The Quantum Separability Problem for Gaussian States

Stefano Mancini [1]

Physics Department, University of Camerino,
I-62032 Camerino, Italy

Simone Severini[2]

Department of Mathematics, University of York,
YO10 5DD York, UK

Abstract

Determining whether a quantum state is separable or entangled is a problem of fundamental importance in quantum information science. This is a brief review in which we consider the problem for states in infinite dimensional Hilbert spaces. We show how the problem becomes tractable for a class of Gaussian states.

Keywords: Quantum Entanglement, Quantum Algorithms, Quantum Complexity.

1 Introduction

The concept of *entanglement* arose with the question of completeness of quantum theory [1]. Nowadays entanglement is regarded as a fundamental property of certain quantum states and it appears to be an important physical resource. In some sense, entanglement is synonymous of inseparability because *entangled states* possess some global properties that cannot be explained in terms of only the parties (subsystems) of the system. Roughly speaking, entangled states possess "strong" correlations among parties that cannot be explained within any classical local theory (because these would imply an instantaneous action at distance). *Separable states* may also exhibit correlations among parties, but these are purely classical and local, hence "weaker" than those underlying entanglement.

---

[1] Email: stefano.mancini@unicam.it

[2] Email: ss54@york.ac.uk

Recently, the role of entanglement became important and often necessary in many different contexts like quantum algorithms, quantum communication protocols, quantum cryptography, *etc.* (see *e.g.* [2]). So, the problem of deciding whether a given quantum state is separable or entangled has become of uppermost importance. This can be called the *Quantum Separability Problem* (QSP). Essentially, it represents an instance of a combinatorial optimization problems called the Weak Membership Problem [3].

Although there exists a number of characterizations of separability, there is still no feasible procedure to solve QSP in its generality (see *e.g.* [4] and references therein). Concerning its computational complexity, QSP is a "difficult" problem. In fact, QSP has been proved to be NP-hard [5]. However, if we restrict ourselves to specific classes of quantum states, there are examples in which QSP can be efficiently solved. For instance, this is the case of states in Hilbert space of dimension 2 or 3 [6] and certain finite sets of states [7].

In infinite dimensional Hilbert spaces, *Gaussian states* give rise to an important class of states for which QSP is "easy" (see *e.g.* [8,9] and the reference therein). In this paper, we review the formulation of QSP for infinite dimensional Hilbert spaces and we show how to tackle the problem for the class of Gaussian states.

The paper is organized as follow. In Sec.2 we review some basic notions of Quantum Theory. In Sec. 3 we formalize the QSP. In Sec.4 we introduce the Gaussian states. In Sec.5 we develop a criterion for separability of Gaussian states. Finally, some conclusions are drawn in Sec.6.

2   Basic Notions of Quantum Theory

In this section, we introduce some terms and notions of Quantum Mechanics needed to approach the paper. Of course, the expert reader may skip this section.

In its standard formulation, Quantum Theory takes place in Hilbert spaces [10]. A Hilbert space $\mathcal{H}$ is a vector space over the field of complex numbers $\mathbb{C}$ endowed with an inner product (which induces a norm), that can have finite or infinite dimension. We use the so-called Dirac notation for a vector $|\psi\rangle$. Its dual is $\langle\psi|$. Then, the inner product between two states $|\psi\rangle$ and $|\phi\rangle$ reads $\langle\psi|\phi\rangle \in \mathbb{C}$. The norm of a vector $|\psi\rangle$ results $\|\,|\psi\rangle\| = \sqrt{\langle\psi|\psi\rangle}$. The following two postulate fix the mathematical representation of quantum states:

Postulate 2.1 *The space of states of a physical system is a Hilbert space. The states are described by unit norm vectors in such Hilbert space.*

Postulate 2.2 *The space of states of a composite system is the tensor product of Hilbert spaces of subsystems.*

The structure of Hilbert space naturally leads, when considering composite systems, to the concept of *entanglement*. In fact, there exist states of the whole system that cannot be factorized into states of the subsystems.

