Quantum Fidelity for Arbitrary Gaussian States

Leonardo Banchi,[1] Samuel L. Braunstein,[2] and Stefano Pirandola[2]
[1]Department of Physics and Astronomy, University College London, Gower Street, London WC1E 6BT, United Kingdom
[2]Computer Science and York Centre for Quantum Technologies, University of York, York YO10 5GH, United Kingdom
(Received 9 July 2015; published 22 December 2015)

We derive a computable analytical formula for the quantum fidelity between two arbitrary multimode Gaussian states which is simply expressed in terms of their first- and second-order statistical moments. We also show how such a formula can be written in terms of symplectic invariants and used to derive closed forms for a variety of basic quantities and tools, such as the Bures metric, the quantum Fisher information, and various fidelity-based bounds. Our result can be used to extend the study of continuous-variable protocols, such as quantum teleportation and cloning, beyond the current one-mode or two-mode analyses, and paves the way to solve general problems in quantum metrology and quantum hypothesis testing with arbitrary multimode Gaussian resources.

DOI: 10.1103/PhysRevLett.115.260501 PACS numbers: 03.67.Mn, 03.65.-w, 03.67.Hk, 42.50.-p

The quantification of the similarity between two quantum states is a crucial issue in quantum information theory [1–4] and, more generally, in the entire field of quantum physics [5]. Among the various notions, that of quantum fidelity [6–8] is perhaps the most well known for its use as a quantifier of performance in a variety of quantum protocols. Quantum fidelity is the standard tool for assessing the success of quantum teleportation [9–13], where an unknown state is destroyed in one location and reconstructed in another (see Ref. [14] for a recent review). In quantum cloning [15–19], where an unknown state is transformed into two or more (imperfect) clones, quantum fidelity is the basic tool for quantifying the performance of a quantum cloning machine. Quantum fidelity plays a central role in quantum metrology [20,21], where the goal is to find the optimal strategy for estimating a classical parameter encoded in a quantum state. Similarly, it is important in quantum hypothesis testing [22–24], where the aim is to optimize the discrimination of quantum hypotheses (states or channels).

An important setting for all of the above tasks is that of continuous-variable systems [3,4], which are quantum systems with infinite-dimensional Hilbert spaces, such as the bosonic modes of the electromagnetic field, described by position and momentum quadrature operators. For these systems, the quantum states with a Gaussian Wigner function, so-called Gaussian states [3], are the most typical in theoretical studies and experimental implementations, so quantifying their similarity is of paramount importance. The derivation of a simple formula for the quantum fidelity between two arbitrary bosonic Gaussian states is a long-standing open problem with a number of partial solutions accumulated over the years. We currently know the solutions for one mode [25–28] and two modes [29–31]. A simple formula for multimode Gaussian states is only known in specific cases, namely, when one of the two states is pure [29,32], or for two thermal states [33].

Here, we solve this long-standing problem by deriving a computable formula for the quantum fidelity between two arbitrary multimode Gaussian states, which is simply expressed in terms of their first- and second-order statistical moments. A key step for this derivation relies in proving an exponential Gibbs-like representation for the Gaussian states, extending a result known in the fermionic case [34]. This representation allows us to simplify many calculations involving products and powers of Gaussian states. We also provide a recipe for expressing the quantum fidelity in terms of symplectic invariants, showing specific examples with one, two, and three modes. The new formula for the fidelity allows us to easily derive the Bures metric for Gaussian states, therefore generalizing quantum metrology to multimode Gaussian resources. Similarly, we discuss how quantum hypothesis testing can be extended beyond two-mode Gaussian states.

Preliminary tools.—Consider n bosonic modes described by quadrature operators $Q=(x_1,\ldots,x_n,p_1,\ldots,p_n)^T$, satisfying the canonical commutation relations [35]

$$[Q_k,Q_l]=i\Omega_{kl},\qquad \Omega:=\begin{pmatrix}0&1\\-1&0\end{pmatrix}\otimes\mathbb{1},\tag{1}$$

where $\mathbb{1}$ is the $n\times n$ identity matrix. The coordinate transformations $Q'=SQ$ which preserve the above commutation relations form the symplectic group, i.e., the group of real matrices such that $S\Omega S^T=\Omega$ [36].

