Ann. Acad. Rom. Sci.
Ser. Math. Appl.
ISSN 2066-6594 Vol. 16, No. 1/2024

ENTANGLEMENT AND STEERING WITNESSES FOR GAUSSIAN STATES*

Tatiana Mihaescu† Aurelian Isar‡

Dedicated to Dr. Dan Tiba on the occasion of his 70th anniversary

Abstract

We present a short review on the subject of witnesses based on second moments as a primary tool for the efficient detection of entanglement and steering. In particular, we focus on the example of Gaussian states, which represent the core toolbox for the vast domain of continuous variable states. We fully define and characterise the entanglement and steering Gaussian witnesses, respectively, and then present a set of linear constraints as an alternative characterisation that allows for the implementation of a numerical optimisation semidefinite programming algorithm.

We have the great pleasure to dedicate this paper in the honour of Professor Dan Tiba on the occasion of his 70th Anniversary and to wish him a long life in good health and further success in his scientific activity.

DOI https://doi.org/10.56082/annalsarscimath.2024.1.114

MSC: 81P40, 81P42

Key words: witnesses based on second moments, entanglement witnesses, steering witnesses, Gaussian states, semidefinite programming.

*Accepted for publication on March 3-rd, 2024

†mihaescu.tatiana@theory.nipne.ro Department of Theoretical Physics, National Institute of Physics and Nuclear Engineering, Bucharest-Magurele, Romania.

‡isar@theory.nipne.ro Department of Theoretical Physics, National Institute of Physics and Nuclear Engineering, Bucharest-Magurele; Academy of Romanian Scientists, Bucharest, Romania.

The authors acknowledge the financial support received from the Romanian Ministry of Research, Innovation and Digitisation, through the Project PN 23 21 01 01/2023.

1 Introduction

Quantum entanglement is one the most prominent characteristics of quantum mechanics that is also crucial for the domain of quantum information [1]. Consider a composite bipartite quantum state $\hat{\rho} \in \mathcal{D}(\mathcal{H})$, with $\mathcal{D}(\mathcal{H})$ the set of density matrices defined across the bipartite split $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ of the global Hilbert space $\mathcal{H}$, where $\mathcal{H}_A$, $\mathcal{H}_B$ are local Hilbert spaces of the two subsystems traditionally associated with Alice (A) and Bob (B), respectively. The corresponding global state $\hat{\rho}$ is entangled if it cannot be written as a mixture of the convex combination of local states $\hat{\rho}_A \in \mathcal{D}(\mathcal{H}_A)$ and $\hat{\rho}_B \in \mathcal{D}(\mathcal{H}_B)$ [2],

$$\hat{\rho} \neq \sum_j p_j \; \hat{\rho}_A^{(j)} \otimes \hat{\rho}_B^{(j)}, \tag{1}$$

such that $\sum_j p_j = 1$. In other words, entanglement is present if there are no local states $\hat{\rho}_A$ and $\hat{\rho}_B$ such that the equality in Eq. (1) is fulfilled, otherwise such states are separable.

Quantum steering, on the other hand, is a stronger quantum correlation than entanglement, since it accounts not just for the inseparability between two parties, but also for the ability of one party to steer the state of the other party through local measurements [3, 4, 5]. The simplest quantum steering is featured in bipartite settings where Alice and Bob share a common quantum state $\hat{\rho}$ at distant locations, and one party, say Alice, can instantaneously steer the Bob's state into a number of distinct states emerging from different ensembles of states, depending on which local measurement she chooses to perform.

The alternative operational definition of steering states that $\hat{\rho}$ is steerable if Alice is able to convince Bob that the state they share is entangled. Let us denote by $\hat{M}_A$ the measurement performed by Alice on her system obtaining the outcome a, which she communicates to Bob. Next, Bob is measuring his part of the system and compares his results with the results Alice reported, based on which he then is able to rule out the possible scenario where Bob had a preexisting local hidden state (LHS) $\hat{\rho}_\lambda$ randomly drawn from some priori ensemble of states $F = \{p_\lambda \hat{\rho}_\lambda\}$. In this case Alice might have had some knowledge about the hidden variable λ and use it to mimic the probability distribution $P(a|\hat{M}_A, \lambda)$ such that the conditional state of Bob after Alice's measurements is given by [6, 7]:

$$\tilde{\rho}_B^A = \sum_\lambda P(a|\hat{M}_A, \lambda)\hat{\rho}_\lambda p_\lambda. \tag{2}$$

Therefore, Bob would have to check if there exists $P(a|\hat{M}_A, \lambda)$ such that the relation above holds, in which case Alice failed to convince Bob that she can steer his system.

