

Pure State Estimation and the Characterization of Entanglement

Miguel Navascués

ICFO-Institut de Ciències Fotoniques, Mediterranean Technology Park, 08860 Castelldefels (Barcelona), Spain
(Received 7 August 2007; published 20 February 2008)

A connection between the state estimation problem and the separability problem is noticed and exploited to find efficient numerical algorithms to solve the first one. Based on these ideas, we also derive a systematic method to obtain upper bounds on the maximum local fidelity when the states are distributed among several distant parties.

DOI: [10.1103/PhysRevLett.100.070503](https://doi.org/10.1103/PhysRevLett.100.070503)

PACS numbers: 03.67.Mn

The estimation of specific properties of a quantum system subject to observation was one of the very first problems posed in Quantum Information Theory [1]. This problem has no analog in the classical case, where all measurements commute and a sufficiently subtle observer (a Maxwell demon) is able to make complete tomography of a system without introducing any perturbations in it. In the quantum case, measurements are irreversible and invariably destroy information, and thus we have to design and optimize our measurement strategy according to some figure of merit, that is, we have to decide “what to see” before we can extract conclusions from “what we see.” This figure of merit can be, for instance, the mean variance between our estimator and the quantity we want to determine [2], or the mutual information between the outcome of our measurement and the parameters that describe the possible set of states [3]. When the figure of merit is related to the overlap between two quantum states, then we are dealing with a state estimation problem [4]. In its most usual form, this consists on estimating the whole wave function of an unknown state when only a limited number of copies of this state is available. Initially considered as a purely theoretical problem interesting by itself, it has immediate applications in the calibration of quantum optical devices, where complete tomography is impractical, or even impossible (like when we deal with continuous variable systems, for example). Moreover, a variant of state estimation, namely, state discrimination, has recently been used in quantum computation to find efficient quantum algorithms to solve the Hidden Subgroup Problem [5].

In a general state estimation scenario, a source produces with probability p_i a quantum state Ψ_i that is encoded afterwards into another quantum state Ψ'_i , to which we have full access. Our duty is to measure our given state and thus obtain a classical value x that we may use to make a guess on the original state Ψ_i , which we will assume to be pure along this article. For abbreviation, we will label this type of problems by (p_i, Ψ_i, Ψ'_i) . Games belonging to this family appear quite often in quantum information theory. For example, we could think of quantum tomography as a protocol in which a source produces a state Ψ_i and encodes it into $\Psi'_i = \Psi_i^{\otimes N}$. Analogously, state discrimination can

be easily proven to be equivalent to a state estimation problem where the source produces orthogonal states $\{|i\rangle\langle i|\}$ and encodes them into nonorthogonal states $\{\Psi_i\}$. A usual figure of merit to quantify the knowledge on Ψ_i provided by x is the so called fidelity. The idea is to prepare a state ϕ_x as a guess and then compare this state to the one that was originally encoded by the source just by computing the overlap between the two: $\text{Tr}(\phi_x \Psi_i)$ (remember that we assume the states $\{\Psi_i\}_i$ to be pure). If we denote by M_x each of the positive operator value measure (POVM) elements that mathematically describe our measurement of the state Ψ'_i , then the efficiency of our strategy (M_x, ϕ_x) will then be determined by the average fidelity f :

$$0 \leq f \equiv \sum_{i,x} p_i \text{Tr}(\Psi'_i M_x) \text{Tr}(\phi_x \Psi_i) \leq 1. \quad (1)$$

The state estimation problem consists on determining F , defined as the maximum fidelity among all possible strategies (M_x, ϕ_x) .

Up to now, we have been considering global state estimation. But there are many interesting situations in Quantum Information Theory where the encoded states $\{\Psi'_i\}_i$ are distributed between two or more distant parties. In this situation, the parties will have to agree on a strategy based on local operations and classical communication (LOCC) that allows them to extract enough information about the sent states so that they can make a good guess on the state produced by the source. Then, we will be interested in determining the local fidelity F_L :

$$F_L = \sup \sum_{i,x} p_i \text{Tr}(\Psi'_i (M_x)_{AB}) \text{Tr}(\phi_x \Psi_i), \quad (2)$$

where the $(M_x)_{AB}$ correspond to the POVM elements of a measurement accessible via LOCC.

