Optimality of Gaussian Discord

Stefano Pirandola,[1,*] Gaetana Spedalieri,[1] Samuel L. Braunstein,[1] Nicolas J. Cerf,[2] and Seth Lloyd[3]
[1]*Computer Science, University of York, York YO10 5GH, United Kingdom*
[2]*Ecole Polytechnique de Bruxelles, CP 165, Université Libre de Bruxelles (ULB), 1050 Brussels, Belgium*
[3]*Research Laboratory of Electronics & Department of Mechanical Engineering, MIT, Cambridge, Massachusetts 02139, USA*
(Received 9 September 2013; revised manuscript received 5 July 2014; published 3 October 2014)

In this Letter we exploit the recently solved conjecture on the bosonic minimum output entropy to show the optimality of Gaussian discord, so that the computation of quantum discord for bipartite Gaussian states can be restricted to local Gaussian measurements. We prove such optimality for a large family of Gaussian states, including all two-mode squeezed thermal states, which are the most typical Gaussian states realized in experiments. Our family also includes other types of Gaussian states and spans their entire set in a suitable limit where they become Choi matrices of Gaussian channels. As a result, we completely characterize the quantum correlations possessed by some of the most important bosonic states in quantum optics and quantum information.

DOI: 10.1103/PhysRevLett.113.140405 PACS numbers: 03.65.Ta, 03.67.Mn, 42.50.-p

Quantum correlations represent a fundamental resource in quantum information and computation [1,2]. If we restrict the description of a quantum system to pure states, then quantum entanglement is synonymous with quantum correlations. However, this is not exactly the case when general mixed states are considered: Separable mixed states can still have residual correlations which cannot be simulated by any classical probability distribution [3,4]. These residual quantum correlations are today quantified by quantum discord [5].

Quantum discord is defined as the difference between the total correlations within a quantum state, as measured by the quantum mutual information, and its classical correlations, corresponding to the maximal randomness which can be shared by two parties by means of local measurements and one-way classical communication [6]. This definition not only provides a more precise characterization of quantum correlations but also has direct application in various protocols, including quantum state merging [7], remote state preparation [8], discrimination of unitaries [9], quantum channel discrimination [10], quantum metrology [11], and quantum cryptography [12].

For bosonic systems, like the optical modes of the electromagnetic field, it is therefore crucial to compute the quantum discord of Gaussian states [13]. Despite these states being the most common in experimental quantum optics and the most studied in continuous-variable quantum information [14], no closed formula is yet known for their quantum discord. What is computed is an upper bound, known as Gaussian discord [15,16], which is a simplified version based on Gaussian detections only. Gaussian discord has been conjectured to be the actual discord for Gaussian states, as also supported by recent numerical studies [17,18].

In this Letter, we connect this conjecture on Gaussian discord with the recently solved conjecture on the bosonic minimum output entropy [19], according to which the von Neumann entropy at the output of a single-mode Gaussian channel is minimized by a pure Gaussian state at the input [13]. In particular, this optimal input state is the vacuum, or any other coherent state, when we consider Gaussian channels whose action is symmetric in the quadratures (phase-insensitive), as for instance is the case of lossy or amplifier channels (besides Ref. [19] see also Ref. [20] for an alternate proof).

We show that the minimization of the bosonic output entropy implies the optimality of Gaussian discord for a large family of Gaussian states. This family includes the important class of squeezed thermal states, which are all those states realized by applying two-mode squeezing to a pair of single-mode thermal states [15]. A key point in our analysis is showing that these states can always be decomposed into an Einstein-Podolsky-Rosen (EPR) state plus the local action of a phase-insensitive Gaussian channel. Given such decomposition, we can easily show that heterodyne detection represents the optimal local measurement for computing their quantum discord.

More generally, by extending the previous decomposition to include other forms of local Gaussian channels, we show that we can generate many other types of bipartite Gaussian states, for which the optimal local measurement is Gaussian, given by a (quasi-)projection on single-mode pure squeezed states. Furthermore, our decomposition spans the entire set of Gaussian states in a suitable (and fastly converging) limit where they become Choi matrices of local Gaussian channels.