Example 2.1 Let $|\psi\rangle_1, |\psi_\perp\rangle_1$ be two orthogonal states in $\mathcal{H}_1$ and $|\eta\rangle_2, |\eta_\perp\rangle_2$ be two orthogonal states in $\mathcal{H}_2$. Then, $|\psi\rangle_1 \otimes |\eta\rangle_2 \in \mathcal{H}_1 \otimes \mathcal{H}_2$ as well as $(a|\psi\rangle_1 \otimes |\eta\rangle_2 +$

$b \, |\psi_\perp\rangle_1 \otimes |\eta_\perp\rangle_2) \in \mathcal{H}_1 \otimes \mathcal{H}_2$, with $a, b \in \mathbb{C}$. The first can be factorized into states of the subsystems; this is not the case for the second one.

It is fashinating that this seemingly abstract mathematical notion has a large impact in the description of the quantum mechanical world.

The above postulates can be generalized in terms of mixture of states, $\{p_j, |\psi_j\rangle\}$, where p_j denotes for the probability for the system to be in the state $|\psi_j\rangle$. This can be done by introducing the notion of *density operator*:

Definition 2.2 A density operator $\hat{\rho}$ is a non-negative, self-adjoint, trace-one class operator which is also positive semi-definite (that is $\langle \psi | \hat{\rho} | \psi \rangle \geq 0 \; \forall | \psi \rangle \in \mathcal{H}$.

Thus we can represent the mixture $\{p_j, |\psi_j\rangle\}$ by the density operator $\hat{\rho} = \sum_j p_j |\psi_j\rangle\langle\psi_j|$.

Definition 2.3 A state $\hat{\rho}$ of a composite *bipartite* system is said to be *separable* iff it can be written in the form

$$\hat{\rho} = \sum_j p_j \hat{\rho}_j^{(1)} \otimes \hat{\rho}_j^{(2)}, \tag{1}$$

with non-negative p_j's such that $\sum_j p_j = 1$, and where $\hat{\rho}_j^{(1)}$, $\hat{\rho}_j^{(2)}$ are density operators of the subsystems; the state is said to be *entangled* otherwise.

The physical quantities of a system that can (in principle) be measured are called *observables*. The next postulate fixes the mathematical representation of observables:

Postulate 2.3 *To physical observables correspond self-adjoint operators. The possible measurement results on the observable O are the eigenvalues of the associated self-adjoint operator $\hat{O}$. The expectation value is $\langle \hat{O} \rangle \equiv \mathrm{Tr}(\hat{O}\hat{\rho})$.*

Restrictions on expectation values are imposed by the following famous principle:

Principle 2.1 (The Uncertainty Principle) *Any two observables A and B in $\mathcal{H}$ must satisfy, for all quantum states, the following inequality:*

$$\langle (\Delta \widehat{A})^2 \rangle \langle (\Delta \widehat{B})^2 \rangle \geq \frac{1}{4} \left| \langle [\widehat{A}, \widehat{B}] \rangle \right|^2, \tag{2}$$

where $\Delta \widehat{O} \equiv \widehat{O} - \langle \widehat{O} \rangle$ and $[\widehat{A}, \widehat{B}] \equiv \widehat{A}\widehat{B} - \widehat{B}\widehat{A}$ is the commutator.

3 The Quantum Separability Problem

In this section we introduce the Quantum Separability Problem. Let us consider a quantum system with two parties associated to a Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2 \cong \mathbb{C}^M \otimes \mathbb{C}^N$. Notice that such a Hilbert space is isomorphic to $\mathbb{R}^{M^2 N^2}$ and it is endowed with the Euclidean inner product $(\hat{X}, \hat{Y}) \equiv \mathrm{Tr}(\hat{X}\hat{Y})$ which induces the corresponding norm $\|\hat{X}\| \equiv \sqrt{\mathrm{tr}(\hat{X}^2)}$ and distance measure $\|\hat{X} - \hat{Y}\|$. Let $\mathcal{D} \subset \mathcal{H}_1 \otimes \mathcal{H}_2$ denote the set

of all density operators. The set of bipartite separable quantum states, $\mathcal{S} \subset \mathcal{D}$, is defined as the convex hull of the separable pure states $\{|\psi\rangle_1 \langle\psi| \otimes |\eta\rangle_2 \langle\eta|\}$ where $|\psi\rangle_1$ (resp. $|\eta\rangle_2$) is a normalized vector in $\mathbb{C}^M$ (resp. $\mathbb{C}^N$). An arbitrary density matrix in $\mathcal{D}$ is parametrized by $M^2 N^2 - 1$ real variables. Since we deal with continuous quantities, in defining the separability problem we cannot allow infinite precision, so we need to introduce a precision parameter $\delta \in \mathbb{R}_+$.

