Computable bounds for the discrimination of Gaussian states

Stefano Pirandola[1] and Seth Lloyd[1,2]
[1]Research Laboratory of Electronics, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
[2]Department of Mechanical Engineering, Massachusetts Institute of Technology, Cambridge, Massachusetts 02139, USA
(Received 21 February 2008; published 17 July 2008)

By combining the Minkowski inequality and the quantum Chernoff bound, we derive easy-to-compute upper bounds for the error probability affecting the optimal discrimination of Gaussian states. In particular, these bounds are useful when the Gaussian states are unitarily inequivalent, i.e., they differ in their symplectic invariants.

DOI: 10.1103/PhysRevA.78.012331 PACS number(s): 03.67.Hk, 03.65.Ta, 02.10.Ud

I. INTRODUCTION

One of the central problems in statistical decision theory is the discrimination between two different probability distributions, intended as potential candidates for describing the values of a stochastic variable. In general, this statistical discrimination is affected by a minimal error probability $p^{(N)}$, which decreases with the number N of (independent) observations of the random variable. The general problem of determining $p^{(N)}$ was faced by Chernoff in 1952 [1]. Remarkably, he derived an upper bound, today known as the "Chernoff bound," having the nontrivial property of providing $p^{(N)}$ in the limit of infinite observations (i.e., for $N \to +\infty$). Very recently, a quantum version of this bound has been considered in Refs. [2,3]. Such a "quantum Chernoff bound" allows estimation of the minimal error probability $P^{(N)}$ which affects a corresponding quantum problem, known as *quantum state discrimination*. In this problem, a tester aims to distinguish between two possible quantum states of a system, supposing that N identical copies of the system are available for a generalized quantum measurement. The problem of quantum state discrimination is fundamental in several areas of quantum information (e.g., quantum cryptography [4]) and, in particular, for continuous-variable quantum information [5]. Continuous-variable (CV) systems are quantum systems with infinite-dimensional Hilbert spaces like, for instance, the bosonic modes of a radiation field. In particular, bosonic modes with Gaussian statistics, i.e., in *Gaussian states* [6], are today extremely important, thanks to their experimental accessibility and the relative simplicity of their mathematical description.

In the CV framework, the quantum discrimination of Gaussian states can be seen as a central task. Such a problem was first considered in Ref. [7], where a formula for the quantum Chernoff bound has already been derived. In our paper, we recast this formula by making explicit its dependence on the symplectic spectra of the involved Gaussian states. The computational difficulty of this formula relies on the fact that, besides the symplectic spectra (easy to compute), one must also calculate the symplectic transformations that diagonalize the corresponding correlation matrices. The derivation of these symplectic transformations can be in fact very hard, especially when many bosonic modes are involved in the process. In order to simplify this computational problem, here we resort to standard algebraic inequalities, i.e., the Minkowski and Young's inequalities. Thanks to these inequalities, we can manipulate the formula of the quantum Chernoff bound and derive much simpler upper bounds for the discrimination of Gaussian states. These bounds, which we call the *Minkowski* and *Young bounds*, are much easier to compute since they depend on the symplectic spectra only. Notice that, because of this simplification, these bounds are inevitably weaker than the quantum Chernoff bound. In particular, they are useful when the Gaussian states are *unitarily inequivalent*, i.e., not connected by any unitary transformation (e.g., displacement, rotation, or squeezing). On the one hand, this is surely a restriction for the general application of our results. On the other hand, inequivalent Gaussian states arise in many physical situations, and easy-to-compute upper bounds can represent the unique feasible solution when the number of modes is very high.

The structure of the paper is as follows. In Sec. II we review some of the basic notions about Gaussian states, with a special regard for their normal mode decomposition. In Sec. III we review the quantum Chernoff bound and reformulate the corresponding expression for Gaussian states. Section IV contains the central results of this paper. Here, we derive the computable bounds for discriminating Gaussian states by combining the quantum Chernoff bound with the Minkowski determinant inequality and the Young's inequality. We also provide a simple example in order to compare the various bounds. Section V gives the conclusions.

II. GAUSSIAN STATES IN A NUTSHELL

Let us consider a bosonic system of n modes. This quantum system is described by a tensor product Hilbert space $\mathcal{H}^{\otimes n}$ and a vector of quadrature operators $\hat{\mathbf{x}}^T := (\hat{q}_1, \hat{p}_1, \ldots, \hat{q}_n, \hat{p}_n)$ satisfying the commutation relations

$$[\hat{x}_l, \hat{x}_m] = 2i\Omega_{lm} \quad (1 \leq l, m \leq 2n), \tag{1}$$

where

$$\mathbf{\Omega} := \bigoplus_{k=1}^{n} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{2}$$

defines a symplectic form. An arbitrary state of the system is characterized by a density operator $\rho \in \mathcal{D}(\mathcal{H}^{\otimes n})$ or, equivalently, by a Wigner representation. In fact, by introduction of the Weyl operator [8]

$$\hat{D}(\boldsymbol{\xi}) := \exp(i\hat{\mathbf{x}}^T\boldsymbol{\xi}) \quad (\boldsymbol{\xi} \in \mathbb{R}^{2n}), \tag{3}$$

an arbitrary ρ is equivalent to a Wigner characteristic function

$$\chi(\boldsymbol{\xi}) := \mathrm{Tr}[\rho\hat{D}(\boldsymbol{\xi})], \tag{4}$$

or to a Wigner function

$$W(\mathbf{x}) := \int_{\mathbb{R}^{2n}} \frac{d^{2n}\boldsymbol{\xi}}{(2\pi)^{2n}} \exp(-i\mathbf{x}^T\boldsymbol{\xi})\chi(\boldsymbol{\xi}). \tag{5}$$

In Eq. (5) the continuous variables $\mathbf{x}^T := (q_1, p_1, \ldots, q_n, p_n)$ are the eigenvalues of $\hat{\mathbf{x}}^T$. They span the real symplectic space $\mathcal{K} := (\mathbb{R}^{2n}, \boldsymbol{\Omega})$ which is called the *phase space*.

