A complete criterion for separability detection

Miguel Navascués1, Masaki Owari1,2 and Martin B. Plenio1,2

1Institute for Mathematical Sciences, Imperial College London, SW7 2PE, UK.
2QOLS, The Blackett Laboratory, Imperial College London, Prince Consort Rd., SW7 2BW, UK

Using new results on the separability properties of bosonic systems, we provide a new complete criterion for separability. This criterion aims at characterizing the set of separable states from the inside by means of a sequence of efficiently solvable semidefinite programs. We apply this method to derive arbitrarily good approximations to the optimal measure-and-prepare strategy in generic state estimation problems. Finally, we report its performance in combination with the criterion developed by Doherty et al. 1 for the calculation of the entanglement robustness of a relevant family of quantum states whose separability properties were unknown.

PACS numbers:

Research on separability criteria, that is, on computational methods to determine whether a given state is separable or entangled, is a popular subject in Quantum Information Theory. Starting from the famous PPT (Positive Partial Transpose) criterion, a considerable number of different separability criteria have been discovered (see the references in 2,4,8,11). Unfortunately, the most efficient ones happen to be partial criteria, in the sense that they only detect entanglement or separability in certain situations. This is not surprising, in view of the fact that the separability problem is NP-hard 7.

A complete criterion for entanglement detection is an algorithm or method that allows to characterize the set of separable states with arbitrary precision. Alternatively, we may say that a complete criterion for separability can solve any instance of the Weak Membership Problem of separability 2, i.e., the problem of determining if a given quantum state is close to the core of the set of separable states. Up to now, there exist several different complete separability criteria 1,3,4,7,8,10,11,12,13,14. In all these methods, the set of separable states is approximated successively by an appropriate sequence of sets of states. The complexity of characterizing each of these sets increases as we move along the sequence, that converges to the set of separable states in the asymptotic limit. That way, we can characterize the set of separable states up to a precision that is only limited by our computational resources.

While traditionally Entanglement Theory has focused most of its efforts in developing criteria for entanglement detection 1,3,4,7,8,10,11,12,13,4,8,11,12,13,14, thus characterizing the set of separable states from the outside, there exist a few complete criteria that try to approximate the set of separable states from the inside, i.e., whose aim is to detect separability instead of entanglement. Examples of the latter type are the algorithms invented by Hulpke et al. 10, Brandao et al. 11 or Spedalieri 13. The main drawbacks of the first two are their high time complexity, as estimated in 4. The method designed by Spedalieri, although very promising, does not currently have any proven bounds on its speed of convergence, and cannot be extended to deal with multipartite entanglement 13.

Let us also remark that, in all the above cases, the main algorithm works by almost directly invoking the definition of separability, i.e., no insight from Entanglement Theory itself was employed in their conception.

In this paper, we present a new complete criterion for separability which takes inspiration from the symmetric extension criterion developed by Doherty, Parrilo and Spedalieri (the DPS criterion) 1,14. However, while the DPS criterion tries to approximate the set of separable states from the outside, our new criterion will work from the inside. Our criterion not only detects separability, but also provides an explicit separable decomposition of the separable states in terms of an integral over the Haar measure. Moreover, it has the same proven time complexity as the original DPS criterion. Due to its internal structure, the new criterion can be easily modified to perform linear optimizations over entanglement breaking channels. In particular, given any state estimation problem, the method can output a sequence of measure-and-prepare strategies arbitrarily close to optimal. In the last pages of this letter, as an illustration of its efficiency, we will show its performance by computing the robustness of entanglement of a family of quantum states.

But, first, some remarks about notation. In this letter, we will be mainly concerned with a finite dimensional bipartite Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. The set of all linear operators acting on $\mathcal{H}$ will be denoted as $\mathcal{B}(\mathcal{H})$, and we will use the term state in order to refer to normalized non-negative operators in $\mathcal{B}(\mathcal{H})$. Finally, the cone of separable operators, i.e., the conical combination of all pure product states $\{\langle \psi_A | \psi_A \rangle \otimes \langle \psi_B | \psi_B \rangle\}$, will be called $\mathcal{S}$. Note that any operator in $\mathcal{S}$ must be necessarily non-negative.

