

Majorization Theory Approach to the Gaussian Channel Minimum Entropy Conjecture

Raúl García-Patrón,^{1,2} Carlos Navarrete-Benlloch,^{1,2,3} Seth Lloyd,¹ Jeffrey H. Shapiro,¹ and Nicolas J. Cerf^{1,4}

¹Research Laboratory of Electronics, MIT, Cambridge, Massachusetts 02139, USA

²Max-Planck Institut für Quantenoptik, Hans-Kopfermann-Strasse 1, D-85748 Garching, Germany

³Departament d'Òptica, Universitat de València, Dr. Moliner 50, 46100 Burjassot, Spain

⁴Quantum Information and Communication, Ecole Polytechnique de Bruxelles, CP 165,
Université Libre de Bruxelles, 1050 Bruxelles, Belgium

(Received 3 November 2011; published 16 March 2012)

A long-standing open problem in quantum information theory is to find the classical capacity of an optical communication link, modeled as a Gaussian bosonic channel. It has been conjectured that this capacity is achieved by a random coding of coherent states using an isotropic Gaussian distribution in phase space. We show that proving a Gaussian minimum entropy conjecture for a quantum-limited amplifier is actually sufficient to confirm this capacity conjecture, and we provide a strong argument towards this proof by exploiting a connection between quantum entanglement and majorization theory.

DOI: 10.1103/PhysRevLett.108.110505

PACS numbers: 03.67.Hk, 42.50.-p, 89.70.Kn

During the 1940s, Shannon developed a mathematical theory of the ultimate limits on achievable data transmission rates over a communication channel [1], a work that has been central to the advent of our information era. Since information is necessarily encoded in a physical system and since quantum mechanics is currently our best theory of the physical world, it is natural to seek the ultimate limits on communication set by quantum mechanics. Since the 1970s, scientists started investigating the improvements that quantum technologies may bring to optical communication systems; see, e.g., [2–4]. Because no proper quantum generalization of Shannon's theory existed at that time, the usual approach was to compare the performance of different encoding and decoding schemes for a given optical channel. This provides lower bounds but does not give the ultimate capacity nor the optimal quantum encoding and decoding techniques.

In the 1990s, Holevo and Schumacher and Westmoreland [5,6] set the basis for a quantum generalization of Shannon's communication theory. Consider a quantum channel \mathcal{M} and a source $\mathcal{A} = \{p_a, \rho_a\}$ of independent and identically distributed (i.i.d.) symbols. For each use of the channel \mathcal{M} , Alice sends the quantum state ρ_a with probability p_a , encoding the letter a . One defines the Holevo information

$$\chi(\mathcal{A}, \mathcal{M}) = S[\mathcal{M}(\rho)] - \sum_a p_a S[\mathcal{M}(\rho_a)], \quad (1)$$

where $\rho = \sum_a p_a \rho_a$ and $S(\rho)$ is the von Neumann entropy of the quantum state ρ [7]. The Holevo information χ gives the highest achievable communication rate over the channel \mathcal{M} for a fixed source \mathcal{A} , which may require a collective quantum measurement over multiple uses of the channel in order to achieve the optimal decoding operation. By maximizing Eq. (1) over the ensemble of i.i.d. sources \mathcal{A} under an energy constraint, we obtain the Holevo capacity

$$C_H(\mathcal{M}) = \max_{\mathcal{A}} \chi(\mathcal{A}, \mathcal{M}). \quad (2)$$

For some highly symmetric channels, such as the qubit depolarizing channel, the Holevo capacity actually gives the ultimate channel capacity. For a long time, it was widely believed that this situation prevails for all channels; that is, it was assumed that input entanglement could not improve the classical communication rate over a quantum channel. However, this was disproved in Ref. [8], so that the best definition of the classical capacity that we currently have requires the regularization

$$C(\mathcal{M}) = \lim_{n \rightarrow \infty} \frac{1}{n} C_H(\mathcal{M}^{\otimes n}), \quad (3)$$

where $\mathcal{M}^{\otimes n}$ stands for n uses of the channel.