By definition, a bosonic state ρ is called Gaussian if the corresponding Wigner representation (χ or W) is Gaussian, i.e.,

$$\chi(\boldsymbol{\xi}) = \exp\left[-\frac{1}{2}\boldsymbol{\xi}^T\mathbf{V}\boldsymbol{\xi} + i\bar{\mathbf{x}}^T\boldsymbol{\xi}\right], \tag{6}$$

$$W(\mathbf{x}) = \frac{\exp[-\frac{1}{2}(\mathbf{x}-\bar{\mathbf{x}})^T\mathbf{V}^{-1}(\mathbf{x}-\bar{\mathbf{x}})]}{(2\pi)^n\sqrt{\det \mathbf{V}}}. \tag{7}$$

In such a case, the state ρ is fully characterized by its displacement $\bar{\mathbf{x}} := \mathrm{Tr}(\hat{\mathbf{x}}\rho)$ and its correlation matrix (CM) $\mathbf{V}$, with entries

$$V_{lm} := \frac{1}{2}\mathrm{Tr}[\{\Delta\hat{x}_l, \Delta\hat{x}_m\}\rho], \tag{8}$$

where $\Delta\hat{x}_l := \hat{x}_l - \mathrm{Tr}(\hat{x}_l\rho)$ and $\{\ ,\ \}$ is the anticommutator. The CM is a $2n \times 2n$, real, and symmetric matrix which must satisfy the uncertainty principle

$$\mathbf{V} + i\boldsymbol{\Omega} \geq 0, \tag{9}$$

directly coming from Eq. (1) and implying $\mathbf{V} > 0$.

Fundamental properties of the Gaussian states can be easily expressed via the symplectic manipulation of their CM's. By definition, a matrix $\mathbf{S}$ is called *symplectic* when it preserves the symplectic form of Eq. (2), i.e.,

$$\mathbf{S}\boldsymbol{\Omega}\mathbf{S}^T = \boldsymbol{\Omega}. \tag{10}$$

Then, according to the Williamson theorem, for every CM $\mathbf{V}$ there exists a symplectic matrix $\mathbf{S}$ such that

$$\mathbf{V} = \mathbf{S}\begin{pmatrix} \nu_1 & & & & \\ & \nu_1 & & & \\ & & \ddots & & \\ & & & \nu_n & \\ & & & & \nu_n \end{pmatrix}\mathbf{S}^T = \mathbf{S}\left[\bigoplus_{k=1}^{n} \nu_k \mathbf{I}_k\right]\mathbf{S}^T, \tag{11}$$

where the set $\{\nu_1, \ldots, \nu_n\}$ is called the *symplectic spectrum* [9]. In particular, this spectrum satisfies

$$\prod_{k=1}^{n} \nu_k = \sqrt{\det \mathbf{V}}, \tag{12}$$

since $\det \mathbf{S} = 1$. By applying the symplectic diagonalization of Eq. (11) to Eq. (9), one can write the uncertainty principle in the simpler form [10]

$$\nu_k \geq 1 \quad \text{and} \quad \mathbf{V} > 0. \tag{13}$$

Normal mode decomposition of Gaussian states and its application to power states

An affine symplectic transformation

$$(\bar{\mathbf{x}}, \mathbf{S}): \mathbf{x} \to \mathbf{S}\mathbf{x} + \bar{\mathbf{x}} \tag{14}$$

acting on the phase space $\mathcal{K} := (\mathbb{R}^{2n}, \boldsymbol{\Omega})$ results in a simple congruence transformation $\mathbf{V} \to \mathbf{S}\mathbf{V}\mathbf{S}^T$ at the level of the CM. In the space of density operators $\mathcal{D}(\mathcal{H}^{\otimes n})$, the transformation of Eq. (14) corresponds instead to the transformation

$$\rho \to \hat{U}_{\bar{\mathbf{x}},\mathbf{S}}\rho\hat{U}_{\bar{\mathbf{x}},\mathbf{S}}^\dagger, \tag{15}$$

where the unitary $\hat{U}_{\bar{\mathbf{x}},\mathbf{S}} = \hat{D}(\bar{\mathbf{x}})\hat{U}_{\mathbf{S}}$ is determined by the affine pair $(\bar{\mathbf{x}}, \mathbf{S})$ and preserves the Gaussian character of the state (Gaussian unitary). As a consequence, the symplectic diagonalization of Eq. (11) corresponds to a *normal mode decomposition* of the Gaussian state

$$\rho = \hat{U}_{\bar{\mathbf{x}},\mathbf{S}}\left[\bigotimes_{k=1}^{n} \sigma(\nu_k)\right]\hat{U}_{\bar{\mathbf{x}},\mathbf{S}}^\dagger, \tag{16}$$

where

$$\sigma(\nu_k) := \frac{2}{\nu_k + 1}\sum_{j=0}^{\infty}\left(\frac{\nu_k - 1}{\nu_k + 1}\right)^j |j\rangle_k\langle j| \tag{17}$$

is a thermal state with mean photon number $\bar{n}_k = (\nu_k - 1)/2$ ($\{|j\rangle_k\}_{j=0}^{\infty}$ are the number states for the kth mode). Thanks to the normal mode decomposition $(\bar{\mathbf{x}}, \mathbf{S}, \{\nu_k\})$ of Eq. (16), one can easily compute every positive power of an n-mode Gaussian state ρ. In fact, let us introduce the two basic functions

$$\Phi_p^{\pm}(x) := (x+1)^p \pm (x-1)^p, \tag{18}$$

which are non-negative for every $x \geq 1$ and $p \geq 0$. Let us also construct

$$G_p(x) := \frac{2^p}{\Phi_p^-(x)} = \frac{2^p}{(x+1)^p - (x-1)^p} \tag{19}$$

and

$$\Lambda_p(x) := \frac{\Phi_p^+(x)}{\Phi_p^-(x)} = \frac{(x+1)^p + (x-1)^p}{(x+1)^p - (x-1)^p}. \tag{20}$$

Then, we have the following lemma.