Let us denote by ρ an unnormalized density operator of the n bosonic modes. Its normalized version is here denoted by $\hat\rho=\rho/Z_\rho$, with $Z_\rho=\mathrm{Tr}\rho$ being the normalization factor. For a Gaussian state [3], the density operator $\hat\rho$ has a one-to-one correspondence with the first- and second-order statistical moments of the state. These are the mean value $u:=\langle Q\rangle_{\hat\rho}=\mathrm{Tr}(Q\hat\rho)\in\mathbb{R}^{2n}$ and the covariance matrix (CM) V, with generic element

$$V_{kl} = \frac{1}{2}\langle\{Q_k - u_k, Q_l - u_l\}\rangle_{\hat{\rho}}, \tag{2}$$

where $\{,\}$ is the anticommutator. Equivalently, we may use the following modified version of the CM:

$$W := -2Vi\Omega. \tag{3}$$

According to Williamson's theorem, there exists a symplectic matrix S such that [3]

$$V = S(D \oplus D)S^T, D = \mathrm{diag}(v_1, \ldots, v_n), \tag{4}$$

where the symplectic eigenvalues satisfy $v_k \geq 1/2$. Correspondingly, the matrix W transforms as SWS^{-1} and its standard eigenvalues are $\pm w_k$, where $w_k = 2v_k \geq 1$. Note that standard matrix functions do not preserve the symplectic structure of Eq. (4). In view of this, given any real function $f: \mathbb{R} \to \mathbb{R}$, we define the symplectic action [32] f_* on V as

$$f_*(V) = S[f(D) \oplus f(D)]S^T,$$
$$f(D) = \mathrm{diag}[f(v_1), \ldots, f(v_n)]. \tag{5}$$

The symplectic action is a basic tool which enables us to extend relations from diagonal to completely arbitrary CMs. Furthermore, we prove in the Supplemental Material [37] that this operation can be reduced to a standard matrix function when f is an odd function, in which case we can write $f_*(V) = f(Vi\Omega)i\Omega$. Remarkably, this reduction allows us to remove any residual symplectic matrix or symplectic decomposition [3] from our final formulas.

As a first main result, we show in the Supplemental Material [37] that an arbitrary multimode Gaussian state, with mean u and CM V, can be written in the following Gibbs-exponential form:

$$\rho = \exp\left[-\frac{1}{2}(Q-u)^T G (Q-u)\right], \tag{6}$$

with normalization factor

$$Z_\rho = \det\left(V + \frac{i\Omega}{2}\right)^{1/2}. \tag{7}$$

In Eq. (6) the Gibbs matrix G is simply related to the CM by

$$G = 2i\Omega \coth^{-1}(2Vi\Omega), \qquad V = \frac{1}{2}\coth\left(\frac{i\Omega G}{2}\right)i\Omega. \tag{8}$$

Note that this is the simplest exponential form derived so far for Gaussian states. It is directly expressed in terms of the first- and second-order moments of the quadratures, without the need of performing any symplectic decomposition. *Proof sketch.*—We first note that Eq. (6) is true for thermal states (diagonal CM $D \oplus D$), for which $G = g(D) \oplus g(D)$ and $g(v) = 2\coth^{-1}(2v)$. Then, by imposing that the exponential of Eq. (6) is invariant under coordinate transformations, we find that V and $\Omega G \Omega$ transform in the same way under symplectic transformations. This property allows us to apply the symplectic action g_* and write $\Omega G \Omega = -g_*(V)$. Finally, using the fact that g is an odd function, we derive the matrix relations in Eq. (8). See the Supplemental Material [37] for a detailed proof. ■

Using Eq. (3) we may also write the equivalent relations

$$e^{i\Omega G} = \frac{W - \mathbb{1}}{W + \mathbb{1}}, \qquad W = \frac{\mathbb{1} + e^{i\Omega G}}{\mathbb{1} - e^{i\Omega G}}, \tag{9}$$

where we use the notation $A/B := AB^{-1}$ when A and B commute. Note that, although the matrix G is singular for pure states (so one has to deal carefully with this limit), the introduction of the representation in Eq. (6) significantly simplifies the calculations, and all of the final formulas are valid in general, i.e., for both mixed and pure states.

Fidelity for multimode Gaussian states.—The quantum fidelity between two arbitrary quantum states, $\hat{\rho}_1 = \rho_1/Z_{\rho_1}$ and $\hat{\rho}_2 = \rho_2/Z_{\rho_2}$, is given by

$$\mathcal{F}(\hat{\rho}_1, \hat{\rho}_2) := \mathrm{Tr}\left(\sqrt{\sqrt{\hat{\rho}_1}\hat{\rho}_2\sqrt{\hat{\rho}_1}}\right) = \frac{Z_{\sqrt{\rho_{\mathrm{tot}}}}}{\sqrt{Z_{\rho_1} Z_{\rho_2}}}, \tag{10}$$

where $\rho_{\mathrm{tot}} := \sqrt{\rho_1}\rho_2\sqrt{\rho_1}$. Here, we consider two arbitrary multimode Gaussian states: $\hat{\rho}_1$, with mean u_1 and CM V_1, and $\hat{\rho}_2$, with mean u_2 and CM V_2. Their Gibbs matrices G_1 and G_2 are readily obtained from Eq. (8). The advantage of using the Gibbs-exponential representation of Eq. (6) is twofold in our calculations: First, it makes the evaluation of the operator square root in Eq. (10) straightforward; second, it allows us to use the algebra of quadratic operators [40] to find ρ_{tot} in closed form.