As a result of our study, we are now able to compute the actual unrestricted discord of a large portion of Gaussian states, paving the way for a complete and precise characterization of the most fundamental quantum correlations possessed by bosonic systems.

Quantum discord and its Gaussian formulation.—In classical information theory, the mutual information between two random variables, X and Y, can be written as $I(X,Y) = H(X) - H(X|Y)$, where $H(X)$ is the Shannon entropy of variable X, and $H(X|Y) = H(X,Y) - H(Y)$ is its conditional Shannon entropy. This notion has several inequivalent generalizations in quantum information theory [5], where the two variables are replaced by two quantum systems, A and B, in a joint quantum state ρ_{AB}.

A first generalization is given by the quantum mutual information [2], defined as $I(A,B) = S(A) - S(A|B)$, where $S(A) = -\mathrm{Tr}(\rho_A \log_2 \rho_A)$ is the von Neumann entropy of system A, in the reduced state $\rho_A = \mathrm{Tr}_B(\rho_{AB})$, and $S(A|B) = S(A,B) - S(B)$ is the conditional von Neumann entropy (to be computed from the joint state ρ_{AB} and the other reduced state ρ_B). The quantum mutual information is a measure of the total correlations between the two quantum systems.

A second generalization is given by

$$C(A|B) = S(A) - S_{\min}(A|B), \quad (1)$$

where the conditional term $S_{\min}(A|B)$ is the von Neumann entropy of system A minimized over all possible measurements on system B, generally described as positive operator valued measures (POVMs) $\mathcal{M}_B = \{M_k\}$ (in particular, it is sufficient to consider rank-1 POVMs [5]). Mathematically, this conditional term is written as

$$S_{\min}(A|B) := \inf_{\mathcal{M}_B} S(A|\mathcal{M}_B), \quad (2)$$

where [21]

$$S(A|\mathcal{M}_B) := \sum_k p_k S(\rho_{A|k}), \quad (3)$$

with $p_k = \mathrm{Tr}(\rho_{AB} M_k)$ the probability of outcome k, and $\rho_{A|k} = p_k^{-1} \mathrm{Tr}_B(\rho_{AB} M_k)$ the conditional state of A.

The entropic quantity $C(A|B)$ quantifies the classical correlations in the joint state ρ_{AB}, being the maximum amount of common randomness which can be extracted by local measurements and one-way classical communication [6]. Quantum discord is then defined as the difference between the total and these classical correlations [3–5]

$$D(A|B) := I(A,B) - C(A|B) = S_{\min}(A|B) - S(A|B). \quad (4)$$

When the two systems A and B are bosonic modes, we can consider their Gaussian discord $D_G(A|B) \geq D(A|B)$, where the minimization of the conditional term $S_{\min}(A|B)$ in Eq. (2) is restricted to Gaussian POVMs. Thanks to this restriction, Gaussian discord is easy to compute for two-mode Gaussian states [15,16]. Furthermore, as we have already mentioned, Gaussian discord is conjectured to be optimal for these states, in the sense that it would represent their unrestricted quantum discord, i.e., $D_G(A|B) = D(A|B)$. This conjecture is supported by numerical studies [17,18] and known to be true for a very limited set of Gaussian states ρ_{AB}, namely those which can be purified into a three-mode Gaussian state Φ_{ABE} symmetric in the AE subsystem [16,22].

Normal forms, two-mode squeezed thermal states, and their decomposition.—Since quantum discord and classical correlations are entropic quantities, they are invariant under local unitaries. This means that we may apply displacements to yield a zero mean value, and local Gaussian unitaries to reduce the covariance matrix (CM) into normal form [13]. Thus, without loss of generality, quantum discord can be studied for zero-mean Gaussian states ρ_{AB} with CM

$$\mathbf{V}_{AB} = \begin{pmatrix} a\mathbf{I} & \mathrm{diag}(c,c') \\ \mathrm{diag}(c,c') & b\mathbf{I} \end{pmatrix} := \mathbf{V}(a,b,c,c'), \quad (5)$$

where $\mathbf{I} = \mathrm{diag}(1,1)$ and the parameters satisfy bona fide conditions imposed by the uncertainty principle [25–27].

