\rho) \right\|_1 = 0 \quad \forall \rho. \quad (\text{S81})$$

(c) The topology of strong convergence is stable under tensor products with the identity channel [124] (see also [125, Lemma 2]). Therefore, (S81) and (S79) are in fact equivalent. Since we have proved the former, the latter also follows.

We are now ready to prove that $P_{\leftrightarrow}^{\dagger}(\mathcal{N}_p) \leq D(p\|u)$. For a fixed positive integer $n \in \mathbb{N}_+$, consider a generic protocol as the one depicted in Figure S3, where the channel \mathcal{N} is now \mathcal{N}_p . Since we are dealing with the secret-key-agreement capacity, the final state η_n will approximate a private state γ_n containing $\lceil Rn \rceil$ secret bits [82, 83]. Here, R is an achievable strong converse rate of secret-key agreement. Call $\epsilon_n := \frac{1}{2} \|\eta_n - \gamma_n\|_1$ the corresponding trace norm error, so that

$$\limsup_{n \rightarrow \infty} \epsilon_n < 1. \quad (\text{S82})$$

Imagine now to replace each instance of \mathcal{N}_p with its simulation $\mathcal{N}_{p,d}$. This will yield at the output a state $\eta_{n,d}$, in general different from η_n ; however, because of (S79), and since n here is fixed, we have that the associated error $\delta_{n,d}$ vanishes as $d \rightarrow \infty$, i.e.

$$\delta_{n,d} := \frac{1}{2} \|\eta_{n,d} - \eta_n\|_1 \xrightarrow{d \rightarrow \infty} 0. \quad (\text{S83})$$

Now, after the above replacement the global protocol can be seen as an LOCC manipulation of n copies of the state $\omega_{p,d}$ that is used to simulate $\mathcal{N}_{p,d}$ as per (S71). By the triangle inequality, the trace distance between the final state $\eta_{n,d}$ and the private state γ_n satisfies

$$\frac{1}{2} \|\eta_{n,d} - \gamma_n\|_1 \leq \frac{1}{2} \|\eta_{n,d} - \eta_n\|_1 + \frac{1}{2} \|\eta_n - \gamma_n\|_1 \leq \delta_{n,d} + \epsilon_n. \quad (\text{S84})$$

To apply the results of [129], we need to translate the above estimate into one that uses the fidelity instead of the trace distance. Such a translation can be made with the help of the Fuchs–van de Graaf inequalities [89], here reported as (S1). We obtain that $F(\eta_{n,d}, \gamma_n) \geq (1 - \delta_{n,d} - \epsilon_n)^2$. We can then use [129, Eq. (5.37)] directly to deduce that

$$(1 - \delta_{n,d} - \epsilon_n)^2 \leq F(\eta_{n,d}, \gamma_n) \leq 2^{-n \frac{\alpha-1}{\alpha}} (R - \tilde{E}_{R,\alpha}(\omega_{p,d})) \quad (\text{S85})$$

for all $1 < \alpha \leq \alpha_0$, where

$$\tilde{E}_{R,\alpha}(\rho_{AB}) := \inf_{\sigma \in \mathcal{S}_{AB}} \tilde{D}_{\alpha}(\rho\|\sigma) \quad (\text{S86})$$

is the *sandwiched α -Rényi relative entropy of entanglement*, and

$$\mathcal{S}_{AB} := \text{conv} \{ |\psi\rangle\langle\psi|_A \otimes |\phi\rangle\langle\phi|_B : |\psi\rangle_A \in \mathcal{H}_A, |\phi\rangle_B \in \mathcal{H}_B, \langle\psi|\psi\rangle = 1 = \langle\phi|\phi\rangle \} \quad (\text{S87})$$

is the set of *separable states* over the bipartite quantum system AB . We can immediately recast (S85) to obtain

$$R \leq \frac{2}{n} \frac{\alpha}{\alpha-1} \log_2 \frac{1}{1 - \delta_{n,d} - \epsilon_n} + \tilde{E}_{R,\alpha}(\omega_{p,d}) \quad (\text{S88})$$