Thus, we are able to show in the Supplemental Material [37] that the quantum fidelity between two arbitrary Gaussian states can be directly expressed in terms of $\delta_u := u_2 - u_1$ and their CMs, V_1 and V_2, according to the decomposition

$$\mathcal{F}(\hat{\rho}_1, \hat{\rho}_2) = \mathcal{F}_0(V_1, V_2)\exp\left[-\frac{1}{4}\delta_u^T (V_1 + V_2)^{-1}\delta_u\right], \tag{11}$$

where $\mathcal{F}_0(V_1, V_2)$ has a closed analytical form in terms of V_1 and V_2. Having a simple and handy expression for $\mathcal{F}_0(V_1, V_2)$ has been a major open problem for many years, with partial solutions only known for one- and two-mode cases, or in the very specific case of thermal states. Here, we show that, for two arbitrary Gaussian states, the term $\mathcal{F}_0(V_1, V_2)$ can be easily computed from one of the auxiliary matrices,

$$V_{\mathrm{aux}} := \Omega^T (V_1 + V_2)^{-1}\left(\frac{\Omega}{4} + V_2 \Omega V_1\right), \tag{12}$$

$$W_{\mathrm{aux}} := -2V_{\mathrm{aux}} i\Omega = -(W_1 + W_2)^{-1}(\mathbb{1} + W_2 W_1). \tag{13}$$

More precisely, we find [37]

$$\mathcal{F}_0(V_1, V_2) = \frac{F_{\mathrm{tot}}}{\sqrt[4]{\det(V_1 + V_2)}}, \tag{14}$$

$$F_{\rm tot}^4 = \det\left[2\left(\sqrt{\mathbb{1}+\frac{(V_{\rm aux}\Omega)^{-2}}{4}}+\mathbb{1}\right)V_{\rm aux}\right] \quad (15)$$

$$= \det\left[\left(\sqrt{\mathbb{1}-W_{\rm aux}^{-2}}+\mathbb{1}\right)W_{\rm aux}i\Omega\right]. \quad (16)$$

Proof sketch.—The proof can be broken down into four main steps. (i) First of all, by exploiting the closed algebra spanned by quadratic operators in Q, we show that $\rho_{\rm tot}=\sqrt{\rho_1}\rho_2\sqrt{\rho_1}$ has the Gibbs form $\rho_{\rm tot}=\exp[-(Q-u_{\rm tot})^T\times G_{\rm tot}(Q-u_{\rm tot})/2+K_{\rm tot}]$, where $G_{\rm tot}$ satisfies $e^{-i\Omega G_{\rm tot}}=e^{-i\Omega G_1/2}e^{-i\Omega G_2}e^{-i\Omega G_1/2}$, while $u_{\rm tot}$ and $K_{\rm tot}$ depend on G_1, G_2, u_1, and u_2. (ii) For $k=1$, 2, let us call ρ_{G_k} the Gaussian state ρ_k with the same Gibbs matrix G_k but zero mean. We easily find that $Z_{\rho_k}=Z_{\rho_{G_k}}$. As a consequence, Eq. (10) becomes $\mathcal{F}=\mathcal{F}_0e^{K_{\rm tot}/2}$, where $\mathcal{F}_0=Z_{\sqrt{\rho_{G_{\rm tot}}}}(Z_{\rho_{G_1}}Z_{\rho_{G_2}})^{-1/2}$ and $\rho_{G_{\rm tot}}$ is the zero-mean version of $\rho_{\rm tot}$. After simple algebra, we derive $K_{\rm tot}=\log[Z_{\rho_1\rho_2}/Z_{\rho_{G_1}\rho_{G_2}}]=-\delta_u^T(V_1+V_2)^{-1}\delta_u/2$, yielding the decomposition in Eq. (11). (iii) The further decomposition in Eq. (14) follows from the application of Eq. (7) to $\mathcal{F}_0$. This provides $\mathcal{F}_0=[\det(V_1+V_2)]^{-1/4}F_{\rm tot}$, where $F_{\rm tot}^4=\det[(\sqrt{\mathbb{1}-W_{\rm tot}^{-2}}+\mathbb{1})W_{\rm tot}i\Omega]$ and $W_{\rm tot}=-2V_{\rm tot}i\Omega$ is the modified CM of $\rho_{G_{\rm tot}}$. This CM is still rather complicated. (iv) The most challenging part is indeed the simplification of the residual term $F_{\rm tot}$. Here, we first simplify $W_{\rm tot}$ by means of algebraic manipulations (e.g., using the Woodbury identity); then we compute the similar matrix $W_{\rm aux}=MW_{\rm tot}M^{-1}$ for a suitable invertible M, obtaining Eq. (13). The auxiliary matrix $W_{\rm aux}$ can now replace $W_{\rm tot}$ in $F_{\rm tot}^4$ since the determinant of a matrix function is invariant under similarity transformations. The final result of Eq. (16) is also confirmed by an alternate approach, where we simplify $F_{\rm tot}^4$ using the Gibbs matrices. Finally, we explicitly check to see that all of the quantities are well defined in the singular limit where the symplectic spectra contain vacuum contributions, as is the case for pure states. See the Supplemental Material [37] for a detailed proof. ■