An important step towards the elucidation of the classical capacity of an optical quantum memoryless channel was made in Ref. [9], where the authors showed that $C(\mathcal{M})$ of a pure-loss channel—a good (but idealized) approximation of an optical fiber—is achieved by a single-use random coding of coherent states using an isotropic Gaussian distribution. It had long been conjectured that such an encoding achieves $C(\mathcal{M})$ of the whole class of optical channels called single-mode phase-insensitive Gaussian bosonic channels [4], including noisy optical fibers and amplifiers. Actually, proving a slightly stronger result known as the minimum output-entropy conjecture, namely, that coherent states minimize the output entropy of single-mode phase-insensitive channels, would be sufficient to prove this conjecture on the capacity of such channels [10]. Unfortunately, both conjectures have escaped a proof for all phase-insensitive channels but the pure-loss one.

In this Letter, we attempt to prove the minimum output-entropy conjecture for a single use of a single-mode phase-insensitive Gaussian bosonic channel \mathcal{M} , which is believed to capture the hard part of the conjecture for

multiple uses of the channel. We show, by using a decomposition of any phase-insensitive channel into a pure-loss channel and a quantum-limited amplifier, that solving the conjecture for a quantum-limited amplifier is sufficient. This opens a novel way of attacking the conjecture, using the Stinespring representation of an amplifier channel as a two-mode squeezer, and exploiting the connection between entanglement and majorization theory.

Quantum model of optical channels.—Most common quantum optical single-mode channels can be modeled as a single-mode Gaussian bosonic channel. It is a trace-preserving completely positive map fully characterized by the action on the Weyl operators of two 2×2 real matrices, X and Y [11–13]. An intuitive understanding of X and Y is given by the action of the channel on the mean vector d and covariance matrix γ of the input state:

$$d \rightarrow Xd, \quad \gamma \rightarrow X\gamma X^T + Y. \quad (4)$$

For the map to be completely positive, X and Y must satisfy [14]

$$Y \geq 0, \quad \det Y \geq (\det X - 1)^2, \quad (5)$$

where the variance of the vacuum quadratures was normalized to 1 [11]. The map is called quantum-limited when the second inequality in Eq. (5) is saturated.

Phase-insensitive optical channels, such as optical fibers or amplifiers [4], correspond to $X = \text{diag}(\sqrt{x}, \sqrt{x})$ and $Y = \text{diag}(y, y)$, with x being either the attenuation $0 \leq x \leq 1$ or the amplification $1 \leq x$ of the channel and y the added noise variance. By using the composition rule of Gaussian bosonic channels [14], it is easy to show that every phase-insensitive channel \mathcal{M} is indistinguishable from the concatenation of a pure-loss channel \mathcal{L} of transmissivity T with a quantum-limited amplifier \mathcal{A} of gain G ; see Fig. 1.

