Minimum output entropy of bosonic channels: A conjecture

Vittorio Giovannetti,[1,*] Saikat Guha,[1] Seth Lloyd,[1,2] Lorenzo Maccone,[1,†] and Jeffrey H. Shapiro[1]

[1]*Massachusetts Institute of Technology, Research Laboratory of Electronics, 77 Massachusetts Avenue,
Cambridge, Massachusetts 02139, USA*

[2]*Massachusetts Institute of Technology, Department of Mechanical Engineering 77 Massachusetts Avenue,
Cambridge, Massachusetts 02139, USA*

The von Neumann entropy at the output of a bosonic channel with thermal noise is analyzed. Coherent-state inputs are conjectured to minimize this output entropy. Physical and mathematical evidence in support of the conjecture is provided. A stronger conjecture—that output states resulting from coherent-state inputs majorize the output states from other inputs—is also discussed.

I. INTRODUCTION

A quantum channel can be characterized by a completely positive (CP) linear superoperator on the Hilbert space of the information carrier. In general this evolution is not unitary, so that a pure state loses some coherence in its transit through the channel. Various measures of a channel's ability to preserve the coherence of its input state have been introduced. Arguably, the most useful of these are the information capacities [1–3]. In contrast, we will focus on the minimum von Neumann entropy $\mathbb{S}$ at the channel output. This quantity is related to the minimum amount of noise implicit in the channel: when the channel input is a pure state, $\mathbb{S}$ quantifies the minimum uncertainty occurring in the resulting channel output. More precisely, the output entropy associated with a pure state measures the entanglement that such a state establishes with the environment during the communication. Because the state of the environment is not accessible, this entanglement is responsible for the loss of quantum coherence and hence for the injection of noise into the channel output. Low values of entanglement, i.e., of $\mathbb{S}$, then correspond to low-noise communication. Furthermore, the study of $\mathbb{S}$ yields important information about channel capacities. In particular, an upper bound on the classical capacity derives from a lower bound on the output entropy of multiple channel uses, see, e.g., [4,5]. Finally, the additivity of the minimum entropy implies the additivity of the classical capacity and of the entanglement of formation [6].

Our study of minimum output entropy will be restricted to bosonic channels in which the electromagnetic field, used as the information carrier, interacts with a thermal-like noise source. For these channels we analyze the following conjecture: that minimum output entropy is achieved when the channel input is a coherent state. In what follows, the rationale and some physical justification for this conjecture are presented. We also consider a stronger conjecture—that output states resulting from coherent-state inputs majorize the output states from other inputs—which, if true, would imply the minimum output entropy conjecture. (Note that the minimum output entropy problem was previously treated in [7], which reported some of the results that we will discuss.) Additional supporting evidence for the minimum-entropy conjecture appears in our companion paper [8], where we show that the integer-order Rényi entropies and the Wehrl entropy at the output of the bosonic channel are minimized when the channel input is a coherent state.

In Sec. II we present CP maps for the two bosonic channels that will be considered in this paper. The minimum output entropy conjecture and its stronger (majorization) version are then stated and explained. In Sec. III we analyze the two channel maps in detail, and develop some useful properties of their output entropies. In Sec. IV we prove the minimum output entropy conjecture for the restricted scenario in which only Gaussian states may be fed into the channel. In Sec. V we present a collection of lower bounds on $\mathbb{S}$. These lower bounds are consistent with the minimum output entropy conjecture. Moreover, in the low- and high-noise regimes they approach asymptotically the upper bounds from which the conjecture arises. In Sec. VI we obtain necessary conditions on any input state that minimizes the output entropy. We demonstrate, in particular, that every coherent-state input produces an output state that achieves a local minimum of the output entropy. Finally, in Sec. VII we address the stronger version of the conjecture by exhibiting some evidence that output states produced by coherent-state inputs majorize all other output states. The paper is structured so that Secs. IV and VII may be read independently. The most technical parts of the derivations have been relegated to the Appendices.

II. CHANNEL MODELS

We will consider two bosonic channels—the thermal-noise channel and the classical-noise channel—both of which belong to the class of Gaussian CP maps, i.e., they evolve Gaussian inputs states into Gaussian output states [9]. Although we will limit our attention to single-mode chan-

---

*Present address: NEST-INFM and Scuola Normale Superiore, Piazza dei Cavalieri 7, I-56126, Pisa, Italy.

†Present address: QUIT-Quantum Information Theory Group Dipartimento di Fisica "A. Volta" Università di Pavia, via A. Bassi 6, I-27100, Pavia, Italy.

70 032315-1

nels, our results can be extended to the multimode case (see, e.g., [10]).

Thermal-noise channel. Here the signal photons interact with an environment that is in thermal equilibrium. The channel can be considered to be a beam splitter that couples the input state and the thermal reservoir to an output port, with the input-state transmissivity of this beam splitter being the channel's quantum efficiency $\eta \in [0,1]$. The CP map $\mathcal{E}_\eta^N$ for the thermal-noise channel is easily obtained by tracing away the thermal state of the environment mode (annihilation operator b, with average photon number N) from the unitary evolution

$$U = \exp\left[(ba^\dagger - b^\dagger a)\arctan \sqrt{\frac{1-\eta}{\eta}}\right]. \qquad (1)$$

This unitary evolution leads to the beam-splitter transformation

$$a \rightarrow U^\dagger a U = \sqrt{\eta}a + \sqrt{1-\eta}b,$$
$$b \rightarrow U^\dagger b U = \sqrt{\eta}b - \sqrt{1-\eta}a, \qquad (2)$$

where a is the annihilation operator for the channel mode. The thermal-noise channel's CP map is thus

$$\mathcal{E}_\eta^N(\rho) = \text{Tr}_b[U\rho \otimes \tau_b U^\dagger], \qquad (3)$$

where ρ is the channel input state (of the mode a) and $\tau_b = [N/(N+1)]^{b^\dagger b}/(N+1)$ is the environment thermal state. The case $N=0$ (zero-temperature reservoir) represents the pure-loss channel, in which each input photon has probability η of reaching the output. At positive temperatures the noise source is active, injecting noise photons into the channel mode. For $\eta=1$, the CP map is the identity: the reservoir does not couple to the output, hence the $\eta=1$ channel is noiseless.

Classical-noise channel. Here a classical Gaussian noise is superimposed on the transmitted field, i.e., the classical-noise channel is characterized by the CP map [7]

$$\mathcal{N}_n(\rho) = \int d^2\mu P_n(\mu)D(\mu)\rho D^\dagger(\mu), \qquad (4)$$

where

$$P_n(\mu) = \frac{e^{-|\mu|^2/n}}{\pi n}, \qquad (5)$$

and $D(\mu) \equiv \exp(\mu a^\dagger - \mu^* a)$ is the displacement operator for the mode a. The classical-noise channel's CP map (4) is unital—it maps the identity into the identity—whereas that for the $\eta<1$ thermal-noise channel is not. Nevertheless, the classical-noise channel can be seen to be a limiting case of the thermal-noise channel in which the field transformation (2) is replaced by

$$a \rightarrow a + \mu, \qquad (6)$$

where μ is a classical, complex-valued random variable distributed according to Eq. (5). The map $\mathcal{N}_n$ is then obtained from $\mathcal{E}_\eta^N$ in the limit $\eta \rightarrow 1$ and $N \rightarrow \infty$, with $(1-\eta)N \rightarrow n$ [see Eq. (17)]. For $n=0$ the CP map (4) becomes the identity,

while for $n>0$ it injects noise photons into the channel.

A more realistic construct for the classical-noise channel is the following. We first propagate the input state through a thermal-noise channel with transmissivity η and $N=0$. Then, to compensate for the propagation loss, we employ a phase-insensitive amplifier of gain $\kappa=1/\eta$ [11]. For $\eta=1/(n+1)$ the concatenation of these two maps exactly yields the classical-noise channel $\mathcal{N}_n$ [see Eq. (B5)].

In response to a vacuum-state input, $|0\rangle$, both the thermal- and classical-noise channels produce thermal output states given by the density operator

$$\rho_0' \equiv \frac{1}{M+1}\left(\frac{M}{M+1}\right)^{a^\dagger a}, \qquad (7)$$

with $M=(1-\eta)N$ for the thermal-noise channel $\mathcal{E}_\eta^N$, and $M=n$ for the classical-noise channel $\mathcal{N}_n$. The von Neumann entropy of ρ_0' is easily found to be $S(\rho_0') \equiv -\text{Tr}[\rho_0' \ln \rho_0'] = g(M)$, with [9,12,29]

$$g(x) \equiv (1+x)\ln(1+x) - x \ln x \qquad (8)$$

for $x>0$ and $g(0)=0$ (see Appendix A). The output state that results from the coherent-state input $|\alpha\rangle$ can be obtained by the following displacement-operator transformation of ρ_0',

$$\rho_\alpha' = D(\alpha')\rho_0'D^\dagger(\alpha'), \qquad (9)$$

where $\alpha' = \sqrt{\eta}\alpha$ for the thermal-noise channel and $\alpha' = \alpha$ for the classical-noise channel [see Eqs. (14) and (15)]. Clearly, the states ρ_α' and ρ_0' have identical von Neumann entropies as the former is a unitary transformation of the latter [1].

Minimum output entropy

We are interested in the minimum von Neumann output entropy $\mathbb{S}$, which is defined to be

$$\mathbb{S}(\mathcal{M}) \equiv \min_{\rho \in \mathcal{H}} S(\mathcal{M}(\rho)), \qquad (10)$$

where $\mathcal{M}$ is the channel's CP map and $\mathcal{H}$ is the Hilbert space of the information carrier. The concavity of the von Neumann entropy [1,13] implies that $\mathbb{S}$ in Eq. (10) can be achieved with a pure-state input. Moreover, given two CP maps, $\mathcal{M}_1$ and $\mathcal{M}_2$, we have that

$$\mathbb{S}(\mathcal{M}_2 \circ \mathcal{M}_1) \geqslant \mathbb{S}(\mathcal{M}_2), \qquad (11)$$

where the composition $(\mathcal{M}_2 \circ \mathcal{M}_1)(\rho) \equiv \mathcal{M}_2(\mathcal{M}_1(\rho))$ is the map in which $\mathcal{M}_2$ acts on the output of $\mathcal{M}_1$. Inequality (11) can be shown by noting that every possible input to $\mathcal{M}_2$ on the left-hand side is included in the minimization that is implicit on the right-hand side.

