Gaussian states and geometrically uniform symmetry

Gianfranco Cariolaro, Roberto Corvaja, and Gianfranco Pierobon
Department of Information Engineering, University of Padova, Via G. Gradenigo 6/B, 35131 Padova, Italy
(Received 12 June 2014; published 8 October 2014)

Quantum Gaussian states can be considered as the majority of the practical quantum states used in quantum communications and more generally in quantum information. Here we consider their properties in relation to the geometrically uniform symmetry, a property of quantum states that greatly simplifies the derivation of the optimal decision by means of the square root measurements. In a general framework of the N-mode Gaussian states we show the general properties of this symmetry and the application of the optimal quantum measurements. An application example is presented to quantum communication systems employing pulse position modulation. We prove that the geometrically uniform symmetry can be applied to the general class of multimode Gaussian states.

DOI: 10.1103/PhysRevA.90.042309 PACS number(s): 03.67.Hk

I. INTRODUCTION

In the last years Gaussian states have received tremendous interest [1–4] due to the fact that most quantum operations can be performed with continuous variables, of which Gaussian states represent the most important class. The advantage with respect to discrete variables (qubit) is that the optical implementation of continuous variables is available and robust. A relevant application of Gaussian states is given by quantum communications (QC), which in practice are implemented by coherent states, the most important subclass of Gaussian states. Often in QC coherent states are not related explicitly to Gaussian states [5,6], but their recent developments led to a very elegant and powerful theory, so that it seems important to revisit QC using this theory.

In this context we reconsider QC having as information carrier Gaussian states and we assume that a finite set (constellation) of Gaussian states has a special form of symmetry, called *geometrically uniform symmetry* (GUS). A constellation having the GUS is generated starting from a single reference state through a unitary operator, called the *symmetry operator*. The GUS has the advantage not only of simplifying the theory of QC, but also of deriving the optimal decision measurements, which would otherwise not be possible. It is worth remarking that the standard form of GUS is enjoyed by almost all constellations considered for practical QC, namely *phase shift keying* (PSK) and *pulse position modulation* (PPM). Also *quadrature amplitude modulation* (QAM) verifies a generalized form of GUS.

Since we want to establish completely general results, valid for multimode Gaussian states, a fundamental preliminary is a clear and compact formulation of the most general Gaussian state and of the most general Gaussian transformation (Gaussian unitary). To this end we follow the theory developed by Ma and Rhodes in a seminal paper published in 1990 [7]. This theory has the advantage of handling, through an appropriate algebra of operators, the general N-mode Gaussian states in much the same way as the single-mode Gaussian states. Substantially, it proves that the most general Gaussian unitary is given by a cascade combination of a squeezing, a displacement, and a rotation. Finally, we will prove that, starting from an arbitrary N-mode Gaussian state, we can generate a GUS constellation where the symmetry operator is provided by the rotation operator with an appropriate amount of rotation.

In the literature only QC systems using coherent states have been considered and little attention has been devoted to the appealing possibility of using squeezed states [8]. To this end, we revisit QC where the main problem is the optimization of quantum detection to achieve the minimum error probability. As known, this problem is very difficult and exact solutions are established only in a few cases. To overcome this difficulty, suboptimal solutions are considered, the most important of which is given by the square-root measurements (SRM), introduced by Hausladen *et al.* [9] and subsequently developed as a least-square measurement (LSM) by Eldar and Forney [10,11]. This technique is not in general optimal, but gives a good approximation of the optimum ("pretty good" is the judgment given by the authors and very often echoed in the literature). The SRM or LSM can be applied with any constellation, but in the presence of GUS it provides the optimal solution in an easy and explicit form. This holds when the detection is based on pure states; with mixed states the SRM technique is suboptimal, but gives a very accurate overestimate of the error probability, surely better than the quantum Chernov bound usually considered with Gaussian states [12].

The paper is organized as follows. In Sec. II we introduce the N-mode Gaussian states and Gaussian transformations and discuss their most general representations in terms of unitary Gaussian transformations. Section III is devoted to Gaussian states equipped with the GUS. In Sec. IV we present an application of the theory to the quantum detection for PPM, which requires a nontrivial analysis in a multimode Hilbert space. Explicit examples of error probability are carried out considering as quantum carrier in PPM both coherent and squeezed states.

We adopt the following notation: $\cdot^{\mathrm{T}}$ denotes transposition, while $\cdot^{*}$ has the multiple role of adjoint for operators, Hermitian conjugation for matrices, and complex conjugation for numbers. The *normalization* follows the notation of the authors of [1], where in particular the reduced Planck constant is set to $\hbar = 2$.

II. GAUSSIAN STATES AND GAUSSIAN TRANSFORMATIONS

A. Definition of Gaussian states

In an N-mode bosonic space $\mathcal{H}^{\otimes N}$ quantum states are represented in general by density operators $\rho : \mathcal{H}^{\otimes N} \to \mathcal{H}^{\otimes N}$. Any density operator has an equivalent representation in the *phase space* $\mathbb{R}^{2N}$ given by a characteristic function and Wigner function. In particular, Gaussian states are defined with reference to their characteristic and Wigner functions, which should have a multivariate Gaussian form. For an N-mode Gaussian state with mean $\overline{X}$ and covariance matrix V the characteristic function has the following form

$$\chi(u,v) = \exp\big[-\tfrac{1}{2} u_v{}^{\mathrm{T}} \Omega V \Omega^{\mathrm{T}} u_v - j\,(\Omega \overline{X})^{\mathrm{T}} u_v\big], \quad (u,v) \in \mathbb{R}^{2N} \tag{1}$$

with

$$u_v = [u_1, v_1, \ldots, u_N, v_N]^T, \quad \Omega = \mathrm{diag}\,[\Omega_1, \ldots, \Omega_N], \quad \Omega_i = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}. \tag{2}$$

The relevant property of Gaussian states is that they are specified simply by the pair $(\overline{X}, V)$ and for this reason the density operator of a Gaussian state is often indicated in the form $\rho(\overline{X}, V)$.

B. Gaussian transformations

A *quantum transformation* or *quantum operation* maps the state of the system ρ into a new state $\tilde{\rho} = \Phi(\rho)$. In general a quantum transformation defines a quantum channel, which may refer to an open system [13], while in closed quantum systems the map is provided by a unitary transformation according to

$$\rho \;\to\; \tilde{\rho} = U\,\rho\,U^*. \tag{3}$$

A quantum transformation is *Gaussian* when *it transforms Gaussian states into Gaussian states*. When the Gaussian transformation is performed according to the unitary map (3) it is called *Gaussian unitary*. It can be shown [1] that Gaussian unitaries are generated in the form $U = \exp(-iH/2)$, where H is a Hamiltonian, which is a second-order polynomial in the field operators $q_p := [q_1, p_1, \ldots, q_N, p_N]^{\mathrm{T}}$ or, equivalently, in the bosonic operators $a := [a_1, \ldots, a_N]^{\mathrm{T}}$, $a_* := [a_1^*, \ldots, a_N^*]^{\mathrm{T}}$.

