An improved algorithm for quantum separability and entanglement detection

L. M. Ioannou,[1,*] B. C. Travaglione,[1,2] D. Cheung,[3] and A. K. Ekert[1]

[1] *Centre for Quantum Computation, Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Wilberforce Road, Cambridge CB3 0WA, UK*

[2] *Computer Laboratory, University of Cambridge, JJ Thomson Ave, Cambridge CB3 0FD, UK*

[3] *Combinatorics and Optimization, University of Waterloo, 200 University Avenue West, Waterloo, N2L 3G1, Canada*

Determining whether a quantum state is separable or entangled is a problem of fundamental importance in quantum information science. It has recently been shown that this problem is NP-hard. There is a highly inefficient 'basic algorithm' for solving the quantum separability problem which follows from the definition of a separable state. By exploiting specific properties of the set of separable states, we introduce a new classical algorithm that solves the problem significantly faster than the 'basic algorithm', allowing a feasible separability test where none previously existed e.g. in 3-by-3-dimensional systems. Our algorithm also provides a novel tool in the experimental detection of entanglement.

Entangled quantum states are interesting both from theoretical and practical points of view. Theoretically, entanglement is connected to the confounding issue of nonlocality. Practically, entangled states are useful in quantum cryptography and other quantum information processing tasks (see [1] and references therein). A mixed quantum state is defined as *separable* if and only if it can be written as a convex combination of pure separable states (and defined as *entangled*, otherwise). Solving the quantum separability problem simply means determining whether a given quantum state is entangled or separable. The problem comes in two flavors – one theoretical, and the other experimental. In this paper, we describe an algorithm for solving the quantum separability problem in the theoretical setting. We also describe the algorithm's utility in the experimental setting.

We begin by introducing some notation and precisely defining the quantum separability problem. In what follows, we are considering a bipartite quantum system of dimension $M \times N$. Let $\mathbb{H}_{M,N}$ denote the vector space of all Hermitian operators acting on $\mathbb{C}^M \otimes \mathbb{C}^N$. Noting that $\mathbb{H}_{M,N}$ is isomorphic to $\mathbb{R}^{M^2N^2}$, it is endowed with the Euclidean inner-product $\langle X, Y\rangle \equiv \mathrm{tr}(XY)$, which induces the corresponding norm $||X|| \equiv \sqrt{\mathrm{tr}(X^2)}$ and distance measure $||X - Y||$. Let $\mathcal{D}_{M,N} \subset \mathbb{H}_{M,N}$ denote the set of all density operators. The set of bipartite separable quantum states $\mathcal{S}_{M,N} \subset \mathcal{D}_{M,N}$ is defined as the convex hull of the separable pure states $\{|\alpha\rangle\langle\alpha| \otimes |\beta\rangle\langle\beta|\}$, where $|\alpha\rangle$ ($|\beta\rangle$) is a normalized vector in $\mathbb{C}^M$ ($\mathbb{C}^N$). An arbitrary density matrix in $\mathcal{D}_{M,N}$ is parameterized by $n-1$ real variables, where

$$n \equiv M^2N^2, \tag{1}$$

and an arbitrary separable pure state is parameterized by

$$k \equiv 2(M+N) - 4 \tag{2}$$

real variables. Of course, in defining the separability problem, we cannot allow infinite precision, so we need to introduce a precision parameter $\delta > 0$. We are now ready to define the *(quantum) separability problem* as follows:

Quantum Separability Problem. *Given a density matrix $\rho \in \mathcal{D}_{M,N}$ and a precision δ, assert either*

SEPARABLE: *there exists a separable state σ such that $||\rho - \sigma|| < \delta$; or*

ENTANGLED: *there exists an entangled state τ such that $||\rho - \tau|| < \delta$.*

The separability problem has been shown to be NP-hard [2], thus any devised test for separability is likely to require a number of computing resources that scales exponentially with M and N. There exist efficient "one-sided" tests for separability, where the output of some polynomial-time computable function of the matrix for ρ can indicate that ρ is certainly entangled [3, 4, 5, 6, 7] or certainly separable [8, 9, 10], but not both.

The experimental flavor of the separability problem can be defined as follows: Given many physical copies of a completely unknown quantum state ρ, determine whether ρ is separable. One may solve this problem by performing full state tomography in order to construct the density matrix for ρ to some precision δ, and then solve the theoretical separability problem. If there is some partial knowledge of ρ, then there are more options, such as testing for a violation of a specific Bell inequality [11, 12] or invoking entanglement witnesses [13, 14]. In the case where $MN \leq 6$, the positive partial transpose (PPT) test [3, 15] can be implemented physically [16, 17], though currently this approach is not experimentally viable.