The main result of this Letter is the following:

Proposition 1.—For any global state estimation problem with solution F , there exists a sequence of real numbers $F^{(1)}, F^{(2)}, F^{(3)}, \dots$, where each of the elements can be computed efficiently, and such that $F^{(1)} \geq F^{(2)} \geq F^{(3)} \geq \dots \geq F$ and $\lim_{n \rightarrow \infty} F^{(n)} = F$.

This proposition can be adapted to deal with the problem of local state estimation, and the result is

Proposition 2.—For any local state estimation problem with solution F_L , there exists a sequence of real numbers $F_S^{(1)}, F_S^{(2)}, F_S^{(3)}, \dots$, where each of the elements can be computed efficiently, and such that $F_S^{(1)} \geq F_S^{(2)} \geq F_S^{(3)} \geq \dots$ and $\lim_{n \rightarrow \infty} F_S^{(n)} = F_S \geq F_L$, where F_S corresponds to the separable fidelity, i.e., the maximum attainable fidelity when the POVM is separable with respect to the k parties.

The structure of this Letter is as follows: first, we will show the connection between the state estimation problem and the separability problem and use it to proof proposition 1. An isotropic distribution of states of arbitrary dimension will be considered to illustrate the efficiency of the resulting numerical tools. Proposition 2 will follow naturally from proposition 1, and the problem of local state estimation of an arbitrary probability distribution of Bell states will be solved as an example. Finally, we will expose our conclusions.

For any state estimation problem (p_i, Ψ_i, Ψ'_i) and any state estimation strategy (M_x, ϕ_x) the corresponding fidelity f can always be expressed as

$$f = \text{Tr}(\rho_{AB} \Lambda_{AB}), \quad (3)$$

with $\rho_{AB} = \sum_i p_i \Psi'_i \otimes \Psi_i$, $\Lambda_{AB} = \sum_x M_x \otimes \phi_x$. Note that, while ρ_{AB} is a separable quantum state fixed by the state estimation problem, Λ_{AB} only depends on our measure-and-prepare strategy. It is immediate to see that for Λ_{AB} to describe the action of a strategy over ρ_{AB} , Λ_{AB} must be a separable positive semidefinite operator. Moreover, $\text{Tr}_B \Lambda_{AB} = \sum_x M_x = \mathbb{1}_A$. Conversely, any separable positive semidefinite operator Λ_{AB} with partial trace equal to the identity can be made to correspond to a state estimation strategy. Thus, the state estimation problem can be reformulated in this way:

$$F = \sup\{\text{Tr}(\Lambda_{AB} \rho_{AB}) : \Lambda_{AB} \text{sep}, \text{Tr}_B \Lambda_{AB} = \mathbb{1}\}. \quad (4)$$

To see how this approach works, consider the problem of estimating pure states that are distributed according to an isotropic probability density; i.e., we are dealing with $(dU, U|0\rangle\langle 0|U^\dagger, U|0\rangle\langle 0|U^\dagger)$, where U is a unitary operator and dU denotes the Haar measure of the unitary group $SU(d)$. Then,

$$\rho_{AB} = \int U|0\rangle\langle 0|U^\dagger \otimes U|0\rangle\langle 0|U^\dagger dU = \frac{1}{d(d+1)}(\mathbb{1} + V), \quad (5)$$

where V denotes the flip operator. Now, take Λ_{AB} to be an operator associated to a possible state estimation strategy for this problem. It is easy to see that $f = \text{Tr}(\rho_{AB} \Lambda_{AB}) = \text{Tr}(\rho_{AB} \tilde{\Lambda}_{AB})$, where $\tilde{\Lambda}_{AB} = \int U \otimes U \Lambda_{AB} U^\dagger \otimes U^\dagger dU$. Note that $\tilde{\Lambda}_{AB}/d$ is a separable state and $\text{Tr}_B(\tilde{\Lambda}_{AB}) = \mathbb{1}$; i.e., $\tilde{\Lambda}_{AB}$ corresponds to a strategy.