Lemma 1. An arbitrary positive power ρ^p of an n-mode Gaussian state ρ can be written as

$$\rho^p = (\mathrm{Tr}\,\rho^p)\rho(p), \tag{21}$$

where

$$\mathrm{Tr}\,\rho^p = \prod_{k=1}^{n} G_p(\nu_k) \tag{22}$$

and

$$\rho(p) := \hat{U}_{\bar{\mathbf{x}},\mathbf{S}}\left\{\bigotimes_{k=1}^{n}\sigma[\Lambda_p(\nu_k)]\right\}\hat{U}^{\dagger}_{\bar{\mathbf{x}},\mathbf{S}}. \tag{23}$$

Proof. By setting

$$\nu_k = \frac{1+\eta_k}{1-\eta_k}\left(\Leftrightarrow \eta_k = \frac{\nu_k - 1}{\nu_k + 1}\right) \tag{24}$$

into Eq. (17), we have the following equivalent expression for the thermal state:

$$\sigma(\eta_k) = (1-\eta_k)\sum_{j=0}^{\infty}\eta_k^j |j\rangle_k\langle j|. \tag{25}$$

By iterating Eq. (16) we get

$$\rho^p = \hat{U}_{\bar{\mathbf{x}},\mathbf{S}}\left\{\bigotimes_{k=1}^{n}[\sigma(\eta_k)]^p\right\}\hat{U}^{\dagger}_{\bar{\mathbf{x}},\mathbf{S}} \tag{26}$$

for every $p \geq 0$. Then, from Eq. (25), we get

$$[\sigma(\eta_k)]^p = (1-\eta_k)^p\sum_{j=0}^{\infty}(\eta_k^p)^j|j\rangle_k\langle j| = \frac{(1-\eta_k)^p}{1-\eta_k^p}\sigma(\eta_k^p), \tag{27}$$

which, inserted into Eq. (26), leads to the expression

$$\rho^p = \left[\prod_{k=1}^{n}\frac{(1-\eta_k)^p}{1-\eta_k^p}\right]\left\{\hat{U}_{\bar{\mathbf{x}},\mathbf{S}}\left[\bigotimes_{k=1}^{n}\sigma(\eta_k^p)\right]\hat{U}^{\dagger}_{\bar{\mathbf{x}},\mathbf{S}}\right\}. \tag{28}$$

Now, from Eq. (28) we have

$$\mathrm{Tr}\,\rho^p = \prod_{k=1}^{n}\frac{(1-\eta_k)^p}{1-\eta_k^p}, \tag{29}$$

and, applying Eq. (24), we get

$$\mathrm{Tr}\,\rho^p = \prod_{k=1}^{n}\frac{2^p}{(\nu_k+1)^p - (\nu_k-1)^p}, \tag{30}$$

which is equivalent to Eqs. (22) and (19). Then we can easily derive the symplectic eigenvalue $\nu_{k,p}$ of the thermal state $\sigma(\eta_k^p)$ which is present in Eq. (28). In fact, by using Eq. (24), we get

$$\nu_{k,p} = \frac{1+\eta_k^p}{1-\eta_k^p} = \frac{(\nu_k+1)^p + (\nu_k-1)^p}{(\nu_k+1)^p - (\nu_k-1)^p} := \Lambda_p(\nu_k), \tag{31}$$

i.e., $\nu_{k,p}$ is connected to the original eigenvalue ν_k by the Λ function of Eq. (20). Finally, by inserting all the previous results into Eq. (28) we get the formula of Eq. (21). ■

Notice that, thanks to the formula of Eq. (21), the *unnormalized* power state ρ^p is simply expressed in terms of the symplectic spectrum $\{\nu_k\}$ and the affine pair $(\bar{\mathbf{x}},\mathbf{S})$ decomposing the original Gaussian state ρ according to Eq. (16). In particular, the CM $\mathbf{V}(p)$ of the *normalized* power state $\rho(p)$ is simply related to the CM $\mathbf{V}=\mathbf{V}(1)$ of the original state $\rho=\rho(1)$ by

$$\mathbf{V}(p) = \mathbf{S}\left[\bigoplus_{k=1}^{n}\Lambda_p(\nu_k)\mathbf{I}_k\right]\mathbf{S}^T. \tag{32}$$

III. QUANTUM CHERNOFF BOUND

Let us review the general problem of quantum state discrimination (which we specialize to Gaussian states of bosonic modes later in this section). This problem consists in distinguishing between two possible states ρ_A and ρ_B, which are equiprobable for a quantum system [11]. In this discrimination, we suppose that N identical copies of the quantum system are available for a generalized quantum measurement, i.e., a positive operator valued measure (POVM) [12]. In other words, we apply a POVM to N copies of the quantum system in order to choose between two equiprobable hypotheses about its global state ρ^N, i.e.,

$$H_A : \rho^N = \underbrace{\rho_A \otimes \cdots \otimes \rho_A}_{N} := \rho_A^N, \tag{33}$$

and

$$H_B : \rho^N = \underbrace{\rho_B \otimes \cdots \otimes \rho_B}_{N} := \rho_B^N. \tag{34}$$

In order to achieve an optimal discrimination, it is sufficient to consider a dichotomic POVM $\{\hat{E}_A,\hat{E}_B\}$, whose Kraus operators $\hat{E}_A$ and $\hat{E}_B$ are associated with the hypotheses H_A and H_B, respectively. By performing such a dichotomic POVM $\{\hat{E}_A,\hat{E}_B\}$, we get a correct answer up to an error probability

$$\begin{aligned}P_{\mathrm{err}}^{(N)} &= \frac{1}{2}P(H_A|H_B) + \frac{1}{2}P(H_B|H_A)\\ &= \frac{1}{2}\mathrm{Tr}(\hat{E}_A\rho_B^N) + \frac{1}{2}\mathrm{Tr}(\hat{E}_B\rho_A^N).\end{aligned} \tag{35}$$