Let us now estimate the quantity $\tilde{E}_{R,\alpha}(\omega_{p,d})$. By taking as an ansatz for a separable state to be plugged into (S86) simply $\Omega[\Pi_d/d]$ (see (S61) and (S67)), which is manifestly separable because Π_d is diagonal, we conclude that

$$\begin{aligned} \tilde{E}_{R,\alpha}(\omega_{p,d}) &\leq \tilde{D}_{\alpha} \left(\omega_{p,d} \left\| \Omega \left[\frac{\Pi_d}{d} \right] \right. \right) \\ &\stackrel{\text{(xiii)}}{=} \frac{1}{\alpha-1} \log_2 \text{Tr} \omega_{p,d}^{\alpha} \Omega \left[\frac{\Pi_d}{d} \right]^{1-\alpha} \\ &\stackrel{\text{(xiv)}}{=} \frac{1}{\alpha-1} \log_2 \frac{1}{d} \text{Tr} \left(T_p^{(d)} \right)^{\alpha} \end{aligned} \quad (\text{S89})$$

Here, (xiii) follows from (S9), while in (xiv) we simply recalled (S68).

Now, applying Lemma S6 once again with $a(\phi) = 2\pi p(\phi)$, we know that

$$\lim_{d \rightarrow \infty} \frac{1}{d} \text{Tr} \left[\left(T_p^{(d)} \right)^{\alpha} \right] = \int_{-\pi}^{+\pi} \frac{d\phi}{2\pi} (2\pi p(\phi))^{\alpha} = (2\pi)^{\alpha-1} \int_{-\pi}^{+\pi} d\phi p(\phi)^{\alpha}. \quad (\text{S90})$$

Therefore, from (S89) we deduce that

$$\limsup_{d \rightarrow \infty} \tilde{E}_{R,\alpha}(\omega_{p,d}) \leq \log_2(2\pi) + \log_2 \int_{-\pi}^{+\pi} d\phi p(\phi)^{\alpha} = D_{\alpha}(p\|u), \quad (\text{S91})$$

where D_α is the α -Rényi divergence defined by (S2). Due to both (S91) and (S83), taking the limit $d \rightarrow \infty$ in (S88) yields

$$R \leq \frac{2}{n} \frac{\alpha}{\alpha - 1} \log_2 \frac{1}{1 - \epsilon_n} + D_\alpha(p\|u). \quad (\text{S92})$$

We are now ready to take the limit $n \rightarrow \infty$. In light of (S82), we obtain that

$$R \leq \liminf_{n \rightarrow \infty} \left(\frac{2}{n} \frac{\alpha}{\alpha - 1} \log_2 \frac{1}{1 - \epsilon_n} + D_\alpha(p\|u) \right) = D_\alpha(p\|u). \quad (\text{S93})$$

The limit as $\alpha \rightarrow 1^+$ can be computed via Lemma S1 (and in particular (S4)), due to the condition (S100), which can be rephrased as $D_{\alpha_0}(p\|u) < \infty$. It gives

$$R \leq \liminf_{\alpha \rightarrow 1^+} D_\alpha(p\|u) = D(p\|u). \quad (\text{S94})$$

Since R was an arbitrary achievable strong converse rate for secret-key agreement, we deduce that

$$P_{\leftrightarrow}^\dagger(\mathcal{N}_p) \leq D(p\|u), \quad (\text{S95})$$

completing the proof. \square

C. Extension to multimode channels

We will now see how to extend our main result, Theorem S7, to the case of a multimode bosonic dephasing channel. An m -mode quantum system ($m \in \mathbb{N}_+$) is modelled mathematically by the Hilbert space $\mathcal{H}_m = \mathcal{H}_1^{\otimes m} = L^2(\mathbb{R})^{\otimes m} = L^2(\mathbb{R}^m)$. The annihilation and creation operators a_j, a_j^\dagger ($j = 1, \dots, m$), defined by

$$a_1 := a \otimes \mathbb{1} \otimes \dots \otimes \mathbb{1}, \quad \dots, \quad a_m := \mathbb{1} \otimes \dots \otimes \mathbb{1} \otimes a \quad (\text{S96})$$

in terms of the single-mode operators in (S12), satisfy the canonical commutation relations

$$[a_j, a_k] = 0 = [a_j^\dagger, a_k^\dagger], \quad [a_j, a_k^\dagger] = \delta_{jk} \mathbb{1}. \quad (\text{S97})$$