For simplicity, we start from the most typical zero-mean Gaussian states, i.e., two-mode squeezed thermal states. These states have CMs of the form $\mathbf{V}_{AB} = \mathbf{V}(a,b,c,-c)$ with bona fide conditions $a,b \geq 1$ and $c^2 \leq ab - 1 - |a-b|$. As we prove in Ref. [28] and depict in Fig. 1, these states can always be decomposed as $\rho_{AB} = (\mathcal{E} \otimes \mathcal{I})(\sigma_{aB})$, where $\mathcal{E}$ is a phase-insensitive Gaussian channel (details below), $\mathcal{I}$ is the identity channel, and σ_{aB} is an EPR state with CM

$$\mathbf{V}_{aB} := \begin{pmatrix} b\mathbf{I} & \sqrt{b^2-1}\mathbf{C} \\ \sqrt{b^2-1}\mathbf{C} & b\mathbf{I} \end{pmatrix}, \quad (6)$$

where

$$\mathbf{C} := \begin{pmatrix} \mathrm{sgn}(c) & 0 \\ 0 & -\mathrm{sgn}(c) \end{pmatrix}. \quad (7)$$

At the level of the second order moments, a phase-insensitive Gaussian channel $\mathcal{E}$ performs the transformation $\mathbf{V}_{aB} \to \mathbf{V}_{AB} = (\mathbf{K} \oplus \mathbf{I})\mathbf{V}_{aB}(\mathbf{K}^T \oplus \mathbf{I}) + (\mathbf{N} \oplus \mathbf{0})$, with transmission matrix $\mathbf{K} = \sqrt{\tau}\mathbf{I}$ and noise matrix $\mathbf{N} = \eta\mathbf{I}$, where

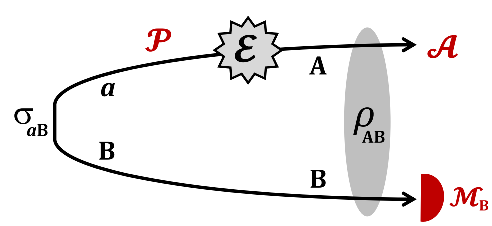

FIG. 1 (color online). State decomposition. A two-mode squeezed thermal state ρ_{AB} can always be decomposed into an EPR state σ_{aB} plus the local application of a phase-insensitive Gaussian channel $\mathcal{E}$. Remote preparation (red elements, see next section). A local measurement $\mathcal{M}_B$ on mode B generates a remote ensemble $\mathcal{A}$ on the output mode A. There will be another ensemble $\mathcal{P}$ generated on the input mode a before the channel. This input ensemble will be made by Gaussianly modulated coherent states if $\mathcal{M}_B$ is heterodyne detection.

$\tau \geq 0$ and $\eta \geq |1-\tau|$. In particular, this is a "lossy channel" for transmissivity $\tau \in [0,1]$ and thermal noise $\eta \geq 1-\tau$, an "additive-noise channel" for $\tau = 1$ and $\eta \geq 0$, or an "amplifier channel" for $\tau > 1$ and $\eta \geq \tau - 1$. (These are the most important canonical forms of a single-mode Gaussian channel, see Refs. [13,28] for this classification.) As a result, the CM of a two-mode squeezed thermal state $\mathbf{V}_{AB} = \mathbf{V}(a,b,c,-c)$ can be expressed in the equivalent form

$$\mathbf{V}_{AB} = \begin{pmatrix} (\tau b + \eta)\mathbf{I} & \sqrt{\tau(b^2-1)}\mathbf{C} \\ \sqrt{\tau(b^2-1)}\mathbf{C} & b\mathbf{I} \end{pmatrix}, \tag{8}$$

for some choice of $\tau \geq 0$ and $\eta \geq |1-\tau|$.