Note that the asymmetry of $V_{\rm aux}$ and $W_{\rm aux}$ upon exchanging the two states is only apparent and comes from the apparent asymmetry in the definition of Eq. (10). One can check that the eigenvalues of $V_{\rm aux}$ and $W_{\rm aux}$, and thus the determinants in Eqs. (15) and (16), are invariant under exchange.

We remark that the formula of Eq. (11) is valid for arbitrary (generally mixed) multimode Gaussian states with arbitrary first- and second-order moments, and it does not involve any symplectic decomposition of the CMs. In the specific case where one of the states is pure (say, ρ_1), we have $V_1=\mathbb{1}/2$, which implies that $V_{\rm aux}=\mathbb{1}/2$ and $F_{\rm tot}=1$, therefore recovering the result of Ref. [32] (and, in different notation, Ref. [41]).

Fidelity in terms of symplectic invariants.—The fidelity can be expressed in terms of symplectic invariants associated with the second-order moments of the Gaussian states. Consider the notation with the W matrices, so that $F_{\rm tot}$ is given by Eq. (16). The standard eigenvalues of $W_{\rm aux}$ are $\pm w_k^{\rm aux}$, where $w_k^{\rm aux}\geq 1$ [42]. As a consequence, we may write

$$F_{\rm tot}=\prod_{k=1}^{n}\left[w_k^{\rm aux}+\sqrt{(w_k^{\rm aux})^2-1}\right]^{1/2}. \quad (17)$$

Thus, the problem reduces to finding the eigenvalues of $W_{\rm aux}$.

For this, let us consider the characteristic polynomial

$$\chi(\lambda)=\det(\lambda\mathbb{1}-W_{\rm aux}), \quad (18)$$

which is clearly a symplectic invariant since $W_{\rm aux}$ transforms as $SW_{\rm aux}S^{-1}$ under symplectic transformations. Using the identity $\det e^X=e^{{\rm Tr}X}$ and the Cayley-Hamilton theorem [43], we may write $\chi(\lambda)$ as a polynomial function of

$$I_{2k}={\rm Tr}(W_{\rm aux}^{2k}),\quad \text{for } k=1,\ldots,n, \quad (19)$$

which are also symplectic invariants with $I_k>I_j$ for $k>j$. Thus, for n modes, we can compute the n invariants I_{2k} and subsequently solve the polynomial equation $\chi(\lambda)=0$, whose roots are the eigenvalues $w_k^{\rm aux}$ to be used in Eq. (17).

Note that the invariants I_{2k} can be connected with other invariants. For instance, one can easily check to see that

$$\chi(0)=(-1)^n\frac{\Gamma}{\Delta},\qquad \chi(1)=(-1)^n\frac{\Lambda}{\Delta}, \quad (20)$$

where $\Delta:=\det(V_1+V_2)$, $\Gamma:=2^{2n}\det(\Omega V_1\Omega V_2-\mathbb{1}/4)$, and

$$\Lambda:=2^{2n}\det(V_1+i\Omega/2)\det(V_2+i\Omega/2) \quad (21)$$

are the invariants considered by Ref. [29]. Using Eq. (20), one can easily express I_2 and I_4 in terms of Γ, Λ, and Δ.