Clearly, the optimal POVM will be the one minimizing $P_{\mathrm{err}}^{(N)}$. Now, since $\hat{E}_A = \hat{I} - \hat{E}_B$, we can introduce the *Helstrom matrix* [13]

$$\gamma := \rho_B^N - \rho_A^N, \tag{36}$$

and write

$$P_{\mathrm{err}}^{(N)} = \frac{1}{2} - \frac{1}{2}\mathrm{Tr}(\gamma\hat{E}_B). \tag{37}$$

The error probability of Eq. (37) can be now minimized over the Kraus operator $\hat{E}_B$ only. Since $\mathrm{Tr}(\gamma)=0$, the Helstrom matrix γ has both positive and negative eigenvalues. As a consequence, the optimal $\hat{E}_B$ is the projector onto the positive part γ_+ of γ (i.e., the projector onto the subspace spanned by the eigenstates of γ with positive eigenvalues). By assuming this optimal operator, we have

$$\mathrm{Tr}(\gamma\hat{E}_B) = \mathrm{Tr}(\gamma_+) = \frac{1}{2}\|\gamma\|_1, \tag{38}$$

where

$$\|\gamma\|_1 := \mathrm{Tr}|\gamma| = \mathrm{Tr}\sqrt{\gamma^\dagger\gamma} \tag{39}$$

is the trace norm of the Helstrom matrix γ. Thus, the *minimal* error probability $P^{(N)} := \min P_{\mathrm{err}}^{(N)}$ is equal to

$$P^{(N)} = \frac{1}{2}\left(1 - \frac{1}{2}\|\rho_B^N - \rho_A^N\|_1\right). \tag{40}$$

The computation of the trace norm in Eq. (40) is rather difficult. Luckily, one can always resort to the quantum Chernoff bound [3]

$$P^{(N)} \leq P_{\mathrm{QC}}^{(N)}, \tag{41}$$

where

$$P_{\mathrm{QC}}^{(N)} = \frac{1}{2}\exp(-\kappa N) \tag{42}$$

and [14]

$$\kappa := -\ln\left[\inf_{0\leq s\leq 1} \mathrm{Tr}(\rho_A^s \rho_B^{1-s})\right]. \tag{43}$$

More simply, this bound can be written as

$$P_{\mathrm{QC}}^{(N)} = \frac{1}{2}\left[\inf_{0\leq s\leq 1} Q_s\right]^N, \tag{44}$$

where

$$Q_s := \mathrm{Tr}(\rho_A^s \rho_B^{1-s}). \tag{45}$$

Notice that the quantum Chernoff bound involves a minimization in the variable s. By setting $s=1/2$ in Eq. (44), one can also define the quantum version of the Bhattacharyya bound [15]:

$$P_B^{(N)} := \frac{1}{2}[\mathrm{Tr}(\sqrt{\rho_A}\sqrt{\rho_B})]^N, \tag{46}$$

which clearly satisfies

$$P_{\mathrm{QC}}^{(N)} \leq P_B^{(N)}. \tag{47}$$

In particular, for $\rho_A - \rho_B = \delta\rho \simeq 0$, one can show that $P_{\mathrm{QC}}^{(N)} \simeq P_B^{(N)}$. Notice that we also have the following inequalities [7,12]:

$$F_- \leq P^{(1)} \leq P_{\mathrm{QC}}^{(1)} \leq F_+, \tag{48}$$

where

$$F_- := \frac{1-\sqrt{1-F(\rho_A,\rho_B)}}{2}, \quad F_+ := \frac{\sqrt{F(\rho_A,\rho_B)}}{2}, \tag{49}$$

and

$$F(\rho_A,\rho_B) := [\mathrm{Tr}(\sqrt{\sqrt{\rho_A}\rho_B\sqrt{\rho_A}})]^2 \tag{50}$$

is the fidelity between ρ_A and ρ_B [16]. In particular, if one of the two states is pure, e.g., $\rho_A = |\varphi\rangle_A\langle\varphi|$, then we simply have

$$P_{\mathrm{QC}}^{(1)} = \frac{F(|\varphi\rangle_A\langle\varphi|,\rho_B)}{2}. \tag{51}$$

Formula for Gaussian states

Let us now specialize the problem of quantum state discrimination to Gaussian states of n bosonic modes. In this case, the quantum Chernoff bound can be expressed by a relatively simple formula thanks to the normal mode decomposition $(\bar{\mathbf{x}},\mathbf{S},\{\nu_k\})$ of Eq. (16).

Theorem 2. Let us consider two arbitrary n-mode Gaussian states ρ_A and ρ_B with normal mode decompositions $(\bar{\mathbf{x}}_A,\mathbf{S}_A,\{\alpha_k\})$ and $(\bar{\mathbf{x}}_B,\mathbf{S}_B,\{\beta_k\})$. Then we have

$$Q_s = \bar{Q}_s \exp\left\{-\frac{1}{2}\mathbf{d}^T[\mathbf{V}_A(s)+\mathbf{V}_B(1-s)]^{-1}\mathbf{d}\right\}, \tag{52}$$

where

$$\bar{Q}_s := \frac{2^n\prod_{k=1}^n G_s(\alpha_k)G_{1-s}(\beta_k)}{\sqrt{\det[\mathbf{V}_A(s)+\mathbf{V}_B(1-s)]}}. \tag{53}$$

In these formulas $\mathbf{d} := \bar{\mathbf{x}}_A - \bar{\mathbf{x}}_B$ and

$$\mathbf{V}_A(s) = \mathbf{S}_A\left[\bigoplus_{k=1}^n \Lambda_s(\alpha_k)\mathbf{I}_k\right]\mathbf{S}_A^T, \tag{54}$$

$$\mathbf{V}_B(1-s) = \mathbf{S}_B\left[\bigoplus_{k=1}^n \Lambda_{1-s}(\beta_k)\mathbf{I}_k\right]\mathbf{S}_B^T. \tag{55}$$