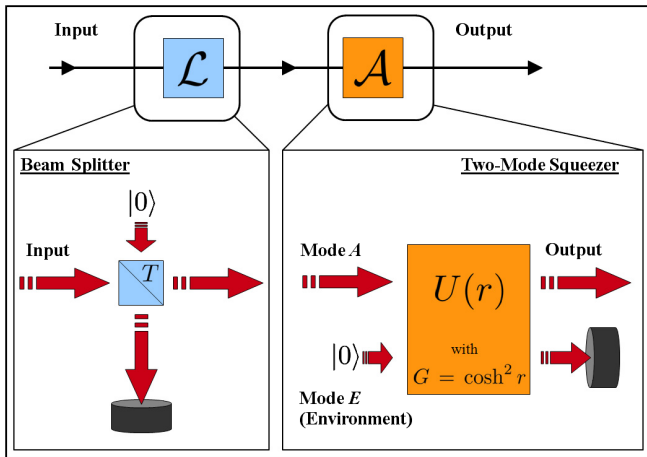


FIG. 1 (color online). Any phase-insensitive Gaussian bosonic channel \mathcal{M} is indistinguishable from a composed channel $\mathcal{A} \circ \mathcal{L}$, where \mathcal{L} is a pure-loss channel and \mathcal{A} a quantum-limited amplifier. The Stinespring dilation of \mathcal{L} is a beam splitter of transmissivity T , while the amplifier \mathcal{A} of gain G becomes a two-mode squeezer of parameter r ($G = \cosh^2 r$) in which the input mode A interacts with a vacuum environmental mode E .

The parameters T and G must satisfy the relations $x = TG$ and $y = G(1 - T) + (G - 1)$ in order to guarantee $\mathcal{M} = \mathcal{A} \circ \mathcal{L}$. Three limiting cases are of particular interest: (i) the pure-loss channel, corresponding to $G = 1$ and $0 \leq T \leq 1$, having a quantum-limited noise of $y = 1 - T$; (ii) the quantum-limited amplifier [4] corresponding to $T = 1$ and $G \geq 1$, with noise $y = G - 1$ resulting from spontaneous emission during the amplification process; (iii) the additive classical noise channel, corresponding to $x = TG = 1$ and added thermal noise $y = 2(G - 1)$.

Reduction of the minimum entropy conjecture.—As stated earlier, our ultimate goal is to address the following conjecture.

Conjecture C1.—Coherent input states minimize the output entropy of any phase-insensitive Gaussian bosonic channel \mathcal{M} .

Three simplifications can be made at this point. First, due to the concavity of the von Neumann entropy, the minimization can be reduced to the set of pure input states. Second, applying a displacement $D(\alpha)$ at the input of the channel has the same effect as applying $D(\sqrt{x}\alpha)$ at the output, i.e., $\mathcal{M} \circ D(\alpha) = D(\sqrt{x}\alpha) \circ \mathcal{M}$. So, because the von Neumann entropy is invariant under unitary evolution, we can restrict our search to zero-mean input states, that is, states $|\varphi\rangle$ satisfying $\langle \varphi | a | \varphi \rangle = 0$, where a is the modal annihilation operator. Finally, by exploiting the decomposition $\mathcal{M} = \mathcal{A} \circ \mathcal{L}$, it is easy to see, by using the concavity of the von Neumann entropy, that the minimum output entropy of channel \mathcal{M} is lower-bounded by that of channel \mathcal{A} , i.e., $\min_{\phi} S[\mathcal{M}(\phi)] \geq \min_{\psi} S[\mathcal{A}(\psi)]$ [15]. Since the vacuum state is invariant under \mathcal{L} , we conclude that proving that vacuum minimizes the output entropy of channel \mathcal{A} implies that vacuum also minimizes the output entropy of channel \mathcal{M} .

The previous straightforward derivation shows that conjecture C1 is strictly equivalent to the following one.

Conjecture C2.—Among all zero-mean pure input states, the vacuum state minimizes the output entropy of the quantum-limited amplifier \mathcal{A} .

Entanglement and majorization theory.—The Stinespring dilation of a quantum-limited amplifier of gain G is a two-mode squeezer of parameter r , with $G = \cosh^2 r$, which effects the unitary transformation (see Fig. 1)

$$U(r) = \exp[r(a_A a_E - a_A^\dagger a_E^\dagger)/2], \quad (6)$$

between the input mode A and an environmental mode E , where a_Z^\dagger and a_Z are the creation and annihilation operators, respectively, of mode Z . Because the entanglement $E[|\psi\rangle_{AE}]$ of a pure bipartite state $|\psi\rangle_{AE}$ is uniquely quantified by the von Neumann entropy of its reduced density operator $\rho_A = \text{Tr}_E[|\psi\rangle_{AE}\langle\psi|]$, i.e., $E[|\psi\rangle_{AE}] = S(\rho_A)$, we can equivalently rephrase conjecture C2 as follows.