Examples.—Let us consider some examples with the $n=1$, 2, and 3 modes. For single-mode Gaussian states, we derive $\chi(\lambda)=\lambda^2-I_2/2$, so that $w^{\rm aux}=\sqrt{I_2/2}$. Equivalently, we may compute $I_2/2=1+\Lambda/\Delta$ so that we retrieve the known result [26–28]

$$\mathcal{F}_0^2(V_1,V_2)=\frac{1}{\sqrt{\Delta+\Lambda}-\sqrt{\Lambda}}. \quad (22)$$

For two-mode Gaussian states, we derive $\chi(\lambda)=(I_2^2-2I_4-4I_2\lambda^2+8\lambda^4)/8$ with the solutions

$$w_\pm^{\rm aux}=\frac{1}{2}\sqrt{I_2\pm\sqrt{4I_4-I_2^2}}. \quad (23)$$

Once plugged into Eq. (17), we have the fidelity in terms of I_2 and I_4. The latter invariants can then be expressed in terms of Γ/Δ and Λ/Δ, so that we retrieve the known result [29]

$$\mathcal{F}_0^2(V_1,V_2)=\frac{1}{\sqrt{\Gamma}+\sqrt{\Lambda}-\sqrt{(\sqrt{\Gamma}+\sqrt{\Lambda})^2-\Delta}}. \quad (24)$$

For three-mode Gaussian states, the characteristic polynomial may be written as $\chi=t^3+pt+q$, where

$$t=\lambda^2-I_2/6, \qquad p=\frac{I_2^2}{24}-\frac{I_4}{4},$$
$$q=-\frac{I_2^3}{108}+\frac{I_2I_4}{12}-\frac{I_6}{6}. \quad (25)$$

The solutions of the characteristic equation $\chi=0$ are real [37] and are given by

$$w_k^{\mathrm{aux}}=\sqrt{\frac{I_2}{6}+2\sqrt{-\frac{p}{3}}\cos\left[\frac{\theta-2\pi(k-1)}{3}\right]}, \quad (26)$$

where $\theta{:=}\arccos[3\sqrt{3}q(2p\sqrt{-p})^{-1}]$ and $k=1, 2, 3$ (in particular, note that $w_k^{\mathrm{aux}}=\sqrt{I_2/6}$ for $p=0$). To the best of our knowledge, Eqs. (25) and (26), together with Eqs. (11) and (17), provide the first expression for the quantum fidelity between two arbitrary three-mode Gaussian states. Such an expression can be readily exploited to compute the fidelity of recovery [44] for three bosonic modes.

Implications: Geometry of Gaussian states.—Once the quantum fidelity is expressed in terms of the first two statistical moments, we can easily compute the Bures distance between two arbitrary multimode Gaussian states, $\hat{\rho}_1$ and $\hat{\rho}_2$, which is given by

$$D_B(\hat{\rho}_1,\hat{\rho}_2)=2[1-\mathcal{F}(\hat{\rho}_1,\hat{\rho}_2)]. \quad (27)$$

From this expression we can derive the Bures metric by expanding the fidelity. Consider two infinitesimally close Gaussian states $\hat{\rho}_1=\hat{\rho}$, with statistical moments u and V, and $\hat{\rho}_2=\hat{\rho}+d\hat{\rho}$, with statistical moments $u+du$ and $V+dV$. The Bures metric is computed by using Eq. (11) in Eq. (27) and expanding to the second order in du and dV. The zeroth and first-order terms clearly vanish since $\mathcal{F}$ has a maximum for $d\hat{\rho}\to 0$, where $\mathcal{F}=1$. Thus, we find [37]

$$ds^2=2[1-\mathcal{F}(\hat{\rho},\hat{\rho}+d\hat{\rho})]=\frac{du^TV^{-1}du}{4}+\frac{\delta}{8}, \quad (28)$$

where $\delta{:=}4\mathrm{Tr}[dV(4\mathcal{L}_V+\mathcal{L}_\Omega)^{-1}dV]$, $\mathcal{L}_AX{:=}AXA$, and the inverse of the superoperator $4\mathcal{L}_V+\mathcal{L}_\Omega$ refers to the pseudoinverse [43]. Note that a result equivalent to Eq. (28) has been derived in Ref. [45] using a different method based on the computation of the symmetric logarithmic derivative (SLD). Our explicit expressions in Eqs. (11)–(16) allow us to avoid the evaluation of the SLD, which is notably difficult, and to obtain Eq. (28) directly from second-order perturbation theory.

Numerically, the easiest way of evaluating the inverse of the superoperator in δ is using the W matrices and performing the calculations in the basis in which W is diagonal. Indeed, in this basis where $W=\mathrm{diag}(w_i)$, one finds

$$\delta=\sum_{ij}\frac{dW_{ij}dW_{ji}}{w_iw_j-1}, \quad (29)$$

and the sum is taken over the elements such that $w_iw_j\neq 1$. For pure states, we simply have $\delta_{\mathrm{pure}}=\mathrm{Tr}(V^{-1}dVV^{-1}dV)$.