Both correlations are extremely important for the today cutting edge technologies motivated by the quantum information science, such as quantum computation, quantum communication and quantum cryptography [2, 8]. A promising platform of experimental implementation of these applications is given by continuous variable (CV) systems featuring infinite-dimensional quantum systems [9]. Among them, a large amount of study is dedicated to the class of Gaussian states, which are the most commonly accessible in quantum optics setups, while featuring all the quantum correlations and being describable in an elegant mathematical formalism [10].

This article unfolds as follows. In Section 2 the essential tools for describing the CV systems are presented, aiming at introducing Gaussian states and the symplectic mathematical formalism. A subsection is dedicated to the entanglement and steering criteria based on variances of the canonical operators. Section 3 introduces and fully characterises the entanglement and steering witnesses based on second moments, also providing a proof for some of their properties. In Section 4 we introduce alternative linear constraints characterising the entanglement and steering witnesses, respectively, and present an optimisation algorithm based on semidefinite programming (SDP) capable of detecting quantum correlations in any given Gaussian state.

2 Preliminaries

Henceforth we will consider the continuous variable (CV) states of a bipartite system with $N_A \geq 1$ and $N_B \geq 1$ modes, describable in the infinite dimensional Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. The pair of selfadjoint canonical operators, arranged in a vector $\hat{R} = (\hat{R}_A, \hat{R}_B)^{\mathrm{T}} = \hat{R}_A \oplus \hat{R}_B$ with $\hat{R}_A = (\hat{x}_1, \hat{p}_1, \cdots, \hat{x}_{N_A}, \hat{p}_{N_A})$ and $\hat{R}_B = (\hat{x}_{N_A+1}, \hat{p}_{N_A+1}, \cdots, \hat{x}_N, \hat{p}_N)$, satisfy the canonical commutation relation (CCR) giving rise to the symplectic form on the phase space $\mathbb{R}^{2N} = \mathbb{R}^{2N_A} \oplus \mathbb{R}^{2N_B}$ [9, 10]:

$$[\hat{R}, \hat{R}^{\mathrm{T}}] = \mathrm{i}\ \Omega, \tag{3}$$

$$\Omega = \bigoplus_{1}^{N} \Omega_1, \quad \text{with} \quad \Omega_1 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \tag{4}$$

where Ω_1 denotes the symplectic matrix of one mode, and the commutator of row and column vectors should be taken as an outer product[1]. Throughout this paper we will denote by Ω_{N_A} and Ω_{N_B} the symplectic matrix defined on the subsystem of Alice and Bob, respectively.

A general approach in describing CV systems employs the phase space description of quantum quasiprobability distributions, and it hinges on the exponential form of the CCR by defining the Weyl operators [11],

$$\hat{D}(r) := \mathrm{e}^{\mathrm{i}\ r^{\mathrm{T}}\Omega\ \hat{R}}, \tag{5}$$

where $r^{\mathrm{T}} = (x_1, p_1, \ldots, x_N, p_N) \in \mathbb{R}^{2N}$ is a real vector of phase space variables. The Weyl operators, also known as the displacement operators, form a complete set which have been proven in the form of the Fourier-Weyl relation between density matrices and characteristic functions

$$\hat{\rho} = \frac{1}{(2\pi)^N} \int d^{2N}r\ \mathrm{Tr}[\hat{D}^\dagger(r)\hat{\rho}]\hat{D}(r), \tag{6}$$

with $d^{2N}r = dx_1dp_1 \ldots dx_Ndp_N$, and $\chi(r) = \mathrm{Tr}[\hat{D}^\dagger(r)\hat{\rho}]$ is the characteristic function. Gaussian states are described by a characteristic function of a particular form

$$\chi(r) = \mathrm{e}^{-\frac{1}{4}r^{\mathrm{T}}\Omega^{\mathrm{T}}\gamma\Omega r}\mathrm{e}^{\mathrm{i}\ r^{\mathrm{T}}\Omega^{\mathrm{T}}d}, \tag{7}$$

where $d = \mathrm{Tr}[\hat{R}\hat{\rho}] \in \mathbb{R}^{2N}$ is the vector of displacements representing the first order statistical moments, while γ is the associated bipartite covariance matrix (CM). The displacements can be set to zero via suitable local displacement transformations, whereas the CM with the entries given by the second order statistical moments,

$$\gamma = \mathrm{Tr}[\{(\hat{R} - d), (\hat{R} - d)^{\mathrm{T}}\}_+\hat{\rho}], \tag{8}$$

retains all the information about the quantum correlations present in the state. A generic CM is a real symmetric positive definite matrix, however a covariance matrix of a quantum state satisfies a stronger constraint imposed by the quantum uncertainty condition,

$$\gamma + \mathrm{i}\ \Omega \geq 0. \tag{9}$$

[1]For a vector of Hermitian operators $\hat{R}$, one has $\hat{R}\hat{R}^{\mathrm{T}} \neq (\hat{R}\hat{R}^{\mathrm{T}})^{\mathrm{T}}$. Therefore, it is useful to define the commutator as an outer product in the anti-symmetrized form as: $[\hat{R}, \hat{R}^{\mathrm{T}}] = \hat{R}\hat{R}^{\mathrm{T}} - (\hat{R}\hat{R}^{\mathrm{T}})^{\mathrm{T}}$.