The sequences of sets employed to approximate $\mathcal{S}$ in the DPS criterion are either the sets $\{\mathcal{S}^N\}$ of $N$-(Bose) symmetrically extendible operators or the sets $\{S_p^N\}$ of PPT $N$-(Bose) symmetrically extendible operators. These sets are defined as follows: $\Lambda_{AB} \in \mathcal{B}(\mathcal{H}_{AB})$ belongs to $\mathcal{S}^N$ iff there exists an opera-
tor $\Lambda_{ABN} \in B(\mathcal{H}_{ABN})$ that satisfies the following three conditions:

1. $\Lambda_{ABN} \geq 0$.
2. $\text{tr}_{B,N-1}(\Lambda_{ABN}) = \Lambda_{AB}$.
3. $\Lambda_{ABN}$ is Bose symmetric in $\mathcal{H}_B^{\otimes N}$, i.e., $\Lambda_{ABN}(I_A \otimes P_{\text{Sym}}^N) = \Lambda_{ABN}$, where $P_{\text{Sym}}^N$ denotes the projector onto the symmetric subspace of $\mathcal{H}_B^{\otimes N}$.

Similarly, $\Lambda_{AB} \in S_p^N$ if there exists an operator $\Lambda_{ABN} \in B(\mathcal{H}_{ABN})$ fulfilling 1-3 and the additional constraint:

4. $\Lambda_{ABN}$ has a Positive Partial Transpose (i.e., it is PPT) w.r.t. the bipartition $AB^{[N/2]}|B^{[N/2]}$.

Doherty et al. [14] proved that both sequences \{${S}^N_p$\}$_{N=1}^\infty$ and \{${S}^N_p$\}$_{N=1}^\infty$ converge to $\mathcal{S}$ from the outside:

\[
\mathcal{S}_P \supset \mathcal{S}_P^2 \supset \mathcal{S}_P^3 \supset \cdots \supset \mathcal{S}, \text{ with } \lim_{N \to \infty} \mathcal{S}_P^N = \mathcal{S}. \quad (1)
\]

The DPS criterion consists, precisely, in checking if $\rho_{AB} \in S_p^N$ for all $N$. From the relations above, the DPS criterion is clearly complete: if $\rho_{AB}$ is separable, then there exists an $M$ such that $\rho_{AB} \notin S^M_p$, so all entangled states can be eventually detected. As all these sets are defined through linear matrix inequalities, the problem of determining whether a given state belongs to one of them can be cast as a semidefinite program (SDP) [15].

In [16] it was shown that, for any $\rho_{AB} \in S^N$ or $S_p^N$, a small perturbation on system $B$ results in a separable state $\tilde{\rho}_{AB}$. More concretely, define $d \equiv \dim(\mathcal{H}_B)$ and

\[
\epsilon_N \equiv \frac{d}{2(d-1)} \min\{1-x : P((N/2)+1,mod 2) (x) = 0\}, \quad (2)
\]

with $P_{\alpha,\beta} (x)$ being the Jacobi polynomials [20]. Then, the following closed cones of operators satisfy $\mathcal{S}^N_P \supset \mathcal{S}^N_P \subset \mathcal{S}$, for all $N$. Moreover, for any given $\rho_{AB} \in S_{P}^{(N)}$, we can find a corresponding separable decomposition in terms of an integral over a Haar measure. Suppose, for instance, that $\sigma_{ABN}$ is a Bose symmetric extension of $\sigma_{AB} \in S^N$. Then, the separable decomposition of the state $\rho_{AB} \in \mathcal{S}$ that results from perturbing $\sigma_{AB}$ as in equation (3) is given by

\[
\rho_{AB} = C \int d\phi_B \text{ tr}_{B,N} \{I_A \otimes \phi_B \otimes \sigma_{ABN}\} \otimes \phi_B, \quad (5)
\]

where $C$ is a normalization constant and $d\phi_B$ is a Haar measure over all pure states $\phi_B$ on $\mathcal{H}_B$. The reader can find a similar decomposition for any state $\rho_{AB} \in S_p^N$ in [16].