Implications: Multimode quantum metrology.—Let us consider a real parameter θ which is encoded in a multimode Gaussian state $\hat{\rho}_\theta$. To estimate θ with high precision, it is necessary to distinguish the two infinitesimally close states $\hat{\rho}_\theta$ and $\hat{\rho}_{\theta+d\theta}$ for an infinitesimal change $d\theta$. Assume that N copies of the state $\hat{\rho}_\theta$ are available to an observer, who performs N independent measurements to obtain an unbiased estimator $\tilde{\theta}$ for parameter θ. Then, the mean-square error affecting the parameter estimation $\mathrm{Var}(\theta){:=}\langle(\tilde{\theta}-\theta)^2\rangle$ satisfies the quantum Cramer-Rao (QCR) bound $\mathrm{Var}(\theta)\geq[NH(\theta)]^{-1}$, where $H(\theta)$ is the quantum Fisher information (QFI) [20]. The latter can be computed from the fidelity as

$$H(\theta)=\frac{8[1-\mathcal{F}(\hat{\rho}_\theta,\hat{\rho}_{\theta+d\theta})]}{d\theta^2}. \quad (30)$$

Thus, for any parametrization of the Gaussian states, we can easily compute the fidelity $\mathcal{F}(\hat{\rho}_\theta,\hat{\rho}_{\theta+d\theta})$ using Eq. (11) and, therefore, the QFI in Eq. (30).

More generally, suppose that the Gaussian state is labeled by a vectorial parameter with m real components, i.e., $\theta=\{\theta_i\}$ for $i=1,\ldots,m$. In this case, the performance of the parameter estimation is expressed by the classical covariance matrix $\mathrm{Cov}_{ij}(\theta){:=}\langle\tilde{\theta}_i\tilde{\theta}_j\rangle-\langle\tilde{\theta}_i\rangle\langle\tilde{\theta}_j\rangle$, which satisfies the matrix version of the QCR bound [21,46,47] $\mathrm{Cov}(\theta)\geq[NH(\theta)]^{-1}$. Here, the QFI is a matrix with elements $H_{ij}(\theta)$, which can be evaluated from the Bures metric. In fact, for any parametrization, we may write Eq. (28) as $ds^2=g_{ij}(\theta)d\theta_id\theta_j$ and show that $H_{ij}(\theta)=4g_{ij}(\theta)$.

Implications: Multimode quantum hypothesis testing.—An efficient computation of the quantum fidelity is important to extend binary quantum hypothesis testing [22–24] to considering multimode Gaussian states. In turn, this would allow one to extend a variety of quantum sensing protocols, such as quantum illumination [48–50] and quantum reading [51–56].

Consider N copies of two multimode Gaussian states, $\hat{\rho}_1^{\otimes N}$ and $\hat{\rho}_2^{\otimes N}$, with the same *a priori* probability. The minimum error probability $p_{\mathrm{err}}(N)$ in their statistical discrimination is provided by the Helstrom bound [24], which is typically hard to compute for mixed states. For this reason, one resorts to other computable bounds, such as the quantum Chernoff bound [57–59] or fidelity-based bounds [59–61]. Thanks to our result, the latter are now the simplest to compute.

For any number of copies N, we may write

$$\frac{1-\sqrt{1-[\mathcal{F}(\hat{\rho}_1,\hat{\rho}_2)]^{2N}}}{2} \le p_{\mathrm{err}}(N) \le \frac{[\mathcal{F}(\hat{\rho}_1,\hat{\rho}_2)]^N}{2}. \quad (31)$$

In particular, the lower bound in Eq. (31) is the tightest known. Note that Eq. (31) can be derived by using the known result for a single copy ($N=1$) [60] and then applying the multiplicative property of the fidelity under tensor products of density operators, so that $\mathcal{F}(\hat{\rho}_1^{\otimes N},\hat{\rho}_2^{\otimes N}) = \mathcal{F}(\hat{\rho}_1,\hat{\rho}_2)^N$.

The computation of the quantum fidelity is also important for asymmetric quantum hypothesis testing where the two quantum hypotheses have unbalanced Bayesian costs [62]. In this context, the quantum fidelity can be used to estimate the quantum Hoeffding bound [63] which quantifies the optimal error exponent associated with the rate of false negatives.