Proof. By applying Lemma 1 to Eq. (45), we get

$$Q_s = \mathcal{N}\,\mathrm{Tr}[\rho_A(s)\rho_B(1-s)], \tag{56}$$

where

$$\mathcal{N} := (\mathrm{Tr}\ \rho_A^s)(\mathrm{Tr}\ \rho_B^{1-s}) = \prod_{k=1}^n G_s(\alpha_k)G_{1-s}(\beta_k), \tag{57}$$

and $\rho_A(s),\rho_B(1-s)$ are two Gaussian states defined according to Eq. (23). In particular, the CM's of these states are given by Eqs. (54) and (55) [according to Eq. (32)]. For an arbitrary pair of n-mode Gaussian states ρ,ρ' with characteristic functions χ,χ' and moments $(\mathbf{V},\bar{\mathbf{x}})$ and $(\mathbf{V}',\bar{\mathbf{x}}')$, we have the trace rule

$$\mathrm{Tr}(\rho\rho') = \int_{\mathbb{R}^{2n}} \frac{d^{2n}\boldsymbol{\xi}}{\pi^n}\chi(\boldsymbol{\xi})\chi'(-\boldsymbol{\xi})$$
$$= 2^n\frac{\exp[-\frac{1}{2}(\bar{\mathbf{x}}-\bar{\mathbf{x}}')^T(\mathbf{V}+\mathbf{V}')^{-1}(\bar{\mathbf{x}}-\bar{\mathbf{x}}')]}{\sqrt{\det(\mathbf{V}+\mathbf{V}')}}. \tag{58}$$

Then, by using Eq. (58) in Eq. (56), we easily get Eqs. (52) and (53). ■

Thanks to the previous theorem, the Chernoff quantity Q_s can be directly computed from the normal mode decompositions $(\bar{\mathbf{x}}_A,\mathbf{S}_A,\{\alpha_k\})$ and $(\bar{\mathbf{x}}_B,\mathbf{S}_B,\{\beta_k\})$ of the Gaussian states. Notice that this theorem is already contained in Ref. [7], but here the formula of Eqs. (52) and (53) is conveniently expressed in terms of the symplectic spectra $\{\alpha_k\}$ and $\{\beta_k\}$.

In applying this theorem, the more difficult task is the algebraic computation of the symplectic matrices $\mathbf{S}_A$ and $\mathbf{S}_B$ to be used in Eqs. (54) and (55). In fact, while finding the symplectic eigenvalues $\{\nu_k\}$ is relatively easy (since they are the degenerate solutions of a $2n$-degree polynomial), finding the diagonalizing symplectic matrix $\mathbf{S}$ is computationally harder (since it corresponds to the construction of a symplectic basis [17]). For this reason, it is very helpful to derive bounds for the minimal error probability $P^{(N)}$ that do not depend on $\mathbf{S}$ and, therefore, are much easier to compute.

IV. COMPUTABLE BOUNDS FOR DISCRIMINATING GAUSSIAN STATES

Let us derive bounds that do not depend on the affine symplectic transformations $(\bar{\mathbf{x}}_A,\mathbf{S}_A)$ and $(\bar{\mathbf{x}}_B,\mathbf{S}_B)$, but only on the symplectic spectra $\{\alpha_k\}$ and $\{\beta_k\}$. This is possible by simplifying the determinant in Eq. (53) involving the two positive matrices $\mathbf{V}_A(s)$ and $\mathbf{V}_B(1-s)$. Such a determinant can be decomposed into a sum of determinants by resorting to the Minkowski determinant inequality [18]. In general, such an algebraic theorem is valid for non-negative complex matrices in any dimension (see, e.g., the Appendix). In particular, it can be specialized to positive real matrices in even dimension and, therefore, to correlation matrices.

Lemma 3. Let us consider a pair of $2n\times 2n$ real, symmetric, and positive matrices $\mathbf{K}$ and $\mathbf{L}$. Then, we have the Minkowski determinant inequality

$$[\det(\mathbf{K}+\mathbf{L})]^{1/2n} \geq (\det \mathbf{K})^{1/2n} + (\det \mathbf{L})^{1/2n}. \tag{59}$$

By combining Theorem 2 and Lemma 3, we can prove the following theorem.

Theorem 4. Let us consider two arbitrary n-mode Gaussian states ρ_A and ρ_B with symplectic spectra $\{\alpha_k\}$ and $\{\beta_k\}$. Then we have the “Minkowski bound”

$$P_{\mathrm{QC}}^{(N)} \leq M^{(N)} := \frac{1}{2}\Big[\inf_{0\leq s\leq 1} M_s\Big]^N, \tag{60}$$

where

$$M_s := 4^n\left[\prod_{k=1}^{n}\Psi_s(\alpha_k,\beta_k)+\prod_{k=1}^{n}\Psi_{1-s}(\beta_k,\alpha_k)\right]^{-n} \tag{61}$$

and

$$\Psi_p(x,y) := [\Phi_p^+(x)\Phi_{1-p}^-(y)]^{1/n}. \tag{62}$$

Proof. By taking the nth power of Eq. (59), we get

$$[\det(\mathbf{K}+\mathbf{L})]^{1/2} \geq [(\det \mathbf{K})^{1/2n} + (\det \mathbf{L})^{1/2n}]^n. \tag{63}$$

This inequality can be directly applied to the CM’s $\mathbf{V}_A(s)$ and $\mathbf{V}_B(1-s)$ of Eqs. (54) and (55). Then, by inserting the result into Eq. (53), we get

$$\bar{Q}_s \leq \frac{2^n\prod_{k=1}^{n}G_s(\alpha_k)G_{1-s}(\beta_k)}{\{[\det \mathbf{V}_A(s)]^{1/2n}+[\det \mathbf{V}_B(1-s)]^{1/2n}\}^n} := M_s. \tag{64}$$

By using the binomial expansion and the relations

$$\det \mathbf{V}_A(s) = \prod_{k=1}^{n}[\Lambda_s(\alpha_k)]^2, \tag{65}$$

$$\det \mathbf{V}_B(1-s) = \prod_{k=1}^{n}[\Lambda_{1-s}(\beta_k)]^2, \tag{66}$$

we get

$$M_s^{-1} = \frac{1}{2^n}\sum_{i=0}^{n}\binom{n}{i}\prod_{k=1}^{n}\frac{[\Lambda_s(\alpha_k)]^{i/n}[\Lambda_{1-s}(\beta_k)]^{(n-i)/n}}{G_s(\alpha_k)G_{1-s}(\beta_k)}. \tag{67}$$