Note that, in both definitions, taking the limit $N \to d$ implies, on one hand, that $\mathcal{S}^N \approx S_p^N$, $\mathcal{S}^N \approx S_p^N$ [23], and, on the other hand, that $S_p^N$, $S^N \approx \mathcal{S}$. It follows that the closures of the limiting sets $\lim_{N \to \infty} \mathcal{S}^N, S_p^N$ coincide with the set of separable states.

Therefore, as opposed to the DPS criterion, the sequences of sets $\{\mathcal{S}_P^N\}_N, \{S_p^N\}_N$ converge to the set of separable states from the inside. These sets can be characterized using semidefinite programming; in fact, a small modification of the computer codes employed to search over the sets $\mathcal{S}^N, S_p^N$ allows to perform optimizations over the sets $\mathcal{S}_P, S_p$ [23]. We thus arrive at a novel algorithm for entanglement detection complementary to the DPS criterion, and with a very similar structure [24]. In view to its strong link with the latter criterion, from now on we will refer to this new algorithm as $\text{DPS}^*$.

We will now proceed to study the speed of convergence of $\text{DPS}^*$. First, notice that, as $\mathcal{S} \subset \mathcal{S}_P^N$, equation (2) tells us that we can perturb any general separable state $\rho_{AB}$ to a state $\tilde{\rho}_{AB}$ inside $\mathcal{S}^N$ and $\mathcal{S}_P^N$. This observation, together with the techniques employed in [16], allows us to derive the following proposition:

**Proposition 1.** Denote by $\| \cdot \|_p$ the $p$-norm, i.e., $\|Z\|_p = (\text{tr}(\sqrt[p]{ZZ^\dagger}))^{1/p}$, and let $\rho \in \mathcal{S}$ be a separable state. Then, there exists a normalized state $\sigma \in \mathcal{S}_P^N$ such that:

\[
\|\rho - \sigma\|_1 \leq \frac{2(d-1)}{N + d}, \quad \text{and} \quad \|\rho - \sigma\|_\infty \leq \frac{d - 1}{N + d}.
\]

Analogously, there exists a normalized state $\sigma_p \in \mathcal{S}_p^N$ such that:

\[
\|\rho - \sigma_p\|_1 \leq \frac{2(d-1)}{d}, \quad \text{and} \quad \|\rho - \sigma_p\|_\infty \leq \frac{(d-1)\epsilon_N}{d}.
\]
It is worth noting that all the above bounds cannot be improved, since they correspond to the exact distances of $\rho_{AB}$ to the sets $S^N$ or $S^N_p$ whenever $\rho_{AB}$ is a pure product state.

Proposition 1 allows us to study the efficiency of the criterion based on the sequence of sets $(S^N)$ as opposed to the one based on $(S^N_p)$ when applied to solve the weak membership problem of separability (WMEM(S)) [7, 8], i.e., the problem of determining whether a state $\rho_{AB}$ is separable or not up to some precision $\delta$. Since our bounds on the speed of convergence of DPS* have the same scaling as those derived for the DPS criterion in [16], our conclusions on the complexity of the former cannot but be the same, namely:

1. From the point of view of time complexity, it is always preferable to consider the sets $S^N_p$ rather than $S^N$. Whereas the time complexity of the latter scales with $\delta$ as $O\left(d_A^4 (k_3/\delta)^{d_B}\right)$, the number of operations required under the PPT constraint scales as $O\left(d_A^4 (k_2/\delta)^{d_B}\right)$.

2. From the point of view of space complexity, sometimes it may be more convenient to search over the sets $\{S^N\}$ rather than over $\{S^N_p\}$.