The bipartite block representation of CM γ is defined as follows:

$$\gamma = \begin{pmatrix} \gamma_A & \gamma_C \\ \gamma_C^{\mathrm{T}} & \gamma_B \end{pmatrix}, \tag{10}$$

where γ_A and γ_B are $2N_A \times 2N_A$ and $2N_B \times 2N_B$ CMs pertaining to the quantum state of Alice and Bob, respectively, whereas γ_C is the correlation matrix between the two partitions.

The canonical transformations on the phase space variables which preserve the symplectic structure of the CCR are known as symplectic operations, which form the real symplectic group defined as [12]:

$$Sp(\mathbb{R}^{2N}) = \{S \in \mathcal{M}(\mathbb{R}^{2N}) : S\Omega S^{\mathrm{T}} = \Omega\}, \tag{11}$$

where S is a symplectic transformation acting as: $\hat{R}' = S\hat{R}$, and $\mathcal{M}(\mathbb{R}^{2N})$ denotes the set of $2N \times 2N$ real matrices. Every positive semidefinite matrix $M \geq 0$ can be brought to a diagonal form by a symplectic transformation as follows:

$$SMS^{\mathrm{T}} = \mathrm{diag}(s_1, s_1, \ldots, s_N, s_N), \tag{12}$$

where $s_1, \ldots, s_N \geq 0$ are the symplectic eigenvalues of M, and the symplectic trace of the matrix M is denoted as

$$\mathrm{str}[M] := \sum_{i=1}^{N} s_i. \tag{13}$$

2.1 Gaussian quantum entanglement and steering

As stated in the previous section, all the relevant information about quantum correlations in Gaussian states is contained in the associated CM, and therefore, separability in Eq. (1) is easily transferred to the phase space structure in terms of the local CMs, i.e. a CM γ of N modes is bi-separable if there exist local CMs $\sigma_A \geq \mathrm{i}\Omega_{N_A}$ and $\sigma_B \geq \mathrm{i}\Omega_{N_B}$ of N_A and N_B modes, respectively, such that [13]:

$$\gamma \geq \sigma_A \oplus \sigma_B. \tag{14}$$

Conversely, if this holds then any CV (not only Gaussian) states with CM γ are separable, which is opposite to entangled.

In order to characterise steering of Gaussian states we have to delve into the particularities of Gaussian measurements. Consider a positive Gaussian operator that describes the Gaussian measurement applied on the Alice subsystem $\hat{M}_A$ with the CM given by T^A satisfying the uncertainty relation criterion: $T^A + \mathrm{i}\Omega_{N_A} \geq 0$. The Bob conditional state after the measurement $\tilde{\rho}_B = \mathrm{Tr}_A[(\hat{M}_A \otimes \hat{I}_B)\hat{\rho}]$ represents also a Gaussian state with the CM given by: $\gamma_m^A = \gamma_B - \gamma_C^{\mathrm{T}}(\gamma_A + T^A)^{-1}\gamma_C$, using the notation from Eq. (10). The CM γ_m^A is identified with the Schur complement of the matrix $\gamma + T^A \oplus 0_B$ with respect to the submatrix $\gamma_A + T^A$.

Based on the definition of steering provided in the Introduction it is easy to convince oneself that the composite CM γ is A $\to$B non-steerable if there exists a $2N_B \times 2N_B$ matrix U such that

$$U + \mathrm{i}\Omega_{N_B} \geq 0 \qquad \text{and} \qquad \gamma_m^A - U \geq 0. \tag{15}$$

The first condition assures that U is a CM of a physical CV quantum state of N_B bosonic modes, that is to say, there exists a definite ensemble of Gaussian states with U as their CM, but distinguished by their mean vectors. The second condition can be restated to

$$\exists P \geq 0 \qquad \text{such that} \qquad U + P = \gamma_m^A, \tag{16}$$

meaning that a CM γ_B^A can be obtained as a classical mixture of the states with CM U via a classical multivariate Gaussian distribution with variances encoded in P [10]. There is an ensemble which always satisfies Eq. (16) and that is the Schur complement of γ with respect to the submatrix γ_A, i.e. $U = \gamma_B^A$ where

$$\gamma_B^A = \gamma_B - \gamma_C^{\mathrm{T}}\gamma_A^{-1}\gamma_C. \tag{17}$$

Moreover, in Ref. [7] it was proven that a Gaussian states with CM γ is A$\to$B steerable by means of Gaussian measurements if and only if

$$\gamma_B^A + \mathrm{i}\Omega_{N_B} \geq 0. \tag{18}$$

An equivalent criterion for Gaussian steering which bears some resemblance with the entanglement criterion in Eq. (14) was proven in Ref. [14]. Namely, a Gaussian state is A$\to$B steerable if and only if there exists a local covariance matrix $\eta_B + \mathrm{i}\Omega_{N_B} \geq 0$ such that

$$\gamma \geq 0_A \oplus \eta_B. \tag{19}$$

The proof is based on the properties of Schur complement (see Ref. [14]).