Conclusions.—In this Letter we have solved a long-standing open problem in continuous-variable quantum information by deriving a simple computable formula for the quantum fidelity between two arbitrary multimode Gaussian states. Our main formula is expressed in terms of the statistical moments of the Gaussian states, but another formulation is also given in terms of suitable symplectic invariants. By using our formula, one can extend the study of quantum teleportation, cloning, quantum metrology, and hypothesis testing well beyond the standard case of two-mode Gaussian states to consider multimode Gaussian resources, with unexplored implications for all of these basic quantum information protocols.

L. B. is currently supported by the European Research Council under the European Union's Seventh Framework Programme (FP/2007–2013)/ERC Grant Agreement No. 308253. S. P. has been supported by the Leverhulme Trust (the "qBIO" fellowship) and EPSRC via "qDATA" (Grant No. EP/L011298/1) and the UK Quantum Communications Hub (Grant No. EP/M013472/1).

[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] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[4] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[5] J. J. Sakurai and J. Napolitano, *Modern Quantum Mechanics*, 2nd ed. (Addison-Wesley, San Francisco, 2011).
[6] Note that there are two definitions of quantum fidelity in the literature. One is the square-root or Bures fidelity $\mathcal{F}$, which is given by Eq. (10). The other is the Uhlmann-Jozsa fidelity, which is the square of the previous one, i.e., $\mathcal{F}_{\mathrm{U-J}} = \mathcal{F}^2$. Bures fidelity is the direct generalization of the classical fidelity. In fact, if two density operators commute, we can write $\rho = \sum_k p_k|k\rangle\langle k|$ and $\sigma = \sum_k q_k|k\rangle\langle k|$ for an orthonormal basis $\{|k\rangle\}$. Then, we have $F_B(\rho,\sigma) = \sum_k \sqrt{p_k q_k}$, which is the classical fidelity $F(p_k, q_k)$ between the two probability distributions p_k and q_k.
[7] A. Uhlmann, Rep. Math. Phys. **9**, 273 (1976).
[8] R. Jozsa, J. Mod. Opt. **41**, 2315 (1994).
[9] C. H. Bennett, G. Brassard, C. Crépard, R. Jozsa, A. Peres, and W. K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[10] D. Bouwmeester, J.-Wei Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, Nature (London) **390**, 575 (1997).
[11] S. L. Braunstein and H. J. Kimble, Phys. Rev. Lett. **80**, 869 (1998).
[12] A. Furusawa *et al.*, Science **282**, 706 (1998).
[13] S. Pirandola and S. Mancini, Laser Phys. **16**, 1418 (2006).
[14] S. Pirandola, J. Eisert, C. Weedbrook, A. Furusawa, and S. L. Braunstein, Nat. Photonics **9**, 641 (2015).
[15] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[16] G. Lindblad, J. Phys. A **33**, 5059 (2000).
[17] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000).
[18] S. L. Braunstein, N. J. Cerf, S. Iblisdir, P. van Loock, and S. Massar, Phys. Rev. Lett. **86**, 4938 (2001).
[19] J. Fiurášek, Phys. Rev. Lett. **86**, 4942 (2001).
[20] S. L. Braunstein and C. M. Caves, Phys. Rev. Lett. **72**, 3439 (1994).
[21] M. G. A. Paris, Int. J. Quantum. Inform. **07**, 125 (2009).
[22] A. Chefles, Contemp. Phys. **41**, 401 (2000).
[23] S. M. Barnett and S. Croke, Adv. Opt. Photonics **1**, 238 (2009).
[24] C. W. Helstrom, *Quantum Detection and Estimation Theory*, Mathematics in Science and Engineering Vol. 123 (Academic Press, New York, 1976).
[25] J. Twamley, J. Phys. A **29**, 3723 (1996).
[26] H. Nha and H. J. Carmichael, Phys. Rev. A **71**, 032336 (2005).
[27] S. Olivares, M. G. A. Paris, and U. L. Andersen, Phys. Rev. A **73**, 062330 (2006).
[28] H. Scutaru, J. Phys. A **31**, 3659 (1998).
[29] P. Marian and T. A. Marian, Phys. Rev. A **86**, 022340 (2012).
[30] P. Marian, T. A. Marian, and H. Scutaru, Phys. Rev. A **68**, 062309 (2003).
[31] P. Marian and T. A. Marian, Phys. Rev. A **77**, 062319 (2008).
[32] G. Spedalieri, C. Weedbrook, and S. Pirandola, J. Phys. A **46**, 025304 (2013).
[33] Gh.-S. Părăoanu and H. Scutaru, Phys. Rev. A **61**, 022306 (2000).
[34] L. Banchi, P. Giorda, and P. Zanardi, Phys. Rev. E **89**, 022102 (2014).
[35] Arvind, B. Dutta, N. Mukunda, and R. Simon, Pramana J. Phys. **45**, 471 (1995).
[36] Note that S symplectic implies that $\det S = +1$, and also that S^T and $S^{-1} = -\Omega S^T \Omega$ are symplectic.
[37] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.115.260501, which includes Refs. [38,39]. In the various supplementary sections, we provide the following technical details. Section I: Proof