3. In any case, due to its fast proven convergence as compared to other methods [3], the DPS* criterion is one of the most efficient algorithms for entanglement detection. Because of the polynomial dependence on $d_A$ of its bounds on time or space complexity, DPS* is especially useful to attack problems where the dimension of one of the systems is much bigger than the other one’s.

We will now illustrate the power and versatility of this algorithm by showing how to use it to obtain approximate solutions for two important problems that appear frequently in quantum information:

a) State Estimation Problems

In a generic pure state estimation scenario, a source randomly chooses a pure state $\Psi_i$ out of a probability distribution $p_i$ and then encodes it into a state $\Psi'_i$ to which we are given full access. The state estimation problem consists on finding the optimal measure-and-prepare strategy that allows us to reconstruct the original state $\Psi_i$ with high fidelity. In [16], it is explained how to map state estimation (SE) problem into a linear optimization over the set $S$ of separable operators, via the relation

$$F = \max \{\text{tr}(\rho_{AB}\Lambda_{AB}) : \Lambda_{AB} \in S, \Lambda_A = I\},$$

where $F$ is the optimal average fidelity and $\rho_{AB}$ = $\sum_i p_i \Psi'_i \otimes \Psi_i$ is given by the particular SE problem. In [16], it is also shown that any separable decomposition $\Lambda_{AB} = \sum_x M_x \otimes \phi_x$ of an operator $\Lambda_{AB}$ satisfying the above conditions can be interpreted as a measure-and-prepare strategy consisting of applying the POVM $\{M_x\}_x$ and preparing the state $\phi_x$ depending on the outcome $x$.

Now, consider the sequence of optimization problems:

$$\tilde{F}^N = \max \{\text{tr}(\rho_{AB}\tilde{\Lambda}_{AB}) : \tilde{\Lambda}_{AB} \in S^N, \tilde{\Lambda}_A = I\},$$

$$\tilde{F}^N_p = \max \{\text{tr}(\rho_{AB}\Lambda_{AB}) : \Lambda_{AB} \in S^N_p, \Lambda_A = I\}.$$  

(7)

These optimizations can also be cast as a semidefinite program. Therefore, they can be efficiently computed as long as the index $N$ is not very high (note nevertheless, that, in general, if we fix $N$ for increasing $d_B$, we will end up with a very bad approximation). Also, because we are optimizing over particular regions of $S$, in general we will get a suboptimal result, i.e., $\tilde{F}^N, \tilde{F}^N_p \leq F$ for all $N$. However, it is clear that $\lim_{N \to \infty} \tilde{F}^N, \tilde{F}^N_p = F$.

As we have already mentioned, we can write down a separable decomposition for the operator $\Lambda_{AB}$ output by the computer, via Eq. (5) in case $\tilde{\Lambda}_{AB} \in S^N$ or by means of a similar formula [16] in case $\Lambda_{AB} \in S^N_p$.

This separable decomposition can be subsequently interpreted as a measure-and-prepare strategy; for any SE problem, the DPS* method can thus provide us with a sequence of states estimation strategies that converge asymptotically to the optimal one.

It would be natural to wonder how fast this convergence is, i.e., how far $\tilde{F}^N$ is from $F$ for finite $N$. Following the lines of [16], we arrive at a sequence of upper and lower bounds on $F$ given by

$$\tilde{F}^N \leq F \leq \tilde{F}^N + \frac{d}{N} \left(\tilde{F}^N - \frac{1}{d}\right),$$

$$\tilde{F}^N_p \leq F \leq \tilde{F}^N_p + \frac{\epsilon_N}{1 - \epsilon_N} \left(\tilde{F}^N_p - \frac{1}{d}\right).$$  

(8)

To get an idea of the efficiency of these algorithms, we refer the reader to [16], since the lower bounds on the maximal fidelity of the state estimation problems considered in that paper actually correspond to the values computed through DPS*.