3 Witnesses based on second moments

Witnesses originate from an important result in convex geometry, known as the *Hahn-Banach separation theorem*, which states that given a closed convex set and an outside point, there always exists a hyperplane[2] (or witness, test) that lays between them [15]. In the space of symmetric positive definite $2N \times 2N$ matrices the set of all quantum CMs defined in Eq.(9) represents a closed convex set. Furthermore, the set of separable CMs as defined in Eq. (14) as well as of non-steerable CMs (19) each form a closed convex set in the space of symmetric matrices. Therefore, one can define entanglement witnesses based on second moments that detect entangled CMs with respect to the set of separable CMs, and steering witnesses, respectively.

Definition 1. *[16, 17] An entanglement (steering) witness based on second moments can be characterized by a real matrix $Z > 0$ satisfying*

(i) $\mathrm{Tr}[Z\gamma'] \geq 1$ *for all separable (non-steerable)* γ'*,*

(ii) $\mathrm{Tr}[Z\gamma] < 1$ *for some entangled (steerable)* γ*.*

Let us define the set of bi-separable CMs as given by the separability criterion in Eq. (14), as follows:

$$\Gamma_{A|B}(\mathbb{R}^{2N}) := \{\gamma | \gamma = \sigma_A \oplus \sigma_B + P, \text{ with } \sigma_A \geq \mathrm{i}\Omega_{N_A}, \sigma_B \geq \mathrm{i}\Omega_{N_B}, P \geq 0\}. \tag{20}$$

This represents a closed and convex set, and according to the Hahn-Banach separation theorem, there exist a symmetric $2N \times 2N$ matrix Y and a real number c such that

$$\mathrm{Tr}[Y\gamma'] \geq c \quad \text{for all separable} \quad \gamma' \in \Gamma_{A|B}(\mathbb{R}^{2N}), \tag{21}$$

$$\mathrm{Tr}[Y\gamma] < c \quad \text{for some non-separable (entangled)} \quad \gamma \notin \Gamma_{A|B}(\mathbb{R}^{2N}). \tag{22}$$

In Ref. [17] it was proven by contradiction that any hyperplane cutting the space of CMs is a nonegative matrix $Y \geq 0$, and the coefficient is a strictly positive real number $c > 0$. Therefore we have

$$\mathrm{Tr}[Z\gamma] < 1 \leq \mathrm{Tr}[Z\gamma'], \tag{23}$$

where $Z = \frac{Y}{c}$ is also a symmetric positive definite matrix witnessing the separation of CM γ from the set of separable CMs. The same reasoning

[2] A hyperplane is a linear subspace with dimension one less than the dimension of the space itself.

applies also to the steering witnesses, since the set of non-steerable CMs is also closed and convex. Due to the steering asymmetry there are two types of non-steerability, denoted as

$$\Gamma_{A\not\to B}(\mathbb{R}^{2N}) := \{\gamma|\ \gamma = 0_A \oplus \eta_B + P,\ \text{with}\ \eta_B \geq \mathrm{i}\Omega_{N_B}\ \text{and}\ P \geq 0\}, \quad (24)$$

for the A→B non-steerability, and as

$$\Gamma_{B\not\to A}(\mathbb{R}^{2N}) := \{\gamma|\ \gamma = \eta_A \oplus 0_B + P,\ \text{with}\ \eta_A \geq \mathrm{i}\Omega_{N_A}\ \text{and}\ P \geq 0\}. \quad (25)$$

for the B→A non-steerability. Hence, we arrive at a well known fact that separable states are contained into the set of non-steerable states $\Gamma_{A|B}(\mathbb{R}^{2N}) \subset \Gamma_{A\not\to B}(\mathbb{R}^{2N})$, as well as $\Gamma_{A|B}(\mathbb{R}^{2N}) \subset \Gamma_{B\not\to A}(\mathbb{R}^{2N})$, but also $\Gamma_{A|B}(\mathbb{R}^{2N}) \subset \Gamma_{A\not\to B}(\mathbb{R}^{2N}) \cap \Gamma_{B\not\to A}(\mathbb{R}^{2N})$.