The multimode Fock states $|\mathbf{k}\rangle$, indexed by $\mathbf{k} = (k_1, \dots, k_m)^\top \in \mathbb{N}^m$, are given by

$$|\mathbf{k}\rangle := |k_1\rangle \otimes \dots \otimes |k_m\rangle. \quad (\text{S98})$$

Now, for a probability density function p on $[-\pi, \pi]^m$, the corresponding **multimode bosonic dephasing channel** is the quantum channel $\mathcal{N}_p^{(m)} : \mathcal{T}(\mathcal{H}_m) \rightarrow \mathcal{T}(\mathcal{H}_m)$ defined by

$$\mathcal{N}_p^{(m)}(\rho) := \int_{[-\pi, \pi]^m} d^m \boldsymbol{\phi} p(\boldsymbol{\phi}) e^{-i \sum_j a_j^\dagger \phi_j} \rho e^{i \sum_j a_j \phi_j}, \quad (\text{S99})$$

where $j = 1, \dots, m$, and $\boldsymbol{\phi} = (\phi_1, \dots, \phi_m)^\top$.

In perfect analogy with Theorem S7, we can now prove the following.

Theorem S10. *Let $p : [-\pi, +\pi]^m \rightarrow \mathbb{R}_+$ be a probability density function with the property that one of its Rényi entropies is finite for some $\alpha_0 > 1$, i.e.*

$$\int_{[-\pi, \pi]^m} d^m \boldsymbol{\phi} p(\boldsymbol{\phi})^{\alpha_0} < \infty. \quad (\text{S100})$$

Then the two-way assisted quantum capacity, the unassisted quantum capacity, the private capacity, the secret-key capacity, and all of the corresponding strong converse rates of the associated multimode bosonic dephasing channel $\mathcal{N}_p^{(m)}$ coincide, and are given by the expression

$$\begin{aligned} Q(\mathcal{N}_p^{(m)}) &= Q^\dagger(\mathcal{N}_p^{(m)}) = P(\mathcal{N}_p^{(m)}) = P^\dagger(\mathcal{N}_p^{(m)}) = Q_{\leftrightarrow}(\mathcal{N}_p^{(m)}) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_p^{(m)}) = P_{\leftrightarrow}(\mathcal{N}_p^{(m)}) = P_{\leftrightarrow}^\dagger(\mathcal{N}_p^{(m)}) \\ &= D(p\|u) = m \log_2(2\pi) - h(p) \\ &= m \log_2(2\pi) - \int_{[-\pi, \pi]^m} d^m \boldsymbol{\phi} p(\boldsymbol{\phi}) \log_2 \frac{1}{p(\boldsymbol{\phi})}. \end{aligned} \quad (\text{S101})$$

Here, $D(p\|u)$ denotes the Kullback–Leibler divergence between p and the uniform probability distribution u over $[-\pi, \pi]^m$, and $h(p)$ is the differential entropy of p .

Rather unsurprisingly, one of the key technical tools that we need to prove the above generalization of Theorem S7 is a multi-index version of the Szegő theorem reported here as Lemma S6. In fact, the original paper by Serra-Capizzano [66] deals already with multi-indices, so we can borrow the following result directly from [66, Theorem 2] (cf. also the proof of Lemma S6).

An *multi-index infinite Toeplitz matrix* is an operator $T : \ell^2(\mathbb{N}^m) \rightarrow \ell^2(\mathbb{N}^m)$ with the property that its matrix entries $T_{\mathbf{h}, \mathbf{k}}$ (where $|\mathbf{h}\rangle = (h_1, \dots, h_m)^\top \in \mathbb{N}^m$ is a multi-index) depend only on the difference $\vec{h} - \vec{k}$, in formula $T_{\mathbf{h}, \mathbf{k}} = a_{\mathbf{h}-\mathbf{k}}$. The case of interest is when

$$a_{\mathbf{k}} = \int_{[-\pi, \pi]^m} d^m \phi \, a(\phi) \, e^{-i\mathbf{k} \cdot \phi}, \quad (\text{S102})$$

where $a : [-\pi, \pi]^m \rightarrow \mathbb{R}_+$ is a non-negative function, and $\mathbf{k} \cdot \phi := \sum_{j=1}^m k_j \phi_j$. As in the setting of Szegő's theorem, one considers the truncations of T defined for some $\mathbf{d} = (d_1, \dots, d_m)^\top \in \mathbb{N}^m$ by

$$T^{(\mathbf{d})} := \sum_{h_1, k_1=0}^{d_1-1} \dots \sum_{h_m, k_m=0}^{d_m-1} T_{\mathbf{h}, \mathbf{k}} |\mathbf{h}\rangle \langle \mathbf{k}|. \quad (\text{S103})$$