The 'basic algorithm' that follows from the definition of a separable state is simply a straightforward search for a convex combination of separable pure states that gives the required density matrix within precision δ. Since any separable density operator in $\mathcal{S}_{M,N}$ can be written as a convex combination of n separable pure states [18], a lower bound for the worst-case run time, t_1, of this search

*Electronic address: lmi22@cam.ac.uk

is given by

$$t_1(n,\delta) \;>\; \binom{\Omega_\delta}{n}\binom{\lfloor 1/\delta \rfloor}{n-1} \times \mathrm{poly}(n,\log(1/\delta)), \quad (3)$$

where Ω_δ is the number of pure separable states to precision δ. The first binomial factor is a lower bound for the number of combinations of n distinct pure separable states to precision δ; the second is a lower bound for the number of probability distributions over the n states to precision δ. The algorithm that we present here has a worst-case run time, t_2, with an upper bound of

$$t_2(n,\delta) \;<\; \Omega_\delta \times \mathrm{poly}(n,\log(1/\delta)). \quad (4)$$

To compare these run times it is not necessary to compute the exact value of Ω_δ, but note that for realistic values of δ, Ω_δ will be of order $O(2/\delta^k) \gg n$, so t_2 will be significantly less than t_1. Later it will be explained that equation (4) can be improved further in practice with the use of global optimization routines, making the algorithm of practical use in the case where M and N are small (and δ is not too small). Even for $M = N = 3$, there was previously no known better algorithm for the separability problem than the basic one described above. Note also that for $MN \leq 6$, where the PPT test is necessary and sufficient, our algorithm still offers its novel advantage in the experimental setting (as explained later).

Before describing our algorithm for separability, we note the following fact [15]: A state ρ is entangled if and only if there exists an entanglement witness [19] that detects it. An *entanglement witness* is any traceless operator $A \in \mathbb{H}_{M,N}$ for which there exists a state $\rho \in \mathcal{D}_{M,N}$ such that

$$\mathrm{tr}(A\sigma) \;<\; \mathrm{tr}(A\rho) \quad \forall \sigma \in \mathcal{S}_{M,N}. \quad (5)$$

This definition is slightly different from that used in the literature, however it substantially simplifies the description of the algorithm. Recalling that $\mathbb{H}_{M,N}$ is isomorphic to $\mathbb{R}^n$, the above definition implies that for entangled ρ there exists a hyperplane which separates ρ from the set of all separable states $\mathcal{S}_{M,N}$. If one defines the function

$$b_A \;\equiv\; \max_{\sigma \in \mathcal{S}_{M,N}} \mathrm{tr}(A\sigma), \quad (6)$$

then the set $\{X \in \mathbb{H}_{M,N} : \;\mathrm{tr}(AX) = b_A\}$ is one such hyperplane. We (non-uniquely) define σ_A to be any element of $\mathcal{S}_{M,N}$ such that $\mathrm{tr}(A\sigma_A) = b_A$. It suffices only to consider entanglement witnesses A such that $\mathrm{tr}(A^2) = 1$, that is, those which lie on the $(n-2)$-dimensional surface of a $\mathbf{0}$-centered unit-hypersphere in $\mathbb{H}_{M,N}$, where $\mathbf{0}$ is the origin (null operator in $\mathbb{H}_{M,N}$). For our purposes, however, it will be useful to characterize *all potential entanglement witnesses* by the corresponding $(n-1)$-dimensional *unit-hyperball*, $\mathcal{W}$, defined as

$$\mathcal{W} \equiv \{A \in \mathbb{H}_{M,N} : \mathrm{tr}(A) = 0, \mathrm{tr}(A^2) \leq 1\}. \quad (7)$$

We can now define the *(entanglement) witness problem*, a problem slightly harder than the separability problem:

Entanglement Witness Problem. *Given a density matrix $\rho \in \mathcal{D}_{M,N}$ and a precision δ, either assert*

SEPARABLE: *there exists a separable state σ such that $||\rho - \sigma|| < \delta$; or return*

$A \in \mathcal{W}$: *an operator such that $tr(A\sigma) < tr(A\rho) + \delta$ for all $\sigma \in \mathcal{S}_{M,N}$.*

The witness problem is thus to decide that ρ is almost separable, or to find an approximate entanglement witness for ρ. Note that any algorithm solving the witness problem also solves the separability problem. Our algorithm actually solves the witness problem.