Now, by using Eqs. (19) and (20), we get

$$M_s^{-1} = \frac{1}{4^n}\sum_{i=0}^{n}\binom{n}{i}\left\{\left[\prod_{k=1}^{n}\Phi_s^+(\alpha_k)\Phi_{1-s}^-(\beta_k)\right]^{i/n}\times\left[\prod_{k=1}^{n}\Phi_s^-(\alpha_k)\Phi_{1-s}^+(\beta_k)\right]^{(n-i)/n}\right\}, \tag{68}$$

and, by using Eq. (62), we derive

$$M_s^{-1} = \frac{1}{4^n}\sum_{i=0}^{n}\binom{n}{i}\left\{\left[\prod_{k=1}^{n}\Psi_s(\alpha_k,\beta_k)\right]^{i}\left[\prod_{k=1}^{n}\Psi_{1-s}(\beta_k,\alpha_k)\right]^{n-i}\right\}$$
$$= \frac{1}{4^n}\left[\prod_{k=1}^{n}\Psi_s(\alpha_k,\beta_k)+\prod_{k=1}^{n}\Psi_{1-s}(\beta_k,\alpha_k)\right]^n. \tag{69}$$

The latter quantity corresponds to the inverse of the one in Eq. (61). Now, since every convex combination of positive matrices is still positive, we have that $\exp\{\cdots\}\leq 1$ in Eq. (52). Then we get

$$Q_s \leq \bar{Q}_s \leq M_s, \tag{70}$$

leading to the final result of Eq. (60). ■

The basic algebraic property which has been exploited in Theorem 4 is the concavity of the function $\sqrt[2n]{\det}$ on every convex combination of $2n\times 2n$ positive matrices (like the correlation matrices). Such a property is simply expressed by Eq. (59) of Lemma 3. It enables us to decompose the determinant of a sum into a sum of determinants and, therefore, to derive the bound in the “sum form” of Eq. (61). Now, thanks to the Young’s inequality [19], every convex combination of positive numbers is lower bounded by a product of their powers, i.e., for every $k,l>0$ and $0\leq\theta\leq 1$, one has

$$\theta k + (1-\theta)l \geq k^\theta l^{1-\theta}. \tag{71}$$

As a consequence, every sum of positive determinants can be bounded by a product of determinants. Then, by applying the Young’s inequality to Theorem 4, we can easily derive a weaker bound which is in a “product form.” This is shown in the following corollary. Notice that this bound can be equivalently found by exploiting the concavity of the function “log det” on every convex combination of positive matrices. (See the Appendix for details.)

Corollary 5. Let us consider two arbitrary n-mode Gaussian states ρ_A and ρ_B with symplectic spectra $\{\alpha_k\}$ and $\{\beta_k\}$. Then we have the “Young bound”

$$M^{(N)} \leq Y^{(N)} := \frac{1}{2}\Big[\inf_{0\leq s\leq 1} Y_s\Big]^N, \tag{72}$$

where

$$Y_s := 2^n \prod_{k=1}^{n} \Gamma_s(\alpha_k)\Gamma_{1-s}(\beta_k). \qquad (73)$$

and

$$\Gamma_p(x) := [(x+1)^{2p} - (x-1)^{2p}]^{-1/2}. \qquad (74)$$

Proof. From Eq. (71) with $\theta=1/2$, we have that every pair of real numbers $k,l>0$ satisfies

$$k + l \geq 2\sqrt{kl}. \qquad (75)$$

Then, for positive $\mathbf{K}$ and $\mathbf{L}$, we can apply Eq. (75) with

$$k := (\det \mathbf{K})^{1/2n} > 0, \quad l := (\det \mathbf{L})^{1/2n} > 0. \qquad (76)$$

This leads to the further lower bound

$$[(\det \mathbf{K})^{1/2n} + (\det \mathbf{L})^{1/2n}]^n \geq 2^n [\det \mathbf{K} \det \mathbf{L}]^{1/4}. \quad (77)$$

By applying Eq. (77) to the CM's $\mathbf{V}_A(s)$ and $\mathbf{V}_B(1-s)$, and inserting the result into Eq. (64), we get

$$M_s \leq \prod_{k=1}^{n} \frac{G_s(\alpha_k)G_{1-s}(\beta_k)}{\sqrt[4]{\det \mathbf{V}_A(s) \det \mathbf{V}_B(1-s)}} := Y_s. \qquad (78)$$

Then, by using Eqs. (65) and (66), we can write

$$Y_s = \prod_{k=1}^{n} \frac{G_s(\alpha_k)G_{1-s}(\beta_k)}{\sqrt{\Lambda_s(\alpha_k)}\sqrt{\Lambda_{1-s}(\beta_k)}}. \qquad (79)$$

Exploiting Eqs. (19) and (20), we can easily derive Eq. (73), where

$$\Gamma_p(x) := [\Phi_p^+(x)\Phi_p^-(x)]^{-1/2}, \qquad (80)$$

also equivalent to Eq. (74). Finally, since $M_s \leq Y_s$, the result of Eq. (72) is straightforward. ■

As stated in Theorem 4 and Corollary 5, the two bounds $M^{(N)}$ and $Y^{(N)}$ depend only on the symplectic spectra $\{\alpha_k\}$ and $\{\beta_k\}$ of the input states ρ_A and ρ_B. As a consequence, such bounds are useful in discriminating Gaussian states which are unitarily *inequivalent*, i.e., such that

$$\rho_A \neq \hat{U}\rho_B\hat{U}^\dagger \qquad (81)$$

for every unitary $\hat{U}$. In fact, since ρ_A and ρ_B are Gaussian states, every unitary $\hat{U}$ such that $\rho_A = \hat{U}\rho_B\hat{U}^\dagger$ must be a Gaussian unitary $\hat{U}=\hat{U}_{\bar{\mathbf{x}},\mathbf{S}}$. Its action corresponds therefore to an affine symplectic trasformation $(\bar{\mathbf{x}},\mathbf{S})$, which cannot change the symplectic spectrum (so that $\{\alpha_k\}=\{\beta_k\}$). Roughly speaking, the previous bounds are useful when the main difference between ρ_A and ρ_B is due to the noise, whose variations break the equivalence and are stored in the symplectic spectra. This situation is common in several quantum scenarios; for instance, in quantum illumination [20,21], where two different thermal-noise channels must be discriminated, or in quantum cloning, when the outputs of an asymmetric Gaussian cloner [22] must be distinguished.