The above argument shows that we can take Λ_{AB}/d to be a Werner state [6]. Werner states are a monoparametrical family of states whose partial trace is proportional to the

identity and whose separability regions are identified. Following [6], we can write Λ_{AB} as $\Lambda_{AB} = \frac{1}{d(d^2-1)}[(d-t)\mathbb{1} + (dt-1)V]$, where $-1 \leq t \leq 1$ guarantees that Λ_{AB} is positive semidefinite and $t \geq 0$ implies that it is separable. A direct calculation shows that

$$\text{Tr}(\rho_{AB} \Lambda_{AB}) = \frac{1+t}{d+1}. \quad (6)$$

Thus, we get that $F = \frac{2}{d+1}$, recovering the results of Bruß and Macchiavello [7].

To solve the above problem we played with the advantage that the separability properties of Werner states are well known. However, most state estimation problems do not have the symmetries of (5). How could we exploit the reformulation of the problem given by (4) in order to address the general case? The approach we chose makes use of a characterization of the set of all separable states due to Doherty *et al.* [8]. This characterization is based on the notion of PPT symmetric extensions.

A PPT symmetric extension $\tilde{\Lambda}_{AB}^{(n)}$ to n copies of party A of a bipartite quantum state $\tilde{\Lambda}_{AB}$ is a positive semidefinite operator $\tilde{\Lambda}_{AB}^{(n)} \in \mathcal{B}(\mathcal{H}_A^{\otimes n} \otimes \mathcal{H}_B)$ such that (1) $\tilde{\Lambda}_{AB}^{(n)}$ is symmetric with respect to the interchange of any two copies of system A . (2) $\tilde{\Lambda}_{AB}^{(n)}$ returns the state $\tilde{\Lambda}_{AB}$ when $n-1$ copies of system A are traced out. (3) $\tilde{\Lambda}_{AB}^{(n)}$ remains positive under all possible partial transpositions.

We will define $S^{(n)}$ as the set of all bipartite operators $\tilde{\Lambda}_{AB}$ that admit a PPT symmetric extension to n copies of system A .

If we call S to the set of all separable states, it is not difficult to prove that any element of S must belong to $S^{(n)}$ for any n [9]. This observation immediately leads us to an infinite set of necessary conditions for a state to be separable. Moreover, this set of conditions constitutes a hierarchy, since it follows from the definition of PPT symmetric extension that any state belonging to $S^{(n+1)}$ has necessarily to belong to $S^{(n)}$. What it is not so obvious is that this hierarchy is complete. That is, any quantum state belonging to $S^{(n)}$ for all n can be proven to be separable [8].

Let d_A be the dimension of \mathcal{H}_A . Consider now the following problem:

$$F^{(n)} = \sup\{\text{Tr}(\Lambda_{AB} \rho_{AB}) : \Lambda_{AB}/d_A \in S^{(n)}, \text{Tr}_B \Lambda_{AB} = \mathbb{1}\}. \quad (7)$$

From what we have seen, it is evident that $F^{(1)} \geq F^{(2)} \geq F^{(3)} \geq \dots \geq F$ and, moreover, $\lim_{n \rightarrow \infty} F^{(n)} = F$. The advantage of this approach is that each of the bounds $F^{(n)}$ can be computed efficiently using semidefinite programming.

Semidefinite programming is a branch of numerical analysis that is concerned with the following optimization problem:

$$\text{minimize } \vec{c}^T \cdot \vec{x} \text{ subject to } F(\vec{x}) \equiv F_0 + \sum_{i=1}^n x_i F_i \geq 0, \quad (8)$$

where $\{F_i\}_{i=0}^n$ are $N \times N$ matrices. This is known as the primal problem and its solution is usually denoted by p^* . For each primal problem there is an associated dual problem, of the form

$$d^* \equiv \text{maximize } -\text{Tr}(F_0 Z) \text{ subject to } Z \geq 0, \quad (9)$$