Remote state preparation and connection with the bosonic minimum output entropy.—As depicted in Fig. 1, the action of a local POVM $\mathcal{M}_B = \{M_k\}$ on mode B generates a remote ensemble of states $\mathcal{P}$ on the input mode a, and a corresponding ensemble $\mathcal{A}$ on the output mode A. With probability $p_k = \mathrm{Tr}(\sigma_{aB} M_k)$, we have a conditional input state $\sigma_{a|k} = p_k^{-1}\mathrm{Tr}_B(\sigma_{aB} M_k) \in \mathcal{P}$ and its corresponding channel output $\rho_{A|k} = \mathcal{E}(\sigma_{a|k}) \in \mathcal{A}$.

Assuming heterodyne detection $\mathcal{M}_B = \mathrm{het}_B$, the input ensemble $\mathcal{P}$ consists of coherent states $\sigma_{a|k} = |\alpha_k\rangle\langle\alpha_k|$ whose complex amplitudes α_k are Gaussianly distributed (see Ref. [28] for more details on the remote preparation of Gaussian states). As a result, the output ensemble $\mathcal{A}$ will be composed of Gaussian states $\rho_{A|k} = \mathcal{E}(|\alpha_k\rangle\langle\alpha_k|)$ with Gaussianly modulated first moments and CM equal to $(\tau+\eta)\mathbf{I}$.

The output entropy associated with the heterodyne detection is equal to the average entropy of the output ensemble $\mathcal{A}$, i.e.,

$$S(A|\mathrm{het}_B) = \int d^2k\, p_k S[\mathcal{E}(|\alpha_k\rangle\langle\alpha_k|)]. \tag{9}$$

Since entropy is invariant under displacements, we may write [32] $S[\mathcal{E}(|\alpha_k\rangle\langle\alpha_k|)] = S[\mathcal{E}(|0\rangle\langle 0|)]$ and therefore

$$S(A|\mathrm{het}_B) = S[\mathcal{E}(|0\rangle\langle 0|)] = h(\tau+\eta), \tag{10}$$

where

$$h(x) := \frac{x+1}{2}\log_2\frac{x+1}{2} - \frac{x-1}{2}\log_2\frac{x-1}{2}. \tag{11}$$

At this point we can exploit the solved conjecture on the bosonic minimum output entropy, which states that the vacuum (or any other coherent state) minimizes the output entropy of the phase-insensitive Gaussian channel $\mathcal{E}$ among all possible input states [19,20]

$$S[\mathcal{E}(|0\rangle\langle 0|)] = \inf_\rho S[\mathcal{E}(\rho)]. \tag{12}$$

As a result, we may write

$$\begin{aligned} S(A|\mathrm{het}_B) &= \inf_\rho S[\mathcal{E}(\rho)] \\ &\leq \inf_{\mathcal{M}_B} S(A|\mathcal{M}_B) = S_{\min}(A|B), \end{aligned} \tag{13}$$

where the inequality comes from the fact that any $\mathcal{M}_B$, with input ensemble $\mathcal{P} = \{p_k, \sigma_{a|k}\}$ and output ensemble $\mathcal{A} = \{p_k, \rho_{A|k}\}$, must satisfy

$$\begin{aligned} S(A|\mathcal{M}_B) &= \sum_k p_k S(\rho_{A|k}) \geq \inf_{\mathcal{A}} S(\rho_{A|k}) \\ &= \inf_{\mathcal{P}} S[\mathcal{E}(\sigma_{a|k})] \geq \inf_\rho S[\mathcal{E}(\rho)]. \end{aligned} \tag{14}$$

Thus, there is a Gaussian POVM (heterodyne detection) which is optimal for the minimization of the output entropy $S(A|\mathcal{M}_B)$. This is equivalent to saying that the Gaussian discord of the Gaussian state ρ_{AB} is optimal, i.e., equal to its actual discord. Its calculation is therefore easy, since $S_{\min}(A|B) = h(\tau+\eta)$, leading to

$$D(A|B) = h(b) - h(\nu_-) - h(\nu_+) + h(\tau+\eta), \tag{15}$$

where $\{\nu_\pm\}$ is the symplectic spectrum of $\mathbf{V}_{AB}$, which can be easily computed [13] from Eq. (8).