Conjecture C3.—Among all input states $|\phi\rangle_{AE} \equiv |\varphi\rangle \otimes |0\rangle$ of a two-mode squeezer with $|\varphi\rangle$ having a zero mean, the vacuum state $|0\rangle_{AE} \equiv |0\rangle \otimes |0\rangle$ minimizes the output entanglement.

In the remainder of this Letter, we exploit the connection between entanglement and majorization theory to attack the proof of **C3**. Majorization theory provides a partial order relation between probability distributions [15,16]. One says that a probability distribution $\mathbf{p} = (p_0, p_1, \dots)^T$ majorizes another one \mathbf{q} (denoted $\mathbf{p} \succ \mathbf{q}$) if and only if there exists a column-stochastic matrix D (a square matrix whose columns sum to 1) such that $\mathbf{q} = D\mathbf{p}$, showing that \mathbf{q} is more disordered than \mathbf{p} . It implies that all concave functions of a distribution, most notably the entropy, can only increase along such a “disorder-enhancing” transformation. From an operational point of view, an interesting way of proving majorization is by checking the relations

$$\sum_{n=0}^m p_n^\downarrow \geq \sum_{n=0}^m q_n^\downarrow \quad \forall m \in \mathbb{N}, \quad (7)$$

where \mathbf{p}^\downarrow and \mathbf{q}^\downarrow are the original vectors with their components rearranged in decreasing order. The notion of majorization can be extended to entangled states [17]: A bipartite pure state $|\phi\rangle$ majorizes another one $|\psi\rangle$ (denoted $|\phi\rangle \succ |\psi\rangle$) if and only if the Schmidt coefficients of $|\phi\rangle$ majorize those of $|\psi\rangle$. This guarantees the existence of a deterministic protocol involving only “local operations and classical communication” (LOCC) that maps $|\psi\rangle$ into $|\phi\rangle$, ensuring the relation $E[|\psi\rangle] \geq E[|\phi\rangle]$. We are now ready to introduce the following stronger conjecture (it implies **C3**).

Conjecture C4.—For any zero-mean state $|\varphi\rangle$, the state $U(r)(|\varphi\rangle \otimes |0\rangle)$ is majorized by the two-mode squeezed vacuum state $U(r)(|0\rangle \otimes |0\rangle)$.

Infinitesimal two-mode squeezer.—Before addressing the general case, let us prove **C4** for an infinitesimal two-mode squeezer by expanding the unitary transformation (6) to the first order in the squeezing parameter r :

$$U(r) = I + \frac{r}{2}(a_A a_E - a_A^\dagger a_E^\dagger) + O(r^2), \quad (8)$$

where I is the identity operator. By defining the state $|\varphi_\perp\rangle \equiv -a_A^\dagger |\varphi\rangle / (1 + \bar{n}_\varphi)^{1/2}$, where $\bar{n}_\varphi = \langle \varphi | a_A^\dagger a_A | \varphi \rangle$ is the mean photon number of the input state $|\varphi\rangle$, the output state becomes

$$|\phi_{\text{out}}\rangle_{AE} \approx \sqrt{\lambda_\varphi} |\varphi\rangle \otimes |0\rangle + \sqrt{1 - \lambda_\varphi} |\varphi_\perp\rangle \otimes |1\rangle, \quad (9)$$

with $\lambda_\varphi = 1/[1 + r^2(\bar{n}_\varphi + 1)/4]$. For any physical state $|\varphi\rangle$ with finite energy \bar{n}_φ , one can choose r small enough so that the condition $r\bar{n}_\varphi^{1/2} \ll 1$ is satisfied and the approximation (9) holds. The key point is to realize that, since the input state $|\varphi\rangle$ has a zero mean, the states $|\varphi_\perp\rangle$ and $|\varphi\rangle$ are orthogonal, so that the state (9) is already in Schmidt form. Therefore, if $|\varphi\rangle$ and $|\pi\rangle$ are two input states such that $\bar{n}_\varphi < \bar{n}_\pi$, then $\lambda_\varphi > \lambda_\pi$, implying that $U(r)(|\varphi\rangle \otimes |0\rangle) \succ U(r)(|\pi\rangle \otimes |0\rangle)$ as a result of Eq. (7). In other words, any output state is majorized by the states having a lower mean input photon number. Finally, since the vacuum state has the minimum mean photon number