$$\text{Tr} F_i Z = c_i, \quad i = 1, \dots, n,$$

that can also be treated a semidefinite program. It can be seen that $d^* \leq p^*$ [10]. Moreover, a sufficient condition to assure that $d^* = p^*$ is the existence of a strict primal feasible point, that is, a vector \vec{x} such that $F(\vec{x}) > 0$. Note that this condition holds in our case, for it is straightforward that the matrix $\bar{\Lambda}_{AB}^{(n)} \equiv (\mathbb{1}_A/d_A)^{\otimes n} \otimes \mathbb{1}_B/d_B > 0$ corresponds to a PPT symmetric extension to n copies of system A of the quantum state $\Lambda_{AB}/d_A \equiv (\mathbb{1}_A/d_A) \otimes \mathbb{1}_B/d_B$, with $\text{Tr}_B(\Lambda_{AB}) = \mathbb{1}$.

The scheme to solve (7) would then be to run algorithms that try to solve both the dual and the primal problem at the same time. If, after some iterations, our computer returns the points \vec{x} , Z , we know that the solution of our problem lies somewhere in the middle, i.e., $\text{Tr}(ZF_0) \leq p^* \leq \vec{c}^T \cdot \vec{x}$. Because semidefinite programs belong to the P complexity class and the matrices involved in the calculation of each bound $F^{(n)}$ increase in size as $d_A^n d_B$, for fixed n , $F^{(n)}$ can be calculated efficiently, as promised. We have proven Proposition 1.

Although Proposition 1 only guarantees the asymptotic convergence of the series ($F^{(n)}$) to the optimal fidelity, for some specific problems we may find the value of F after a few iterations. Returning to the task of estimating isotropically distributed quantum states, because the maximum of (6) when Λ_{AB} is only demanded to be positive semidefinite is the same as the maximum among the set of all separable operators, it follows that $F^{(1)} = F$, i.e., if we had performed a numerical optimization, the first upper bound would have coincided with the optimal fidelity. Also, in case the original and encoded states of the protocol are elements of a Hilbert space of dimension 2, the PPT criterion is sufficient to guarantee the separability of Λ_{AB} [11], and thus, for all these problems, $F = F^{(1)}$.

These ideas can be extended to obtain upper bounds on the solution of more complicated problems. Suppose that the given state Ψ_i' is a bipartite state that is distributed by a source to two spatially separated parties, Alice and Bob. Then, Alice and Bob would have to agree on a protocol based on local operations and classical communication that allowed them to obtain classical information about the original state Ψ_i .

This problem can be reformulated in a similar fashion as (4)

$$F_L = \sup\{\text{Tr}(\Lambda_{ABC}\rho_{ABC}): \Lambda_{ABC}\text{LOCC}\}, \quad (10)$$

where $\rho_{ABC} = \sum_i p_i (\Psi_i')_{AB} \otimes \Psi_i$, and Λ_{ABC} denotes an element of the set of all strategies that are accessible to Alice and Bob using LOCC. Unfortunately, this problem cannot be solved directly, for up to now no one has been able to characterize the set of all POVMs accessible by LOCC. However, we know that such a set is contained in the set of all separable POVMs, and thus we may conform with an upper bound on F_L , namely, F_S , the separable fidelity, which we could define as

$$F_S = \sup\{\text{Tr}(\Lambda_{ABC}\rho_{ABC}): \Lambda_{ABC}\text{trisep}, \text{Tr}_C \Lambda_{ABC} = \mathbb{1}\}. \quad (11)$$

It is known that F_L and F_S do not coincide in general. For example, the separable fidelity of a uniform distribution of the domino states [12] would be 1, whereas F_L can be proven to be strictly smaller than 1. However, sometimes F_S can be a reasonable approximation to F_L , as we will soon see.