We proceed by presenting the two main theorems characterizing the entanglement and steering witnesses based on CMs. The block representation of the $2N \times 2N$ matrix witness Z is given by

$$Z = \begin{pmatrix} Z_A & Z_C \\ Z_C^{\mathrm{T}} & Z_B \end{pmatrix}, \quad (26)$$

where Z_A and Z_B are the block matrices on the diagonal of Z acting on the subsystem of Alice and Bob, respectively. First, we prove a relation that will be very useful for characterising entanglement and steering witnesses.

Lemma 1. *[17, 18] For a symmetric $2N \times 2N$ positive matrix $Z \geq 0$, and a N-mode CM γ the following relation holds:*

$$\min_{\gamma\in\Gamma(\mathbb{R}^{2N})} \mathrm{Tr}[Z\gamma] = 2\ \mathrm{str}[Z], \quad (27)$$

where $\Gamma(\mathbb{R}^{2N})$ denotes the set of all $2N \times 2N$ CMs satisfying the uncertainty relation in Eq. (9).

Proof. Let us consider that our CM γ is derived from a symplectic transformation $S \in Sp(\mathbb{R}^{2N})$ on some initial CM γ' as follows: $\gamma = S^{\mathrm{T}}\gamma' S$, such that S also brings the matrix Z to its symplectic diagonal form denoted as Z_w:

$$SZS^{\mathrm{T}} = Z_w = \mathrm{diag}(z_1, z_1, \ldots, z_N, z_N), \quad (28)$$

where z_i, $i = 1, \ldots, N$ are the symplectic eigenvalues of Z. Thus we have

$$\mathrm{Tr}[Z\gamma] = \mathrm{Tr}[Z_w\gamma'] = \sum_{i=1}^{N} z_i \mathrm{Tr}[\gamma_i'], \quad (29)$$

where γ_i' is the block diagonal matrix of γ' which corresponds to a single mode indexed i. The trace of a single mode CM is the sum of uncertainties of single mode harmonic oscillator, which is related to the energy expectation value as follows:

$$\mathrm{Tr}[\gamma_i'] = 2(\langle \Delta \hat{x}_i^2 \rangle + \langle \Delta \hat{p}_i^2 \rangle) = 2(2\bar{n}_i + 1) \geq 2, \tag{30}$$

where $\bar{n}_i$ is the average thermal photon number of mode i, defined as $\bar{n}_i = \langle \hat{a}_i^\dagger \hat{a}_i \rangle$. Thus, the CM of a harmonic oscillator with the ground state energy satisfies the equality (27). □

Theorem 1. *[Entanglement Witnesses] [16]. A CM γ of a bipartite system with $N_A + N_B = N$ modes is entangled with respect to this partition if and only if there exists Z such that*

$$\mathrm{Tr}[Z\gamma] < 1, \tag{31}$$

where Z is a real symmetric $2N \times 2N$ matrix satisfying

$$\begin{aligned} Z &\geq 0, \\ \mathrm{str}[Z_A] + \mathrm{str}[Z_B] &\geq \tfrac{1}{2}, \end{aligned} \tag{32}$$

where Z_A and Z_B are defined in Eq. (26). Matrices Z are called entanglement witnesses based on second moments.

Proof. According to Definition 1 the theorem above is equivalent to proving that for any separable CM γ' we have $\mathrm{Tr}[Z\gamma'] \geq 1$ if and only if the inequalities in Eq. (32) are fulfilled, whereas if for a CM γ we have $\mathrm{Tr}[Z\gamma] < 1$, then γ must be entangled. Also, we leave out the discussion about the positive semidefinite constraint on the witness $Z \geq 0$ since it was fully discussed in Ref [17], showing that any hyperplane cutting the set of CMs is given by a positive semidefinite matrix.

⇒ Here we prove that if $\mathrm{Tr}[Z\gamma'] \geq 1$ for some separable CM γ', then $\mathrm{str}[Z_A] + \mathrm{str}[Z_B] \geq \frac{1}{2}$ is fulfilled. According to the definition of separable states in Eq. (20) and Lemma 1 we have:

$$\begin{aligned} \mathrm{Tr}[Z\gamma'] &\geq \mathrm{Tr}[Z_A\sigma_A] + \mathrm{Tr}[Z_B\sigma_B] \\ &\geq 2\ \mathrm{str}[Z_A] + 2\ \mathrm{str}[Z_B]. \end{aligned} \tag{33}$$

⇐ Conversely, we start with a positive symmetric matrix $Z \geq 0$ as given by Eq. (26) and fulfilling the inequality in Eq. (32) and show that if there exists CM γ' such that $\mathrm{Tr}[Z\gamma'] \geq 1$, then it has to be separable. Using Lemma 1 we obtain

$$\begin{aligned}\frac{1}{2} \leq \mathrm{str}[Z_A] + \mathrm{str}[Z_B] \leq \frac{1}{2}\mathrm{Tr}[Z_A\sigma_A] + \frac{1}{2}\mathrm{Tr}[Z_B\sigma_B] \\ = \frac{1}{2}\mathrm{Tr}[Z(\sigma_A \oplus \sigma_B)]. \end{aligned} \tag{34}$$

Thus, if there exists a CM γ' such that

$$\mathrm{Tr}[Z\gamma'] \geq \mathrm{Tr}[Z(\sigma_A \oplus \sigma_B)], \tag{35}$$

then it represents a separable state, according to the separability criterion in Eq. (14). □

We consider here only bipartite entanglement for a simpler comparison with steering, while the instances of multipartite entanglement witnesses are covered in Ref. [19].