Our algorithm is an iterative one, which calls a computationally expensive subroutine at each iteration. It is convenient to treat this subroutine as a black box, or oracle, when describing the algorithm's main structure. Simply define the *oracle*, $\mathcal{O}$, such that it takes an operator A, and returns $\mathcal{O}(A) \equiv \sigma_A$. Whichever way $\mathcal{O}(A)$ is computed, it suffices that the maximization in (6) is done over the *pure* separable states (and that σ_A is a pure state). Thus, the motivation behind reducing the separability problem to the oracle $\mathcal{O}$ is quite simple: we are exploiting the fact that the separable pure states, which are the extreme points of $\mathcal{S}_{M,N}$, are parameterized by k variables rather than n. Thus, from a practical point of view, the complexity of computing $\mathcal{O}(A)$ scales much better than that of either a brute-force search through all entanglement witnesses, or the 'basic algorithm'.

Before delving into the details, we give a high-level description of our algorithm. The algorithm maintains a set $\mathcal{K} \subseteq \mathcal{W}$ of operators which are potential entanglement witnesses for ρ. If (and only if) ρ is entangled, there exists a closed, convex subset of $\mathcal{W}$, which we call $\mathcal{W}_\rho$, consisting of *all entanglement witnesses that detect* ρ. Throughout the algorithm, we have $\mathcal{W}_\rho \subset \mathcal{K}$. Initially, $\mathcal{K}$ is set equal to $\mathcal{W}$. In each iteration, the algorithm selects a *test-witness*, $A \in \mathcal{K}$, and computes $\sigma_A = \mathcal{O}(A)$. If $\mathrm{tr}(A\sigma_A) < \mathrm{tr}(A\rho) + \delta$, then the algorithm returns A; else, $\mathcal{K}$ is reduced and the next iteration begins. The algorithm keeps reducing the set $\mathcal{K}$ until it either finds an (approximate) element of $\mathcal{W}_\rho$, or it decides that $\mathcal{W}_\rho$ is empty, and therefore ρ is separable. To decide $\mathcal{W}_\rho$ is empty means that $\mathcal{K}$ is too small to contain $\mathcal{W}_\rho$. This requires having a lower bound on the size of $\mathcal{W}_\rho$. By exploiting the role of δ in the problem definitions, such a lower bound can be derived in terms of δ and n. In what follows, we will ignore the role of δ, as it obfuscates the main idea of the algorithm.

We now describe how to reduce the set $\mathcal{K}$, that is, to discard elements of $\mathcal{K}$ that are not elements of $\mathcal{W}_\rho$. Suppose A is not in $\mathcal{W}_\rho$, but is sufficiently close to $\mathcal{W}_\rho$. Then, A, ρ, and σ_A can be used to define a half-space $\{X \in \mathbb{H}_{M,N} : \mathrm{tr}(KX) \geq 0\}$ that contains $\mathcal{W}_\rho$. Specifically, we have the following: Let W be any operator in $\mathcal{W}_\rho$ and suppose $A \notin \mathcal{W}_\rho$. If $\mathrm{tr}(WA) \geq 0$, then choosing

$$K \;\equiv\; (\rho - \sigma_A) - \frac{\mathrm{tr}(A(\rho - \sigma_A))}{\mathrm{tr}(A^2)} A \quad (8)$$

(and then normalizing K) gives $\mathrm{tr}(KA) = 0$ by construction, and it is easy to verify that $\mathrm{tr}(KW) > 0$. The idea is that, at each iteration, the test-witness A is chosen so that it is (approximately) in the center of the current $\mathcal{K}$ (relative to the Euclidean geometry). If the oracle $\mathcal{O}$ returns σ_A such that $\mathrm{tr}(A\rho) < \mathrm{tr}(A\sigma_A)$, then, as long as $\mathrm{tr}(WA) \geq 0$ for all $W \in \mathcal{W}_\rho$, equation (8) gives a *cutting plane* $\{X \in \mathbb{H}_{M,N} : \mathrm{tr}(KX) = 0\}$ that slices through A and $\mathbf{0}$. This allows us to discard the half of $\mathcal{K}$ consisting of operators X such that $\mathrm{tr}(KX) \leq 0$. Because $\mathcal{K}$ is being approximately halved at each step, the algorithm quickly either finds an entanglement witness for ρ or concludes that ρ is separable.