Conjecture (i). The minimum output entropies for the thermal- and classical-noise channels are achieved by coherent-state inputs, so that

$$\mathbb{S} = \begin{cases} g((1-\eta)N) & \text{for } \mathcal{E}_\eta^N, \\ g(n) & \text{for } \mathcal{N}_n, \end{cases} \qquad (12)$$

Discussion. Because the two entropies on the right-hand side of (12) are achieved by coherent-state inputs, they immedi-

ately provide upper bounds for the minimum output entropies of the thermal- and classical-noise channels, respectively. Thus the conjecture states that they are also lower bounds. The conjecture is trivially satisfied by the zero-temperature ($N=0$) thermal-noise channel, because the purity of a coherent state is preserved under the action of the loss map [14]. The conjecture is again trivially satisfied by the $\eta=0$ thermal-noise channel, because the map $\mathcal{E}_0^N$ sends every input state into a thermal state with an average photon number N.

A physical justification for our conjecture resides in the fact that in each channel the input state is contaminated by noise from a reservoir whose quantum phase is completely random. [The reservoirs are the thermal state τ_b for $\mathcal{E}_\eta^N$ and the classical random source associated with the distribution $P_n(\mu)$ for $\mathcal{N}_n$.] One thus expects that the extraction of any coherence from the reservoir—which could be used to reduce the output entropy below the level when no photons are sent through the channel—will be impossible. Some preliminary results in this sense were obtained in [15], where it was shown that, for the thermal-noise map, the linearized entropy is minimized by a vacuum-state input in the limit of low coupling $\eta \ll 1$ and high temperature $N \gg 1$. In the sections to come we will provide further evidence in support of this conjecture. We will also investigate the following stronger version of conjecture (i).

Conjecture (ii). The output states produced by coherent-state inputs majorize all other output states.

Discussion. By definition, a state ρ majorizes a state σ (a property which we denote by $\rho \succ \sigma$) if all ordered sums of the eigenvalues of ρ equal or exceed the corresponding sums for σ [1], i.e.,

$$\rho \succ \sigma \Leftrightarrow \sum_{i=0}^{q} \lambda_i \geq \sum_{i=0}^{q} \mu_i \quad \forall \; q \geq 0, \quad (13)$$

where λ_i and μ_i are the eigenvalues of ρ and σ, respectively, arranged in decreasing order (e.g., $\lambda_0 \geq \lambda_1 \geq \cdots$). If $\rho \succ \sigma$ then $S(\rho) \leq S(\sigma)$, so that conjecture (ii) implies conjecture (i). The converse is generally not true, in that $S(\rho) \leq S(\sigma)$ does not guarantee that $\rho \succ \sigma$. A necessary and sufficient condition for a state ρ to majorize a state σ is that σ be obtainable from ρ by the action of a unital map [1]. Conjecture (ii) for the thermal-noise channel would then be proved if, for each input state ρ, we could find a unital map $\mathcal{L}_\rho$ such that $\mathcal{E}_\eta^N(\rho) = \mathcal{L}_\rho(\rho_0')$, where ρ_0' from Eq. (7) is the output state that is due to a vacuum-state input. For the classical-noise channel proof we would want a unital map satisfying $\mathcal{N}_n(\rho) = \mathcal{L}_\rho(\rho_0')$. We postpone further discussion of conjecture (ii) until Sec. VII, where we will present some evidence that supports its validity. The next four sections will concentrate on conjecture (i).

III. CHANNEL PROPERTIES

In this section we develop some useful properties of the thermal- and classical-noise bosonic channels, and we provide some insights into their output entropies.

A. Covariance

From (4), it is easy to show that the classical-noise channel's CP map is covariant under displacement, i.e.,

$$\mathcal{N}_n(D(\alpha)\rho D^\dagger(\alpha)) = D(\alpha)\mathcal{N}_n(\rho)D^\dagger(\alpha). \quad (14)$$

The thermal-noise channel's CP map enjoys a similar relation, viz.,

$$\mathcal{E}_\eta^N(D(\alpha)\rho D^\dagger(\alpha)) = D(\sqrt{\eta}\alpha)\mathcal{E}_\eta^N(\rho)D^\dagger(\sqrt{\eta}\alpha), \quad (15)$$

where the $\sqrt{\eta}$ factor comes from the beam-splitter transformation (2). Moreover, the circular symmetries of the probability distribution P_n of Eq. (5) and of the environment thermal state τ_b imply that both noise maps are invariant under the action of a phase-shift transformation $e^{i\phi a^\dagger a}$. From these two properties plus the unitary invariance of the von Neumann entropy [13], it follows that any two input states that differ by a displacement and/or a phase-shift transformation will produce output states with the same entropy. In particular, this means that all coherent states produce the same output entropy, as discussed previously.

B. Composition rules

A complete description of the channels $\mathcal{E}_\eta^N$ and $\mathcal{N}_n$ is provided by the transformation of the symmetrically ordered characteristic function of the input state [19]

$$\chi(\mu) \equiv \mathrm{Tr}[\rho D(\mu)], \quad (16)$$

from which ρ is recovered as $\int d^2\mu \chi(\mu)D(-\mu)/\pi$. Evaluated on the ρ' state at the channel output, this function becomes

$$\chi'(\mu) = \begin{cases} \chi(\sqrt{\eta}\mu)e^{-(1-\eta)(N+1/2)|\mu|^2} & \text{for } \mathcal{E}_\eta^N, \\ \chi(\mu)e^{-n|\mu|^2} & \text{for } \mathcal{N}_n. \end{cases} \quad (17)$$

As a consequence of the Gaussian character of this evolution, thermal states [for which $\chi(\mu)$ is proportional to a zero-mean Gaussian distribution] evolve into thermal states. The following composition rules, summarized in Fig. 1, follow immediately from Eq. (17):

$$\mathcal{N}_{n_2} \circ \mathcal{N}_{n_1} = \mathcal{N}_{n_1 + n_2}, \quad (18)$$

$$\mathcal{E}_{\eta_2}^{N_2} \circ \mathcal{E}_{\eta_1}^{N_1} = \mathcal{E}_{\eta_1 \eta_2}^{N'}, \quad (19)$$

where $N' = [\eta_2(1-\eta_1)N_1 + (1-\eta_2)N_2]/(1-\eta_1\eta_2)$. From Eq. (18) we see that concatenating two identical classical-noise channels yields another classical-noise channel that is twice as random. From Eq. (19) we see that concatenating two identical thermal-noise maps results in another thermal-noise channel with the same reservoir, but whose transmissivity has been squared. It is also possible, using Eq. (17), to express the thermal-noise channel as either a pure-loss channel followed by a classical-noise channel, or vice versa,

$$\mathcal{E}_\eta^N = \mathcal{N}_{(1-\eta)N} \circ \mathcal{E}_\eta^0 = \mathcal{E}_\eta^0 \circ \mathcal{N}_{(1-\eta)N/\eta}. \quad (20)$$

From these equations, some useful properties of the output entropy can be derived. In particular:

FIG. 1. Top panel: graphical representations of the thermal- and classical-noise channels' CP maps; the signal photons propagate from left to right in these diagrams. Bottom panel: composition rules for these channel models; from top to bottom are representations of Eqs. (18), (19), and (20), respectively.

(1) Because a unital channel increases entropy (the output always majorizes the input [1]), Eq. (18) implies that the entropy $S(\mathcal{N}_n(\rho))$ at the output of the classical channel is an increasing function of n, i.e., for any ρ and $\Delta \geqslant 0$,

$$S(\mathcal{N}_{n+\Delta}(\rho)) \geqslant S(\mathcal{N}_n(\rho)). \qquad (21)$$

(2) Because $\mathcal{N}_n$ is unital, we can also infer that the entropy $S(\mathcal{E}_\eta^N(\rho))$ at the output of the thermal-noise channel is an increasing function of N. This follows because for any ρ and $\Delta \geqslant 0$ we have that

$$S(\mathcal{E}_\eta^{N+\Delta}(\rho)) = S((\mathcal{N}_{\Delta(1-\eta)} \circ \mathcal{E}_\eta^N)(\rho)) \geqslant S(\mathcal{E}_\eta^N(\rho)), \qquad (22)$$

where Eq. (18) and the first equality of Eq. (20) have been used.

(3) Using (19) with $N_1 = N_2 = N$ in conjunction with relation (11) shows that the minimum output entropy of the thermal-noise channel is a decreasing function of η,

$$S(\mathcal{E}_\eta^N) \geqslant S(\mathcal{E}_{\eta'}^N) \text{ for } \eta' \geqslant \eta. \qquad (23)$$

Note, however, that the output entropy $S(\mathcal{E}_\eta^N(\rho))$ is *not* a decreasing function of η for every ρ. This is because the thermal-noise map does necessarily increase the entropy of the input. Consider what happens when the channel input is a thermal state with an average photon number N_0 satisfying $N_0 > N$, so that $g(N_0) > g(N)$ holds. According to Eq. (17), the output state is a thermal state with an average photon number $\eta N_0 + (1-\eta)N < N_0$. Its entropy is therefore $g(\eta N_0 + (1-\eta)N)$, which is smaller than $g(N_0)$ and is an increasing function of η.

(4) A stronger version of (23) can be obtained by using relation (19) with $N_1 \neq N_2$. In this case, (11) implies

$$S(\mathcal{E}_\eta^N) \geqslant S(\mathcal{E}_{\eta'}^{N'}) \text{ for } \eta' \geqslant \eta, \qquad (24)$$

and $N \geqslant N'(1-\eta')/(1-\eta)$.

FIG. 2. Plot of the minimum entropy regions for the thermal-noise channel as constrained by (22)–(25). Each (η, N) point corresponds to a different thermal-noise channel described by the CP map $\mathcal{E}_\eta^N$. Given a channel with transmissivity η_1 and average thermal photon number N_1, the gray (hatched) region represents channels whose minimum entropies are greater (less) than $S(\mathcal{E}_{\eta_1}^{N_1})$. [The line $(\eta, 0)$ has minimum entropy zero, and belongs to the hatched region.] In the white regions, the composition rules from this section do not establish the relation between $S(\mathcal{E}_\eta^N)$ and $S(\mathcal{E}_{\eta_1}^{N_1})$; in Fig. 6 these regions will be partially filled by exploiting the lower bounds that will be introduced in Sec. V. Showing that the upper white region is gray and the lower white region is hatched would complete the proof of conjecture (i). Regions 1 and 4 follow from (22) and (23), regions 3 and 6 follow from (24), while regions 2 and 5 are consequences of (25). The plot assumes $\eta_1 = 0.7$ and $N_1 = 0.6$.