In terms of quadrature operators q_p, a Gaussian unitary gives a *symplectic transformation*, which has the form

$$q_p \to S\,q_p + d, \tag{4}$$

where S is a $2N \times 2N$ real matrix and $d \in \mathbb{R}^{2N}$. S has the property (symplectic matrix) $S\,\Omega\,S^{\mathrm{T}} = \Omega$.

A symplectic transformation modifies the mean vector $\overline{X} = \overline{q_p}$ and the covariance matrix V in the form

$$\overline{X} \;\to\; S\,\overline{X} + d, \quad V \;\to\; S\,V\,S^{\mathrm{T}}. \tag{5}$$

These are the key results because they allow us to specify a Gaussian transformations in terms of the parameters (S,d), which "live" in the phase space $\mathbb{R}^{2N}$.

C. Fundamental Gaussian unitaries

In the literature we find a plethora of forms for the Gaussian unitaries with specific expressions in the single mode, in the two mode, and in the N mode. Here we follow the unified form developed by Ma and Rhodes [7] for the N mode. This form, using appropriate matrix notations, turns out to have extremely similar algebraic properties as that of the single mode and is very useful in establishing general results.

There are only three fundamental Gaussian unitaries, which are specified by the following unitary operators.

(1) N-mode displacement operator

$$D(\alpha) := \mathrm{e}^{a^*\alpha\, -\alpha^* a}, \quad \alpha = [\alpha_1, \ldots, a_N]^{\mathrm{T}} \in \mathbb{C}^N. \tag{6}$$

(2) N-mode rotation operator

$$R(\phi) := \mathrm{e}^{i\,a^*\phi\,a}, \quad \phi \quad N \times N \text{ Hermitian matrix}. \tag{7}$$

(3) N-mode squeeze operator

$$S(z) := \mathrm{e}^{\frac{1}{2}[(a^*\,z\,a_* - a^{\mathrm{T}}\,z^*\,a)]}, \quad z \quad N \times N \text{ symmetric matrix}. \tag{8}$$

In these definitions $a = [a_1, \ldots, a_N]^{\mathrm{T}}$ and $a_* = [a_1^*, \ldots, a_N^*]^{\mathrm{T}}$ are column vectors, while $a^* = [a_1^*, \ldots, a_N^*]$ is a row vector. In (7) the $N \times N$ symmetric matrix z can always be written in the forms [7] $z = r\,\mathrm{e}^{i\theta} = \mathrm{e}^{i\theta^{\mathrm{T}}}\,r^{\mathrm{T}}$, where r and θ are $N \times N$ Hermitian (in general noncommuting) matrices and r is positive semidefinite. A particular case of (7) with $N = 2$ gives the beam splitter, while the most popular forms of squeezing (single mode and two mode) are particular cases of (8) for $N = 1,2$.

Note that the above fundamental unitaries are special cases of the general Gaussian unitary $U = \mathrm{e}^{-iH/2}$ with H a Hamiltonian, quadratic in the creation and annihilation operators collected in a_* and a. As we shall see below, all Gaussian transformations are obtained as a combination of these operators, and the corresponding Gaussian states are typically generated starting from replicas of vacuum states or of coherent states.

We are particularly interested in the cascade combination, where one can switch the order of operators with an appropriate change in the parameters [7]

$$D(\alpha)\,S(z) = S(z)\,D(\beta), \quad \beta = \cosh(r)\,\alpha - \sinh(r)\,\mathrm{e}^{i\theta}\,\alpha_* \tag{9}$$

$$S(z)\,R(\phi) = R(\phi)\,S(z_0), \quad z_0 = \mathrm{e}^{-i\phi}\,z\,\mathrm{e}^{-i\phi^{\mathrm{T}}} \tag{10}$$

$$D(\alpha)\,R(\phi) = R(\phi)\,D(\beta), \quad \beta = \alpha\,\mathrm{e}^{-i\phi}. \tag{11}$$

D. Most general Gaussian unitary

The importance of the fundamental unitaries lies in the following.

Theorem 1. The most general Gaussian unitary is given by the cascade combination of the three fundamental Gaussian unitaries: $S(z)$, $D(\alpha)$, and $R(\phi)$, cascaded in any arbitrary order by a proper adjustment of the parameters.

The proof can be obtained for the general multimode using the Lie algebra. Ma and Rhodes [7], generalizing a previous result obtained for the single mode [14,15], proved that a unitary operator $\mathrm{e}^{-iH/2}$, where H is a general N-mode

quadratic Hamiltonian, can be written in the form

$$U = e^{i\gamma}\, S(z)\, D(\alpha)\, R(\phi), \tag{12}$$

where the phasor $e^{i\gamma}$ with $\gamma \in \mathbb{R}$ is irrelevant for the state generation. On the other hand, we can apply the switching rules (10) and (11) to change the order of the fundamental unitaries in (12), with appropriate modifications of the parameters.

In phase space a Gaussian unitary is equivalent to a symplectic map (4), specified by the pair (S,d). The Gaussian unitary can always be written in the form $U_{S,d} = D(\alpha)U_S$, where U_S corresponds to the map $q_p \to Sq_p$ and the displacement operator $D(\alpha)$ in the phase space provides the displacement $q_p \to q_p + d$, with $d_{2i-1} = \mathrm{Re}\,\alpha_i$ and $d_{2i} = \mathrm{Im}\,\alpha_i$.

E. Most general Gaussian state

The most general Gaussian state can be derived by combination of the *thermal decomposition* and Theorem 1.

In a Gaussian state with the pair $(V,\overline{X})$, the covariance matrix V and the mean vector $\overline{X}$ can be handled separately. The covariance matrix V is fully described by powerful Williamson's theorem, which states that an N-mode covariance matrix V can be decomposed in the form

$$\boxed{V = S_w\, V^{\oplus}\, S_w^{\mathrm{T}}, \quad V^{\oplus} = \mathrm{diag}\,\left[\sigma_1^2,\sigma_1^2,\ldots,\sigma_N^2,\sigma_N^2\right]}, \tag{13}$$

where S_w is a $2N \times 2N$ symplectic matrix and the σ_i^2 are positive real values, called the *symplectic eigenvalues* of V.