Definition 3.1 [The Quantum Separability Problem] Given $\hat{\rho} \in \mathcal{D}$ and a precision δ assert either $\hat{\rho}$ is:

- *Separable*: there exists a separable state $\hat{\sigma}$ such that $\|\hat{\rho} - \hat{\sigma}\| < \frac{1}{\delta}$
    or

- *Entangled:* there exists an entangled state $\hat{\tau}$ such that $\|\hat{\rho} - \hat{\tau}\| < \frac{1}{\delta}$.

In this formulation, this problem is equivalent to an instance of a combinatorial optimization problem called Weak Membership Problem [3]. In its complete generality, QSP has been shown to be NP-hard [5]. Thus, any devised test for separability is likely to require a number of computational steps that increases very quickly with M and N. For $MN \leq 6$ the positivity under *Partial Transpose* (see the next section) represents a necessary and sufficient test [6]. Otherwise, there only exist sufficient 'one-sided' tests for separability. In these tests, the output of some polynomial-time computable function of $\hat{\rho}$ can indicate that this is certainly entangled or certainly separable, but not both (see *e.g.* [4] and reference therein).

4   Gaussian States

In this section we introduce Gaussian states. Let us now move to $M, N \to \infty$, thus considering two infinite dimensional Hilbert spaces $\mathcal{H}_1$ and $\mathcal{H}_2$. In such spaces we can introduce continuous spectrum self-adjoint operators corresponding to canonical position and momentum variables [10]. Let us arrange them into four-dimensional column vectors

$$\hat{\mathbf{v}}^T = (\hat{q}_1, \hat{p}_1, \hat{q}_2, \hat{p}_2), \quad \mathbf{z}^T = (x_1, y_1, x_2, y_2).$$

The operators in $\hat{\mathbf{v}}$ obey commutation relations [10] that take the compact form

$$[\hat{\mathbf{v}}_\alpha, \hat{\mathbf{v}}_\beta] = i\,\Omega_{\alpha\beta}, \quad \alpha, \beta = 1, 2, 3, 4, \tag{3}$$

with

$$\Omega = \begin{pmatrix} J & 0 \\ 0 & J \end{pmatrix}, \quad J = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{4}$$

There is a one-to-one correspondence between density operators and c-number Wigner distribution functions in phase space [11], the space of variables $\mathbf{z}$, *i.e.* $\mathbb{R}^4$, in this case.

Definition 4.1 For a given density operator $\hat{\rho}$ in $\mathcal{H}_1$ and $\mathcal{H}_2$ the corresponding Wigner function is defined as follows[3]

$$W(\mathbf{z}) := \mathrm{Tr}\left(\hat{\rho}\hat{T}(\mathbf{z})\right), \tag{5}$$

where

$$\hat{T}(\mathbf{z}) := \frac{1}{(2\pi)^4} \int d^4\mathbf{z}' \exp\left[i\mathbf{z}'^T \cdot (\hat{\mathbf{v}} - \mathbf{z})\right]. \tag{6}$$

In turn, it results

$$\hat{\rho} = \int d^4\mathbf{z}\, W(\mathbf{z})\hat{T}(\mathbf{z}). \tag{7}$$

A density operator $\hat{\rho}$ has finite second order moments if $\mathrm{Tr}(\hat{\rho}\hat{q}_j^2) < \infty$ and $\mathrm{Tr}(\hat{\rho}\hat{p}_j^2) < \infty$ for all j. In this case we can define the vector mean $\mathbf{m}$ as

$$\begin{aligned} \mathbf{m} :=& \mathrm{Tr}(\hat{\rho}\hat{\mathbf{v}}) \\ =& \int d^4\mathbf{z}\, \mathbf{z}\, W(\mathbf{z}), \end{aligned} \tag{8}$$

and the real symmetric correlation matrix V as

$$V_{\alpha\beta} := \frac{1}{2}\langle\{\Delta\hat{\mathbf{v}}_\alpha, \Delta\hat{\mathbf{v}}_\beta\}\rangle, \quad \alpha, \beta = 1, 2, 3, 4, \tag{9}$$