(5) The transmissivity inequality in (23) can be inverted if the thermal photon numbers are appropriately chosen, viz.,

$$S(\mathcal{E}_\eta^N) \geqslant S(\mathcal{E}_{\eta'}^{N'}) \text{ for } \eta \geqslant \eta', \qquad (25)$$

where now $N' \leqslant [(1-\eta)N + \eta' - \eta]/(1-\eta')$. This relation is proven in Appendix B and, together with (22)–(24), is illustrated in Fig. 2.

(6) Using the first equality in Eq. (20), along with (11), we can establish the following relation between the minimum output entropies of the classical- and thermal-noise maps,

$$S(\mathcal{E}_\eta^N) = S(\mathcal{N}_{(1-\eta)N} \circ \mathcal{E}_\eta^0) \geqslant S(\mathcal{N}_{(1-\eta)N}). \qquad (26)$$

Physically, this says that deleting the pure-loss beam-splitter map $\mathcal{E}_\eta^0$ can only decrease the output noise. An important consequence of (26) is that if conjecture (i) holds for the classical-noise channel, then it must also hold for the thermal-noise channel.

(7) The reverse counterpart of (26) is given by

$$S(\mathcal{N}_n) \geqslant S(\mathcal{E}_{1-n'}^{(n-n')/n'}), \qquad (27)$$

for all $n' \in [0, \min\{1, n\}]$ (see Appendix B for the derivation). The key consequence of (27) is that if conjecture (i) is true for the thermal-noise channel, then it is must also be valid for the classical-noise channel.

IV. GAUSSIAN INPUT STATES

Here we show that conjecture (i) is true if we restrict the channel input to be a Gaussian state ρ_G. Such an input has a symmetric characteristic function that is a Gaussian form [9],

$$\chi(\mu) = \exp\left[-\zeta_0 \cdot \zeta^\dagger - \frac{1}{2}\zeta \cdot \Gamma \cdot \zeta^\dagger\right], \quad \zeta \equiv (\mu*, -\mu),$$

which is fully characterized by its first moment $\zeta_0 \equiv (\langle a \rangle, \langle a^\dagger \rangle)$ and its covariance matrix

$$\Gamma \equiv \begin{bmatrix} \langle\{\Delta a, \Delta a^\dagger\}\rangle/2 & \langle(\Delta a^\dagger)^2\rangle \\ \langle(\Delta a)^2\rangle & \langle\{\Delta a, \Delta a^\dagger\}\rangle/2 \end{bmatrix} \quad (28)$$

(here $\langle \cdot \rangle \equiv \text{Tr}[\cdot \rho_G]$ is expectation with respect to ρ_G, $\Delta a \equiv a - \langle a \rangle$, and $\{\cdot, \cdot\}$ denotes the anticommutator). The coherent state $|\alpha\rangle$ is Gaussian with $\Gamma = 1/2$ and $\zeta_0 = (\alpha, \alpha^*)$. The entropy of ρ_G depends only on its covariance matrix [9,16,29] and is equal to $g(\sqrt{\det \Gamma} - 1/2)$. Both $\mathcal{E}_\eta^N$ and $\mathcal{N}_n$ transform Gaussian input states into Gaussian output states. Moreover, by means of Eq. (17), evolution under these CP maps transforms covariance matrices according to

$$\Gamma \to \Gamma' = \begin{cases} \Gamma + n\mathbb{1} & \text{for } \mathcal{N}_n, \\ \eta\Gamma + (1-\eta)(N+1/2)\mathbb{1} & \text{for } \mathcal{E}_\eta^N, \end{cases} \quad (29)$$

and first moments according to $\zeta_0 \to \zeta_0$ for $\mathcal{N}_n$, and $\zeta_0 \to \sqrt{\eta}\zeta_0$ for $\mathcal{E}_\eta^N$. The output entropy of a Gaussian input state is, hence, equal to $g(\sqrt{\det \Gamma'} - 1/2)$, which is always greater than or equal to the output entropy of the vacuum, i.e., the right-hand side of Eq. (12), as we now will show.

For the classical map $\mathcal{N}_n$ it is possible to rewrite (29) as

$$\det \Gamma' = \det \Gamma + n(n + \langle\{\Delta a, \Delta a^\dagger\}\rangle), \quad (30)$$

which is always greater than $(n+1/2)^2$ because $\langle\{\Delta a, \Delta a^\dagger\}\rangle \geq 1$ and, from the strong version of the uncertainty relation [17,18], $\det \Gamma \geq 1/4$. In other words, we have that

$$S(\mathcal{N}_n(\rho_G)) = g(\sqrt{\det \Gamma + n(n + \langle\{\Delta a, \Delta a^\dagger\}\rangle)} - 1/2) \geq g(n). \quad (31)$$

Likewise, we see that conjecture (i) is true for the thermal-noise channel $\mathcal{E}_\eta^N$ whose input is limited to be a Gaussian state because

$$\det \Gamma' = \eta^2 \det \Gamma + (1-\eta)(N+1/2)[(1-\eta)(N+1/2) + \eta\langle\{\Delta a, \Delta a^\dagger\}\rangle], \quad (32)$$

which implies $\det \Gamma' \geq [(1-\eta)N + 1/2]^2$.

V. LOWER BOUNDS

In this section we present some lower bounds on the output entropy. These bounds are consistent with conjecture (i), and collectively they are asymptotically tight in the limits of low and high noise. We will treat the two channel models in succession, starting with the classical-noise case.

A. Classical-noise channel

Because $g(n)$ is the output entropy that results when the input is a coherent state, $g(n)$ is an upper bound on the mini-
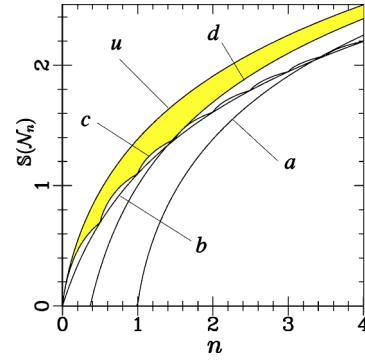
FIG. 3. Bounds on the minimum output entropy of the classical-noise channel $\mathcal{N}_n$ vs average photon number of the classical noise, n. Curves a, b, c, and d are the lower bounds given in (33), (38), (39), and (41), respectively. The upper bound u is the function $g(n)$. The minimum entropy $S(\mathcal{N}_n)$ is constrained by these bounds to lie in the gray region, and is required to be an increasing function of n. Conjecture (i) states that $S(\mathcal{N}_n) = g(n)$.

mum output entropy $S(\mathcal{N}_n)$ of the classical-noise channel. Four different lower bounds on $S(\mathcal{N}_n)$ are given below. As seen in Fig. 3, bound a is implied by bound d and bound b is implied by bound c. Nevertheless, we explain all of them because the derivations of a and b are simpler. In the limits of low and high values of the noise parameter n, it can be shown that this collection of bounds is asymptotically tight, i.e., $\lim_{n\to 0} S_c(\mathcal{N}_n)/g(n) = \lim_{n\to\infty} S_d(\mathcal{N}_n)/g(n) = 1$, where $S_j(\mathcal{N}_n)$ denotes bound j.

Lower bound a. By considering the Husimi function of the output state, we find that for $n \geq 1$,

$$S(N_n) \geq g(n-1), \quad (33)$$

by the following argument. Any initial state ρ can be written as [19]

$$\rho = \int d^2\alpha\, Q(\alpha)\sigma(\alpha), \quad (34)$$

where $Q(\alpha) \equiv \langle\alpha|\rho|\alpha\rangle/\pi$ is that state's Husimi function and

$$\sigma(\alpha) = \int \frac{d^2\lambda}{\pi} D(\lambda) e^{\lambda^*\alpha - \lambda\alpha^* + |\lambda|^2/2}. \quad (35)$$

Under the action of the map $\mathcal{N}_n$, the state ρ evolves to

$$\mathcal{N}_n(\rho) = \int d^2\alpha\, Q(\alpha)\mathcal{N}_n(\sigma(\alpha)). \quad (36)$$

The operator $\mathcal{N}_n(\sigma(\alpha))$ is not in general a quantum state. However, for $n > 1$ it is a displaced thermal state with average photon number $n-1$, i.e.,

$$\mathcal{N}_n(\sigma(\alpha)) = D(\alpha)\int \frac{d^2\mu}{\pi}\frac{e^{-\frac{|\mu|^2}{n-1}}}{n-1}|\mu\rangle\langle\mu|D^\dagger(\alpha)$$

$$= D(\alpha)\frac{1}{n}\left(\frac{n-1}{n}\right)^{a^\dagger a}D^\dagger(\alpha), \quad (37)$$

which has entropy $g(n-1)$. Lower bound a then can be ob-

tained from Eq. (36) because $Q(\alpha)$ is a probability distribution, and the von Neumann entropy is concave [13].

Lower bound b. By considering the Rényi entropy $S_2(\rho') \equiv -\ln \mathrm{Tr}[(\rho')^2]$ calculated on the channel output $\rho' = \mathcal{N}_n(\rho)$, we find

$$\mathbb{S}(\mathcal{N}_n) \geq \ln(2n+1), \tag{38}$$

via two simple steps. As discussed in [8], it is possible to show that $S_2(\rho')$ achieves its minimum $\ln(2n+1)$ when the channel input is a coherent state. Lower bound (38) is then a trivial consequence of the von Neumann entropy S being greater than or equal to the Rényi entropy S_2 [20].

Lower bound c. By using a more sophisticated connection between the von Neumann entropy and the Rényi entropy [21,22], we find for $k \geq 1$ an integer and $n \in [(k-1)/2, k/2]$,

$$\mathbb{S}(\mathcal{N}_n) \geq -\lambda_k(n)\ln \lambda_k(n) - [1 - \lambda_k(n)]\ln \frac{1 - \lambda_k(n)}{k}, \tag{39}$$

where

$$\lambda_k(n) = \frac{1 - \sqrt{1 - (k+1)(1 - k/(2n+1))}}{k+1}. \tag{40}$$

The derivation of (39) is shown in Appendix C.