Theorem 2. *[Steering Witnesses] [14]. A CM γ of two parties consisting of $N = N_A + N_B$ modes is A→B steerable by means of Gaussian measurements if and only if there exists Z such that*

$$\mathrm{Tr}[Z\gamma] < 1, \tag{36}$$

where Z is a real symmetric $2N \times 2N$ matrix satisfying

$$Z \geq 0, \qquad \mathrm{str}[Z_B] \geq \frac{1}{2}, \tag{37}$$

where Z_B denotes the submatrix of Z belonging to the subsystem of Bob, as defined in Eq. (26). Matrices Z are called steering witnesses based on second moments.

Proof. As in the case of entanglement witnesses in Theorem 1, it suffices to prove that a witness satisfying constraints in Eq. (37) gives $\mathrm{Tr}[Z\gamma] \geq 1$ for any non-steerable CM γ, and if we have $\mathrm{Tr}[Z\gamma] < 1$, then γ is steerable. This statement is provable in the same fashion as for entanglement witnesses. □

4 Semidefinite algorithm

The semidefinite programming (SDP) represents the optimization over a linear function subject to matrix inequality constraints [21]. It can be thought as a form of generalization of linear and quadratic programming, where the inequalities of vectors are replaced by matrix inequalities, and yet, SDP are still easily and very efficiently solvable. Therefore, it can come at hand for finding the optimal test function, or witness, detecting entanglement or steering in a given states.

The equations describing the entanglement and steering witnesses in Theorem 1 and Theorem 2 impose constraints on the symplectic eigenvalues of the witnesses which are clearly nonlinear[3]. Therefore, we propose a set of linear constraints for the characterisation of entanglement and steering witnesses, respectively, that are stronger than the constraints from the previous section.

Proposition 1. *[19] For the entanglement witness Z of a bipartite entangled $N-$mode CM with $N_A + N_B = N$, the inequalities (32) are satisfied if the following conditions are fulfilled:*

$$\begin{gathered} Z \geq 0, \\ Z_A + \mathrm{i}\tfrac{x}{N_A}\Omega_{N_A} \geq 0, \quad x \in \mathbb{R}, \\ Z_B + \mathrm{i}\tfrac{1}{N_B}\left(\tfrac{1}{2} - x\right)\Omega_{N_B} \geq 0. \end{gathered} \tag{38}$$

Proof. 1. Let us start with $N = 2$, i.e. for a two-mode CM the witness is a 4×4 matrix $Z \geq 0$ with the block form in Eq. (26), where $Z_A \geq 0$ and $Z_B \geq 0$ are 2×2 matrices. In the following inequality

$$Z_A + \mathrm{i}\ x\ \Omega_{N_A} \geq 0, \quad \text{where} \quad \Omega_{N_A} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad x \in \mathbb{R}, \tag{39}$$

we apply a symplectic transformation S such that the positive matrix above can be diagonalised as follows[4]:

$$S(Z_A + \mathrm{i}\ x\ \Omega_{N_A})S^T = Z_A^w + \mathrm{i}\ x\ \Omega_1 = \begin{pmatrix} z_1 & \mathrm{i}\ x \\ -\mathrm{i}\ x & z_1 \end{pmatrix}, \tag{40}$$

where $Z_A^w = \mathrm{diag}(z_1, z_1)$, with z_1 the positive symplectic eigenvalue of Z_A. The eigenvalues α of matrix (40) are determined from the equation

$$(z_1 - \alpha)^2 - x^2 = (z_1 - \alpha - x)(z_1 - \alpha + x) = 0, \tag{41}$$

[3]The symplectic eigenvalues of a matrix M are calculated as the eigenvalues of the matrix $M^{\frac{1}{2}}(\mathrm{i}\Omega_N)M^{\frac{1}{2}}$.