where $\{\Delta\hat{\mathbf{v}}_\alpha, \Delta\hat{\mathbf{v}}_\beta\} \equiv \Delta\hat{\mathbf{v}}_\alpha\Delta\hat{\mathbf{v}}_\beta + \Delta\hat{\mathbf{v}}_\beta\Delta\hat{\mathbf{v}}_\alpha$ is the anticommutator. It results

$$\begin{aligned} V_{\alpha\beta} =& \mathrm{Tr}\left(\hat{\rho}\, \frac{1}{2}\{\Delta\hat{\mathbf{v}}_\alpha, \Delta\hat{\mathbf{v}}_\beta\}\right) \\ =& \int d^4\mathbf{z}\, (\mathbf{z} - \mathbf{m})_\alpha\, (\mathbf{z} - \mathbf{m})_\beta\, W(\mathbf{z}). \end{aligned} \tag{10}$$

A given V is the correlation matrix a *physical* state iff it satisfies

$$K \equiv V + \frac{i}{2}\Omega \geq 0, \tag{11}$$

as consequence of the Uncertainty Principle [2] and commutation relation ([3]). The correlation matrix forms a 4×4 matrix that transforms as an irreducible second rank tensor under the linear canonical (symplectic) transformations and has 4 invariants. If we write the correlation matrix in the block form

$$V = \begin{pmatrix} A & C \\ C^T & B \end{pmatrix}, \tag{12}$$

---

[3] Throughout the paper, if not specified, the integration is intended from $-\infty$ to $+\infty$.

the invariants are $\det A$, $\det B$, $\det C$ and $\mathrm{Tr}(AJCJBJC^T J)$. The condition (11) implies $A \geq 1/4$ and $B \geq 1/4$. Moreover, Eq.(11) can be read as

$$\det A \det B - \mathrm{Tr}(AJCJBJC^T J) - \frac{1}{4}(\det A + \det B) + \left(\frac{1}{4} - \det C\right)^2 \geq 0. \quad (13)$$

It is also worth remarking that any correlation matrix can be brought into the standard form

$$V = \begin{pmatrix} a & c & & \\ & a & d & \\ c & & b & \\ & d & & b \end{pmatrix}, \quad (14)$$

with $a, b, c, d \in \mathbb{R}$, by effecting suitable local canonical transformations corresponding to some element of $\mathrm{Sp}(2, \mathbb{R}) \times \mathrm{Sp}(2, \mathbb{R}) \subset \mathrm{Sp}(4, \mathbb{R})$. Now we are ready to give the definition of Gaussian state:

Definition 4.2 A state $\hat{\rho}$ is called *Gaussian* if its Wigner function takes the form

$$W(\mathbf{z}) = \frac{1}{4\pi^2 \sqrt{\det V}} \exp\left[-\frac{1}{2}(\mathbf{z} - \mathbf{m})^T V^{-1}(\mathbf{z} - \mathbf{m})\right], \quad (15)$$

with $\mathbf{m}$ a real 4-vector and V a real symmetric 4×4 -matrix.

One can show that $\mathbf{m}$ is indeed the mean and V is the correlation matrix. These define the Gaussian state uniquely. In what follows, we simply consider the case $\mathbf{m} = \mathbf{0}$, because $\mathbf{m}$ can be easily removed by some local displacement and thus has no influence on the separability or inseparability of the state.

5   A separability criterion for Gaussian states

In this section, we describe how to solve QSP for Gaussian states. Let us consider a separable state $\hat{\rho}_{sep}$ of the form (1) in the Hilbert space $\mathcal{H}_1 \otimes \mathcal{H}_2$. Let us choose a generic couple of observables for each subsystem, say $\hat{r}_j, \hat{s}_j$ on $\mathcal{H}_j$ $(j = 1, 2)$, with

$$\hat{\mathcal{C}}_j = i\left[\hat{r}_j, \hat{s}_j\right], \quad j = 1, 2. \quad (16)$$