Lower bound d. Using the properties of the map $\mathcal{N}_n$ we find

$$\mathbb{S}(\mathcal{N}_n) \geq 1 + \ln n, \tag{41}$$

as we now demonstrate. Consider a pure state $|\psi\rangle$ that generates an output state with spectral decomposition,

$$\rho' = \mathcal{N}_n(|\psi\rangle\langle\psi|) = \sum_k \gamma_k |\gamma_k\rangle\langle\gamma_k|, \tag{42}$$

where $\{\gamma_k\}$ is a probability distribution and $\{|\gamma_k\rangle\}$ are the orthonormal eigenvectors. From definition (4) of the classical-noise channel's CP map, we have

$$\gamma_k = \langle\gamma_k|\rho'|\gamma_k\rangle = \int d^2\mu \, P_n(\mu)|\langle\gamma_k|D(\mu)|\psi\rangle|^2. \tag{43}$$

The quantity $|\langle\gamma_k|D(\mu)|\psi\rangle|^2$ is a probability distribution over k, and $|\langle\gamma_k|D(\mu)|\psi\rangle|^2/\pi$ is a probability distribution over μ [23]. Therefore, the convexity of x^z for $z \geq 1$ ensures that

$$\mathrm{Tr}[(\rho')^z] = \sum_k \left(\int d^2\mu \, P_n(\mu)|\langle\gamma_k|D(\mu)|\psi\rangle|^2 \right)^z$$
$$\leq \sum_k \int \frac{d^2\mu}{\pi} (\pi P_n(\mu))^z |\langle\gamma_k|D(\mu)|\psi\rangle|^2. \tag{44}$$

Because $P_n(\mu)$ is a Gaussian, it follows that

$$[\pi P_n(\mu)]^z = \frac{\pi P_{n/z}(\mu)}{z n^{z-1}}, \tag{45}$$

and the right-hand side of (44) can be rewritten in terms of the image of $|\psi\rangle$ under the action of the map $\mathcal{N}_{n/z}$, i.e.,
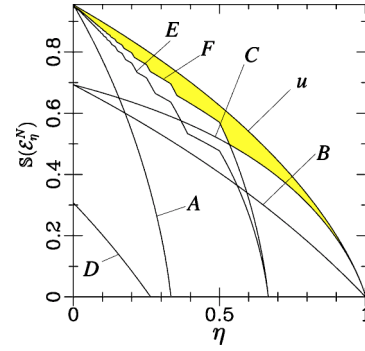
FIG. 4. Bounds on the minimum output entropy of the thermal-noise channel $\mathcal{E}_\eta^N$ as functions of channel transmissivity η for $N = 1/2$. Curves A, E, and F are the lower bounds (48), (50), and (51), respectively. [Here E is the maximum over k of the right-hand side of (50) and F is the maximum over k of the right-hand side of (51).] Curves B, C, and D are the lower bounds (38), (39), and (41), respectively, with $n = (1-\eta)N$. The upper bound u is the function $g((1-\eta)N)$. The minimum output entropy $\mathbb{S}(\mathcal{E}_\eta^N)$ is constrained to lie in the gray region, and is required to be a decreasing function of η. Conjecture (i) states that $\mathbb{S}(\mathcal{E}_\eta^N) = g((1-\eta)N)$.

$$\mathrm{Tr}[(\rho')^z] \leq \frac{\mathrm{Tr}[\mathcal{N}_{n/z}(|\psi\rangle\langle\psi|)]}{z n^{z-1}} = \frac{1}{z n^{z-1}}. \tag{46}$$

This relation can be used to calculate a lower bound for the von Neumann entropy by observing that [20]

$$S(\rho') = \lim_{z \to 1} -\frac{\ln \mathrm{Tr}[(\rho')^z]}{z-1} \geq \lim_{z \to 1} \frac{\ln(z n^{z-1})}{z-1} = 1 + \ln n. \tag{47}$$

Inequality (47) applies for any pure state $|\psi\rangle$, so we conclude that (41) holds.

B. Thermal-noise channel

The same techniques that we used to derive lower bounds for the classical-noise channel can also be employed for the thermal-noise channel $\mathcal{E}_\eta^N$. The bounds we obtain in this case are reported in Figs. 4–6.

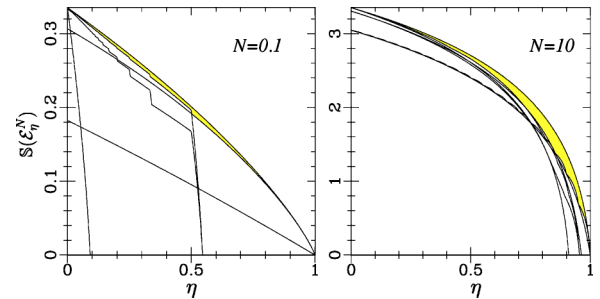*Lower bound A.* Repeating the Husimi function calculation employed above, we find

FIG. 5. Same as Fig. 4 but for different values of the parameter N: in the left plot $N = 0.1$, in the right plot $N = 10$. At both high and low average thermal photon numbers, the greatest of these lower bounds approaches the upper bound.

$$S(\mathcal{E}_\eta^N) \geq g((1-\eta)N - \eta), \tag{48}$$

as follows. We replace Eq. (37) with

$$\mathcal{E}_\eta^N(\sigma(\alpha)) = D(\sqrt{\eta}\alpha) \int \frac{d^2\mu}{\pi} \frac{e^{-\frac{|\mu|^2}{(1-\eta)N-\eta}}}{(1-\eta)N - \eta} |\mu\rangle\langle\mu| D^\dagger(\sqrt{\eta}\alpha), \tag{49}$$

which for $(1-\eta)N \geq \eta$ is a displaced thermal state whose entropy equals $g((1-\eta)N - \eta)$. Bound A then follows from the concavity of the von Neumann entropy.

Lower bounds B, C, and D. A simple strategy to derive bounds on $S(\mathcal{E}_\eta^N)$ is to exploit relation (26), which links the minimum output entropy of $\mathcal{E}_\eta^N$ to that of $\mathcal{N}_{(1-\eta)N}$. Thus, by replacing n with $(1-\eta)N$, inequalities (38), (39), and (41) of bounds *b, c,* and *d* immediately become bounds *B, C,* and *D*

on $S(\mathcal{E}_\eta^N)$, respectively, which we have plotted versus channel transmissivity η in Fig. 4. [Applying this same method to lower bound a, we obtain $g((1-\eta)N-1)$, which is not useful, as it is already implied by (48).]

Lower bound E. A further lower bound for the thermal-noise channel can be derived from the properties of the beam splitter; for all integer k it states that

$$S(\mathcal{E}_\eta^N) \geq \begin{cases} \frac{k-1}{k} g\left(\frac{k}{k-1}(1-\eta)N\right) & \text{for } \eta \leq \frac{1}{k} \\ \frac{k-1}{k} g\left(\frac{k}{k-1}\left[(1-\eta)N - \eta + \frac{1}{k}\right]\right) & \text{for } \eta \geq \frac{1}{k} \end{cases}. \tag{50}$$

The proof appears in Appendix D. Curve E in Fig. 4 is the maximum over k of the right-hand side of (50).

Lower bound F. A more sophisticated version of bound E is given by

$$S(\mathcal{E}_\eta^N) \geq \begin{cases} \frac{k-1}{k} g((1-\eta)N) + \frac{1}{k} S(\mathcal{N}_{(1-\eta)N}) & \text{for } \eta \leq \frac{1}{k}, \\ \frac{k-1}{k} g\left((1-\eta)N - \eta + \frac{1}{k}\right) + \frac{1}{k} S(\mathcal{N}_{(1-\eta)N-\eta+1/k}) & \text{for } \eta \geq \frac{1}{k}, \end{cases} \tag{51}$$

which is also proven in Appendix D. Even though $S(\mathcal{N}_n)$ is not known, (51) provides a usable lower bound for $S(\mathcal{E}_\eta^N)$ when we replace $S(\mathcal{N}_n)$ with any of the lower bounds discussed in Sec. V A. Curve F in Fig. 4 is the maximum over k of the right-hand side of (51). If conjecture (i) is true, then (51) becomes an equality for $\eta \leq 1/k$, i.e., this bound is tight. The same is not true for bound (50).

VI. NECESSARY CONDITIONS FOR MINIMUM OUTPUT ENTROPY

In this section we study the conditions that an input state must to satisfy in order to provide a (local or global) mini-
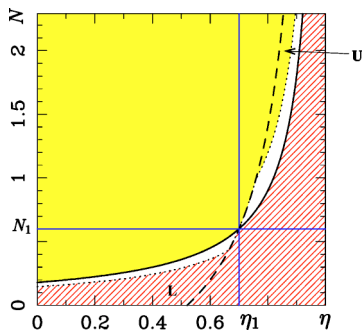
FIG. 6. Plot of the minimum entropy regions for the thermal-noise channel for the same parameters used in Fig. 2. Here, the region **L** has been added to the hatched region of Fig. 2 by comparing the lower bounds *A-F* of the channel $\mathcal{E}_{\eta_1}^{N_1}$ with the upper bound $g((1-\eta)N)$ for generic η and N: if the former is larger than the latter, we can conclude that $S(\mathcal{E}_{\eta_1}^{N_1})$ is greater than $S(\mathcal{E}_\eta^N)$. Likewise, the region **U** has been added to the gray region of Fig. 2, by comparing the upper bound on $S(\mathcal{E}_{\eta_1}^{N_1})$ with the lower $S(\mathcal{E}_\eta^N)$.

mum for the output entropy. We will show that coherent-state inputs satisfy all of these conditions for both the classical- and thermal-noise channels. We begin, in Sec. VI A, by deriving a local minimum condition from the directional derivative of the output entropy. Then, in Sec. VI B, we generalize this result into a more stringent condition for minimality.