b) Computation of the robustness of entanglement

Let $\rho \in B(H)$ be a quantum state. We will define its (separable) robustness of entanglement [17] $R(\rho)$ as

$$R(\rho) = \min\{\text{tr}(\sigma) : \sigma \in S, \rho + \sigma \in S\}.$$  

(9)

Used in combination with the DPS criterion, the DPS* criterion allows us to determine the robustness of entanglement of any quantum state $\rho_{AB}$ up to arbitrary precision. Indeed, note that, optimizing over $S^N(S^N_p)$ or $S^N(S^N_p)$ instead of $S$ in the previous definition, we would obtain lower and upper bounds on $R(\rho)$, respectively. And, of course, both optimizations can be performed using semidefinite programming.

In [18], the authors introduced a class of uniparametric families of $n$-partite quantum states. Given a unitary
operator $V$ acting over $n - 1$ qubits, the corresponding family of states is defined as

$$\rho^V_\alpha \equiv \frac{1}{2^n} (\mathbb{1}_{1} \otimes I_{23} \ldots I_n + \frac{1}{\alpha} \alpha |0\rangle \langle 1| \otimes V + \frac{1}{2^n} \alpha |1\rangle \langle 0| \otimes V^\dagger).$$

The separability properties of these states are very important, for if one could prove that any such state $\rho^V_\alpha$ is multiseparable for all $\alpha \leq 1/\text{poly}(n)$, then one would have an example of a quantum computation that supersedes any classical algorithm but nevertheless does not require entanglement [18]. For the case $n = 3$, the authors showed that, for any unitary $V$, the state $\rho^V_\alpha$ is always separable with respect to the partition $1|2|3$. Moreover, their numerical tests suggested that $\rho^V_\alpha$ is PPT with respect to the partition $1|2|3$ for all $\alpha \leq 1/2$. Nevertheless, they conjectured that, in some cases, the state should remain entangled for lower values of $\alpha$. The DPS* criterion presented above strongly suggests that this is not the case.

We generated 1000 random unitaries $\{V_i\} \subset SU(4)$ according to the Haar measure and applied the DPS* criterion to derive upper bounds on the robustness of entanglement of the corresponding states $\{\rho^V_\alpha\}$, by considering extensions over the last qubit. We used the MATLAB package YALMIP [21] in combination with SeDuMi [22] to perform the numerical calculations. After an appropriate optimization over the set $\tilde{S}^3$, all the corresponding upper bounds turned out to be zero, thus proving the separability of the previous sample of states.

In order to discard statistical effects, we considered the unitary operator $U = 2P_{\text{sym}}^2 - I_2 \otimes I_2$, whose associated states $\rho^U_\alpha$ appear to have the greatest negativity of the whole family for fixed $\alpha > 0.5$ [23]. Fig. 2 shows upper (DPS*) and lower (DPS) bounds on the robustness of entanglement for different values of $\alpha$. This time, we optimized over the sets $\tilde{S}^3$, $\tilde{S}^{15}$ and $\tilde{S}^3_p$, respectively. It is clear that for all values of $\alpha$ below 0.5, the state $\rho^U_\alpha$ is separable.

In conclusion, in this letter we have introduced a new criterion for separability detection. This criterion has been inspired by and it is in a sense complementary to the one conceived by Doherty et al. [1]. Whereas the latter one aims at approximating the set of separable states from the outside, our new method works from the inside, i.e., by defining a sequence of sets of states contained in $\mathcal{S}$. From [10], it follows that the method can be easily extended to deal with multiseparable problems.

This new criterion works basically by taking the states defined by Doherty et al. and applying a perturbation to make them separable. We believe, however, that the size of this perturbation is larger than required: in the PPT case, at least for small dimensions of Alice’s system, a smaller transformation (in some cases the identity) should be enough to guarantee the separability of the output state. Note that the bounds on the distance to arbitrary separable states are actually independent of $d_A$. If future research found an optimal linear map to turn Doherty et al.’s states into separable states that took into account the dimensionalities of both systems, the speed of convergence of the resulting improved DPS* criterion would be much faster.