Then, we introduce the following observables on $\mathcal{H}_1 \otimes \mathcal{H}_2$:

$$\begin{aligned} \hat{u} &= a_1 \hat{r}_1 + a_2 \hat{r}_2, \\ \hat{v} &= b_1 \hat{s}_1 + b_2 \hat{s}_2, \end{aligned} \quad (17)$$

with $a_j, b_j \in \mathbb{R}$. From the the Uncertainty Principle 2, it follows that every state $\hat{\rho}$ on $\mathcal{H}_1 \otimes \mathcal{H}_2$ must satisfy

$$\langle(\Delta \hat{u})^2\rangle \langle(\Delta \hat{v})^2\rangle \geq \frac{|a_1 b_1 \langle \hat{\mathcal{C}}_1 \rangle + a_2 b_2 \langle \hat{\mathcal{C}}_2 \rangle|^2}{4}. \quad (18)$$

However, for separable states, a stronger bound exists. We have in fact the following theorem [12]:

Theorem 5.1 *For any separable state the following implication holds:*

$$\hat{\rho}_{sep} \quad \Longrightarrow \quad \langle(\Delta\hat{u})^2\rangle\langle(\Delta\hat{v})^2\rangle \geq \mathcal{W}^2\,, \tag{19}$$

where

$$\mathcal{W} = \frac{1}{2}\big(\,|a_1 b_1|\,\mathcal{W}_1 + |a_2 b_2|\,\mathcal{W}_2\,\big)\,, \tag{20}$$

with

$$\mathcal{W}_j \equiv \sum_k p_k\,|\langle\hat{\mathcal{C}}_j\rangle_k|\,, \qquad j = 1, 2, \tag{21}$$

being $\langle\hat{\mathcal{C}}_j\rangle_k \equiv \mathrm{Tr}[\,\hat{\mathcal{C}}_j\hat{\rho}_k^{(j)}]$.

The theorem can be proved with the help of a family of linear inequalities

$$\alpha\langle(\Delta\hat{u})^2\rangle + \beta\langle(\Delta\hat{v})^2\rangle \geq 2\sqrt{\alpha\beta}\,\mathcal{W}, \qquad \alpha, \beta \in \mathbb{R}_+, \tag{22}$$

which must be always satisfied by separable states. The convolution of such relations gives the condition (19), representable by a region in the $\langle(\Delta\hat{u})^2\rangle$, $\langle(\Delta\hat{v})^2\rangle$ plane delimited by an hyperbola.

Notice that, since

$$\mathcal{W}_j = \sum_k p_k|\langle\hat{\mathcal{C}}_j\rangle_k| \geq \left|\sum_k p_k\langle\hat{\mathcal{C}}_j\rangle_k\right| = |\langle\hat{\mathcal{C}}_j\rangle|, \tag{23}$$

the following inequalities hold

$$\begin{aligned}\mathcal{W} &\geq \frac{1}{2}\big(\,|a_1 b_1|\,|\langle\hat{\mathcal{C}}_1\rangle| + |a_2 b_2|\,|\langle\hat{\mathcal{C}}_2\rangle|\,\big) \\ &\geq \frac{1}{2}\big(\,|a_1 b_1\,\langle\hat{\mathcal{C}}_1\rangle + a_2 b_2\,\langle\hat{\mathcal{C}}_2\rangle|\,\big)\,.\end{aligned} \tag{24}$$

In particular, Eq. (24) tells us that the bound (19) for separable states is much stronger than Eq. (18) for generic states. Moreover, Eq. (24) gives us a simple separability criterion. In fact, while $\mathcal{W}$ is not easy to evaluate directly, as it depends on the type of convex decomposition (1) that one is considering, the right hand side of Eq. (24) is easily measurable, as it depends on the expectation value of the observables $\hat{\mathcal{C}}_j$. Then, we can claim that Eq.(19) is a necessary criterion for separability, *i.e.*

$$\langle(\Delta\hat{u})^2\rangle\langle(\Delta\hat{v})^2\rangle < \mathcal{W}^2 \quad \Longrightarrow \quad \hat{\rho} \quad \text{entangled}\,. \tag{25}$$

Example 5.2 An important simplification applies when the observable $\hat{\mathcal{C}}_j$ is proportional to the identity operator, *e.g.* $\hat{r}_j \equiv \hat{q}_j$ and $\hat{s}_j \equiv \hat{p}_j$. In such a case, Eq.(18) reduces to

$$\langle(\Delta\hat{u})^2\rangle\langle(\Delta\hat{v})^2\rangle \geq \frac{1}{4}\,, \tag{26}$$

while Eq.(19) reduces to

$$\langle (\Delta \hat{u})^2 \rangle \langle (\Delta \hat{v})^2 \rangle \geq 1 \,, \tag{27}$$