[4]Any symplectic transformation preserves the symplectic eigenvalues, and since we know that $\mathrm{Tr}[M] \geq 2\ \mathrm{str}[M]$ holds for any positive matrix M [20], then we can say that symplectic transformations preserve also the positivity.

and hence

$$z_1 \pm x = \alpha \geq 0. \tag{42}$$

Thus, the symplectic eigenvalue z_1 fulfills the inequality $z_1 \geq \pm x$, or $z_1 \geq |x|$. Similarly for the second party we have:

$$Z_B + \mathrm{i}(\frac{1}{2} - x)\Omega_{N_B} \geq 0, \tag{43}$$

and the symplectic eigenvalue z_2 satisfies:

$$z_2 \geq \left|\frac{1}{2} - x\right|. \tag{44}$$

Now, the sum of symplectic eigenvalues gives

$$z_1 + z_2 \geq |x| + \left|\frac{1}{2} - x\right| \geq \left|x + \frac{1}{2} - x\right| = \frac{1}{2}. \tag{45}$$

The above inequality assures that the condition (32) is always fulfilled. Furthermore, due to the triangle inequality in Eq. (45) it is also stronger than required in Theorem 1, since it accounts for all possible values of x. Yet, the above inequality is tight if we consider x to take values from a fixed interval

$$0 \leq x \leq \frac{1}{2}. \tag{46}$$

2. Here we consider a three-mode state and the bipartition between the first and the other two modes. The witness Z is a 6×6 matrix where $Z_A \equiv Z_1$ is the 2×2 block diagonal matrix of Z acting on the first mode, and we denote by Z_B the 4×4 block matrix acting on the other two modes:

$$Z = \left(\begin{array}{c|cc} Z_1 & Z_{12} & Z_{13} \\ \hline Z_{12}^{\mathrm{T}} & Z_2 & Z_{23} \\ Z_{13}^{\mathrm{T}} & Z_{23}^{\mathrm{T}} & Z_3 \end{array}\right), \tag{47}$$

where all the elements are 2×2 block matrices, and the block diagonal matrices under interest are Z_1 and $Z_B = \begin{pmatrix} Z_2 & Z_{23} \\ Z_{23}^{\mathrm{T}} & Z_3 \end{pmatrix}$. Then the corresponding constraints on the witness are

$$\begin{gathered} Z \geq 0, \\ Z_1 + \mathrm{i}\ x\ \Omega_1 \geq 0, \quad x \in \mathbb{R}, \\ Z_B + \mathrm{i}\tfrac{1}{2}(\tfrac{1}{2} - x)\Omega_{N_B} \geq 0. \end{gathered} \tag{48}$$

If we denote by z_1 the symplectic eigenvalue of Z_1, and by z'_1, z'_2 the two symplectic eigenvalues of Z_B, then the conditions above are equivalent to

$$\begin{aligned} z_1 &\geq |x|, \quad x \in \mathbb{R}, \\ z'_1 &\geq \tfrac{1}{2}\left|\tfrac{1}{2} - x\right|, \\ z'_2 &\geq \tfrac{1}{2}\left|\tfrac{1}{2} - x\right|, \end{aligned} \tag{49}$$

which imply the condition (32). The generalization of the proof to N modes and k parties is straightforward and is presented in Ref. [19], showing that the above linear conditions are stronger for $k-$partite entanglement (with $k < N$) than for genuine multipartite entanglement (i.e. $k = N$).

□

Proposition 2. *[14] For the steering witness Z of a N-mode CM steerable from Alice to Bob, with $N = N_A + N_B$, the inequalities (37) are satisfied if (if and only if for $N_B = 1$) the following conditions are fulfilled:*

$$\begin{aligned} Z &\geq 0, \\ Z_B + \mathrm{i}\tfrac{1}{2N_B}\Omega_{N_B} &\geq 0. \end{aligned} \tag{50}$$

Proof. This is easily provable given the example of Proposition 1. □

At this stage we are ready to present a SDP optimizing algorithm finding the best entanglement or steering witness for a given CM γ given the constraints in Proposition 1 or Proposition 2, respectively. The witness is constructed from a set of measurement operators M_i arranged in a vector of measurement matrices $\mathbf{M}$, such that $Z = \sum_i c_i M_i$, where c_i are the optimization coefficients that form a vector $\mathbf{c}$.

For example, entanglement is detected in two-mode CMs, where $N_A = N_B = 1$, by the following SDP algorithm:

$$\begin{aligned} \underset{x,\mathbf{c}}{\text{minimize}} \quad & \mathbf{c} \cdot \mathbf{m} \\ \text{subject to} \quad & Z = \sum_i c_i M_i, \\ & Z = \begin{pmatrix} Z_A & Z_C \\ Z_C^{\mathrm{T}} & Z_B \end{pmatrix} \geq 0, \\ & Z_A + \mathrm{i}x\ \Omega_{N_A} \geq 0, \\ & Z_B + \mathrm{i}(\frac{1}{2} - x)\Omega_{N_B} \geq 0, \end{aligned} \tag{51}$$

where $\mathbf{m} = \mathrm{Tr}[\mathbf{M}\gamma]$ is the vector of measurements outcome and i is the index counting the number of measurements used in the algorithm. For two-mode CMs there are 10 different measurement forming the tomographycally complete set, and if the result of this algorithm gives $\mathrm{Tr}[Z\gamma] = \mathbf{c} \cdot \mathbf{m} < 1$, then we may conclude that γ is entangled.