A. Local minimum condition

Given a CP map $\mathcal{M}$, a necessary condition for an input state σ_0 to provide a local minimum of the output entropy $S(\mathcal{M}(\rho))$ can be obtained from the directional derivatives of this quantity [9]. Given $t \in [0,1]$ and a generic state σ, this condition requires that

$$\frac{\partial}{\partial t} S(\mathcal{M}(\sigma(t)))\bigg|_{t=0} = \text{Tr}\{[\mathcal{M}(\sigma_0) - \mathcal{M}(\sigma)]\ln \mathcal{M}(\sigma_0)\} \geq 0, \tag{52}$$

where $\sigma(t)$ is the mixed state $(1-t)\sigma_0 + t\sigma$. For both the thermal-noise map $\mathcal{E}_\eta^N$ and the classical-noise map $\mathcal{N}_n$, this condition is satisfied by the arbitrary coherent state $\sigma_0 = |\alpha\rangle\langle\alpha|$, as can be shown by using covariance properties of the noise (see Sec. III A) to rewrite the output entropy derivative as follows:

$$\frac{\partial}{\partial t} S(\mathcal{M}(\sigma(t)))\bigg|_{t=0^+} = \text{Tr}[\{\rho_0' - \mathcal{M}(\tilde{\sigma})\}\ln \rho_0']$$

$$= -\text{Tr}[a^\dagger a\{\mathcal{M}(\tilde{\sigma}) - \rho_0'\}]\ln \frac{M}{M+1}$$

$$= -\zeta \text{Tr}[a^\dagger a\tilde{\sigma}]\ln \frac{M}{M+1} \geq 0, \tag{53}$$

where $\zeta = 1$ for $\mathcal{N}_n$ and $\zeta = \eta$ for $\mathcal{E}_\eta^N$, ρ_0' is the output-state equation (7) generated by using a vacuum-state input, and $\tilde{\sigma}$ is the state $D^\dagger(\alpha)\sigma D(\alpha)$. The last equality in (53) derives from

$$\mathrm{Tr}[a^\dagger a \mathcal{M}(\tilde{\sigma})] = \zeta \mathrm{Tr}[a^\dagger a \tilde{\sigma}] + M, \tag{54}$$

which holds because M is the average number of photons in the state ρ_0'. Physically, the inequality in (53) is a consequence of the vacuum's being the input state that produces the output state with lowest average photon number.

B. Eigenvalue minimum condition

In deriving (52) we required that the entropy be locally increasing when moving along the trajectory $\sigma(t)$, whose intermediate states are all mixed. A more stringent requirement follows from using the pure-state trajectory $\sigma_\theta = |\sigma_\theta\rangle\langle\sigma_\theta|$ with

$$|\sigma_\theta\rangle = \cos\theta |\sigma_0\rangle + \sin\theta |\sigma_\perp\rangle, \tag{55}$$

where $\sigma_0 \equiv |\sigma_0\rangle\langle\sigma_0|$ is the putative minimizing state for the output entropy, and $|\sigma_\perp\rangle$ is any state that is orthogonal to $|\sigma_0\rangle$. Expanding the output-state entropy in a Taylor's series, we have

$$S(\mathcal{M}(\sigma_\theta)) = S(\mathcal{M}(\sigma_0)) + \theta \left. \frac{\partial}{\partial\theta'} S(\mathcal{M}(\sigma_{\theta'})) \right|_{\theta'=0} + \cdots. \tag{56}$$

(The entropies of the channels we are considering are differentiable.) If the state $|\sigma_0\rangle$ is a local minimum for the output entropy, then the term that is linear in θ must vanish. This requirement implies the following necessary condition for local minimality:

$$\left. \frac{\partial}{\partial\theta} S(\mathcal{M}(\sigma_\theta)) \right|_{\theta=0} = -2 \, \mathrm{Re}\langle\sigma_\perp|\mathcal{M}*(\ln\mathcal{M}(\sigma_0))|\sigma_0\rangle = 0, \tag{57}$$

where $\mathcal{M}*$ is the dual map associated with $\mathcal{M}$, such that for any two operators A and B, $\mathrm{Tr}[A\mathcal{M}(B)] = \mathrm{Tr}[\mathcal{M}*(A)B]$. Inasmuch as this condition must be valid for all $|\sigma_\perp\rangle$, we can conclude that the operator

$$\mathcal{F}(\sigma_0) \equiv -\mathcal{M}*(\ln\mathcal{M}(\sigma_0)) \tag{58}$$

has $|\sigma_0\rangle$ as an eigenvector. The properties of $\mathcal{F}(\sigma_0)$ guarantee that the eigenvalue associated with $|\sigma_0\rangle$ is its output entropy. Shor [24] has a different way of introducing the operator $\mathcal{F}(\sigma_0)$ to study the minima of a channel's output entropy; his approach does not require the output entropy to be differentiable.

For the channels we are considering, the vacuum input evolves into the thermal state ρ_0' of Eq. (7), so that

$$\mathcal{F}(|0\rangle\langle0|) = \mathcal{M}*\left[a^\dagger a \ln\frac{M+1}{M} + \ln(M+1) \right]. \tag{59}$$

In particular, for the classical-noise channel, this quantity simplifies appreciably because $\mathcal{N}_n$ is its own dual. Indeed, because $\mathcal{N}_n(a^\dagger a) = a^\dagger a + n$, we find

$$\mathcal{F}(|0\rangle\langle0|) = g(n)\mathbb{1} + a^\dagger a \ln\frac{n+1}{n}, \tag{60}$$

which shows that the vacuum is an eigenvector of $\mathcal{F}(|0\rangle\langle0|)$, and hence satisfies the local minimum condition of Eq. (57). The positivity of the operator $a^\dagger a$ implies that the vacuum is also the eigenvector with minimum eigenvalue. Using the definition of $\mathcal{F}$, Eq. (60) can be used to express the output entropy of a general pure-state input ρ as

$$S(\mathcal{N}_n(\rho)) = g(n) + E \ln\frac{n+1}{n} - S(\mathcal{N}_n(\rho)\|\rho_0'), \tag{61}$$

where $E = \mathrm{Tr}[a^\dagger a \rho]$ is the average photon number of the input ρ and $S(\rho_1\|\rho_2) \equiv \mathrm{Tr}[\rho_1(\ln\rho_1 - \ln\rho_2)]$ is the relative entropy between states ρ_1 and ρ_2 [1]. This equation allows us to restate conjecture (i) in the form

$$E \ln\frac{n+1}{n} \geqslant S(\mathcal{N}_n(\rho)\|\rho_0'). \tag{62}$$

Proving this relation for all ρ is equivalent to proving conjecture (i). For coherent-state inputs, we can use the covariance properties of the noise under displacements to show that

$$\mathcal{F}(|\alpha\rangle\langle\alpha|) = D(\alpha)\mathcal{F}(|0\rangle\langle0|)D^\dagger(\alpha), \tag{63}$$

which guarantees that the coherent state $|\alpha\rangle$ is an eigenvector of $\mathcal{F}(|\alpha\rangle\langle\alpha|)$. If we could prove that the coherent states are the only ones which satisfy this condition, we would have succeeded in proving the conjecture: the coherent states would be the only states that satisfy the necessary condition (57) for minimality. Unfortunately, such is not the case because Fock states $|n\rangle$ are also eigenvectors of the corresponding $\mathcal{F}(|n\rangle\langle n|)$; this follows from the states $\mathcal{N}_n(|n\rangle\langle n|)$ being diagonal in the Fock basis [25,26]. Fock states other than the vacuum are not, however, minima for the output entropy, as discussed in Sec. VII. Note that condition (58) was first introduced in Ref. [7], where it was claimed that conjecture (i) was proven. A more careful analysis of [7] reveals a fundamental missing link in that proof: even though it is shown that displaced number states satisfy condition (58) and that the vacuum is the number state with the lowest output entropy, it is not proven that they are the *only* states that satisfy this condition. Hence, there is still a possibility that another state (with output entropy lower than the vacuum) might satisfy the condition.

The case of the thermal-noise channel can be treated in a similar manner, showing that here too coherent states are eigenvectors of the corresponding $\mathcal{F}$ operators. In this case, the dual map of $\mathcal{E}_\eta^N$ can be written as

$$(\mathcal{E}_\eta^N)*(\rho) = \mathrm{Tr}_b[(\mathbb{1}_a \otimes \tau_b)U^\dagger(\rho \otimes \mathbb{1}_b)U], \tag{64}$$

which is unital and satisfies

$$(\mathcal{E}_\eta^N)*(a^\dagger a) = \eta a^\dagger a + (1-\eta)N. \tag{65}$$

Using these properties and Eq. (59), we find

$$\mathcal{F}(|0\rangle\langle 0|) = g((1-\eta)N)\mathbb{1} + \eta a^\dagger a \ln \frac{(1-\eta)N+1}{(1-\eta)N}. \quad (66)$$

As in the case of Eq. (60), the vacuum is the eigenvector with minimum eigenvalue of the operator $\mathcal{F}$. Moreover, Eq. (63) applies here, i.e., the coherent state $|\alpha\rangle$ is an eigenvector of $\mathcal{F}(|\alpha\rangle\langle\alpha|)$, and Eq. (61) becomes

$$S(\mathcal{E}_\eta^N(\rho)) = g((1-\eta)N) + \eta E \ln \frac{(1-\eta)N+1}{(1-\eta)N} - S(\mathcal{E}_\eta^N(\rho)\|\rho_0'). \quad (67)$$

VII. MAJORIZATION

In the previous sections we gave some justifications in support of conjecture (i). Here we focus on the stronger version of this conjecture, i.e., conjecture (ii). We begin by presenting evidence that the output states generated by coherent states majorize the ones generated by Fock states.

A. Fock-state inputs

Because the output states generated by the coherent state are all unitarily equivalent, we can focus on the ordered eigenvalue sums for the thermal state ρ_0' from Eq. (7), i.e.,

$$\frac{1}{M+1}\sum_{i=0}^{q}\left(\frac{M}{M+1}\right)^i = 1 - \left(\frac{M}{M+1}\right)^{q+1}. \quad (68)$$

The ordered partial sums (68) for all q must be compared with their Fock-state-input counterparts. In the case of classical-noise, these can be numerically evaluated by observing that, for a Fock input state $|k\rangle$, the output is diagonal in the Fock basis and takes the form [25]

$$\mathcal{N}_n(|k\rangle\langle k|) = \sum_{i=0}^{\infty} \lambda_i |i\rangle\langle i|, \quad (69)$$

where

$$\lambda_i \equiv \sum_{j=0}^{\min(k,i)} \binom{i}{j}\binom{k}{j}\frac{n^{k+i-2j}}{(n+1)^{k+i+1}}. \quad (70)$$