Let us now consider the case in which $\hat{r}_j$, $\hat{s}_j$ are linear combinations of canonical observables $\hat{q}_j$ and $\hat{p}_j$, *i.e.*

$$
\begin{aligned}
\hat{r}_1 &\equiv \hat{q}_1 + \frac{a_3}{a_1}\hat{p}_1 & \hat{s}_1 &\equiv \hat{p}_1 + \frac{b_3}{b_1}\hat{q}_1 \\
\hat{r}_2 &\equiv \hat{q}_2 + \frac{a_4}{a_2}\hat{p}_2 & \hat{s}_2 &\equiv \hat{p}_2 + \frac{b_4}{b_2}\hat{q}_2 \,,
\end{aligned}
\tag{28}
$$

where $a_3, a_4, b_3, \ b_4 \in \mathbb{R}$ are generic real parameters. Then Eq. (19), taking into account Eq.(3), becomes

$$\langle (\Delta u)^2 \rangle \langle (\Delta v)^2 \rangle \geq \frac{1}{4} \big(\ |a_1 b_1 - a_3 b_3| + |a_2 b_2 - a_4 b_4| \ \big)^2, \tag{29}$$

that should be compared with

$$\langle (\Delta u)^2 \rangle + \langle (\Delta v)^2 \rangle \geq |a_1 b_1 - a_3 b_3| + |a_2 b_2 - a_4 b_4| \,. \tag{30}$$

It is easy to verify that, given a_j, b_j $(j = 1, \ldots, 4)$, the "product condition" (29) implies the "sum condition" (30). However, if we require Eqs. (29) and (30) to be verified for *all* possible values of the coefficients a_j, b_j, the two are equivalent since it is possible to re-obtain one from another using a convolution trick, like the used with Eqs.(19) and (22) (the one-to-one correspondence between quadratic and linear tests under all circumstances has been also pointed out in Ref.[13]).

It turns out that the restriction

$$\langle (\Delta u)^2 \rangle + \langle (\Delta v)^2 \rangle \geq |a_1 b_1 - a_3 b_3| + |a_2 b_2 - a_4 b_4|, \quad \forall a_j, b_j \in \mathbb{R}, \tag{31}$$

is *necessary* and *sufficient* for separability of Gaussian states [14,15].

However, solving QSP by testing the condition (31) would be hard from a complexity point of view, due to the presence of the universal quantifier at right hand side.

Nevertheless, the condition (31) can be rephrased in a simpler way. First notice that the uncertainty relation satisfied by all (separable and inseparable) states

$$\langle (\Delta u)^2 \rangle \langle (\Delta v)^2 \rangle \geq \frac{1}{4} |a_1 b_1 - a_3 b_3 + a_2 b_2 - a_4 b_4|^2, \tag{32}$$

and corresponding to $\hat{u}$ and $\hat{v}$ formed from Eq.(19), is equivalent to

$$\langle (\Delta u)^2 \rangle + \langle (\Delta v)^2 \rangle \geq |a_1 b_1 - a_3 b_3 + a_2 b_2 - a_4 b_4|, \tag{33}$$

as much as like Eqs.(29) and (30).

Then, what is the relation between conditions (30) and (33)?

They are simply related by the *partial transpose* transform

$$PT: \quad \hat{\mathbf{v}} \longrightarrow \Lambda \hat{\mathbf{v}}, \quad \Lambda = \mathrm{diag}(1,1,1,-1). \tag{34}$$

This operation inverts $\hat{p}_2$, leaving $\hat{q}_1$, $\hat{p}_1$, and $\hat{q}_2$ unchanged [4]. In fact, separable states satisfies the usual uncertainty relation (33) and the analogous one obtained under partial transpose; thus these satisfy the condition (30).