The application of Williamson's theorem gives the so-called *thermal decomposition* of a Gaussian state [4], that is, an arbitrary N-mode zero-mean Gaussian state can be generated by the *tensor product of N single-mode thermal states*, with covariance matrix $V_k = \sigma_k^2\, I_2$, where I_2 is the 2×2 identity, and number of thermal photons $\mathcal{N}_k = \frac{1}{2}(\sigma_k^2 - 1)$. In fact, a single-mode thermal state is specified by a covariance matrix $\sigma^2 I_2$, with average photon number $\mathcal{N} = \frac{1}{2}(\sigma^2 - 1)$. Now, according to (13), the N-mode Gaussian state with the diagonal covariance matrix $V^{\oplus}$ is given by

$$\rho_{\mathrm{th}}(0,V^{\oplus}) = \rho\big(0,\sigma_1^2\, I_2\big) \otimes \cdots \otimes \rho\big(0,\sigma_N^2\, I_2\big). \tag{14}$$

However, by Theorem 1, we know that U_S can be written as the cascade combination $U_S = S(z)\, R(\phi)$ or $U_S = R(\phi)\, S(z)$. Then, a zero-mean Gaussian state with covariance matrix V is generated from $\rho_{\mathrm{th}}(0,V^{\oplus})$ in the form $\rho(0,V) = U_S\, \rho_{\mathrm{th}}(0,V^{\oplus})\, U_S^*$, where U_S is the unitary operator corresponding to the symplectic transformation S_w of decomposition (13).

A Gaussian state with *non-zero mean* is generated by introducing in $\rho(d,V)$ an appropriate displacement operator. In conclusion, by the combination of the previous statements the following theorem holds.

Theorem 2. The most general N-mode Gaussian state is generated from thermal state (14) by application of the three fundamental unitaries as

$$\rho(d,V) = D(\alpha)\, R(\phi)\, S(z)\, \rho_{\mathrm{th}}(0,V^{\oplus})\, S^*(z)\, R^*(\phi)\, D^*(\alpha), \tag{15}$$

where the order $D(\alpha)\, R(\phi)\, S(z)$ can be permuted according to (10) and (11).

For the particular case of pure states, the thermal decomposition degenerates into the product of N replicas of the vacuum state, say $|0_N\rangle$, and then $\rho(d,V) = |\psi(d,V)\rangle\langle\psi(d,V)|$, with $|\psi(d,V)\rangle = D(\alpha)\, R(\phi)\, S(z)\, |0_N\rangle$. But we can invert the order of squeezing and rotation with the rules (10) and (11) and after the change, $R(\phi)|0_N\rangle = |0_N\rangle$. In conclusion, we present the following corollary.

Corollary 1. The most general N-mode pure Gaussian state is obtained from the N replica of the vacuum $|0_N\rangle$ as

$$|\psi(d,V)\rangle = D(\alpha)\, S(z)\, |0_N\rangle \;:=\; |z,\alpha\rangle. \tag{16}$$

In other words, the most general N-mode Gaussian pure state is a squeezed-displaced state or a displaced-squeezed state.

III. GEOMETRICALLY UNIFORM SYMMETRY WITH GAUSSIAN STATES

The context of GUS is provided by *QC systems* where the transmission of classic information uses quantum states as physical carriers. A classical source emits a symbol A belonging to a set of K elements, $A \in \mathcal{A} = \{0,1,\ldots,K-1\}$, with assigned *a priori* probabilities $q_i = P[A = i], i \in \mathcal{A}$. The transmitter (Alice) encodes the symbol A into a quantum state $|\gamma_A\rangle$ in a *constellation* of K pure states $\{|\gamma_0\rangle,\ldots,|\gamma_{K-1}\rangle\}$, and more generally, in a constellation of mixed states with density operators $\{\rho_0,\ldots,\rho_{K-1}\}$.

The receiver (Bob) performs a quantum measurement from the received state ρ_A with positive-operator valued measure (POVM) measurement operators $\{P_k, k \in \mathcal{A}\}$. On the basis of the measurement, Bob estimates the state sent by Alice. The *correct decision probability* is [16]

$$P_c = \sum_{i\in\mathcal{A}} q_i\, \mathrm{Tr}(\rho_i\, P_i). \tag{17}$$

The choice of the measurement operators maximizing P_c is a (generally difficult) key problem in QC. In particular, if Alice uses pure states, i.e., $\rho_i = |\gamma_i\rangle\langle\gamma_i|$, according to Kennedy's theorem [17], the optimal POVM have rank one $P_i = |\mu_i\rangle\langle\mu_i|$, where the μ_i are called *measurement vectors* and (17) becomes

$$P_c = \sum_{i\in\mathcal{A}} q_i\, |\langle\mu_i|\gamma_i\rangle|^2\,. \tag{18}$$

A. Definition of GUS

Since the beginning of QC [16,18] particular attention has been paid to constellations enjoying a high degree of symmetry with uniform *a priori* probabilities. The interest of this case resides both in the fact that it corresponds to many practical situations and that the optimal measurements are easy to obtain [5,6,10,19]. We now define the GUS for pure states and we assume equiprobable symbols, $q_i = 1/K$, but the definition can be extended to generic *a priori* probabilities q_i substituting the states with the weighted states $\sqrt{q_i}|\gamma_i\rangle$ or $q_i\ \rho_i$ (see [10]).

A constellation of K pure states $\{|\gamma_0\rangle,|\gamma_1\rangle,\ldots,|\gamma_{K-1}\rangle\}$ has the *geometrically uniform symmetry* when the two properties are verified. (1) There exists a unitary operator Q with the property $Q^K = I_{\mathcal{H}^{\otimes N}}$, where $I_{\mathcal{H}^{\otimes N}}$ is the identity operator of

$\mathcal{H}^{\otimes N}$, and (2) the K states $|\gamma_i\rangle$ are obtained from a single reference state $|\gamma_0\rangle$ in the following way

$$|\gamma_i\rangle = Q^i|\gamma_0\rangle, \quad i = 0,1,\ldots,K-1. \tag{19}$$

The operator Q, which is given by a Kth root of the identity operator, is called the *symmetry operator*. Thus, in the presence of the GUS, the specification of the constellation is limited to the symmetry operator Q and to the reference state $|\gamma_0\rangle$. In addition, it simplifies the quantum decision because we can choose the POVMs of the form $P_i = |\mu_i\rangle\langle\mu_i|$, where the μ_i (measurement vectors) have the same symmetry as the states, that is, $|\mu_i\rangle = Q^i|\mu_0\rangle$, $i = 0,1,\ldots,K-1$.