Extending the family of Gaussian states.—Here we extend the previous derivation to include other Gaussian states. We first generalize the local Gaussian POVM $\mathcal{M}_B$, whose element M_k becomes a quasiprojector on the squeezed state $|k,u\rangle$ [13] with variable amplitude k but fixed CM $\mathbf{V}_{\mathrm{sq}}(u) = \mathrm{diag}(u, u^{-1})$, where $u > 0$. This measurement $\mathcal{M}_B(u)$ corresponds to a heterodyne detection for $u = 1$, and becomes a homodyne detection for $u \to 0$ or $u \to +\infty$. By applying $\mathcal{M}_B(u)$ to an EPR state σ_{aB} with variance b as in Eq. (6), we generate an ensemble $\mathcal{P}$ of amplitude-modulated squeezed states with CM $\mathbf{V}_{\mathrm{sq}}(r)$, where $r = (1+ub)(u+b)^{-1}$. The value of this squeezing ranges from $r = b^{-1}$ to $r = b$, extremes which are achieved by the two homodyne detectors (see Ref. [28] for more details).

We may now "rectify" the ensemble $\mathcal{P}$ by applying the antisqueezing operator [13] $\hat{S}^{-1}(r)$ which transforms its states into coherent states (see Fig. 2). In this way we are sure that optimal states are fed into the Gaussian channel $\mathcal{E}$,

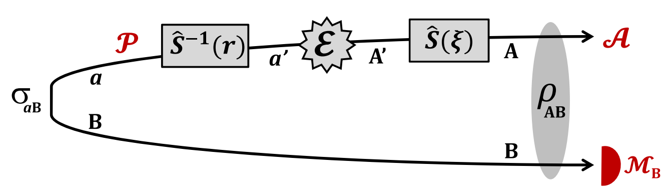

FIG. 2 (color online). General decomposition. We consider Gaussian states ρ_{AB} which can be decomposed into an EPR state σ_{aB} by locally applying a Gaussian channel $\mathcal{E}$ plus input-output squeezing operators. Here the local detection $\mathcal{M}_B$ is a quasiprojection onto squeezed states, so that the input ensemble $\mathcal{P}$ is composed of amplitude-modulated squeezed states.

whose output entropy is therefore minimized. Furthermore, this output entropy does not change if we apply another squeezing operator $\hat{S}(\xi)$, with a suitable ξ putting the Gaussian state ρ_{AB} into normal form. Thus the optimality of Gaussian discord is proven for any Gaussian state which is decomposable into an EPR state as

$$\rho_{AB} = (\mathcal{S}_\xi \mathcal{E} \mathcal{S}_r^{-1} \otimes \mathcal{I})(\sigma_{aB}), \qquad \mathcal{S}_x(\rho) := \hat{S}(x)\rho\hat{S}^\dagger(x), \quad (16)$$

with optimal detection given by the Gaussian $\mathcal{M}_B(u)$.