On the other hand, the transformation (34) changes the correlation matrix as $V \to \tilde{V} = \Lambda V \Lambda$. Hence, the compact uncertainty relation (11) becomes

$$\tilde{V} + \frac{i}{2}\,\Omega \geq 0. \tag{35}$$

Expressed in terms of invariants, the condition (35) for $\tilde{V}$ takes a form identical to (13). The signature in front of $\det C$ in the second term on the left hand side is changed. Thus, if we write

$$f(V) := \det A \det B + \left(\frac{1}{4} - |\det C|\right)^2$$
$$- \mathrm{tr}(AJCJBJC^T J) - \frac{1}{4}(\det A + \det B), \tag{36}$$

the requirement that the correlation matrix of a separable state has to obey (35), in addition to the fundamental uncertainty principle (11), can be stated as follow

Theorem 5.3 *A bipartite Gaussian state is separable iff $f(V) \geq 0$.*

The necessity follows from theorem 5.1. The sufficiency follows from the fact that Gaussian states with correlation matrix having $\det C \geq 0$ are separable [14].

The statement 5.3 is equivalent to the condition (31), but much more effective to be used.

Given the standard form (14) of the correlation matrix V we can consider the space of all possible Gaussian states as isomorphic to $\mathbb{R}^4$, while the set of *physical* states is a subspace $\mathcal{G} \subset \mathbb{R}^4$ defined through (11). Furthermore, the equation $f(V) = 0$ reads

$$f(V) = 4(ab - c^2)(ab - d^2) - (a^2 + b^2) - 2|cd| - \frac{1}{4} = 0. \tag{37}$$

The equation defines the surface S of the subset $\mathcal{S} \subset \mathcal{G}$ of separable states. Then, by simply evaluating f we can say whether a given state (point in $\mathcal{G}$) is within $\mathcal{S}$ (hence separable) or not (hence entangled). This is an easy computational task that can be efficiently accomplished. In reality, taking into account a finite accuracy δ, we can only say that the state is *almost* separable (resp. *almost* entangled) within δ. Nevertheless, if we want to assert that the state is *strictly* separable (resp. *strictly*

---

[4] The partial transposition of a density matrix, *i.e.* the transposition with respect to the subsystem 2, is equivalent to a mirror reflection in the phase space subsystem 2. That is, $\hat{\rho} \to \hat{\rho}^{T_2} \Leftrightarrow W(x_1, y_1, x_2, y_2) \to W(x_1, y_1, x_2, -y_2)$.

entangled), we have to be sure that the distance of the state $\hat{\rho}$ from the surface S is greater than $1/\delta$. That is

$$\min_{\hat{\rho}' \in S} \|\hat{\rho} - \hat{\rho}'\| > \frac{1}{\delta}. \tag{38}$$

According to Sec.3, the distance between two states is considered as $\|\hat{\rho} - \hat{\rho}'\| \equiv \sqrt{\text{Tr}\left[(\hat{\rho} - \hat{\rho}')^2\right]}$ and for Gaussian states this can be expressed through Wigner functions (hence correlation matrices) as

$$\|\hat{\rho} - \hat{\rho}'\| = \int d^4\mathbf{z} \left[W(\mathbf{z}) - W'(\mathbf{z})\right]^2. \tag{39}$$

Such a task can be efficiently accomplished with the aid of geometrical arguments and simple algorithms. For instance, a software package that efficiently find all hyperplanes tangent to the surface S, from which evaluate the l.h.s. of Eq.(38), is already available [16].

6   Conclusions

Summarizing, we have given a brief review of QSP for Gaussian states of two parties. The problem has been approached by developing tests that involve variances to arrive at an efficient solution based on the invariance (positivity) of only separable states under partial transpose. Notice that this argument can be further generalized to partial scaling transforms to which partial transpose belongs. In fact, while K and V are always invariant under linear canonical transformations, they are not invariant under scale changes on the $\hat{\mathbf{v}}$ that are not contained in $\text{Sp}(4, \mathbb{R})$. In particular under partial scaling K is not necessarily positive definite [17]. These arguments could be extended to multipartite systems, with *e.g.* N degrees of freedom. Starting from the uncertainty relation $K \equiv V + \frac{i}{2}\Omega \geq 0$, we can perform an arbitrary scaling described by the real vector $\mathbf{x} = (x_1, x_2, \ldots x_{2N})$ and then compute

$$K^{\mathbf{x}} = V^{\mathbf{x}} + \frac{i}{2}\Omega, \quad V^{\mathbf{x}} = \Lambda_{\mathbf{x}} V \Lambda_{\mathbf{x}}, \tag{40}$$

with $\Lambda_{\mathbf{x}} \equiv \text{diag}(x_1, x_2, \ldots x_{2N})$. The $2N$ real quantities $\mathbf{x}$ parameterize the Abelian scaling semigroup with the requirement that

$$|x_1 x_2| \geq 1, \; |x_3 x_4| \geq 1, \ldots, |x_{2N-1} x_{2N}| \geq 1. \tag{41}$$