($\bar{n}_\varphi = 0$), this majorization relation proves conjecture **C4** for infinitesimal two-mode squeezers.

Majorization relations in a two-mode squeezer.—In order to address conjecture **C4** for any r , let us consider the number-state expansion of an arbitrary input state $|\varphi\rangle = \sum_{k=0}^{\infty} c_k |k\rangle$, which leads to the output state

$$U(r)(|\varphi\rangle \otimes |0\rangle) = \sum_{k=0}^{\infty} c_k |\Psi_\lambda^{(k)}\rangle, \quad (10)$$

where $\lambda = \tanh r$ and $|\Psi_\lambda^{(k)}\rangle$ stands for the output state corresponding to an input Fock state $|\varphi\rangle = |k\rangle$. As shown in Ref. [15], we have

$$|\Psi_\lambda^{(k)}\rangle = \sum_{n=0}^{\infty} \sqrt{p_n^{(k)}(\lambda)} |n+k\rangle \otimes |n\rangle, \quad (11)$$

with Schmidt coefficients

$$p_n^{(k)}(\lambda) = (1 - \lambda^2)^{k+1} \lambda^{2n} \binom{n+k}{n}. \quad (12)$$

We have been able to prove two chains of majorization relations by considering either different Fock states $|k\rangle$ at the input (for a fixed squeezing parameter r) or different values of r (for a fixed input Fock state $|k\rangle$). First, when restricting to Fock states $|k\rangle$, we can prove that

$$|\Psi_\lambda^{(k)}\rangle \succ |\Psi_\lambda^{(k+1)}\rangle, \quad (13)$$

since there exists a column-stochastic matrix

$$D_{nm} = (1 - \lambda^2) \lambda^{2(n-m)} H(n-m), \quad (14)$$

such that $\mathbf{p}^{(k+1)}(\lambda) = D\mathbf{p}^{(k)}(\lambda)$, where $H(x)$ is the Heaviside step function defined as $H(x) = 0$ for $x < 0$ and $H(x) = 1$ for $x \geq 0$. The details of the proof are provided in Ref. [15], where we also give the explicit form of an LOCC protocol that deterministically maps $|\Psi_\lambda^{(k+1)}\rangle$ into $|\Psi_\lambda^{(k)}\rangle$. Iterating this procedure, we can easily prove that $|\Psi_\lambda^{(k)}\rangle \succ |\Psi_\lambda^{(k')}\rangle$, $\forall k' \geq k$, for which we also give the corresponding column-stochastic matrix and deterministic LOCC protocol.

For our matters here, the central consequence is that $|\Psi_\lambda^{(0)}\rangle \succ |\Psi_\lambda^{(k)}\rangle$, $\forall k \geq 0$; that is, we have proved conjecture **C4** for the restricted, but complete, set of input Fock states. Remarkably, this would be sufficient to prove the single-use minimum entropy conjecture if it could be shown that the output-entropy minimizing input state is isotropic, i.e., its Wigner distribution is rotationally invariant. This is because the Fock states are the only isotropic, zero-mean pure states.