The second generalization consists of extending the Gaussian channel $\mathcal{E}$ to include negative transmissivities $\tau \leq 0$, where the channel describes the conjugate of an amplifier, which is another Gaussian channel (phase sensitive) whose output entropy is minimized by coherent states at the input [19,20]. We can then consider an extended Gaussian channel $\mathcal{E}$ with arbitrary $\tau \in \mathbb{R}$ and $\eta \geq |1-\tau|$, which is described by the matrices $\mathbf{K} = \sqrt{|\tau|}\mathrm{diag}[1, \mathrm{sgn}(\tau)]$ and $\mathbf{N} = \eta\mathbf{I}$. Thus, the optimality of Gaussian discord is proven for all Gaussian states ρ_{AB} decomposable as in Eq. (16) with $\mathcal{E}$ being such an extended channel. As we show in Ref. [28], these states have CMs in the normal-form $\mathbf{V}(a, b, c, c')$, where

$$a = \theta(r)\theta(r^{-1}), \qquad \theta(r) := \sqrt{\eta r + |\tau| b}, \quad (17)$$

$$c = \pm\sqrt{|\tau|(b^2-1)\theta(r^{-1})/\theta(r)}, \quad (18)$$

$$c' = \mp \mathrm{sgn}[\tau]\sqrt{|\tau|(b^2-1)\theta(r)/\theta(r^{-1})}, \quad (19)$$

with $\tau \in \mathbb{R}$, $\eta \geq |1-\tau|$ and $r \in [b^{-1}, b]$. Here the sign ambiguity comes from the type of EPR state considered in the decomposition, whose CM in Eq. (6) is generally defined with $\mathbf{C} = \pm\mathrm{diag}(1, -1)$. Also note that negative transmissivities allow us to include states with $cc' \geq 0$.

For arbitrary fixed values of $a \geq 1$ and $b \geq 1$, we generate all accessible values of the correlation parameters c and c' by exploiting the remaining degrees of freedom in the parameters τ, η and r. As shown in the numerical investigation of Fig. 3, our family represents a wide portion of all Gaussian states. It includes all states whose CMs have the form $\mathbf{V}(a, b, c, c')$ with $|c| = |c'|$, corresponding to the bisectors of the correlation plane (c, c'). Furthermore, for increasing b, our family tends to invade the entire Gaussian set very quickly. This set is completely filled for $b \to +\infty$, where the EPR state σ_{aB} becomes maximally entangled and the Gaussian state ρ_{AB} becomes the Choi matrix of the Gaussian channel $\mathcal{S}_\xi \mathcal{E} \mathcal{S}_r^{-1}$.

By increasing the entanglement in the EPR state, we increase the amount of squeezing r that we can generate in the input ensemble $\mathcal{P}$. The effect of this squeezing is to include output states where $|c|$ and $|c'|$ are very different, as also evident from the r dependence in Eqs. (18) and (19). In particular, in the limit of $b \to +\infty$, homodyne detectors generate infinite squeezing in $\mathcal{P}$ and we approach all the exotic states on the axes of the plane, for which one of the correlation parameters is zero ($cc' = 0$).

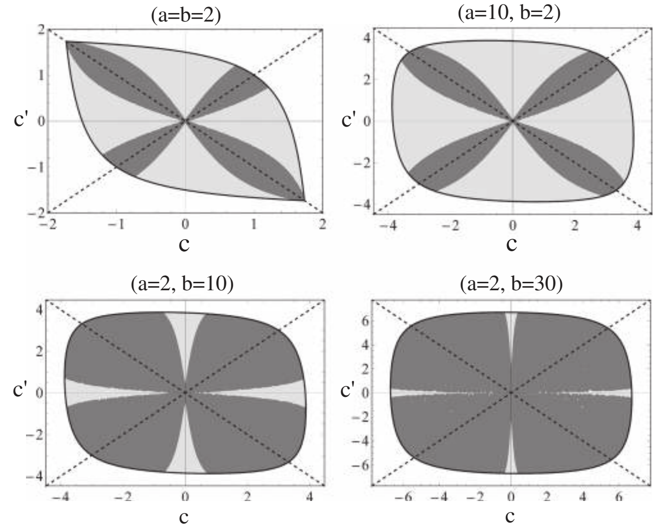

FIG. 3. For given values of a and b, the correlation parameters c and c' can only take a restricted range of physical values corresponding to the delimited regions in the panels. Within these regions, the darker points are members of our Gaussian family. Plots are created by randomly testing 5×10^5 points.