Discrimination of single mode Gaussian states: An example

Let us compare the bounds of Theorem 4 and Corollary 5 with the fidelity bounds of Eq. (48) in a simple case. According to Ref. [23], the fidelity between two single-mode Gaussian states ρ_A and ρ_B, with moments $(\mathbf{V}_A, \bar{\mathbf{x}}_A)$ and $(\mathbf{V}_B, \bar{\mathbf{x}}_B)$, is given by the formula

$$F(\rho_A,\rho_B) = \frac{2}{\sqrt{\Delta+\delta}-\sqrt{\delta}} \exp\left[-\frac{1}{2}\mathbf{d}^T(\mathbf{V}_A+\mathbf{V}_B)^{-1}\mathbf{d}\right], \qquad (82)$$

where

$$\Delta := \det(\mathbf{V}_A+\mathbf{V}_B), \quad \delta := (\det \mathbf{V}_A - 1)(\det \mathbf{V}_B - 1), \qquad (83)$$

and $\mathbf{d} := \bar{\mathbf{x}}_A - \bar{\mathbf{x}}_B$. Let us discriminate between the two single-mode states: $\rho_A = \sigma(1) = |0\rangle\langle 0|$ (vacuum state) and $\rho_B = \sigma(\beta)$ (arbitrary thermal state). In such a case, it is very easy to compute the infima of M_s and Y_s in Eqs. (60) and (72), respectively. In fact, by exploiting

$$\Phi_p^{\pm}(1) = [\Gamma_p(1)]^{-1} = 2^p, \quad \Phi_p^+(x) + \Phi_p^-(x) = 2(x+1)^p, \qquad (84)$$

we get

$$M_s = \left(\frac{2}{1+\beta}\right)^{1-s}, \quad Y_s = \frac{2^s}{\sqrt{(\beta+1)^{2s} - (\beta-1)^{2s}}}, \qquad (85)$$

whose infima are taken at $s=0$ and 1, respectively. As a consequence, for a single copy of the state, we have

$$M^{(1)} = (1+\beta)^{-1}, \quad Y^{(1)} = \frac{1}{2\sqrt{\beta}}. \qquad (86)$$

At the same time, we have

$$F(\rho_A,\rho_B) = 2(1+\beta)^{-1}, \qquad (87)$$

which implies

$$F_- = \frac{1}{2} - \frac{1}{2}\sqrt{\frac{\beta-1}{\beta+1}}, \quad F_+ = \frac{1}{\sqrt{2(1+\beta)}}. \qquad (88)$$

By using Eq. (51), we also derive

$$P_{\mathrm{QC}}^{(1)} = (1+\beta)^{-1}. \qquad (89)$$

As evident from Fig. 1, the Young bound $Y^{(1)}$ is tighter than the fidelity bound F_+, while the Minkowski bound $M^{(1)}$ coincides exactly with $P_{\mathrm{QC}}^{(1)}$ in this case.

V. CONCLUSION

We have considered the general problem of discriminating two Gaussian states of n bosonic modes, supposing that N copies of the state are provided. To face this problem, we have suitably recast the formula for the quantum Chernoff bound given in Ref. [7]. By combining this formula with classical algebraic inequalities (the Minkowski determinant inequality and Young's inequality) we have derived easy-to-compute upper bounds whose computational hardness is equivalent to finding the symplectic eigenvalues of the involved Gaussian states. Since these upper bounds depend only on the symplectic spectra, they are useful in distinguish-

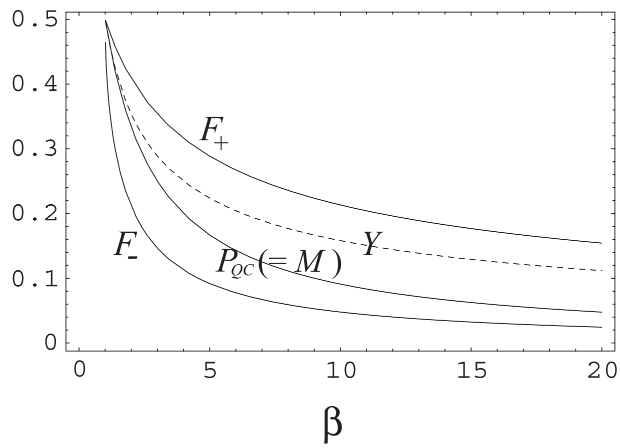

FIG. 1. Behavior of the various bounds $Y^{(1)}$, $M^{(1)}$, $P_{\mathrm{QC}}^{(1)}$, F_+, and F_- versus the eigenvalue β in the discrimination of a thermal state $\sigma(\beta)$ from a vacuum state. Notice that $M^{(1)}=P_{\mathrm{QC}}^{(1)}$ in this example.

ing Gaussian states which are unitarily inequivalent. This is indeed a common situation in various quantum scenarios where the noise is the key element to be discriminated. For instance, the discrimination between two different thermal-noise channels is a basic process in quantum sensing and imaging, where nearly transparent objects must be detected [20,21]. Potential applications of our results concern also quantum cryptography, where the presence of noise is related to the presence of a malicious eavesdropper.

ACKNOWLEDGMENTS

S.P. was supported by a Marie Curie Action within the 6th European Community Framework Programme. S.L. was supported by the W. M. Keck center for extreme quantum information processing (xQIT).

APPENDIX: BASIC ALGEBRAIC INEQUALITIES

For completeness we report some of the basic algebraic tools used in our derivation (see also Refs. [18,24,25]). Here we denote by $\mathbb{M}(m,\mathbb{C})$ the set of $m\times m$ matrices with complex entries.