Note that $T^{(\mathbf{d})}$ is an operator on a space of dimension

$$D(\mathbf{d}) := \prod_{j=1}^m d_j. \quad (\text{S104})$$

The multi-index Szegő theorem then reads

$$\lim_{\mathbf{d} \rightarrow \infty} \frac{1}{D(\mathbf{d})} \text{Tr} F(T^{(\mathbf{d})}) = \lim_{\mathbf{d} \rightarrow \infty} \frac{1}{D(\mathbf{d})} \sum_{j=1}^{D(\mathbf{d})} F(\lambda_j(T^{(\mathbf{d})})) = \int_{[-\pi, \pi]^m} \frac{d\phi}{(2\pi)^m} F(a(\phi)), \quad (\text{S105})$$

where $F : \mathbb{R} \rightarrow \mathbb{R}$, and $\mathbf{d} \rightarrow \infty$ means that $\min_{j=1, \dots, m} d_j \rightarrow \infty$. Conditions on a and F so that (S105) holds are as follows.

Lemma S11 (Serra-Capizzano [66], multi-index case). *If $a : [-\pi, \pi]^m \rightarrow \mathbb{R}_+$ is such that*

$$\int_{[-\pi, \pi]^m} \frac{d^m \phi}{(2\pi)^m} a(\phi)^\alpha < \infty \quad (\text{S106})$$

for some $\alpha \geq 1$, and moreover $F : \mathbb{R}_+ \rightarrow \mathbb{R}$ is continuous and satisfies

$$F(x) = O(x^\alpha) \quad (x \rightarrow \infty), \quad (\text{S107})$$

then (S105) holds.

The proof of Theorem S10 follows very closely that of Theorem S7. Let us briefly summarize the main differences.

Proof of Theorem S10. As an ansatz in the coherent information (S69), we use a multimode maximally entangled state, defined by

$$|\Phi_{\mathbf{d}}\rangle := \frac{1}{D(\mathbf{d})} \sum_{k_1=0}^{d_1-1} \dots \sum_{k_m=0}^{d_m-1} |\mathbf{k}\rangle_A |\mathbf{k}\rangle_{A'}, \quad (\text{S108})$$

where $\mathbf{d} \in \mathbb{N}^m$ is fixed for now. Since

$$\omega_{p, \mathbf{d}} := \left(I \otimes \mathcal{N}_p^{(m)} \right) (\Phi_{\mathbf{d}}) = \frac{1}{D(\mathbf{d})} \Omega[T_p^{\mathbf{d}}] \quad (\text{S109})$$

is still a maximally correlated state, the derivation in (S69) is unaffected, provided that one employs in (v) Lemma S11.

As for the converse bound on the strong converse rate, one replaces (S71) with

$$(\mathcal{N}_{p, \mathbf{d}}^{(m)})_{A' \rightarrow B}(\rho_{A'}) := \left(\bigotimes_{j=1}^m \mathcal{T}_{A'_j A_j B_j \rightarrow B_j}^{(d_j)} \right) (\rho_{A'} \otimes \omega_{p, \mathbf{d}}^{AB}), \quad (\text{S110})$$

where A_j denotes the j^{th} mode of A , and analogously for A' and B . Then (S72) becomes

$$(\mathcal{N}_{p,\mathbf{d}}^{(m)})_{A' \rightarrow B}(\rho_{A'}) = \sum_{h_1, k_1=0}^{d_1-1} \cdots \sum_{h_m, k_m=0}^{d_m-1} \left(\frac{1}{D(\mathbf{d})} \sum_{x_1=0}^{d_1-1} \cdots \sum_{x_m=0}^{d_m-1} (T_p)_{\mathbf{h} \oplus \mathbf{x}, \mathbf{k} \oplus \mathbf{x}} \right) \rho_{\mathbf{h}, \mathbf{k}} |\mathbf{h}\rangle\langle\mathbf{k}|_B. \quad (\text{S111})$$