Conclusion and discussion.—In this Letter, we have shown that the validity of the bosonic minimum output entropy conjecture implies the optimality of Gaussian discord for a large family of Gaussian states, decomposable into EPR states subject to local Gaussian channels. In particular, this family includes the class of two-mode squeezed thermal states [15]. From this point of view, our work completely characterizes the quantum correlations possessed by the most typical states in continuous variable quantum information and experimental quantum optics. The exact size of these quantum correlations, i.e., their unconstrained quantum discord, can now be computed efficiently (note that computing discord is nondeterministic polynomial-time complete in the general case [33]).

We have shown that we can rapidly fill the entire set of Gaussian states by increasing their parameter b, i.e., the thermal variance in the mode under detection. The reason is because this parameter corresponds to the variance of the EPR state involved in the decomposition. By increasing this parameter, we increase the EPR entanglement and therefore the amount of squeezing that we can remotely generate at the input of the Gaussian channel.

We could further improve our results if an energy-constrained version of the entropy conjecture were proven for the "pathological" canonical forms [13,34,35]. In fact, there exist highly phase-sensitive Gaussian channels which completely destroy the correlations in only one of the quadratures, therefore being particularly suitable to decompose exotic Gaussian states with $cc' = 0$. Unfortunately, no finite-energy state is known to be optimal for the minimization of the output entropy of these channels. If such a state were Gaussian, then it could be prepared with a limited amount of squeezing and we would span the entire set of Gaussian states more straightforwardly.

Finally, we remark that the complete characterization of the quantum correlations possessed by Gaussian states is important not only in quantum information and quantum optics (e.g., for problems of quantum metrology), but also in other fields. These include condensed matter physics (e.g., Bose-Einstein condensates), solid-state physics, relativistic quantum field theory (where Gaussian states arise from Bogoliubov transformations, e.g., in the Unruh effect or the Hawking radiation), statistical mechanics, and foundations of quantum mechanics.

This work was funded by a Leverhulme Trust research fellowship and EPSRC (Grants No. EP/J00796X/1 and No. EP/L011298/1). S. P. would like to thank M. G. A. Paris for enlightening discussions.