of the Gibbs-exponential form for bosonic Gaussian states; in particular, Sec. I A contains the computation of the symplectic action for odd functions. Section II: Computations with Gaussian states. Section III: Proof of the main formula for the quantum fidelity. Section IV: Proof that the solutions for the three-mode case are real. Section V: Derivation of the Bures metric.

[38] T. Kato, *Perturbation Theory for Linear Operators* (Springer-Verlag, Berlin, 1995).

[39] R. Meenakshi and C. Rajian, Linear Algebra Appl. **295**, 3 (1999).

[40] R. Balian and E. Brezin, Nuovo Cimento B **64**, 37 (1969).

[41] Reference [32] uses $[Q, Q^T] = 2i\Omega$, so that the vacuum CM is $\mathbb{1}$.

[42] In fact, $W_{\rm aux}$ is equal to $W_{\rm tot}$ of the total state $\rho_{\rm tot}$ up to a similarity transformation. This means that $W_{\rm aux}$ and $W_{\rm tot}$ have the same spectrum of eigenvalues. In turn, we know that the eigenvalues of $W_{\rm tot}$ are $\pm w_k^{\rm tot}$, where $w_k^{\rm tot} = 2\nu_k^{\rm tot}$ and $\{\nu_k^{\rm tot}\}$ is the symplectic spectrum of $\rho_{\rm tot}$. Thus, we have it that the eigenvalues of $W_{\rm aux}$ are $\pm w_k^{\rm aux}$, with $w_k^{\rm aux} = 2\nu_k^{\rm tot} \geq 1$.

[43] R. Piziak and P. L. Odell, *Matrix Theory: From Generalized Inverses to Jordan Form* (CRC Press, Boca Raton, FL, 2007).

[44] K. P. Seshadreesan and M. M. Wilde, Phys. Rev. A **92**, 042321 (2015).

[45] A. Monras, arXiv:1303.3682.

[46] I. Bengtsson and K. Zyczkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement* (Cambridge University Press, Cambridge, England, 2006).

[47] Contrary to the single-parameter bound, the multiparameter version is not necessarily achievable.

[48] S.-H. Tan, B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, and J. H. Shapiro, Phys. Rev. Lett. **101**, 253601 (2008).

[49] S. Lloyd, Science **321**, 1463 (2008).

[50] S. Barzanjeh, S. Guha, C. Weedbrook, D. Vitali, J. H. Shapiro, and S. Pirandola, Phys. Rev. Lett. **114**, 080503 (2015).

[51] S. Pirandola, Phys. Rev. Lett. **106**, 090504 (2011).

[52] R. Nair, Phys. Rev. A **84**, 032312 (2011).

[53] O. Hirota, arXiv:1108.4163.

[54] A. Bisio, M. Dall'Arno, and G. M. D'Ariano, Phys. Rev. A **84**, 012310 (2011).

[55] M. Dall'Arno, A. Bisio, G. M. D'Ariano, M. Miková, M. Ježek, and M. Dušek, Phys. Rev. A **85**, 012308 (2012).

[56] G. Spedalieri, C. Lupo, S. Mancini, S. L. Braunstein, and S. Pirandola, Phys. Rev. A **86**, 012315 (2012).

[57] K. M. R. Audenaert, J. Calsamiglia, R. Muñoz-Tapia, E. Bagan, Ll. Masanes, A. Acin, and F. Verstraete, Phys. Rev. Lett. **98**, 160501 (2007).

[58] J. Calsamiglia, R. Muñoz-Tapia, Ll. Masanes, A. Acin, and E. Bagan, Phys. Rev. A **77**, 032311 (2008).

[59] S. Pirandola and S. Lloyd, Phys. Rev. A **78**, 012331 (2008).

[60] C. A. Fuchs and J. V. de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).

[61] C. Fuchs, Ph.D. thesis, University of New Mexico, 1995.

[62] K. M. R. Audenaert, M. Nussbaum, A. Szkola, and F. Verstraete, Commun. Math. Phys. **279**, 251 (2008).

[63] G. Spedalieri and S. L. Braunstein, Phys. Rev. A **90**, 052307 (2014).