Second, given an input Fock state $|k\rangle$, one can show that there exists a majorization relation in the direction of decreasing squeezing parameter, that is,

$$|\Psi_{\lambda'}^{(k)}\rangle \succ |\Psi_\lambda^{(k)}\rangle \quad \forall \lambda' < \lambda, \quad (15)$$

since one can build [15] a column-stochastic matrix

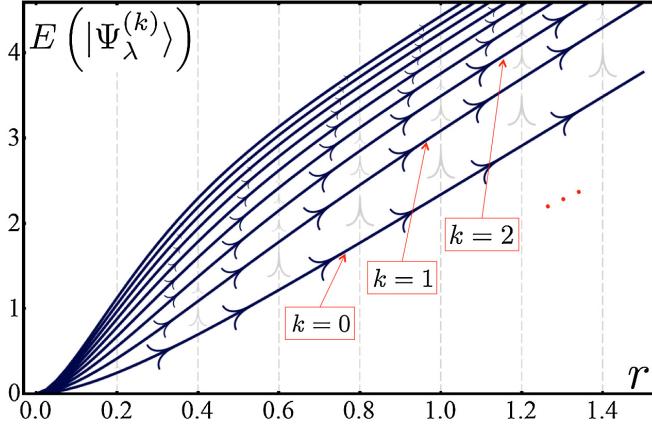


FIG. 2 (color online). Entanglement of the output state $|\Psi_\lambda^{(k)}\rangle$ as a function of the squeezing parameter r . As explained in the text, the entanglement is monotonically increasing with r for all Fock input states, while, for a fixed r , it monotonically increases with k . This behavior is in full agreement with the majorization relations (13) and (15) proved in the text. The arrows in the figure indicate the majorization order.

$$R_{nm}^{(k)} = \binom{m+k}{m}^{-1} \left(\frac{1-\lambda^2}{1-\lambda'^2} \right) H(n-m) \times [L_{n-m}^{(k,m)} \lambda^2 - L_{n-m-1}^{(k,m+1)} \lambda'^2] \lambda^{2(n-m-1)}, \quad (16)$$

with

$$L_m^{(k,n)} = n \binom{n+k}{k} \binom{m+k}{k} \lambda^{l-2n} B(\lambda^2; n, 1+k), \quad (17)$$

and $B(z; a, b) = \int_0^z dx x^{a-1} (1-x)^{b-1}$ being the incomplete beta function, such that $\mathbf{p}^{(k)}(\lambda) = R^{(k)}(\lambda, \lambda') \mathbf{p}^{(k)}(\lambda')$. In Ref. [15], we give a deterministic LOCC protocol performing the transformation $|\Psi_\lambda^{(k)}\rangle \rightarrow |\Psi_{\lambda'}^{(k)}\rangle$.

In Fig. 2, we summarize the two chains of majorization relations and their implications on the output entanglement. From this, as well as the case of the infinitesimal two-mode squeezer, it is tempting to conclude that $\bar{n}_\varphi < \bar{n}_\pi$ always implies $U(r)(|\varphi\rangle \otimes |0\rangle) > U(r) \times (|\pi\rangle \otimes |0\rangle)$. However, we have numerically observed that this does not hold in general, which probably reflects the difficulty of proving the conjecture. As a concrete example, we note that the state $U(r)[(\sqrt{0.4}|1\rangle + \sqrt{0.6}|2\rangle) \otimes |0\rangle]$ has $\bar{n} = 1.6$ mean input photons but is less entangled for $r \geq 0.75$ than $|\Psi_\lambda^{(1)}\rangle$. Nevertheless, our numerical investigations have shown that, for an arbitrary input state $|\varphi\rangle$, the output states corresponding to different squeezing parameters satisfy the majorization relation $U(r') \times (|\varphi\rangle \otimes |0\rangle) > U(r)(|\varphi\rangle \otimes |0\rangle)$ for $r' < r$. Furthermore, we have numerically checked that, for a fixed r , the majorization relation $U(r)(|0\rangle \otimes |0\rangle) > U(r)(|\varphi\rangle \otimes |0\rangle)$ is satisfied by tens of thousands of random superpositions of the first 21 Fock states, which strongly suggests that conjecture **C4** holds.