B. GUS with Gaussian states

We now investigate the possibility that a constellation of Gaussian states have GUS. Let $\mathcal{S} = \{|\psi(p)\rangle, p \in \mathcal{P}\}$ be a class of pure quantum states, dependent on a parameter p. The class is *closed with respect to rotations* if $R(\phi)|\psi\rangle \in \mathcal{S}$, where $R(\phi)$ is the rotation operator. With such a class we can construct constellations of any order K with the GUS property. In practice in the single mode we get a K-ary PSK constellations, by choosing an arbitrary reference state $|\psi_0\rangle$ in $\mathcal{S}$ and using as symmetry operator $Q = R(2\pi/K)$. In the multimode a relevant application is given by the PPM (see below). We know that the new state is still Gaussian, but we want to find the new parameters α and z determined by the rotation. We apply relation (11) to get $R(\phi)\,D(\alpha) = D(\mathrm{e}^{i\phi}\,\alpha)\,R(\phi)$. Next we apply (11) to get $R(\phi)\,S(z) = S(\mathrm{e}^{i\phi}\,z\,\mathrm{e}^{i\phi^{\mathrm{T}}})\,R(\phi)$. Hence

$$\begin{aligned}|\psi(z,\alpha,\phi)\rangle &= D(\mathrm{e}^{i\phi}\,\alpha)\,S\left(\mathrm{e}^{i\phi}z\,\mathrm{e}^{i\phi^{\mathrm{T}}}\right)\,R(\phi)\,|0_N\rangle \\ &:= |z,\alpha,\phi\rangle.\end{aligned} \tag{20}$$

But $R(\phi)|0_N\rangle = |0_N\rangle$, so that the rotation can be dropped. In conclusion the rotation modifies the parameters in the form

$$z = \to\ \mathrm{e}^{i\phi}z\,\mathrm{e}^{i\phi}, \quad \alpha\ \to\ \alpha\,\mathrm{e}^{i\phi}, \tag{21}$$

and we have the following theorem.

Theorem 3. The class of pure displaced-squeezed states is closed under rotations. A rotated-displaced-squeezed state can be obtained from a displaced-squeezed state by modification of the squeeze factor and of the displacement amount as

$$\boxed{|z,\alpha,\phi\rangle = |\mathrm{e}^{i\phi}z\,\mathrm{e}^{i\phi^{\mathrm{T}}},\mathrm{e}^{i\phi}\,\alpha\rangle}. \tag{22}$$

With reference to the class $\mathcal{S} = \{|\psi(p)\rangle, p \in P\}$ the statement of Theorem 3 can be formulated as follows. The class $\mathcal{S}$ becomes explicitly the class of squeezed displaced states with the correspondence

$$p = (z,\alpha), \quad P = \mathbb{C}^2, \quad |\psi(p)\rangle = |(z,\alpha)\rangle. \tag{23}$$

If $p_0 = (z_0,\alpha_0) \in \mathbb{C}^2$ is an arbitrary value of p, after the rotation, the parameter becomes

$$p_\phi = (z_\phi,\alpha_\phi) = (\mathrm{e}^{i\phi}z\,\mathrm{e}^{i\phi},\alpha\,\mathrm{e}^{i\phi}). \tag{24}$$

The statement can be reformulated also in the phase space as follows. Let $V(p) = V(z,\alpha)$ be the covariance matrix of the squeezed displaced state $|(z,\alpha)\rangle$, then the rotation provides the change

$$V(z_0,\alpha_0) \to V(z_\phi,\alpha_\phi) = S_{\mathrm{rot}}(\phi)\,V(z_0,\alpha_0)\,S_{\mathrm{rot}}^{\mathrm{T}}(\phi), \tag{25}$$

where $S_{\mathrm{rot}}(\phi)$ is the symplectic matrix of the rotation transformation, which is given by [7]

$$S_{\mathrm{rot}}(\phi) = \begin{bmatrix}\cos\phi & -\sin\phi \\ \sin\phi & \cos\phi.\end{bmatrix} \tag{26}$$

C. Extension of the GUS to mixed Gaussian states

First, the definition of GUS can be extended to mixed states as follows. A constellation of K density operators $\{\rho_0,\rho_1,\ldots,\rho_{K-1}\}$ has GUS when the two properties are verified: (1) there exists a unitary operator Q with the property $Q^K = I_{\mathcal{H}}$ and (2) the K density operators ρ_i are obtained from a single reference density operator ρ_0 in the following way

$$\rho_i = Q^i\rho_0\,(Q^i)^*, \quad i = 0,1,\ldots,K-1. \tag{27}$$

This extension is in harmony with the fact that with pure states the density operators become $\rho_i = |\gamma_i\rangle\langle\gamma_i|$. In addition, with the factorization of the density operators $\rho_i = \gamma_i\gamma_i^*$, relation (27) gives $\gamma_i = Q^i\gamma_0$, which generalizes (19). In the context of optimal decision [11] the POVMs can be chosen in the form $P_i = \mu_i\mu_i^*$, where the *measurement factors* have the symmetry $\mu_i = Q^i\mu_0$, $i = 0,1,\ldots,K-1$.

In terms of the characterization of Gaussian states, the previous results obtained for pure states cannot be extended straightforwardly to the whole class of mixed Gaussian states. In fact, the critical point in the proof of Theorem 3 is represented by the relation $R(\phi)|0_N\rangle = |0_N\rangle$, in which the ground state $|0_N\rangle$ "absorbs the rotation." This property does not hold when the ground state is replaced by a general thermal state.

We remind that a general Gaussian channel [13] is completely specified by a triplet (E,ℓ,F), where E and F are $2N \times 2N$ real matrices and $\ell \in \mathbb{R}^{2N}$. A Gaussian channel transforms the mean $\overline{X}$ and the covariance matrix V of an input state ρ in the form

$$\overline{X}\ \to\ E^{\mathrm{T}}\,\overline{X} + \ell, \quad V\ \to\ E^{\mathrm{T}}\,V\,E + F. \tag{28}$$

To get useful results we have to limit the class of mixed states to a suitable subclass of Gaussian states obtained in the following way, which comprises all the cases of interest for the applications. We suppose that a pure Gaussian state $|\psi(p)\rangle$ is sent through a Gaussian channel specified by the triplet (E,ℓ,F). At the output the noisy state is still Gaussian, but mixed, with a density operator $\rho(\psi(p))$ as in Fig. 1. We

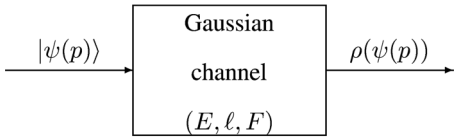

FIG. 1. A pure Gaussian state $|\psi(p)\rangle$ is sent through a Gaussian channel specified by the triplet (E,ℓ,F). The state at the output is still Gaussian, but in general mixed and described by the density operator $\rho(\psi(p))$.

denote by $\mathcal{S}_{(E,\ell,F)} = \{\rho(\psi), p \in P\}$ this restricted subclass of Gaussian mixed states.