There exists a complete characterization of the set of all k -separable states, also due to Doherty *et al.* [13], and also implementable using semidefinite programming packages. This characterization is just a generalization of the previous one. In this case, we would demand from any triseparable (normalized) state $\bar{\Lambda}_{ABC}$ that it admits a PPT symmetric extension to n copies of systems A and B , for any n . Analogously to the global state estimation case, we would obtain a sequence of upper bounds $F_S^{(1)} \geq F_S^{(2)} \geq \dots \geq F_L$. However, this time $\lim_{n \rightarrow \infty} F_S^{(n)} = F_S \geq F_L$. This scheme can be easily generalized to any number of distant parties. Proposition 2 has been proven.

To see the usefulness of this method, consider the particular example where Alice and Bob are distributed one of the four Bell states with different probabilities, and that each of these states encodes the very same Bell state, that is, if we call $\{\psi_i\}_{i=1}^4$ to the four Bell states, we would be dealing with the problem $(p_i, \psi_i, (\psi_i)_{AB})$. Take

$$\psi_{1,2} = \frac{1}{2}(|00\rangle \pm |11\rangle)(\langle 00| \pm \langle 11|), \quad (12)$$

$$\psi_{3,4} = \frac{1}{2}(|01\rangle \pm |10\rangle)(\langle 01| \pm \langle 10|).$$

We are going to calculate $F_S^{(1)}$. The corresponding primal problem is

$$\text{maximize } \text{Tr}(\rho_{ABC}\Lambda_{ABC}) \text{ subject to } \text{Tr}_C(\Lambda_{ABC}) = \mathbb{1}, \quad (13)$$

$$\Lambda_{ABC}, \quad \Lambda_{ABC}^{T_A}, \quad \Lambda_{ABC}^{T_B}, \quad \Lambda_{ABC}^{T_C} \geq 0,$$

with $\rho_{ABC} = \sum_i p_i (\psi_i)_{AB} \otimes (\psi_i)_C$.

The dual of this problem (module some simplifications) is

$$\begin{aligned} & \text{minimize } \text{Tr}(\tilde{\rho}) \text{ subject to } A, B, C \geq 0, \\ & \tilde{\rho} \otimes \mathbb{1}_C - A^{T_A} - B^{T_B} - C^{T_C} - \rho_{ABC} \geq 0. \end{aligned} \quad (14)$$

From our previous discussion about semidefinite programming, it follows that any feasible point of the dual of a semidefinite program provides an (in this case) upper bound on the solution of the primal problem. The fact that $\psi_i^{T_A} = \mathbb{1} - 2\psi_{5-i}$ suggests that we may try to solve the dual problem using the following ansatz:

$$A = \sum_i \frac{\lambda_i}{2} \psi_{5-i} \otimes \psi_i, \quad B = C = 0, \quad \tilde{\rho} = \sum_j \mu_j \psi_j. \quad (15)$$

$A \geq 0$ implies that $\lambda_i \geq 0$, $\forall i$. Analogously, $\tilde{\rho} \otimes \mathbb{1}_C - A_A^T - \rho_{ABC} \geq 0$ implies that

$$\mu_i \geq p_i - \frac{\lambda_i}{2} \quad \mu_j \geq \frac{\lambda_j}{2}, \quad \forall j = i. \quad (16)$$

What we have to minimize is the quantity $\tilde{f} = \sum_j \mu_j$. If we fix the λ s, the minimum value of each μ_i will be $\mu_i = \max(\{\frac{\lambda_i}{2} : j \neq i\}, p_i - \frac{\lambda_i}{2})$. Therefore, $\tilde{f} = \sum_i \max(\{\frac{\lambda_i}{2} : j \neq i\}, p_i - \frac{\lambda_i}{2})$. Because of the symmetry of the problem, we can suppose that $\lambda_1 \geq \lambda_2$ are the two greatest λ s. Then, $\tilde{f} = \max(\frac{\lambda_2}{2}, p_1 - \frac{\lambda_1}{2}) + \sum_{i=2}^4 \max(\frac{\lambda_i}{2}, p_i - \frac{\lambda_i}{2})$. This quantity can only be made smaller if we take $\lambda_{3,4} = \lambda_2$, and so we can assume $\tilde{f} = \max(\frac{\lambda_2}{2}, p_1 - \frac{\lambda_1}{2}) + \sum_{i=2}^4 \max(\frac{\lambda_i}{2}, p_i - \frac{\lambda_i}{2})$.