We can write an inequality analogous to (S77) as

$$\begin{aligned} & \left| (T_p)_{\mathbf{h}, \mathbf{k}} - \frac{1}{D(\mathbf{d})} \sum_{x_1=0}^{d_1-1} \cdots \sum_{x_m=0}^{d_m-1} (T_p)_{\mathbf{h} \oplus \mathbf{x}, \mathbf{k} \oplus \mathbf{x}} \right| \\ & \leq \left| (T_p)_{\mathbf{h}, \mathbf{k}} - \frac{\prod_{j=1}^m (d_j - |h_j - k_j|)}{D(\mathbf{d})} (T_p)_{\mathbf{h}, \mathbf{k}} \right| + \frac{D(\mathbf{d}) - \prod_{j=1}^m (d_j - |h_j - k_j|)}{D(\mathbf{d})} \\ & \leq 2 \frac{D(\mathbf{d}) - \prod_{j=1}^m (d_j - |h_j - k_j|)}{D(\mathbf{d})} \xrightarrow{\mathbf{d} \rightarrow \infty} 0. \end{aligned} \quad (\text{S112})$$

In the exact same way, one uses the above inequality to prove a generalized version of (S79) as

$$\lim_{\mathbf{d} \rightarrow \infty} \left\| \left((\mathcal{N}_{p,\mathbf{d}}^{(m)} - \mathcal{N}_p^{(m)})_{A' \rightarrow B} \otimes I_E \right) (\rho_{A'E}) \right\|_1 = 0 \quad \forall \rho_{A'E}. \quad (\text{S113})$$

The combination of (S89) and (S90) now becomes

$$\tilde{E}_{R,\alpha}(\omega_{p,\mathbf{d}}) \leq \frac{1}{\alpha-1} \log_2 \frac{1}{D(\mathbf{d})} \text{Tr} \left[(T_p^{\mathbf{d}})^{\alpha} \right] \xrightarrow{\mathbf{d} \rightarrow \infty} \frac{1}{\alpha-1} \log_2 (2\pi)^{m(\alpha-1)} \int_{[-\pi, \pi]^m} d\boldsymbol{\phi} p(\boldsymbol{\phi})^{\alpha}, \quad (\text{S114})$$

so that we find, precisely as in (S91), that

$$\limsup_{\mathbf{d} \rightarrow \infty} \tilde{E}_{R,\alpha}(\omega_{p,\mathbf{d}}) \leq m \log_2(2\pi) + \frac{1}{\alpha-1} \log_2 \int_{[-\pi, \pi]^m} d\boldsymbol{\phi} p(\boldsymbol{\phi})^{\alpha} = D_{\alpha}(p\|u). \quad (\text{S115})$$

The rest of the proof is formally identical. \square

III. EXAMPLES

A. Wrapped normal distribution

The most commonly studied [30, 51] example of the bosonic dephasing channel is that which yields in (S51) a matrix T_p with entries

$$(T_{p_{\gamma}})_{hk} = e^{-\frac{\gamma}{2}(h-k)^2}, \quad (\text{S116})$$

where $\gamma > 0$ is a parameter. The probability density function $p : [-\pi, +\pi] \rightarrow \mathbb{R}_+$ that gives rise to this matrix is a **wrapped normal distribution**, that is, a normal distribution on \mathbb{R} with variance γ ‘wrapped’ around the unit circle. In formula, this is given by

$$p_{\gamma}(\phi) = \frac{1}{\sqrt{2\pi\gamma}} \sum_{k=-\infty}^{+\infty} e^{-\frac{1}{2\gamma}(\phi+2\pi k)^2}. \quad (\text{S117})$$

Its entropy can be expressed as [59, Chapter 3, § 3.3]

$$h(p_{\gamma}) = \frac{1}{\ln 2} \left(-\ln \left(\frac{\varphi(e^{-\gamma})}{2\pi} \right) + 2 \sum_{k=1}^{\infty} \frac{(-1)^k e^{-\frac{\gamma}{2}(k^2+k)}}{k(1-e^{-k\gamma})} \right), \quad (\text{S118})$$