Theorem 4. The class of states $\mathcal{S}_{(E,\ell,F)} = \{\rho(\psi(p))\}$, obtained at the output of a Gaussian channel with input pure Gaussian states, is closed under rotations, provided that the matrix E commutes with the rotation matrix $S_{\rm rot}(\phi)$ and F has the form $f\, I_{2N}$, with f a scalar.

Proof. The mean vector is modified as $\overline{X} \rightarrow E^{\rm T}\,\overline{X} + \ell$, while the covariance matrix is modified as

$$V \rightarrow E^{\rm T}\, V\, E + F. \tag{29}$$

Consider a generic generic pure state $|\psi(p_0)\rangle$ in the class $\mathcal{S}$ with covariance $V(p_0)$. Let $V(p_\phi)$ be the covariance matrix after the rotation ϕ in the class $\mathcal{S}$, obtained according to (25). Then

$$S_{\rm rot}(\phi)(E^{\rm T}V(p_0)E + F)S_{\rm rot}(\phi)^{\rm T} = E^{\rm T}V(p_\phi)E + F. \tag{30}$$

In fact,

$$\begin{aligned} &S_{\rm rot}(\phi)(E^{\rm T}V(p_0)E + F)S_{\rm rot}(\phi)^{\rm T} \\ &\quad = S_{\rm rot}(\phi)E^{\rm T}V(p_0)E\,S_{\rm rot}(\phi)^{\rm T} + S_{\rm rot}(\phi)F\,S_{\rm rot}(\phi)^{\rm T} \\ &\quad = E^{\rm T}S_{\rm rot}(\phi)V(p_0)S_{\rm rot}(\phi)^{\rm T}E + f\,S_{\rm rot}(\phi)I_{2N}\,S_{\rm rot}(\phi)^{\rm T}, \end{aligned} \tag{31}$$

where $S_{\rm rot}(\phi)$ verifies the condition $S_{\rm rot}(\phi)S_{\rm rot}^{\rm T}(\phi) = I_{2N}$. Hence the conclusion. ■

This model includes the most relevant cases [13,20], such as the following.

(1) The *classical noise channel*, which merely adds classical Gaussian noise to a quantum state, i.e., $E = I_{2N}$, $f \geqslant 0$.

(2) The *lossy (or attenuation) channel* in which $E = \sqrt{\eta} I_{2N}$ and $F = (1-\eta)\, I_{2N}$, with $\eta < 1$ so that $V \rightarrow \eta\, V + (1-\eta) I_{2N}$. This is the model, for example, for the propagation along an optical fiber, where each photon is lost with probability $(1-\eta)$.

(3) The *amplification channel* in which $E = \sqrt{\eta} I_{2N}$ and $F = (\eta - 1)\, I_{2N}$, with the gain $\eta > 1$, so that $V \rightarrow \eta\, V + (\eta - 1) I_{2N}$.

(4) The *thermal noise channel* also called sometimes the *attenuation channel* [13], with $E = \sqrt{\eta} I_{2N}$ and $F = (1-\eta)\sigma^2\, I_{2N}$, with $\eta < 1$ and $\sigma^2\, I_{2N}$, $\sigma^2 \geqslant 1$ is the covariance matrix of a thermal state with average photon number $\mathcal{N} = (\sigma^2 - 1)/2$.

Remark. Note that in these channels the assumption is that the parameters are the same for all the N modes. In particular, for the thermal noise channel, in all the modes the average number of thermal photons is considered the same. In general, denoting by σ_k^2 the thermal contribution in the k mode, the matrix F in the covariance relation should be modified as

$$F = (1-\eta) \bigoplus_{k=1}^{N} \sigma_k^2\, I_2.$$

However, the assumption $\sigma_k^2 = \sigma^2$ is acceptable for PPM or other modulations in quantum communications.

IV. EXAMPLES OF APPLICATIONS

In this section we recall the quantum detection based on the square-root measurements (SRM) in general and then in the presence of GUS. Finally we give an explicit application to PPM.

A. SRM in general

In the case of pure states, the measurement vectors $|\mu_i\rangle$ are chosen with the criterion of making the differences between the states and the measurement vectors $|e_i\rangle = |\gamma_i\rangle - |\mu_i\rangle$ as small as possible and we look for *the measurement vectors* $|\mu_i\rangle$*, which minimize the quadratic error* [10]

$$\mathcal{E} = \sum_{i=0}^{K-1} \langle e_i | e_i \rangle = \sum_{i=0}^{K-1} (\langle \gamma_i | - \langle \mu_i |)(|\gamma_i\rangle - \mu_i\rangle) \tag{32}$$

with the constraint of the resolution of the identity $\sum_{i=0}^{K-1} |\mu_i\rangle\langle\mu_i| = I_{\mathcal{H}}$.

The evaluation of the measurement vector is obtained by computing the inner products $\langle\gamma_i|\gamma_j\rangle$ between the states of the constellation, thus obtaining the *Gram's matrix*

$$\underset{K\times K}{G} = \Gamma^* \Gamma = [\langle\gamma_i|\gamma_j\rangle], \quad i,j = 0,\ldots,K-1. \tag{33}$$

Then we evaluate, by eigendecomposition, the square root and the inverse square root $G^{\pm 1/2}$. The measurement vectors are given explicitly by

$$|\mu_i\rangle = \sum_{j=0}^{K-1} (G^{-1/2})_{ij} |\gamma_j\rangle. \tag{34}$$

The transition probabilities result in $p_c(j|\, i) = |(G^{\frac{1}{2}})_{ij}|^2$, from which we obtain the correct decision probability

$$P_c = \frac{1}{K} \sum_{i=0}^{K-1} |(G^{\frac{1}{2}})_{ii}|^2. \tag{35}$$

The advantage of the SRM method is that it gives explicit results for any constellation, that is, for any modulation format.

B. SRM in the presence of GUS

When the constellation has the GUS, the Gram's matrix becomes *circulant*. In fact, the inner products result in $G_{ij} = \langle\gamma_i|\gamma_j\rangle = \langle\gamma_0|(Q^*)^i Q^j|\gamma_0\rangle = \langle\gamma_0|Q^{j-i}|\gamma_0\rangle$ and depend upon the difference $i - j \pmod K$. This property provides two advantages. (1) The performance evaluation becomes easier with the technique of the discrete Fourier transform (DFT) and (2) the corresponding quantum detection becomes optimal [10,21].