Theorem 6 (Minkowski determinant inequality). Let us consider $\mathbf{K},\mathbf{L}\in\mathbb{M}(m,\mathbb{C})$ such that $\mathbf{K}^\dagger=\mathbf{K}\geq 0$ and $\mathbf{L}^\dagger=\mathbf{L}\geq 0$. Then

$$[\det(\mathbf{K}+\mathbf{L})]^{1/m}\geq(\det\mathbf{K})^{1/m}+(\det\mathbf{L})^{1/m}. \tag{A1}$$

More generally

$$\{\det[\theta\mathbf{K}+(1-\theta)\mathbf{L}]\}^{1/m}\geq\theta(\det\mathbf{K})^{1/m}+(1-\theta)(\det\mathbf{L})^{1/m}, \tag{A2}$$

for every $0\leq\theta\leq 1$.

By taking the mth power of Eq. (A1), it is trivial to check that

$$\det(\mathbf{K}+\mathbf{L})\geq\det\mathbf{K}+\det\mathbf{L}. \tag{A3}$$

Then, by using the Young's inequality of Eq. (71), we can easily prove the following corollary.

Corollary 7. Let us consider $\mathbf{K},\mathbf{L}\in\mathbb{M}(m,\mathbb{C})$ such that $\mathbf{K}^\dagger=\mathbf{K}>0$ and $\mathbf{L}^\dagger=\mathbf{L}>0$. Then

$$\det[\theta\mathbf{K}+(1-\theta)\mathbf{L}]\geq(\det\mathbf{K})^{\theta}(\det\mathbf{L})^{1-\theta}, \tag{A4}$$

for every $0\leq\theta\leq 1$.

Proof. By setting $k:=(\det\mathbf{K})^{1/m}>0$ and $l:=(\det\mathbf{L})^{1/m}>0$, we can apply Eq. (71) to the right-hand side of Eq. (A2). Then, we get the result of Eq. (A4) by taking the mth power. ■

Notice that, by taking the logarithm of Eq. (A4), we get

$$f[\theta\mathbf{K}+(1-\theta)\mathbf{L}]\geq\theta f(\mathbf{K})+(1-\theta)f(\mathbf{L}), \tag{A5}$$

where

$$f(\mathbf{M}):=\log\det(\mathbf{M}). \tag{A6}$$

In other words, Corollary 7 states that the function "log det" is concave on convex combinations of positive matrices. Theorem 6 instead states that the function $\sqrt[m]{\det}$ is concave on convex combinations of m-square non-negative matrices.

[1] H. Chernoff, Ann. Math. Stat. **23**, 493 (1952).

[2] M. Nussbaum and A. Szkola, e-print arXiv:quant-ph/0607216.

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

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] S. L. Braunstein and A. K. Pati, *Quantum Information Theory with Continuous Variables* (Kluwer Academic, Dordrecht, 2003); S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).

[6] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Quantum Information* (Bibliopolis, Naples, 2005); J. Eisert and M. B. Plenio, Int. J. Quantum Inf. **1**, 479 (2003).

[7] J. Calsamiglia, R. Munoz-Tapia, L. Masanes, A. Acin, and E. Bagan, Phys. Rev. A **77**, 032311 (2008).

[8] Notice that our choice of the Weyl operator is different from $\hat{D}(\boldsymbol{\xi}):=\exp(i\hat{\mathbf{x}}^T\boldsymbol{\Omega}\boldsymbol{\xi})$, whose definition directly comes from the standard displacement operator of quantum optics. The choice of Eq. (3) avoids the presence of $\boldsymbol{\Omega}$ in the characteristic functions.

[9] The symplectic eigenvalues of $\mathbf{V}$ can also be computed as the "standard" eigenvalues of the matrix $|i\boldsymbol{\Omega}\mathbf{V}|$ where the modulus must be understood in the operatorial sense. In fact, the matrix $i\boldsymbol{\Omega}\mathbf{V}$ is Hermitian and, therefore, diagonalizable by a unitary transformation. Then, by taking the modulus of its $2n$ real eigenvalues, one gets the n symplectic eigenvalues of $\mathbf{V}$.

[10] A. Serafini, G. Adesso, and F. Illuminati, Phys. Rev. A **71**, 032349 (2005).

[11] More generally, the problem can be formulated for quantum states which are not equiprobable.

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

[13] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[14] Notice that the infimum instead of the minimum is used in this formula since a discontinuity may affect the border points $s = 0$ and 1 [3,7].
[15] T. Kailath, IEEE Trans. Commun. Technol. **15**, 52 (1967).
[16] C. A. Fuchs and J. V. de Graaf, IEEE Trans. Inf. Theory **45**, 1216 (1999).
[17] V. I. Arnold, *Mathematical Methods of Classical Mechanics* (Springer-Verlag, New York, 1978).
[18] R. Bhatia, *Matrix Analysis* (Springer-Verlag, New York, 1997).
[19] W. H. Young, Proc. R. Soc. London, Ser. A **87**, 331 (1912).
[20] S. Lloyd, e-print arXiv:0803.2022.
[21] B. I. Erkmen, V. Giovannetti, S. Guha, S. Lloyd, L. Maccone, S. Pirandola, J. H. Shapiro, and S.-H. Tan (unpublished).
[22] N. J. Cerf, A. Ipe, and X. Rottenberg, Phys. Rev. Lett. **85**, 1754 (2000); N. J. Cerf, S. Iblisdir, and G. Van Assche, Eur. Phys. J. D **18**, 211 (2002).
[23] H. Scutaru, J. Phys. A **31**, 3659 (1998); H. Nha and H. J. Carmichael, Phys. Rev. A **71**, 032336 (2005); S. Olivares, M. G. A. Paris, and U. L. Andersen, *ibid.* **73**, 062330 (2006).
[24] M. Marcus and H. Minc, *A Survey of Matrix Theory and Matrix Inequalities* (Dover, New York, 1992).
[25] R. A. Horn and C. R. Johnson, *Matrix Analysis* (Cambridge University Press, Cambridge, U.K., 2006).