Nevertheless, a wide range of applications follow from our method in its present state. We have seen that the method alone can be used to determine the best experimental setup in quantum tomography protocols, and we have also shown how the combination of both the DPS and DPS* methods allows to solve with arbitrary precision computationally hard problems, like the calculation of the entanglement robustness. Since some important problems in Complexity Theory like PARTITION or CLIQUE can be reduced to the separability problem [7, 8], it is not unrealistic to expect that, with time, our method will find new applications outside the scope of Quantum Information Science.

The authors thank Animesh Datta and Fernando G. S. L. Brandão for useful discussions. This work is part of the EPSRC QIP-IRC and is supported by EPSRC grant EP C546237 1, the Royal Society, the EU Integrated Project QAP and an Institute for Mathematical Sciences postdoc fellowship.

[1] A. C. Doherty, P. A. Parrilo, F. M. Spedalieri, Phys. Rev. Lett. 88, 187904 (2002).
[2] A. Peres, Phys. Rev. Lett. 77, 1413 (1996).
[3] M. B. Plenio and S. Virmani, Quant. Inf. Comp. 7, 1 (2007).
[4] R. Horodecki, P. Horodecki, M. Horodecki, and K.
Horodecki, *e-print* arXiv:quant-ph/0702225

[5] O. Gühne, G. Tóth *e-print* arXiv:0811.2803

[6] L.M. Ioannou, Quant. Inf. Comp. 7, 335 (2007)

[7] L. Gurvits, *Proceedings of the thirth fifth ACM symposium on Theory of computing*, 10, New York, ACM Press (2003).

[8] S. Gharibian, *e-print* arXiv:0810.4507.

[9] L. M. Ioannou, B. C. Travaglione, Phys. Rev. A 73, 052314 (2006).

[10] F. Hulpke and D. Bruss, J. Phys. A 38, 5573, (2005)

[11] F. G. S. L. Brandão, R. O. Vianna, Phys. Rev. Lett. 93, 220503 (2004).

[12] J. Eisert, P. Hyllus, O. Guehne, M. Curty, Phys. Rev. A 70, 062317 (2004).

[13] F.M. Spedalieri, Phys. Rev. A 76, 032318 (2007)

[14] A. C. Doherty, P. A. Parrilo, F. M. Spedalieri, Phys. Rev. A 69, 022308 (2004).

[15] L. Vandenberghe and S. Boyd, SIAM Review 38, 49 (1996).

[16] M. Navascués, M. Owari and M. B. Plenio, *e-print* arXiv:0906.2731.

[17] G. Vidal and R. Tarrach, Phys. Rev. A 59, 141 (1999).

[18] A. Datta, S.T. Flammia, C.M. Caves, Phys. Rev. A 72, 042316 (2005)

[19] M. Navascués, Phys. Rev. Lett. 100, 070503 (2008).

[20] M. Abramowitz and I. A. Stegun, *Handbook of Mathematical Functions with Formulas, Graphs and Mathematical Tables*, New York: Dover Publications (1972).

[21] J. Löfberg, *YALMIP : A Toolbox for Modeling and Optimization in MATLAB*, [http://control.ee.ethz.ch/~joloef/yalmip.php](http://control.ee.ethz.ch/~joloef/yalmip.php).

[22] J.F. Sturm, *ScDuMi, a MATLAB toolbox for optimization over symmetric cones*, [http://sedumi.mcmaster.ca](http://sedumi.mcmaster.ca).

[23] Notice that $\epsilon_N \approx \frac{d_{d-2,1}^2}{(d-1)^2}$ for $N >> 1$ [20], where $d_{d-2,1}$ denotes the first positive zero of the Bessel function $J_{d-2}(x)$. It follows that $\lim_{N \to \infty} \epsilon_N = 0$.

[24] In this case, though, we do not have a hierarchy anymore, i.e., in general, $\tilde{S}^N \not\subset \tilde{S}^{N+1}$.

[25] Animesh Datta, private communication.