The eigendecomposition of the circulant Gram matrix is simply given by $G = W^* \Lambda W$, where $\Lambda = \text{diag}\ [\lambda_0, \lambda_1, \ldots, \lambda_{K-1}]$ collects the eigenvalues and W is the $K \times K$ DFT matrix $W = K^{-\frac{1}{2}}[W_K^{-rs}]$, $r,s = 0,\ldots,K-1$, with $W_K := \mathrm{e}^{i2\pi/K}$. Moreover, the eigenvalues are given by the DFT of the first row of G

$$\lambda_p = \sum_{q=0}^{K-1} G_{0q}\, W_K^{-pq}. \tag{36}$$

The square roots of G are simply obtained as $G^{\pm\frac{1}{2}} = W^* \Lambda^{\pm\frac{1}{2}} W$ and the transition probabilities are

$$p_c(j|i) = \left| \frac{1}{K} \sum_{p=0}^{K-1} \lambda_p^{\frac{1}{2}} W_K^{-p(i-j)} \right|^2, \quad i,j = 0,1,\ldots,K-1. \tag{37}$$

In particular, the diagonal transition probabilities are all equal $p_c(i|i) = [\frac{1}{K} \sum_{p=0}^{K-1} \lambda_p^{\frac{1}{2}}]^2$, independent of i, and the correct decision probability (35) becomes explicitly

$$P_c = \left[\frac{1}{K} \sum_{p=0}^{K-1} \lambda_p^{\frac{1}{2}} \right]^2. \tag{38}$$

It is possible to obtain the explicit expression of the measurement vectors $|\mu_i\rangle$, given by $|\mu_0\rangle = \sum_{j=0}^{K-1} (G^{-1/2})_{ij} |\gamma_j\rangle$.

C. Extension of the SRM to mixed Gaussian states

The SRM method can be extended to mixed states. The preliminary step is the factorization of the density operators $\rho_i = \gamma_i \gamma_i^*$ and it can be shown [11] that the measurement operators can be factored as the density operators $P_i = \mu_i \mu_i^*$, where the rank of μ_i is the same as that of γ_i.

In this case the error is considered between the state factors and the measurement factors $e_i = \gamma_i - \mu_i$. From the factors γ_i, we first form the Gram matrix $G = [\gamma_i^* \gamma_j]_{i,j=0,1,\ldots,K-1}$, then from the square roots $G^{\pm 1/2}$ we can obtain both the measurement factors μ_i and the transition probabilities in a similar way as for the pure states.

The SRM method always leads to explicit results and, in general, provides a good overestimation of the error probability, also compared to other suboptimal methods such as the Chernoff bound [12].

D. Application to pulse position modulation

Pulse position modulation (PPM) is widely adopted in free-space optical transmission, and is a candidate for deep-space transmission, also in quantum form. Here we evaluate the error probability in K-ary quantum optical PPM systems, considering the most general Gaussian states.

In the quantum PPM the modulation format and the states belong to a composite Hilbert space, given by the tensor product $\mathcal{H} = \mathcal{H}_0 \otimes \mathcal{H}_0 \otimes \cdots \otimes \mathcal{H}_0$ of K equal Hilbert spaces $\mathcal{H}_0$ [18,22], where $\mathcal{H}_0$ has dimension n and $\mathcal{H}$ has dimension $N = n^K$

$$|\gamma_i\rangle = |\gamma_{i,0}\rangle \otimes |\gamma_{i,1}\rangle \otimes \cdots \otimes |\gamma_{i,K-1}\rangle, \quad i = 0,1,\ldots,K-1. \tag{39}$$

Considering Gaussian states, with the most general squeezed-displaced states, symbolized by $|z,\alpha\rangle$, the natural choice for PPM is to associate the symbol 0 to the ground state $|\gamma_{ik}\rangle = |0,0\rangle$ and to the symbol 1 the generic state $|\gamma_{ik}\rangle = |z,\alpha\rangle$. With this choice (39) represents a constellation of K-mode Gaussian States. For instance, for $K = 3$ we have country="Italy" explicitly

$$\begin{aligned} |\gamma_0\rangle &= |z,\alpha\rangle \otimes |0,0\rangle \otimes |0,0\rangle, \\ |\gamma_1\rangle &= |0,0\rangle \otimes |z,\alpha\rangle \otimes |0,0\rangle, \\ |\gamma_2\rangle &= |0,0\rangle \otimes |0,0\rangle \otimes |z,\alpha\rangle. \end{aligned} \tag{40}$$

Note that, without loss of generality, we can choose a real displaced parameter α, while we let a generic complex squeezing factor $z = r\, e^{i\theta}$.

The application of GUS to PPM is not trivial because the states are multimode. The symmetry operator Q is given by [22,23]

$$Q = \sum_{k=0}^{n-1} w_n(k) \otimes I_{N'} \otimes w_n^{\mathrm{T}}(k), \quad N' = n^{K-1}, \tag{41}$$

where $\otimes$ is the Kronecker's product, $w_n(k)$ is a column vector of length n with null elements except for one unitary element at position k, and $I_{N'}$ is the $N' \times N'$ identity matrix. Then Q has dimension $N = n^K$ and the property $Q^K = I_N$.

Now, it is not immediate to see that Q is a rotation operator, that is, of the form $R(\phi) = \mathrm{e}^{i\phi}$, with ϕ an $N \times N$ Hermitian matrix. To find the "phase" ϕ we use the eigen-decomposition (EID) of S written in the form $Q = \sum_{m=0}^{K-1} \lambda_m P_m$ where $\lambda_m = \mathrm{e}^{i2\pi m/K} := W_K^m$ are the K distinct eigenvalues and P_m are K orthogonal projectors. In this EID the eigenvalues are known, while the projectors should be evaluated from the the expression (41), which defines a complicated permutation matrix. The alternative is the evaluation through the powers of Q, $Q^k = \sum_{m=0}^{K-1} W_K^{mk} P_m$. According to this relation $[Q^0, Q^1, \ldots, Q^{K-1}]$ turns out to be the DFT of $[P_0, P_1, \ldots, P_{K-1}]$. Thus, taking the inverse DFT one gets $P_m = \frac{1}{K} \sum_{k=0}^{K-1} W_K^{-mk} Q^k$, which is easy to evaluate. Next we recall that Q is unitary and therefore it can be written in the form $Q = \mathrm{e}^{i\,\phi}$, where ϕ is a Hermitian matrix. Then, by comparison to the EID of Q we find that the EID of ϕ is given by

$$\phi = \sum_{m=0}^{K-1} \frac{2\pi m}{K} P_m, \tag{42}$$

where the eigenvalues become $2\pi\, m/K$ and the projectors are the same as in the EID of Q.