where

$$\varphi(q) := \prod_{k=1}^{\infty} (1 - q^k) \quad (\text{S119})$$

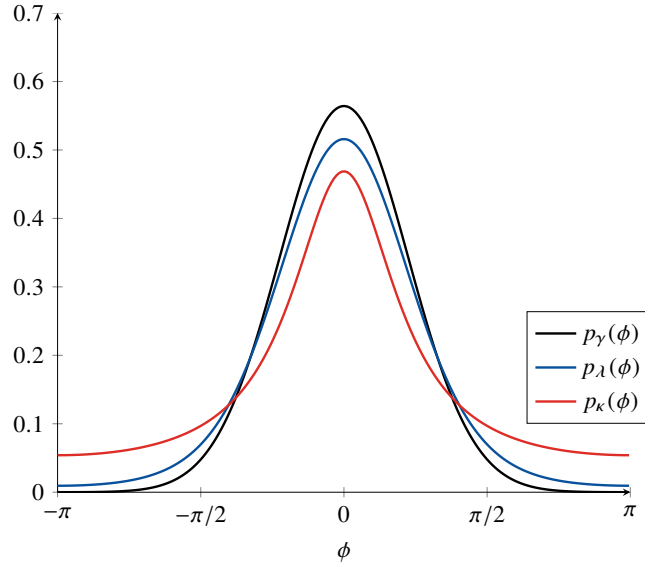


FIG. S4: The probability density functions of the wrapped normal (S117), von Mises (S126), and wrapped Cauchy distributions (S132), plotted as a function of $\phi \in [-\pi, \pi]$ for the

is the Euler function. Therefore, the capacities of the channel \mathcal{N}_{p_γ} are given by

$$\begin{aligned} Q(\mathcal{N}_{p_\gamma}) &= Q^\dagger(\mathcal{N}_{p_\gamma}) = P(\mathcal{N}_{p_\gamma}) = P^\dagger(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) \\ &= D(p_\gamma \| u) = \log_2 \varphi(e^{-\gamma}) + \frac{2}{\ln 2} \sum_{k=1}^{\infty} \frac{(-1)^{k-1} e^{-\frac{\gamma}{2}(k^2+k)}}{k(1-e^{-k\gamma})}. \end{aligned} \quad (\text{S120})$$

It is instructive to obtain asymptotic expansions of the above expressions in the limits $\gamma \ll 1$ (small dephasing) and $\gamma \gg 1$ (large dephasing).

- *Small dephasing.* When $\gamma \rightarrow 0^+$, the channel \mathcal{N}_{p_γ} approaches the identity over an infinite-dimensional Hilbert space. Therefore, it is intuitive to expect that its capacities will diverge. To determine its asymptotic behavior, it suffices to note that in this limit the entropy of the wrapped normal distribution, which is very concentrated around 0, is well approximated by that of the corresponding normal variable on the whole \mathbb{R} , i.e., $\frac{1}{2} \log_2(2\pi e\gamma)$. Thus

$$\begin{aligned} Q(\mathcal{N}_{p_\gamma}) &= Q^\dagger(\mathcal{N}_{p_\gamma}) = P(\mathcal{N}_{p_\gamma}) = P^\dagger(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) \\ &\approx \frac{1}{2} \log_2 \frac{2\pi}{e\gamma}. \end{aligned} \quad (\text{S121})$$

- *Large dephasing.* A straightforward computation using the series representation

$$-\ln \varphi(q) = \sum_{k=1}^{\infty} \frac{1}{k} \frac{q^k}{1-q^k}, \quad (\text{S122})$$

yields the expansion

$$\begin{aligned} \ln \varphi(q) + 2 \sum_{k=1}^{\infty} \frac{(-1)^{k-1} q^{-\frac{1}{2}(k^2+k)}}{k(1-q^k)} &= q + \frac{q^2}{2} - \frac{q^3}{3} + \frac{q^4}{4} - \frac{q^5}{5} + \frac{2q^6}{3} + O(q^7) \\ &= 2q - \ln(1+q) + O(q^6). \end{aligned} \quad (\text{S123})$$

This can be plugged into (S120) to give

$$\begin{aligned} Q(\mathcal{N}_{p_\gamma}) &= Q^\dagger(\mathcal{N}_{p_\gamma}) = P(\mathcal{N}_{p_\gamma}) = P^\dagger(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) \\ &= \frac{2}{\ln 2} e^{-\gamma} - \log_2(1+e^{-\gamma}) + O(e^{-6\gamma}) \\ &= \frac{e^{-\gamma}}{\ln 2} + O(e^{-2\gamma}). \end{aligned} \quad (\text{S124})$$