On the other hand, for any choice of λ_1, λ_2 , it can be proven that \tilde{f} becomes strictly smaller if we take $\lambda'_1 = \lambda'_2 = (\lambda_1 + \lambda_2)/2 \equiv \lambda$. Finally, $\tilde{f} = \sum_{i=1}^4 \max(\frac{\lambda}{2}, p_i - \frac{\lambda}{2})$. If we order the probabilities such that $p_a \geq p_b \geq p_c \geq p_d$, it is immediate to check that the guess $\lambda = p_c$ provides the minimum value $\tilde{f} = p_a + p_b$. Therefore, $F_L \leq F_S^{(1)} \leq p_a + p_b$.

But such fidelity is actually attainable. All Alice and Bob have to do is to measure either in the computational or in the X basis each and prepare the Bell states with greatest probability that are compatible with their measurements. For example, in the case where $p_a = p_1, p_b = p_2$, Alice and Bob should measure in the X basis. If their results are correlated, they should prepare the state ψ_1 . Otherwise, they should prepare the state ψ_2 . It is straightforward to see that this strategy attains a fidelity $f_L = p_1 + p_2$.

Incidentally, because the Bell states are orthogonal to each other, this state estimation problem is equivalent to

the state discrimination problem $(p_i, |i\rangle\langle i|, \Psi_i)$, that is, F_L also corresponds to the maximum probability of determining which Bell state was sent to Alice and Bob.

In conclusion, we have shown a systematic method to numerically solve the state estimation problem, and we have seen how this approach can be slightly modified to attack the local state estimation problem. Semidefinite programming had already been used in the resolution of state discrimination problems [5,14], but, to the author's knowledge, this is the first time such a mathematical tool is proposed to deal with the general state estimation scenario.

Along this Letter, we have been tacitly assuming that we were dealing with state estimation problems in finite dimensions. We have ideas about how to treat the infinite dimensional case, that will be developed in future publications.

We thank Antonio Acín for useful discussions and the Fundación Ramón Areces for financial support.

-
- [1] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory* (North-Holland, Amsterdam, 1982).
 - [2] H. P. Yuen and M. Lax, *IEEE Trans. Inf. Theory* **19**, 740 (1973).
 - [3] A. S. Holevo, *Statistical Problems in Quantum Physics*, Proceedings of the Second Japan-USSR Symposium on Probability Theory, Vol. 330 (Springer, Berlin/Heidelberg, 1973), p. 104.
 - [4] S. Massar and S. Popescu, *Phys. Rev. Lett.* **74**, 1259 (1995).
 - [5] L. Ip, Shors algorithm is optimal, <http://lawrenceip.com/papers/hspdpabstract.html> (2003).
 - [6] R. F. Werner, *Phys. Rev. A* **40**, 4277 (1989).
 - [7] D. Bruß and C. Macchiavello, *Phys. Lett. A* **253**, 249 (1999).
 - [8] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *Phys. Rev. A* **69**, 022308 (2004).
 - [9] If $\bar{\Lambda}_{AB}$ is a separable state, then there exists a decomposition $\bar{\Lambda}_{AB} = \sum_i p_i \Lambda_i \otimes \Lambda'_i$. It is immediate to check that the state $\sum_i p_i \Lambda_i^{\otimes n} \otimes \Lambda'_i$ is a PPT symmetric extension of $\bar{\Lambda}_{AB}$ to n copies of party A .
 - [10] L. Vandenberghe and S. Boyd, *SIAM Rev.* **38**, 49 (1996).
 - [11] M. Horodecki, P. Horodecki, and R. Horodecki, *Phys. Lett. A* **223**, 1 (1996).
 - [12] C. H. Bennett *et al.*, *Phys. Rev. A* **59**, 1070 (1999).
 - [13] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *Phys. Rev. A* **71**, 032333 (2005).
 - [14] M. Ježek, J. Rehacek, and J. Fiurasek, *Phys. Rev. A* **65**, 060301 (2002).