Example. We give an example with $K = 3$ and $n = 2$, where the matrices are 8×8. The symmetry operator is

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}. \tag{43}$$

The projectors $[P_0, P_1, P_2]$ are obtained by the DFT of $[Q^0, Q^1, Q^2]$ and finally we have the phase matrix ϕ from(42).

It reads

$$\phi = \frac{3}{\pi}\begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & -1-\frac{i}{\sqrt{3}} & 0 & -1+\frac{i}{\sqrt{3}} & 0 & 0 & 0 \\ 0 & -1+\frac{i}{\sqrt{3}} & 2 & 0 & -1-\frac{i}{\sqrt{3}} & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & -1+\frac{i}{\sqrt{3}} & -1-\frac{i}{\sqrt{3}} & 0 \\ 0 & -1-\frac{i}{\sqrt{3}} & -1+\frac{i}{\sqrt{3}} & 0 & 2 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1-\frac{i}{\sqrt{3}} & 0 & 2 & -1+\frac{i}{\sqrt{3}} & 0 \\ 0 & 0 & 0 & -1+\frac{i}{\sqrt{3}} & 0 & -1-\frac{i}{\sqrt{3}} & 2 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}. \tag{44}$$

We can verify (e.g., with MATHEMATICA) that $e^{i\phi} = Q$ and that $e^{iK\phi} = I_N$.

E. Statistics of the quantum states in PPM

To evaluate the error probability of QC systems with PPM we need the following statistics of the single-mode state $|z,\alpha\rangle$.

(1) The mean photon number, which is given by [24]

$$\bar{N}_{|z,\alpha\rangle} = |\alpha|^2 + \sinh^2(r). \tag{45}$$

Then all the K PPM symbols have the same *mean number of photons per symbol*, given by

$$N_s = |\alpha|^2 + \sinh^2(r). \tag{46}$$

(2) The inner product between two states was evaluated by Yuen [24] and reads

$$\langle z_1,\alpha_1|z_0,\alpha_0\rangle = A^{-\frac{1}{2}} \exp\left[-\frac{A(|\beta_1|^2+|\beta_0|^2) - 2\beta_1\beta_0^* + B\,\beta_1^{*2} - B^*\beta_0^2}{2A}\right], \tag{47}$$

where $\mu_i = \cosh(r_i)$, $\nu_i = \sinh(r_i)e^{i\theta_i}$, $\beta_i = \mu_i\alpha_i - \nu_i\alpha_i^*$, $A = \mu_0\mu_1^* - \nu_0\nu_1^*$, $B = \nu_0\mu_1 - \mu_0\nu_1$.

F. Error probability in the quantum PPM

The analysis of a quantum PPM system (limited to coherent states) has been done in a famous article by Yuen, Kennedy, and Lax [18] who found the optimal elementary projectors using an algebraic method developed "ad hoc" for this kind of modulation. In [22] we proposed an original method based on the SRM, which gave the minimum error probability for the GUS of the quantum PPM. Also in [22] the analysis was limited to coherent states. Here we extend the evaluation to general Gaussian states.

In the SRM the error probability depends only on the inner product between the single-mode states $|z,\alpha\rangle$ and $|0,0\rangle$. In fact, the Gram matrix is given by

$$G = \begin{bmatrix} 1 & \Gamma & \dots & \Gamma \\ \Gamma & 1 & \dots & \Gamma \\ \vdots & & \ddots & \\ \Gamma & \Gamma & \dots & 1 \end{bmatrix}, \tag{48}$$

where $\Gamma := |\langle z,\alpha|0,0\rangle|^2$.

About the inner product

The squared inner product can be written in the form

$$\Gamma = \frac{1}{\cosh r}\exp[-\alpha^2\, f(r,\theta)], \tag{49}$$

where

$$f(r,\theta) = \cosh(2r) + \tanh(r)\sinh(2r) - [\sinh(2r) + \tanh(r)\cosh(2r)]\cos\theta\,. \tag{50}$$

Clearly, for r and α given, Γ has a minimum for $\theta = \pi$, as shown in Fig. 2. The interpretation in the phase space may be the following. In the phase space, thinking to the Wigner function, an inner product as $\langle re^{i\theta},\alpha|0,0\rangle$ depends on the

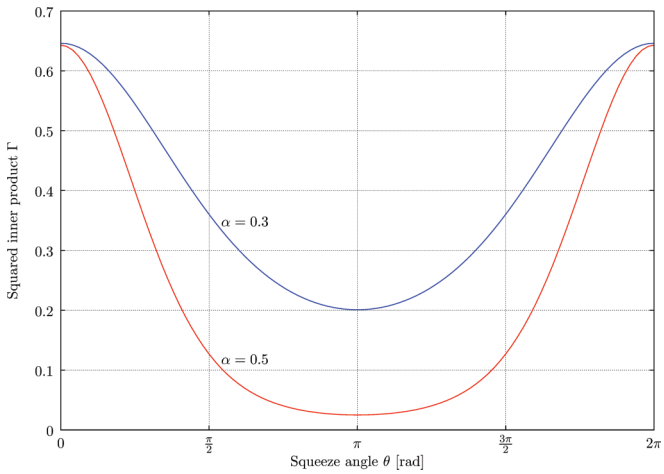

FIG. 2. (Color online) Squared inner product $\Gamma = |\langle re^{i\theta},\alpha|0,0\rangle|^2$ versus the phase θ for $r = 1.0$ and two values of the displacement.

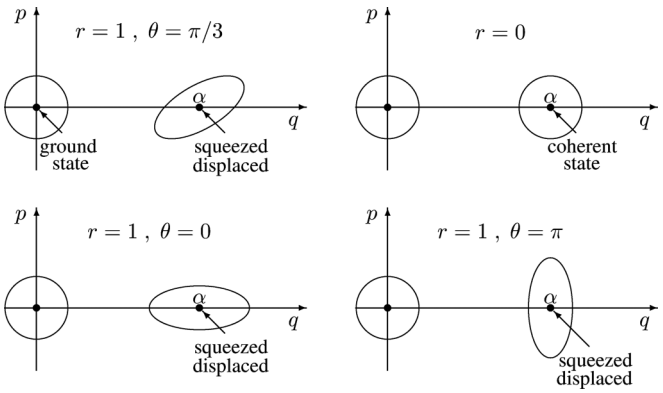

FIG. 3. Representation of the states $|z,\alpha\rangle$ and $|0,0\rangle$ in the phase space for different values of $z = r\,e^{i\theta}$. Pictorially the noise variances are represented by a tilted "error ellipse."

distance between the two states, which is provided by the displacement α, but also on the "orientation" of the squeezing, which is determined by the phase θ. We know that in a squeezed displaced state $|re^{i\theta},\alpha\rangle$ the noise variances are different and pictorially this difference can be represented by a tilted ellipse, as shown in Fig. 3. The ellipse degenerates into a circle in the case of a coherent state (and for the ground state). With the objective to minimize the error probability, the minimum value of Γ is sought. From the figure we can easily realize that a squeezing factor with $\theta = 0$ gives a worse error probability than the use of a coherent state, while the best performance is achieved with $\theta = \pi$.