[Note that in the case $k=0$, Eq. (69) reduces to the vacuum evolution equation (7).] Evaluation of the ordered partial sums is tedious but can be performed analytically. In particular, for $k=1$ and $n\geq 1$, the ordered partial sums $\{\Sigma_q\}$ of the first $q+1$ eigenvalues are

$$\Sigma_q = 1 - \left(1 + \frac{q+1}{n(n+1)}\right)\left(\frac{n}{n+1}\right)^{q+1}, \quad (71)$$

which, for all q, are smaller than the corresponding sums in Eq. (68). The case $n<1$ is analogous: for sufficiently large values of q the sum is the same as in Eq. (71), while for small q it is given by

$$\Sigma_q = 1 - \left(1 + \frac{q+2}{n(n+1)}\right)\left(\frac{n}{n+1}\right)^{q+2} - \frac{n}{(n+1)^2}, \quad (72)$$

which again is smaller than the sum in Eq. (68). In Fig. 7, a numerical comparison between Eq. (68) and the ordered par-
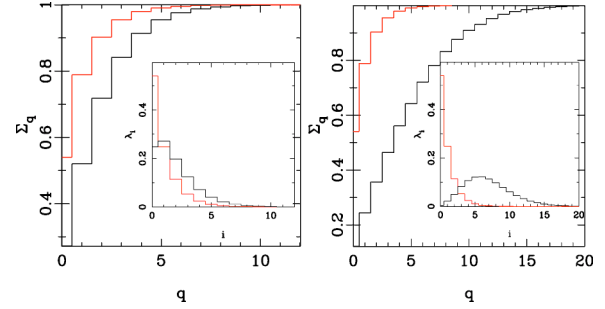

FIG. 7. Majorization analysis of the map $\mathcal{N}_n$. Plots of Σ_q, the sum of the $q+1$ largest eigenvalues, for the thermal state ρ_0' (gray staircase) and the evolved Fock state $\mathcal{N}_n(|k\rangle\langle k|)$ (black staircase). In both cases the thermal state majorizes the evolved Fock state, which implies that the entropy of the former is smaller than the entropy of the latter [1]. The insets show the eigenvalues $\{\lambda_i\}$ as functions of the photon number i. Here $k=1$, $n=0.85$ for the left plot, and $k=6$, $n=0.85$ for the right plot.

tial sums of the eigenvalues from Eq. (69) is presented for two specific cases; ρ_0' majorizes $\mathcal{N}_n(|k\rangle\langle k|)$ in both.

The same analysis can be repeated in the case of the thermal channel, observing that

$$\mathcal{E}_\eta^0(|k\rangle\langle k|) = \sum_{m=0}^{k} p_m |m\rangle\langle m|, \quad (73)$$

where $\{p_m\}$ is the binomial distribution

$$p_m = \binom{k}{m}\eta^m(1-\eta)^{k-m}. \quad (74)$$

Using Eq. (69) and decomposition (20), the thermal evolution of the Fock state $|k\rangle$ can be calculated as

$$\mathcal{E}_\eta^N(|k\rangle\langle k|) = \sum_{m=0}^{k} p_m \mathcal{N}_{(1-\eta)N}(|m\rangle\langle m|). \quad (75)$$

Note that the output is again diagonal in the Fock basis. Moreover, if the output of the vacuum majorizes the output of the other Fock states for the classical channel $\mathcal{N}_n$, Eq. (75) can be used to prove that this must also be true for the thermal channel $\mathcal{E}_\eta^N$. In fact, if $\mathcal{N}_n(|0\rangle\langle 0|)$ majorizes $\mathcal{N}_n(|m\rangle\langle m|)$, then there exists [1] a unital map $\mathcal{L}_m$ such that $\mathcal{N}_n(|m\rangle\langle m|) = \mathcal{L}_m(\mathcal{N}_n(|0\rangle\langle 0|))$. Now, because $\mathcal{E}_\eta^N(|0\rangle\langle 0|) = \mathcal{N}_{(1-\eta)N}(|0\rangle\langle 0|)$, Eq. (75) implies that

$$\mathcal{E}_\eta^N(|k\rangle\langle k|) = \sum_{m=0}^{k} p_m \mathcal{L}_m(\mathcal{E}_\eta^N(|0\rangle\langle 0|)). \quad (76)$$

The convex sum of unital maps is a unital map, hence $\mathcal{E}_\eta^N(|k\rangle\langle k|)$ is obtained from a unital transformation of $\mathcal{E}_\eta^N(|0\rangle\langle 0|)$, which implies [1] that the latter majorizes the former.

B. Arbitrary input states

Further insight into conjecture (ii) is provided by generalizing our analysis to the case of an arbitrary pure-state
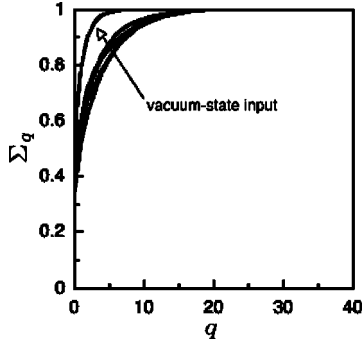
FIG. 8. Majorization analysis of the map $\mathcal{N}_n$ for $n=0.85$. Plots of the sum of the $q+1$ largest eigenvalues for the thermal state $\rho_0' = \mathcal{N}_n(|0\rangle\langle0|)$ and the evolved pure state $\mathcal{N}_n(|\psi\rangle\langle\psi|)$ for five randomly generated $|\psi\rangle$. In all cases the thermal state majorizes the evolved $|\psi\rangle$ state, which implies that the entropy of the former is smaller than the entropy of the latter [1].

input. Because it is sufficient to establish conjecture (ii) for the classical-noise channel, we shall only consider that case. As shown in Appendix E (see also [25]), when an arbitrary pure state $|\psi\rangle$ is fed into the classical-noise map $\mathcal{N}_n$, the resulting output state ρ' has the following Fock-state representation:

$$\langle k+l|\rho'|k\rangle = \sqrt{\frac{k!}{(k+l)!}} \sum_{j=0}^{\infty} \sqrt{\frac{j!}{(j+l)!}}$$
$$\times \psi_{j+l} \psi_j^* \frac{(j+k+l)!}{j!\,k!} \frac{n^{j+k}}{(1+n)^{j+k+l+1}}$$
$$\times F(-j,-k;-(j+k+l);1-n^{-2}), \quad (77)$$

for $k, l \geq 0$, where $\{\psi_n\}$ are the Fock-state coefficients of $|\psi\rangle$, and $F(\alpha,\beta;\gamma;z)$ is the hypergeometric function.

To probe the output-state eigenvalue behavior associated with an arbitrary pure-state input with up to ten photons, we used the following procedure. Eleven complex numbers, $\{\phi_n : 0 \leq n \leq 10\}$, whose real and imaginary parts were randomly distributed on the interval $[-1, 1]$, were used to generate a pure state, via

$$|\psi\rangle = \sum_{n=0}^{10} \phi_n |n\rangle \left/ \sqrt{\sum_{n=0}^{10} |\phi_n|^2} \right. . \quad (78)$$

Using the $\{\psi_n\}$ for this state we diagonalized ρ' [found from Eq. (77) truncated to the Fock states $\{|n\rangle : 0 \leq n \leq 40\}$] and then calculated the ordered eigenvalue sum, Σ_q, for $0 \leq q \leq 40$. In all 100 trials of this procedure, we found that the output state generated by the vacuum majorized the output state produced by the arbitrary pure state. Figure 8 shows this comparison for five of our 100 trials. These particular input states had average amplitudes $1.805 - 0.002i$, $1.318 - 0.340i$, $1.596 + 0.404i$, $1.810 - 0.255i$, $1.546 + 0.276i$, and average photon numbers 5.059, 3.375, 4.976, 4.748, 4.163, respectively.
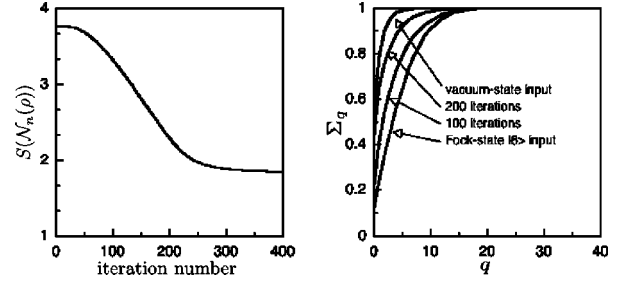

FIG. 9. Left: simulated annealing minimization of the classical-noise channel's output entropy for $n=0.85$. Plot of the output entropy $S(\mathcal{N}_n(\rho))$ vs iteration number when the minimization algorithm is initiated with the Fock-state input $|6\rangle$. Right: majorization analysis of the map $\mathcal{N}_n$ for $n=0.85$. Plots of Σ_q (the sum of the $q+1$ largest eigenvalues) for the thermal state $\rho_0' = \mathcal{N}_n(|0\rangle\langle0|)$, the evolved Fock state $|6\rangle$, and the output states obtained after 100, 200, and 400 iterations of the simulated annealing algorithm. The curves for the vacuum-state input and the output state after 400 iterations are indistinguishable on this scale.

C. Simulated annealing optimization

As a final test of conjecture (ii), we used simulated annealing [27]—a well known technique for finding global extrema—to minimize the classical-noise channel's output entropy. As in Sec. VII B, the input state was truncated to lie in span $\{|n\rangle : 0 \leq n \leq 10\}$, the output states were constrained to lie in span $\{|n\rangle : 0 \leq n \leq 40\}$, and we limited our consideration to the classical-noise channel. A variety of initial pure-state inputs were employed, in conjunction with an exponential cooling schedule. In all cases, the resulting minimum output entropy was extremely close to that achieved by a vacuum-state input. Indeed, in every case the associated input state, at the end of the simulated annealing iterations, was very nearly a coherent state. Figure 9 shows the progression of output entropy values for the $n=0.85$ classical-noise channel when the simulated annealing procedure was initiated with the Fock-state input $|6\rangle$ and 400 iterations were performed. The initial output entropy in this run was 3.754; the final output entropy in this run was 1.846. The latter is very close to $g(0.85)=1.841$, which is the output entropy for a coherent-state input. The final input state $|\psi\rangle_{400}$, after the 400 iterations, had a mean amplitude of $-0.116+1.861i$, an average photon number of 3.47, and a 99.9% overlap with the coherent state $|\alpha\rangle$ for $\alpha=-0.12+1.88i$, viz., $|\langle\alpha|\psi\rangle_{400}|^2=0.999$. For this Fock-state input, we found that the output-state eigenvalues at every iteration majorized those for preceding iterations (see, e.g., Fig. 9).

VIII. CONCLUSIONS

We conjectured that the minimum entropies at the output of two Gaussian bosonic channels (with thermal or classical noise) are achieved by inputs that are coherent states. Physically, this conjecture is plausible: the complete absence of correlation between the input state and the channel's environment state would seem to forbid the existence of an input whose injection reduces the output entropy to a level lower than that achieved when no photons are transmitted. In sup-

port of our conjecture, we presented four separate arguments. First, we proved that the conjecture is true when we restrict the analysis to Gaussian-state inputs. Second, we established a suite of lower bounds on the minimum output entropy, which are all compatible with the conjecture and which show that the conjecture is asymptotically correct at low and high noise levels. Third, we studied local minimum conditions on the output entropy; input coherent states were shown to be local minima that satisfy the operator identities that are necessary conditions for minimality. Fourth, we analyzed a stronger version of the conjecture, namely, that the output state produced by a coherent-state input majorizes all other output states. In support of this stronger conjecture, we presented evidence for number-state and randomly selected inputs. In a companion paper [8], we show that coherent states minimize the output Rényi and Wehrl entropies for the classical- and thermal-noise channels, thus lending further credence to the conjecture in the present work.