Our problem of determining whether the convex set $\mathcal{W}_\rho$ is empty using cutting planes is well studied in the field of convex optimization. However, because of our special requirement that $\mathrm{tr}(WA) \geq 0$ for all $W \in \mathcal{W}_\rho$, none of the existing algorithms can be applied directly. Fortunately, though, the analytic-central-section algorithm due to Atkinson and Vaidya [20] can be adapted for our purpose, giving an algorithm with the desired complexity.

We now describe the algorithm. Let I_{MN} be the maximally mixed state, which is properly contained in $S_{M,N}$ [8, 10]. It is easy to verify that $\mathcal{W}_\rho$ must be contained in the half-space $\{X : \mathrm{tr}((\rho - I_{MN})X) \geq 0\}$. Let $K_1 \equiv (\rho - I_{MN})/||\rho - I_{MN}||$. Thus, straight away, $\mathcal{K}$ is reduced to the half-ball $\mathcal{W} \cap \{X : \mathrm{tr}(K_1 X) \geq 0\}$. The first test-witness to give to the oracle is $A = \rho - I_{MN}$ (which is along the center-line of the half-ball). If the oracle confirms that A detects ρ, then we are done. Otherwise, we use equation (8) to generate a cutting plane. By way of mathematical induction, assume that, at some later stage in the algorithm, $\mathcal{K}$ has been reduced to

$$\mathcal{K} \;=\; \mathcal{W} \bigcap \cap_{i=1}^{h} \{X : \mathrm{tr}(K_i X) \geq 0\}, \tag{9}$$

by the generation of h cutting planes $\{X : \mathrm{tr}(K_i X) = 0\}$, as described above. Recall that we want to choose a test-witness that is approximately in the center of $\mathcal{K}$. An easily computable candidate is the *analytic center*, C, of $\mathcal{K}$ [21], which is defined as the unique minimizer of the real convex function

$$F(X) \;\equiv\; -\sum_{i=1}^{h} \log(\mathrm{tr}(K_i X)) - \log(1 - ||X||^2), \tag{10}$$

defined for $X \in \mathcal{K}$. The relation $\nabla F(C) = 0$ gives $C = \frac{1-||C||^2}{2} \sum_{i=1}^{h} \frac{K_i}{\mathrm{tr}(K_i C)}$, which, by the inductive hypothesis, implies that $\mathrm{tr}(WC) \geq 0$ for all $W \in \mathcal{W}_p$. Thus, $A = C$ is a suitable test-witness to give to the oracle and to use in equation (8). Full details of a robust algorithm are too numerous to include here but can be derived with the help of [20, 21, 22]. The important point is that the separability of a given density matrix can be decided with only $n \times \mathrm{polylog}\,(n, 1/\delta)$ calls to the oracle.

Now consider the complexity of computing $\mathcal{O}(A)$, which so far has been black-boxed. The most naïve way to carry out this computation is to one-by-one calculate $\mathrm{tr}(A\sigma)$ for each of the Ω_δ pure separable states σ (to precision δ) and return the σ that produced the largest value of $\mathrm{tr}(A\sigma)$. Even with this naïve way of computing $\mathcal{O}(A)$, the total run time of our algorithm is significantly shorter than that of the 'basic algorithm' for quantum separability (compare (3) and (4)). However, for any given orthogonal Hermitian basis of $\mathbb{H}_{M,N}$, the closed, general form of the function $\mathrm{tr}(A\sigma)$ can be written down in terms of the k real parameters of the separable pure states. Armed with the closed form of the function to be maximized, various well-studied global maximization techniques are at one's disposal, for example, Lipschitz optimization [23] or interval analysis [24]. Call the function to be maximized f and denote its global maximum by f^*. As the global optimization algorithm proceeds, it gives progressively better lower and upper bounds on f^*. Call these bounds $\underline{f}$ and $\overline{f}$, respectively. A key advantage of our algorithm is that, during any computation of $\mathcal{O}(A)$, the search for f^* may be halted early when either (i) $\mathrm{tr}(A\rho) \leq \underline{f}$, in which case equation (8) can be invoked to generate a new cutting plane, or (ii) $\overline{f} < \mathrm{tr}(A\rho)$, in which case the algorithm has found an entanglement witness for ρ. Thus, the algorithm's run time may be significantly shorter than the worst-case analysis predicts.