The error probability computed from (35) becomes [22]

$$P_e = 1 - \frac{1}{K^2}(\sqrt{1+(K-1)\Gamma} + (K-1)\sqrt{1-\Gamma})^2, \quad (51)$$

in perfect agreement with the results of the findings in [18]. Also in this case P_e can be expressed in terms of the mean photon number per symbol N_s by writing Γ as

$$\Gamma = \frac{1}{\cosh r}\exp[-(N_s - \sinh^2 r)\ f(r,\theta)],$$
$$N_s \geqslant \sinh^2 r. \quad (52)$$

In the representation of the error probability it is convenient to consider as a variable the *average number of photons per bit* $N_R = N_s/\log_2 K$. We see in the expression of N_s (46) that a contribution comes from the displacement and one form the squeezing. If we fix a value of r, the minimum of N_s becomes $\sinh^2(r)$ and for $N_s < \sinh^2(r)$ there is no room for the displacement.

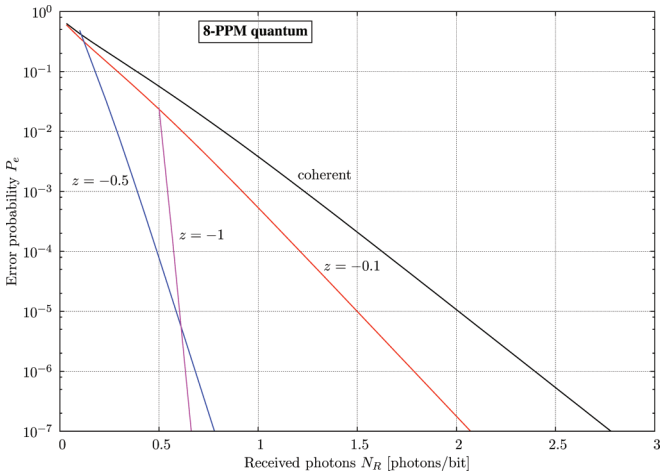

FIG. 4. (Color online) Error probability of quantum 8-PPM for coherent states and three values of squeezing. For $z = -0.1$ we must have $N_R \geqslant 3.3 \times 10^{-3}$, for $z = -0.5$, $N_R \geqslant 0.09$, and for $z = -1$, $N_R \geqslant 0.46$.

In Fig. 4 we present the error probability as a function of N_R for coherent states and the other three values of the squeezing factor. Note that by properly choosing the value of z one can reduce dramatically the error probability with respect to the use of coherent states.

V. CONCLUSION

We have seen that GUS plays a fundamental role in quantum communications due to the optimality of measurement operators obtained by the SRM in the quantum discrimination. The considerations on Gaussian states and their invariance properties with respect to unitary transformations and in particular rotations allow one to construct constellations of Gaussian states having GUS, for example, coherent states for their use in quantum optical communications. Moreover, the transmission of such states through and additive-noise channel preserves the GUS. The theory of the GUS applied to the most general Gaussian states extends the analysis of the performance of a QC system employing PPM (or other modulations with GUS) to the most general case, not limiting the evaluation to the case of coherent states.

ACKNOWLEDGMENTS

This work has been supported in part by the Project "Q-FUTURE" (Project No. STPD08ZXSJ) of the University of Padova.

[1] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, C. J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).

[2] S. Olivares and M. G. A. Paris, The European Physical Journal Special Topics **203**, 185 (2012).

[3] G. Adesso, S. Ragy, and A. R. Lee, Open Syst. & Inform. Dynamics **21**, 1440001 (2014).

[4] A. Ferraro, S. Olivares, and M. G. A. Paris, *Gaussian States in Continuous Variable Quantum Information* (Bibliopolis, Napoli, 2005).

[5] K. Kato, M. Osaki, M. Sasaki, and O. Hirota, IEEE Trans. Comm. **47**, 248 (1999).

[6] G. Cariolaro and G. Pierobon, IEEE Trans. Comm. **58**, 623 (2010).

[7] X. Ma and W. Rhodes, Phys. Rev. A **41**, 4625 (1990).
[8] E. S. Slusher and B. Yurke, J. Lightwave Techn. **4**, 466 (1990).
[9] P. Hausladen and W. K. Wooters, J. Modern Opt. **41**, 2385 (1994).
[10] Y. C. Eldar and G. D. Forney, Jr., IEEE Trans. on Inform. Theory **47**, 858 (2001).
[11] Y. C. Eldar, A. Megretski, and G. C. Verghese, IEEE Trans. on Inform. Theory **50**, 1198 (2004).
[12] R. Corvaja, Phys. Rev. A **87**, 042329 (2013).
[13] A. S. Holevo and V. Giovannetti, Rep. Prog. Phys. **75**, 046001 (2012).
[14] B. L. Schumaker, Phys. Rep. **135**, 317 (1986).
[15] X. Ma, J. Mod. Optics **36**, 1059 (1989).
[16] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic, New York, 1976).
[17] R. S. Kennedy, MIT Research Laboratory of Electronics Quarterly Progress Report No. 108, pp. 219–225, 1973.
[18] H. P. Yuen, R. S. Kennedy, and M. Lax, IEEE Trans. Inform. Theory **21**, 125 (1975).
[19] M. Ban, K. Kurokawa, R. Momose, and O. Hirota, Int. J. Theor. Phys. **36**, 1269 (1997).
[20] A. S. Holevo and R. F. Werner, Phys. Rev. A **63**, 032312 (2001).
[21] A. Assalini, G. Cariolaro, and G. Pierobon, Phys. Rev. A **81**, 012315 (2010).
[22] G. Cariolaro and G. Pierobon, IEEE Trans. Comm. **58**, 1213 (2010).
[23] H. V. Henderson and S. R. Searle, Linear and Multivariate Algebra **9**, 271 (1981).
[24] H. P. Yuen, Phys. Rev. A **13**, 2226 (1976).