The necessary condition for the separability of the state is

$$K^{\mathbf{x}} \geq 0, \quad \forall \mathbf{x}. \tag{42}$$

Notice, however, that for multipartite systems besides separability (resp. inseparability) there can be the possibility of partial separability (resp. partial inseparability), *e.g.* separability of a subsystem with respect to the others which in turns are entangled [9]. Hence QSP becomes much more subtle and even for Gaussian states it is not completely understood.

Acknowledgemts

We warmly thank Jens Eisert for useful comments.

References

[1] Einstein, A., B. Podolski, and N. Rosen, Can quantum mechanical description of physical reality be considered complete?, *Phys. Rev.* **47** (1935), 777.

[2] Nielsen, M., and I. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, Cambridge, 2000.

[3] Grötschel, M., L. Lovasz and A. Schrijver, *Geometric Algorithms and Combinatorial Optimization*, Springer-Verlag, Berlin, 1988.

[4] Ioannou, L. M., B. C. Travaglione, D. Cheung, and A. K. Ekert, *An improved algorithm for quantum separability and entanglement detection*, Physical Review A **70** (2004) 060303(R), http://arxiv.org/quant-ph/0403041

[5] Gurvits, L., *Classical deterministic complexity of Edmonds' problem and quantum entanglement*, in Proceedings of the 35th ACM Symposium on Theory of Computing, ACM Press, New York, 2003.

[6] Peres, A., *Separability criterion for density matrices*, Physical Review Letters **77** (1996), 1413; Horodecki, M., P. Horodecki and R. Horodecki, *On the necessary and sufficient condition for separability of mixed quantum states*, Physics Letters A **223** (1996), 1.

[7] Braunstein, S. L., S. Ghosh, and S. Severini, *The laplacian of a graph as a density matrix: a basic combinatorial approach to separability of mixed states*, http://arxiv.org/quant-ph/0406165 Braunstein, S. L., S. Ghosh, and S. Severini, *Some families of density matrices for which separability is easily tested*, Physical Review A **73** (2006) 012320, http://arxiv.org/quant-ph/0508020

[8] Laurat, J., *Entanglement of two-mode Gaussian states: characterization and experimental production and manipulation*, Journal of Optics B **7** (2005) S577, http://arxiv.org/quant-ph/0507067

[9] Braunstein S. L., and P. van Loock, *Quantum information with continuous variables*, Review Modern Physics **77** (2005), 513, http://arxiv.org/quant-ph/0410100

[10] Dirac, P. A. M., *Principles of Quantum Mechanics*, Pergamon, Oxford, 1958.

[11] Kim, Y. S., and M. E. Noz, *Phase Space Picture of Quantum Mechanics*, World Scientific, Singapore, 1986.

[12] Giovannetti V., S. Mancini, D. Vitali, and P. Tombesi, *Characterizing the entanglement of bipartite quantum systems*, Physical Review A **67** (2003), 022320, http://arxiv.org/quant-ph/0210155

[13] Hyllus, P., and J. Eisert, *Optimal entanglement witnesses for continuous-variable entanglement*, http://arxiv.org/quant-ph/0510077

[14] Simon, R., *Peres-Horodecki separability criterion for continuous variable systems*, Physical Review Letters **84** (2000), 2726, http://arxiv.org/quant-ph/9909044

[15] Duan, L. M., G. Giedke, J. I. Cirac, and P. Zoller. *Inseparability criterion for continuous variable systems*, Physical Review Letters **84** (2000), 2722, http://arxiv.org/quant-ph/9908056

[16] Hyllus, P., and J. Eisert, FullyWit, available from http://www.imperial.ac.uk/quantuminformation

[17] Man'ko, O. V., V. I. Man'ko, G. Marmo, A. Shaji, E. C. G. Sudarshan, and F. Zaccaria, *Partial positive scaling transform: a separability criterion*, http://arxiv.org/quant-ph/0502089