Conclusion.—Using the decomposition of phase-insensitive Gaussian bosonic channels into a pure-loss

channel and a quantum-limited amplifier, we have shown that proving a reduced conjecture for the quantum-limited amplifier is sufficient to prove the single-use minimum entropy conjecture. By using Stinespring's theorem, this boils down to proving that the vacuum minimizes the output entanglement of a two-mode squeezer. Then, using the connection between entanglement and majorization theory, we have provided a partial proof of this conjecture for a special class of input states, namely, photon number states, as well as a full solution for the infinitesimal channel. To prove the conjecture in general, we are left with the (possibly simpler) task of showing that the output-entropy minimizing input state is isotropic in phase space; that is, no symmetry breaking occurs. Thus, apart from reinforcing the conjecture even further, we believe that our analysis offers a new possible approach to its proof.

The authors thank G. Giedke and J. I. Cirac for helpful discussions. C.N.-B. and N.J.C. thank the Optical and Quantum Communications Group at RLE for their hospitality. R.G.-P., N.J.C., J.H.S., and S.L. acknowledge financial support from the W.M. Keck Foundation Center for Extreme Quantum Information Theory, R.G.-P. from the Humboldt foundation, C.N.-B. from the FPU program of the MICINN and the European Union FEDER through Project No. FIS2008-06024-C03-01, J.H.S. and S.L. from the ONR Basic Research Challenge Program, and N.J.C. from the F.R.S.-FNRS under project HIPERCOM.

- [1] C. E. Shannon, *Bell Syst. Tech. J.* **27**, 379 (1948).
- [2] H. P. Yuen and J. H. Shapiro, *IEEE Trans. Inf. Theory* **26**, 78 (1980).
- [3] J. H. Shapiro and S. S. Wagner, *IEEE J. Quantum Electron.* **20**, 803 (1984).
- [4] C. M. Caves and P. D. Drummond, *Rev. Mod. Phys.* **66**, 481 (1994).
- [5] A. S. Holevo, *IEEE Trans. Inf. Theory* **44**, 269 (1998).
- [6] B. Schumacher and M. D. Westmoreland, *Phys. Rev. A* **56**, 131 (1997).
- [7] In the definition of Eq. (1), the \sum_a should be replaced by an integral when considering a continuous alphabet a .
- [8] M. B. Hastings, *Nature Phys.* **5**, 255 (2009).
- [9] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, J. H. Shapiro, and H. P. Yuen, *Phys. Rev. Lett.* **92**, 027902 (2004).
- [10] V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, and J. H. Shapiro, *Phys. Rev. A* **70**, 032315 (2004).
- [11] C. Weedbrook, S. Pirandola, R. García-Patrón, T. Ralph, N. J. Cerf, J. H. Shapiro, and S. Lloyd, *Rev. Mod. Phys.* (to be published).
- [12] A. S. Holevo and R. F. Werner, *Phys. Rev. A* **63**, 032312 (2001).
- [13] J. Eisert and M. M. Wolf, in *Quantum Information with Continuous Variables of Atoms and Light*, edited by E. S. Polzik, N. J. Cerf, and G. Leuchs (Imperial College, London, 2007).

- [14] F. Caruso, V. Giovannetti, and A. S. Holevo, *New J. Phys.* **8**, 310 (2006).
- [15] See Supplemental Material at <http://link.aps.org/supplemental/10.1103/PhysRevLett.108.110505> for a detailed explanation of the reduction of the minimum entropy conjecture, as well as a complete proof of the majorization relations inherent to a two-mode squeezing transformation and the corresponding LOCC protocols.
- [16] B. C. Arnold, *Majorization and the Lorenz Order*, Lecture Notes in Statistics Vol. 43 (Springer-Verlag, Berlin, 1987).
- [17] M. A. Nielsen and G. Vidal, *Quantum Inf. Comput.* **1**, 76 (2001).