APPENDIX A: VACUUM OUTPUT ENTROPY

Here we derive the output entropies of the channels $\mathcal{N}_n$ and $\mathcal{E}_\eta^N$ for vacuum-state inputs. Both channels evolve the vacuum into the thermal state ρ_0' of Eq. (7). For the classical-noise channel, this can be seen by expressing ρ_0' in terms of coherent states, i.e.,

$$\mathcal{N}_n(|0\rangle\langle0|) = \int d^2\mu \, P_n(\mu) \, |\mu\rangle\langle\mu| \qquad (A1)$$

$$= \frac{1}{n+1}\left(\frac{n}{n+1}\right)^{a^\dagger a}. \qquad (A2)$$

The same relation applies for the thermal-noise channel, as can be seen by using decomposition (20) and the fact that the pure-loss channel maps the vacuum state into itself, viz.,

$$\mathcal{E}_\eta^N(|0\rangle\langle0|) = \mathcal{N}_{(1-\eta)N}[\mathcal{E}_\eta^0(|0\rangle\langle0|)] = \mathcal{N}_{(1-\eta)N}(|0\rangle\langle0|). \qquad (A3)$$

The entropy of ρ_0' is

$$S(\rho_0') = -\mathrm{Tr}\left[\rho_0'\left(a^\dagger a \ln\frac{M}{M+1} - \ln(M+1)\right)\right] = (M+1)\ln(M+1) - M\ln M, \qquad (A4)$$

where we have used the fact that the average photon number of ρ_0' is M.

APPENDIX B: PROOFS OF EQS. (25) AND (27)

In order to prove (25) and (27), we employ the amplifying channel defined by the field transformation

$$a \to \sqrt{\kappa}a + \sqrt{\kappa-1}c^\dagger, \qquad (B1)$$

where $\kappa \geq 1$ is the amplifier gain and c is the annihilation operator of the amplifier's spontaneous-emission mode. With c in the vacuum state, the symmetrically ordered characteristic function of the amplifying-channel map $\mathcal{A}_\kappa$ is easily shown to be

$$\chi'(\mu) = \chi(\sqrt{\kappa}\mu)e^{-(\kappa-1)|\mu|^2/2}. \qquad (B2)$$

Linking Eqs. (17) and (B2), we find the decomposition rules

$$\mathcal{E}_\eta^N = \mathcal{E}_{\eta'}^{N'} \circ \mathcal{A}_{\eta/\eta'} \text{ for } \eta \geq \eta', \qquad (B3)$$

$$\mathcal{N}_n = \mathcal{E}_{1-n}^0 \circ \mathcal{A}_{1/(1-n)} \text{ for } n \leq 1, \qquad (B4)$$

$$\mathcal{N}_n = \mathcal{A}_{1/\eta} \circ \mathcal{E}_\eta^0 \text{ for } n = (1-\eta)/\eta, \qquad (B5)$$

where, in (B3),

$$N' = \frac{(1-\eta)N + \eta' - \eta}{1-\eta'} \leq N. \qquad (B6)$$

Bound (25) now follows from combining Eq. (B3) and (11), which establishes that minimum entropy is increased by concatenation of two maps. Using relation (B4) together with Eqs. (18) and (20), we obtain the identity

$$\mathcal{N}_n = \mathcal{N}_{n-n'} \circ \mathcal{E}_{1-n'}^0 \circ \mathcal{A}_{1/(1-n')} = \mathcal{E}_{1-n'}^{(n-n')/n'} \circ \mathcal{A}_{1/(1-n')}, \qquad (B7)$$

which applies for $n' \in [0, \min(1,n)]$. Bound (27) follows by removing the amplifier map using inequality (11).

APPENDIX C: DERIVATION OF LOWER BOUND (39)

Here, we derive lower bound (39) for the minimum output entropy $S(\mathcal{N}_n)$. This bound arises from the connection between the von Neumann entropy and the Rényi entropy of order two. Consider the family of states ρ with $\mathrm{Tr}(\rho^2)=t$. As discussed in [21], the minimum values of $S(\rho)$ on this family are obtained from states that have a nondegenerate eigenvalue λ_0 and a k-fold degenerate eigenvalue $\lambda_1 = (1-\lambda_0)/k \geq \lambda_0$, i.e.,
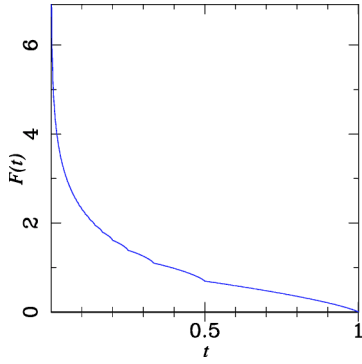
$$S(\rho) \geq -\lambda_0 \ln\lambda_0 - (1-\lambda_0)\ln\frac{1-\lambda_0}{k}, \qquad (C1)$$

$$t = \lambda_0^2 + + \frac{(1-\lambda_0)^2}{k}. \qquad (C2)$$

Equation (C2) can be solved under the constraint $\lambda_1 \geq \lambda_0$, with the result being

$$\lambda_0 = \frac{1 - \sqrt{1-(k+1)(1-kt)}}{k+1}, \qquad (C3)$$

for $t \in [1/(k+1), 1/k]$. Substituting Eq. (C3) into the right-hand side of Eq. (C1), we obtain $S(\rho) \geq F(t)$, with $F(t)$ being the function we have plotted in Fig. 10. Applying this result to the channel's output entropy, we find that

FIG. 10. Function $F(t)$ defined in Eq. (C4).

$$S(\mathcal{N}_n(\rho)) \geq F(\mathrm{Tr}[(\mathcal{N}_n(\rho))^2]) \geq F(1/(2n+1)). \quad (C4)$$

The last inequality is derived by observing that $F(t)$ is a decreasing function of t and that the minimum output Rényi entropy is achieved by a vacuum-state input [8], so that

$$\mathrm{Tr}[\mathcal{N}_n(\rho)^2] \leq 1/(2n+1). \quad (C5)$$

Finally, (39) follows from (C4), because $F(1/(2n+1))$ coincides with the function on the right-hand side of (39).

APPENDIX D: DERIVATION OF LOWER BOUNDS (50) AND (51)

Here we derive lower bounds (50) and (51) on the minimum output entropy $S(\mathcal{E}_\eta^N)$.

1. Proof of lower bound (50)

We first prove that (50) applies for $\eta = 1/k$ for all integers k, and then we generalize to all η. Consider the beam-splitter array shown in Fig. 11, in which $k-1$ beam splitters of transmissivities $\eta_1, \eta_2, \cdots, \eta_{k-1}$ are connected in series and fed with $k-1$ identical thermal states, each with average photon number N. The transmissivity between input port **1** and the jth output port is given by $\epsilon_j \equiv (1-\eta_j)\eta_{j-1}\cdots\eta_1$. The beam splitters are chosen so that $\epsilon_j = 1/k$ for all j, i.e., the jth beam splitter has $\eta_j = (k-j)/(k-j+1)$. For example, with $k=3$ we have two beam splitters with transmissivities $\eta_1 = 2/3$ and $\eta_2 = 1/2$, respectively, so that the transmissivity from input port **1** to each output port is $\epsilon_j = 1/3$. The composition rule
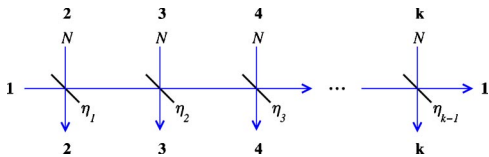

FIG. 11. Beam-splitter array needed to prove (50). The input and output ports are numbered so that the jth input is facing the jth output and the input port 1 is fed with state ρ, the other $k-1$ ports are fed with identical thermal states τ of average photon number N. The transmissivities $\{\eta_j\}$ are chosen in such a way that at each of the k output ports (indicated by arrows) we find the thermal-noise CP map $\mathcal{E}_\eta^N$ with $\eta = 1/k$. This corresponds to choosing $\eta_1 = (k-1)/k$, $\eta_2 = (k-2)/(k-1)$, $\cdots$, $\eta_{k-1} = 1/2$.
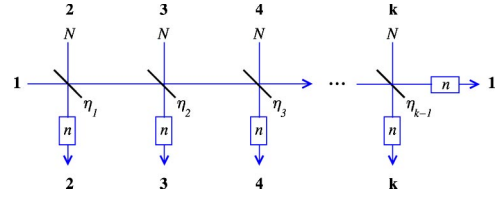

FIG. 12. Beam-splitter array needed to prove (51). Here the signals exiting each beam splitter encounter classical-noise channels. The transmissivities $\{\eta_j\}$ are chosen as in Fig. 11.

(19) can now be used to show that when the array is fed with a state ρ, at each of the output ports (apart from an irrelevant phase factor [28]) we find the state $\mathcal{E}_{1/k}^N(\rho)$. The output entropy of the joint state of all the outputs is equal to the total entropy of the k inputs, because they are connected by a unitary transformation. For ρ a pure state, this entropy is given by the sum of the entropies of the thermal baths, i.e., $(k-1)g(N)$. The subadditivity of the von Neumann entropy [13] implies that this quantity is less than the sum of the entropies of the single outputs,

$$kS(\mathcal{E}_{1/k}^N(\rho)) \geq (k-1)g(N), \quad (D1)$$

which proves (50) for $\eta = 1/k$. The case $\eta \leq 1/k$ follows immediately by using $\eta' = 1/k$ in (24) and applying inequality (D1). Lower bound (50) for $\eta \geq 1/k$ is established by using $\eta' = 1/k$ in (25) and again applying inequality (D1).