Finally, we discuss how the algorithm may be used when only partial information about the state ρ is available. This is of particular use in an experimental setting. Let $\mathcal{B}$ be an orthonormal, Hermitian basis for $\mathbb{H}_{M,N}$. The state ρ can be written $\rho = \sum_{i=1}^{n} \rho_{X_i} X_i$, where $\rho_{X_i} \in \mathbb{R}$. Each coefficient ρ_{X_i} is simply the *expected value of* X_i, which equals $\mathrm{tr}(X_i \rho)$. The expected values of all elements of $\mathcal{B}$ constitute complete information about ρ. Suppose we have only measured $j < n$ expected values. The algorithm can be applied in this reduced, j-dimensional space. If the algorithm finds a hyperplane separating ρ from $\mathcal{S}_{M,N}$, then ρ is entangled; otherwise ρ may be entangled or separable, as the j expected values are consistent with a separable state. As expected values are being gathered through experimental observation, they may be input to the algorithm. If the basis $\mathcal{B}$ is separable, then the entire procedure can be done when the subsystems are spatially separated with local operations and classical communication. The idea of searching for an entanglement witness in the span of operators whose expected values are known was discovered independently and applied, in a special case, to quantum cryptographic protocols in [25].

We have given a classical algorithm for the quantum separability problem which takes as input the density matrix for a quantum state ρ and either decides that ρ is separable, or returns an entanglement witness that detects ρ. Our algorithm is the best-known algorithm for the general separability problem; it gets its advantage over the 'basic algorithm' from reducing the problem to an optimization over the pure separable states. If properly implemented, the algorithm should give a feasible test for separability in low dimensions (e.g. $MN < 10$,

with current technology). The general technique depends only on the convexity of the set of separable states, and thus can, in principle, be applied to test for multi-partite entanglement. The algorithm also gives experimentalists a tool for potentially determining if an unknown state is entangled by measuring only a subset of the expected values which completely describe the state. This method effectively trades quantum resources (additional copies of ρ) for classical resources (a computer able to calculate $\mathcal{O}$).

We would like to thank Carolina Moura Alves, Coralia Cartis, and Tom Stace for useful discussions. We acknowledge support from the EC under project RESQ (IST-2001-37559). LMI, BCT, and DC also acknowledge support from, respectively, CESG and NSERC; CMI; and NSERC and the University of Waterloo.

[1] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[2] L. Gurvits, in *Proceedings of the thirty-fifth ACM symposium on Theory of computing* (ACM Press, New York, 2003), pp. 10–19.
[3] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).
[4] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).
[5] M. A. Nielsen and J. Kempe, Phys. Rev. Lett. **86**, 5184 (2001).
[6] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).
[7] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, *A complete family of separability criteria* (2003), quant-ph/0308032.
[8] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack, Phys. Rev. Lett. **83**, 1054 (1999).
[9] K. Zyczkowski, P. Horodecki, A. Sanpera, and M. Lewenstein, Phys.Rev. A **58**, 883 (1998).
[10] L. Gurvits and H. Barnum, Phys. Rev. A **66**, 062311 (2002).
[11] J. S. Bell, Physics **1**, 195 (1964).
[12] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 881 (1969).
[13] O. Gühne, P. Hyllus, D. Bruß, A. Ekert, M. Lewenstein, C. Macchiavello, and A. Sanpera, Phys. Rev. A **66**, 062305 (2002).
[14] M. Barbieri, F. D. Martini, G. D. Nepi, P. Mataloni, G. M. D'Ariano, and C. Macchiavello, *Experimental detection of entanglement with polarized photons* (2003), quant-ph/0307003.
[15] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).
[16] P. Horodecki and A. Ekert, *Direct detection of quantum entanglement* (2001), quant-ph/0111064.
[17] H. Carteret, *Noiseless circuits for the Peres criterion* (2003), quant-ph/0309216.
[18] P. Horodecki, Phys. Lett. A **232**, 333 (1997).
[19] B. M. Terhal, Phys. Lett. A **271**, 319 (2000).
[20] D. S. Atkinson and P. M. Vaidya, Mathematical Programming **69**, 1 (1995).
[21] Y. Nesterov and A. Nemirovskii, *Interior-Point Polynomial Algorithms in Convex Programming* (SIAM, Philadelphia, 1994).
[22] J. Renegar, *A Mathematical View of Interior-Point Methods in Convex Optimization* (MPS-SIAM, Philadelphia, 2001).
[23] R. Horst and P. Pardalos, eds., *Handbook of Global Optimization* (Kluwer Academic Publishers, Dordrecht, 1995).
[24] E. Hansen and G. Walster, *Global Optimization Using Interval Analysis* (Marcel Dekker Incorporated, Boston, 2004), ISBN 0824740599.
[25] M. Curty, M. Lewenstein, and N. Lütkenhaus, *Entanglement as precondition for secure quantum key distribution* (2003), quant-ph/0307151.