*stefano.pirandola@york.ac.uk

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, England, 2000).
[2] M. M. Wilde, *Quantum Information Theory* (Cambridge University Press, Cambridge, England, 2013).
[3] H. Ollivier and W. H. Zurek, Phys. Rev. Lett. **88**, 017901 (2001).
[4] L. Henderson and V. Vedral, J. Phys. A **34**, 6899 (2001).
[5] K. Modi, A. Brodutch, H. Cable, T. Paterek, and V. Vedral, Rev. Mod. Phys. **84**, 1655 (2012).
[6] I. Devetak and A. Winter, IEEE Trans. Inf. Theory **50**, 3183 (2004).
[7] D. Cavalcanti, L. Aolita, S. Boixo, K. Modi, M. Piani, and A. Winter, Phys. Rev. A **83**, 032324 (2011); V. Madhok and A. Datta, Phys. Rev. A **83**, 032323 (2011).
[8] B. Dakic, Y. O. Lipp, X. Ma, M. Ringbauer, S. Kropatschek, S. Barz, T. Paterek, V. Vedral, A. Zeilinger, C. Brukner, and P. Walther, Nat. Phys. **8**, 666 (2012).
[9] M. Gu, H. M. Chrzanowski, S. M. Assad, T. Symul, K. Modi, T. C. Ralph, V. Vedral, and P. Koy Lam, Nat. Phys. **8**, 671 (2012).
[10] C. Weedbrook, S. Pirandola, J. Thompson, V. Vedral, and M. Gu, arXiv:1312.3332.
[11] D. Girolami, T. Tufarelli, and G. Adesso, Phys. Rev. Lett. **110**, 240402 (2013); D. Girolami, A. M. Souza, V. Giovannetti, T. Tufarelli, J. G. Filgueiras, R. S. Sarthour, D. O. Soares-Pinto, I. S. Oliveira, and G. Adesso, Phys. Rev. Lett. **112**, 210401 (2014).
[12] S. Pirandola, arXiv:1309.2446.
[13] C. Weedbrook, S. Pirandola, R. Garcia-Patron, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[14] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[15] P. Giorda and M. G. A. Paris, Phys. Rev. Lett. **105**, 020503 (2010).
[16] G. Adesso and A. Datta, Phys. Rev. Lett. **105**, 030501 (2010).
[17] P. Giorda, M. Allegra, and M. G. A. Paris, Phys. Rev. A **86**, 052328 (2012).
[18] S. Olivares and M. G. A. Paris, Int. J. Mod. Phys. B **27**, 1345024 (2013).
[19] V. Giovannetti, R. Garcia-Patron, N. J. Cerf, and A. S. Holevo, arXiv:1312.6225 [Nat. Photonics (to be published)].
[20] A. Mari, V. Giovannetti, and A. S. Holevo, Nat. Commun. **5**, 3826 (2014).
[21] Note that the sum can be over a continuous parameter, in which case it must be interpreted as an integral.
[22] By applying the Koashi-Winter relation [23] to the pure state Φ_{ABE}, we may write $S_{\min}(A|B) = \mathcal{F}(A,E)$, where $\mathcal{F}(A,E)$ is the entanglement of formation of the two-mode Gaussian state $\rho_{AE} = \mathrm{Tr}_B(\Phi_{ABE})$. If $\rho_{AE} = \rho_{EA}$, then $\mathcal{F}(A,E)$ can easily be computed as Gaussian entanglement of formation [24] and this calculation confirms that $S_{\min}(A|B)$ can be achieved by Gaussian POVMs.
[23] M. Koashi and A. Winter, Phys. Rev. A **69**, 022309 (2004).
[24] M. M. Wolf, G. Giedke, O. Kruger, R. F. Werner, and J. I. Cirac, Phys. Rev. A **69**, 052320 (2004).
[25] S. Pirandola, A. Serafini, and S. Lloyd, Phys. Rev. A **79**, 052327 (2009).
[26] S. Pirandola, New J. Phys. **15**, 113046 (2013)
[27] Here we use $\hbar = 2$, so that the shot-noise variance of the vacuum is equal to one.
[28] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.113.140405, which includes Refs. [29–31], for the proof of the decomposition of two-mode squeezed thermal states, the parametrization of our general family of Gaussian states, and general notions on single-mode Gaussian channels and the remote preparation of Gaussian states.
[29] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 2008).
[30] J. Eisert and M. Plenio, Int. J. Quantum. Inform. **01**, 479 (2003).
[31] G. Giedke and J. I. Cirac, Phys. Rev. A **66**, 032316 (2002).
[32] Any single-mode Gaussian channel can be dilated into a Gaussian unitary involving the input mode i plus two environmental modes 1 and 2. Globally the transformation of the quadratures $\hat{\mathbf{x}}^T = (\hat{q}_i, \hat{p}_i, \hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2)$ is an affine map $\hat{\mathbf{x}} \to \hat{\mathbf{x}}' = \mathbf{S}\hat{\mathbf{x}} + \mathbf{D}$, where $\mathbf{S}$ is a symplectic matrix and $\mathbf{D}$ is a displacement vector associated with the channel. Now any displacement of the input mode $\hat{\mathbf{x}} \to \hat{\mathbf{x}} + \mathbf{d}$, with $\mathbf{d}^T = (d_q, d_p, 0, 0, 0, 0)$ will be mapped into a corresponding (different) displacement of the output mode $\hat{\mathbf{x}}' \to \hat{\mathbf{x}}' + \mathbf{S}\mathbf{d}$. Since entropy is invariant under unitaries, it is not affected by these output displacements and, therefore, by the input ones.
[33] Y. Huang, New J. Phys. **16**, 033027 (2014).
[34] A. S. Holevo, Probl. Inf. Transm. **43**, 1 (2007).
[35] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).