2. Proof of lower bound (51)

As in the previous case, we first prove the bound for transmissivity $\eta = 1/k$ with integer k and then we extend the proof to arbitrary η. Consider now the beam-splitter array depicted in Fig. 12; it is the scheme considered previously with classical-noise maps added at each of the beam-splitter outputs. The composition rules [Eqs. (19) and (20)] show that the output state of each port is the same [28], and is given by $\mathcal{E}_{1/k}^{N+nk/(k-1)}(\rho)$. To calculate the joint state of all the outputs, we define a_j to be the annihilation operator of the jth input and V the unitary operator associated with the beam-splitter array. This operator is given by $U_1 U_2 \cdots U_{k-1}$, where U_j is the jth beam-splitter operator, defined in Eq. (1), which couples the mode a_{j+1} with one of the output modes of beam splitter $j-1$. V produces the following field transformation:

$$V^\dagger \vec{a} V = \vec{a} \cdot \Lambda, \quad (D2)$$

where Λ is the $k \times k$ real unitary matrix with $|\Lambda_{ij}|$ being the effective transmissivity between the ith input and the jth output. The sign of Λ_{ij} depends on the reflections encountered by the field. The sign convention that follows from Eq. (1) is that fields propagating from left to right (see Fig. 12) acquire a π-rad phase shift when reflected, whereas fields propagating from top to bottom do not suffer any phase shift when reflected. This convention implies that Λ_{ij} is negative if $j > i$ and positive otherwise [e.g., $\Lambda_{23} = -\sqrt{(1-\eta_1)(1-\eta_2)}$, $\Lambda_{32} = 0$]. Given the input state $R = \rho \otimes \tau \otimes \cdots \otimes \tau$ (τ being a thermal state with average photon number N), the joint output state of the Fig. 12 map is obtained by acting on R first

with V and then with the classical-noise maps, i.e.,

$$R' = \int d^2\vec{\mu} P(\vec{\mu}) D(\vec{\mu}) V R V^\dagger D^\dagger(\vec{\mu}), \tag{D3}$$

where $D(\vec{\mu}) \equiv \exp(\vec{\mu}\cdot\vec{a}^\dagger - \vec{a}\cdot\vec{\mu}^\dagger)$ with $\vec{\mu} \equiv (\mu_1, \cdots, \mu_k)$, $\vec{a} \equiv (a_1, \cdots, a_k)$, and

$$P(\vec{\mu}) = \exp(-|\vec{\mu}|^2/n)/(\pi n)^k. \tag{D4}$$

Using Eq. (D2) and performing a change of integration variables $\vec{\nu} \equiv \vec{\mu}\cdot\Lambda^\dagger$, the output state can be written as

$$R' = V\left[\int d^2\vec{\nu} P(\vec{\nu}) D(\vec{\nu}) R D^\dagger(\vec{\nu})\right] V^\dagger$$

$$= V[\mathcal{N}_n(\rho) \otimes \mathcal{N}_n(\tau) \otimes \cdots \otimes \mathcal{N}_n(\tau)] V^\dagger. \tag{D5}$$

The entropy of this state is simply given by

$$S(R') = S(\mathcal{N}_n(\rho)) + (k-1)g(n+N), \tag{D6}$$

where we have used the fact that $\mathcal{N}_n(\tau)$ is a thermal state with $n+N$ photons on average (see Sec. III B). The subadditivity of the von Neumann entropy implies that $S(R')$ cannot be greater than the sum of the entropies of the individual output states, i.e.,

$$kS(\mathcal{E}_{1/k}^{N+nk/(k-1)}(\rho)) \geq S(\mathcal{N}_n(\rho)) + (k-1)g(n+N), \tag{D7}$$

which applies for any input state ρ. Note that when $n=0$ we recover inequality (D1), as expected. Lower bound (51), instead, derives by choosing $N=0$, so that

$$S(\mathcal{E}_{1/k}^{nk/(k-1)}(\rho)) \geq \frac{S(\mathcal{N}_n(\rho))}{k} + \frac{k-1}{k}g(n). \tag{D8}$$

As in Appendix D 1, we can apply the composition rules (24) and (25) (using $\eta' = 1/k$) to extend the bound (D8) to any value of η, obtaining inequality (51).

APPENDIX E: DERIVATION OF THE OUTPUT-STATE REPRESENTATION (77)

Here, we derive the Fock-state representation of the classical-noise channel's output state when its input is an arbitrary pure state. Using the Fock-state expansion of the input state,

$$|\psi\rangle = \sum_n \psi_n |n\rangle, \tag{E1}$$

in Eq. (17) we immediately obtain the symmetric characteristic function at the output of the classical-noise channel,

$$\chi'(\mu) = e^{-n|\mu|^2}\langle\psi|e^{\mu a^\dagger - \mu^* a}|\psi\rangle \tag{E2}$$

$$= e^{-(n+1/2)|\mu|^2}\langle\psi|e^{\mu a^\dagger}e^{-\mu^* a}|\psi\rangle \tag{E3}$$

$$= \sum_{j=0}^\infty L_j^0(|\mu|^2)|\psi_j|^2 + \sum_{j=1}^\infty \sum_{k=0}^{j-1} \sqrt{\frac{j!}{k!}} L_k^{j-k}(|\mu|^2)$$

$$\times [\psi_j^* \psi_k \mu^{j-k} + \psi_j \psi_k^*(-\mu)^{j-k}], \tag{E4}$$

where $\{L_j^k(z)\}$ are the Laguerre polynomials. Recovering the output state ρ' from this characteristic function via $\int d^2\mu \chi'(\mu) D(-\mu)/\pi$, and performing the integration in polar coordinates, we obtain the desired Fock-state representation of ρ':

$$\langle k+l|\rho'|k\rangle = \sqrt{\frac{k!}{(k+l)!}} \sum_{j=0}^\infty \sqrt{\frac{j!}{(j+l)!}}$$

$$\times \psi_{j+l}\psi_j^* \frac{(j+k+l)!}{j!\,k!} \frac{n^{j+k}}{(1+n)^{j+k+l+1}}$$

$$\times F(-j, -k; -(j+k+l); 1-n^{-2}), \tag{E5}$$

for $k, l \geq 0$, where $F(\alpha, \beta; \gamma; z)$ is the hypergeometric function. Note that (E5) becomes diagonal when the input is a Fock state. In this case, (E5) can be reduced to (70) by means of a transformation formula for the hypergeometric function and the connection between hypergeometric functions and the Jacobi polynomials [25].

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).

[2] C. H. Bennett and P. W. Shor, IEEE Trans. Inf. Theory **44**, 2724 (1998).

[3] G. G. Amosov, A. S. Holevo, and R. F. Werner, Probl. Inf. Transm. 36, 305 (2000), eprint math-ph/0003002.

[4] C. King and M. B. Ruskai, IEEE Trans. Inf. Theory **47**, 192 (2001); C. King, *ibid.* **49**, 221 (2003).

[5] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, B. J. Yen, and H. P. Yuen, in *Quantum Information Statistics Probability*, edited by O. Hirota (Rinton Press, New Jersey, 2004), p. 90.

[6] P. W. Shor, Commun. Math. Phys. **246**, 453 (2004); A. S. Holevo, eprint quant-ph/0306196.

[7] M. J. W. Hall and M. J. O'Rourke, Quantum Opt. **5**, 161 (1993); M. J. W. Hall, Phys. Rev. A **50**, 3295 (1994).

[8] V. Giovannetti, S. Lloyd, L. Maccone, J. H. Shapiro, and B. J. Yen, Phys. Rev. A (to be published).

[9] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).

[10] V. Giovannetti and S. Lloyd, Phys. Rev. A **69**, 062307 (2004).

[11] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).

[12] H. P. Yuen and M. Ozawa, Phys. Rev. Lett. **70**, 363 (1992); C. M. Caves and P. D. Drummond, Rev. Mod. Phys. **66**, 481 (1994).

[13] A. Wehrl, Rev. Mod. Phys. **50**, 221 (1978).

[14] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, Phys. Rev. Lett. **92**, 027902 (2004).

[15] W. H. Zurek, S. Habib, and J. P. Paz, Phys. Rev. Lett. **70**, 1187

(1993).

[16] A. S. Holevo, M. Sohma, and O. Hirota, Phys. Rev. A **59**, 1820 (1999); M. Sohma and O. Hirota, Recent Res. Dev. Opt. **1**, 146 (2000); M. Sohma and O. Hirota, Phys. Rev. A **65**, 022319 (2002).

[17] A. S. Holevo in Proceedings of the 4th International Conference on Quantum Communication, Measurement and Computing, Evanston, 1998 (unpublished); e-print quant-ph/9809022.

[18] J. J. Sakurai, *Modern Quantum Mechanics* (Addison-Wesley, Boston, MA, 1994).

[19] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer, Berlin , 1994).

[20] K. Życzkowski, Open Syst. Inf. Dyn. **10**, 297 (2003); C. Beck and F. Schlögl, *Thermodynamics of Chaotic Systems* (Cambridge University Press, Cambridge, 1993).

[21] D. W. Berry and B. C. Sanders, J. Phys. A **36**, 12255 (2003); P. Harremoës and F. Topsøe, IEEE Trans. Inf. Theory **47**, 2944 (2001).

[22] X. Wang, B. C. Sanders and D. W. Berry, Phys. Rev. A **67**, 042323 (2003); V. M. Kendon, K. Życzkowski, and W. J. Munro, *ibid.* **66**, 062310 (2002).

[23] The quantity $q_k(\mu) \equiv |\langle \gamma_k|D(\mu)|\psi\rangle|^2/\pi$ is a probability distribution with respect to μ because [26]

$$\int d^2\mu \, q_k(\mu) = \int \frac{d^2\mu}{\pi} \langle \gamma_k|D(\mu)|\psi\rangle\langle\psi|D^\dagger(\mu)|\gamma_k\rangle$$

$$= \langle \gamma_k|\mathbb{1}|\gamma_k\rangle \mathrm{Tr}[|\psi\rangle\langle\psi|] = 1,$$

which can be proven using Schur's lemma since $D(\mu)$ is a unitary irreducible representation of the Weyl-Heisenberg group.

[24] P. W. Shor (private communication).

[25] C. M. Caves and K. Wódkiewicz, e-print quant-ph/0401149.

[26] R. F. Bishop and A. Vourdas, Phys. Rev. A **50**, 4488 (1994).

[27] P. J. M. van Laarhoven and E. H. L. Aarts, *Simulated Annealing: Theory and Applications* (Reidel, Dordrecht, 1987).

[28] Because the reflected and the transmitted photons have opposite phases, there is always a phase difference between the two. However, in the case we are considering the photons interact with a thermal state so that the phase difference between the two output ports can be compensated by a unitary transformation that does not change the entropy.

[29] G. S. Agarwal, Phys. Rev. A **3**, 828 (1971).