A straightforward generalisation to multipartite and multimode entanglement and steering witnesses, as well as the study of entanglement and steering detection feasibility of our method was analyzed in Refs. [14, 19].

5 Conclusions

In this article we addressed the relation between entanglement and steering quantum correlations in Gaussian states by means of Gaussian measurements. Gaussian states represent a large class of CV systems for which quantum correlations are encoded in their second order statistical moments of the canonical operators, arranged in a covariance matrix. In this case, entanglement and steering criteria suggest that the set of non-steerable CMs contains the set of separable states, and each of them form closed convex sets.

These interesting properties displayed by Gaussian states allow for an elegant detection method of entanglement and steering by means of witness operators, or tests. Geometrically they correspond to hyperplanes cutting into two parts the space of CMs, while operationally witnesses represent specific measurements performed in the experiments, by the result of which we may conclude with high confidence that the state is entangled or steerable.

Here we fully characterized the sets of entanglement and steering witnesses, respectively, and showed that steering witnesses form a subclass of entanglement witnesses, which is in accordance with the known result that every steerable CM also contains entanglement, while the converse not always holds.

Next, we proposed a set of stronger than actually required by Theorem 1 and Theorem 2 linear constraints characterizing the witnesses, giving the advantage of implementing a SDP optimization algorithm for a given CM. With this method, witnesses are constructed from the sequence of tomographically complete set of measurements, or any random measurements, and given the linear constraints it gives a value which, if it exceeds a certain threshold, certifies the detection entanglement or steering. The efficiency and robustness of this method to the statistical errors are presented in Refs. [14, 19].

References

[1] D. Bruß, G. Leuchs. *Quantum information: From foundations to quantum technology applications.* Wiley-VCH, 2019.

[2] R. Horodecki, P. Horodecki, M. Horodecki, K. Horodecki. Quantum entanglement. *Rev. Mod. Phys.* 81:2, 2009.

[3] A. Einstein, B. Podolsky, N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Phys. Rev.* 47:10, 1935.

[4] E. Schrödinger. Discussion of probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31:4, 1935.

[5] E. Schrödinger. Probability relations between separated systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 32:3, 1936.

[6] H. M. Wiseman, S. J. Jones, A. C. Doherty. Steering, Entanglement, Nonlocality, and the Einstein-Podolsky-Rosen Paradox. *Phys. Rev. Lett.* 98:14, 2007.

[7] S. J. Jones, H. M. Wiseman, A. C. Doherty. Entanglement, Einstein-Podolsky-Rosen correlations, Bell nonlocality and steering. *Phys. Rev. A* 76:052116, 2007.

[8] R. Uola, A. C. S. Costa, H. C. Nguyen, O. Gühne. Quantum steering. *Rev. Mod. Phys.*, 92:1, 2020.

[9] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, S. Lloyd. Gaussian quantum information. *Rev. Mod. Phys.* 84:2, 2012.

[10] A. Serafini. *Quantum Continuous Variables: A Primer of Theoretical Methods.* Taylor & Francis Group, 2017.

[11] S. Olivares. Quantum optics in the phase space. *Eur. Phys. J. Spec. Top.* 203:3, 2012.

[12] A. B. Dutta, N. Mukunda, R. Simon. The real symplectic groups in quantum mechanics and optics. *Pramana* 45:6, 1995.

[13] R. F. Werner, M. M. Wolf. Bound entangled Gaussian states. *Phys. Rev. Lett.*, 86:16, 2001.

[14] T. Mihaescu, H. Kampermann, A. Isar, D. Bruß. Steering witnesses for unknown Gaussian quantum states. *New J. Phys.* 25:113023, 2023.

[15] S. Boyd, L.Vandenberghe. *Convex optimization.* Cambridge University Press, 2004.

[16] P. Hyllus, J. Eisert. Optimal entanglement witnesses for continuous variable systems. *New J. Phys.* 8:51, 2006.

[17] J. Anders. Estimating the degree of entanglement of unknown Gaussian states. Diploma Thesis, University of Potsdam, 2003.

[18] T. Mihaescu. Detection and open system dynamics of Gaussian quantum correlations. PhD Thesis, University of Bucharest, 2023.

[19] T. Mihaescu, H. Kampermann, G. Gianfelici, A. Isar, D. Bruß. Detecting entanglement of unknown continuous variable states with random measurements. *New J. Phys.* 22:123041, 2020.

[20] R. Bhatia, T. Jain. On symplectic eigenvalues of positive definite matrices. *J. Math. Phys.* 56:112201, 2015.

[21] L. Vandenberghe, S. Boyd. Semidefinite programming. *SIAM Review* 38:1, 1996.