Incidentally, the combination of these two regimes yields an excellent approximation of the capacities across the whole range of $\gamma > 0$. Namely,

$$\begin{aligned} Q(\mathcal{N}_{p_\gamma}) &= Q^\dagger(\mathcal{N}_{p_\gamma}) = P(\mathcal{N}_{p_\gamma}) = P^\dagger(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}(\mathcal{N}_{p_\gamma}) = P_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\gamma}) \\ &\approx \max \left\{ \frac{1}{2} \log_2 \frac{2\pi}{e\gamma}, \frac{2}{\ln 2} e^{-\gamma} - \log_2 (1 + e^{-\gamma}) \right\}. \end{aligned} \quad (\text{S125})$$

The maximum difference between the left-hand side and the right-hand side for $\gamma > 0$ is less than 4×10^{-3} .

B. Von Mises distribution

The *von Mises distribution* on $[-\pi, +\pi]$ is defined by

$$p_\lambda(\phi) = \frac{e^{\frac{1}{\lambda} \cos(\phi)}}{2\pi I_0(1/\lambda)}, \quad (\text{S126})$$

where I_n denotes a modified Bessel function of the first kind. Here, $\lambda > 0$ is a parameter that plays a role analogous to that $\gamma > 0$ played in the case of the wrapped normal. The matrix T_{p_λ} obtained in (S51) for $p = p_\lambda$ is given by

$$(T_{p_\lambda})_{hk} = \frac{I_{|h-k|}(1/\lambda)}{I_0(1/\lambda)}. \quad (\text{S127})$$

The differential entropy of p_λ can be calculated analytically, yielding [59, Chapter 3, Section 3.3]

$$h(p_\lambda) = \log_2(2\pi I_0(1/\lambda)) - \frac{1}{\ln 2} \frac{I_1(1/\lambda)}{\lambda I_0(1/\lambda)}. \quad (\text{S128})$$

Therefore, the capacities of the corresponding bosonic dephasing channel are given by

$$\begin{aligned} Q(\mathcal{N}_{p_\lambda}) &= Q^\dagger(\mathcal{N}_{p_\lambda}) = P(\mathcal{N}_{p_\lambda}) = P^\dagger(\mathcal{N}_{p_\lambda}) = Q_{\leftrightarrow}(\mathcal{N}_{p_\lambda}) = Q_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\lambda}) = P_{\leftrightarrow}(\mathcal{N}_{p_\lambda}) = P_{\leftrightarrow}^\dagger(\mathcal{N}_{p_\lambda}) \\ &= \frac{1}{\ln 2} \frac{I_1(1/\lambda)}{\lambda I_0(1/\lambda)} - \log_2 I_0(1/\lambda). \end{aligned} \quad (\text{S129})$$

C. Wrapped Cauchy distribution

Our final example of a probability distribution on the circle, and of the bosonic dephasing channel associated to it, is defined similarly to the wrapped normal distribution, but this time starting from the Cauchy probability density function. Namely, for some parameter $\kappa > 0$ we set

$$p_\kappa(\phi) := \sum_{k=-\infty}^{+\infty} \frac{\sqrt{\kappa}}{\pi \left(\kappa + (\phi + 2\pi k)^2 \right)} = \frac{1}{2\pi} \frac{\sinh(\sqrt{\kappa})}{\cosh(\sqrt{\kappa}) - \cos \phi}. \quad (\text{S130})$$

For a proof of the second identity, see [130, p. 51]. The matrix T_{p_κ} obtained in (S51) for $p = p_\kappa$ is given by

$$(T_{p_\kappa})_{hk} = e^{-\sqrt{\kappa}|h-k|}. \quad (\text{S131})$$

The differential entropy of p_κ is equal to $\log_2(2\pi(1 - e^{-2\sqrt{\kappa}}))$ [59, Chapter 3, § 3.3], implying that the various capacities of the corresponding bosonic dephasing channel \mathcal{N}_{p_κ} are equal to

$$\mathcal{C}(\mathcal{N}_{p_\kappa}) = \log_2 \left(\frac{1}{1 - e^{-2\sqrt{\kappa}}} \right). \quad (\text{S132})$$