Proceedings of the 41st IEEE
Conference on Decision and Control
Las Vegas, Nevada USA, December 2002

Entanglement witnesses and semidefinite programming

Pablo A. Parrilo
Automatic Control Laboratory (IfA)
ETH Zürich

Andrew C. Doherty Federico M. Spedalieri
Institute for Quantum Information
California Institute of Technology

Abstract

We study the application of sums of squares decompositions and semidefinite programming in the formulation of computational criteria for distinguishing entangled from separable quantum states. A hierarchy of tests is obtained, the simplest of which corresponds to the well-known positive partial transpose (PPT) sufficient criterion, with the more complicated tests being strictly stronger. The duality structure of the problem allows us to provide an explicit construction of the entanglement witnesses corresponding to our tests.

1 Introduction

Entanglement is one of the most striking features of quantum mechanics. Not only is it at the heart of the violation of Bell inequalities [1], but it has lately been recognized as a very useful resource in the field of quantum information. Entanglement can be used to perform several important tasks such as teleportation, quantum key distribution and quantum computation [10]. Despite its widespread importance, there is not an effective procedure that can tell us whether a given state is entangled or not, and considerable effort has been dedicated to this problem in recent years [6, 8]. In this paper we apply the tools of semidefinite programming to construct a hierarchy of tests that can detect entangled states.

Separable and entangled states. In quantum mechanics the state of a physical system is represented by unit trace positive operators ρ on a complex vector space $\mathcal{H}$. The rank one projectors are termed pure states since they specify a particular vector on $\mathcal{H}$ with probability one. The mixed states are convex combinations of rank one projectors and can be thought of as probability distributions over pure states.

The state of two physical systems A and B (two atoms for example) is specified by a positive operator ρ on the tensor product space $\mathcal{H}_A \otimes \mathcal{H}_B$. If the two systems have definite states independent of each other they are of the form $\rho_A \otimes \rho_B$ and are termed product states. There is an important distinction between local dynamics, for which it is possible to effect the transformation $\rho \to (A \otimes B)\rho(A \otimes B)^\dagger$ with some probability for arbitrary A and B, and dynamics that require a non-trivial interaction between the two systems and which allow for any completely positive map to be performed on ρ. Physically the local operations may be performed even if the two systems are widely separated whereas it is necessary to bring them together to perform an arbitrary completely positive map.

The states which can be constructed by local operations of this kind (essentially the so-called local operations with classical communication), starting with a pure product state, are termed the separable states. All other states of two physical systems are termed entangled and their preparation requires a non-trivial coherent interaction between the two systems. The name is suggestive of the fact that such states have strong correlations between observables of the two parties. Bell inequalities give a mathematical quantification of this fact about entangled states. As a result of these considerations, a bipartite mixed state ρ is said to be separable [18] (not entangled) if it can be written as a convex combination of pure product states

$$\rho = \sum p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i|, \qquad (1)$$

where $|\psi_i\rangle$ and $|\phi_i\rangle$ are state-vectors on the spaces $\mathcal{H}_A$ and $\mathcal{H}_B$ of subsystems A and B respectively, and $p_i > 0, \sum_i p_i = 1$.

Several operational criteria have been proposed to identify entangled states. Typically these are based on simple properties obeyed by all separable states and are thus necessary but not sufficient conditions for separability (although some sufficient conditions for separability are known [2]). The most famous of these criteria is based on the partial transposition and was first introduced by Peres [13]. It was shown by the Horodeckis [5] to be both necessary and sufficient for separability in $\mathcal{H}_2 \otimes \mathcal{H}_2$ and $\mathcal{H}_2 \otimes \mathcal{H}_3$. If ρ has matrix elements $\rho_{ik,jl} = \langle i| \otimes \langle k|\rho|j\rangle \otimes |l\rangle$ then the partial transpose ρ^{T_A} is defined by $\rho^{T_A}_{ik,jl} = \rho_{jk,il}$. If a state is separable, then it must have a positive partial transpose (PPT). To see this consider the decomposition (1) for ρ. Partial transposition takes $|\psi_i\rangle\langle\psi_i|$ to $|\psi_i^*\rangle\langle\psi_i^*|$, so the result of this operation is another valid density matrix and must be positive. Thus any state for which ρ^{T_A} is not positive semidefinite is necessarily entangled.

This criterion has the advantage of being very easy to check, but there are PPT states that are nonetheless entangled as was first demonstrated in [7].

In this paper, we discuss a new hierarchy of tests, introduced in [4], that distinguish separable from entangled quantum states. Our main tools are the use of sums of squares decompositions and convex optimization, in particular semidefinite programming. Crucial to our approach is the notion of an *entanglement witness*, presented in Section 2. These are observables that take only nonnegative values on the set of separable states. While very appealing from a theoretical perspective, their practical drawback is that the computational problem of *verifying* that the witness has the desired properties seems to be hard, being equivalent to checking nonnegativity of a bihermitian form. For these reasons, a natural hierarchy of relaxations, based on sum of squares decompositions, is employed to check the required nonnegativity properties.

The proposed criteria are not just efficient numerical schemes, but also have very appealing theoretical interpretations. On the one hand, as mentioned earlier and presented in the following section, they implement a search for entanglement witnesses that certify the impossibility of a decomposition as in (1), and for which the nonnegativity condition can be effectively verified. By convex duality, there is the complementary viewpoint, as a search for state extensions with a particular structure, that reduce to the given state ρ under the partial trace operation, as will be explained in Section 3.

These two apparently different procedures *turn out to be one and the same*, being the primal and dual side, respectively, of a single semidefinite programming problem. In Section 5, a fully worked out example of an entangled state with the corresponding witness is presented.

2 Entanglement witnesses

A crucial feature in convex geometry and convex programming, is the existence of *separating hyperplanes*, or equivalently, of a dual problem. If $\mathcal{C}$ is a closed convex set with nonempty interior, then any point that does not belong to $\mathcal{C}$ can be *separated* from it by a linear functional that takes only nonnegative values on $\mathcal{C}$, but is negative on x.

In the context of entanglement, the set $\mathcal{C}$ will be the set of separable states, and the role of separating hyperplanes or *certificates* is played by observables known as *entanglement witnesses* (EW) [5, 16]. Prototypical examples of entanglement witnesses are the classical Bell inequalities [1]. An EW for a state ρ is a linear functional W that satisfies

$$\mathrm{Tr}[W\rho] < 0 \quad \text{and} \quad \mathrm{Tr}[W\rho_{sep}] \geq 0, \tag{2}$$

for every separable state ρ_{sep}. Clearly, if there exists a W satisfying these conditions, then the state ρ cannot possibly be separable, and the observable W serves as a *certificate* or *witness* of this fact.

If W is a candidate entanglement witness, then it follows from (1) that to establish the second condition in (2) it is sufficient to verify it only for the pure product states, since they are the generators of the cone of separable states.

According to this, for any product state $|xy\rangle$ we should have

$$\begin{aligned} E(x,y) &:= \mathrm{Tr}\, W|xy\rangle\langle xy| = \langle xy|W|xy\rangle \\ &= \sum_{ijkl} W_{ijkl} x_i^* y_j^* x_k y_l \geq 0, \end{aligned} \tag{3}$$

where $\{x_i, y_i\}$ are the components of $|x\rangle, |y\rangle$ in some basis, and W_{ijkl} are the matrix elements of W in the same basis. Equation (3) states that the bihermitian form E associated with W must be positive semidefinite (PSD).

In general, checking nonnegativity of multivariate forms is a hard problem, and therefore sufficient conditions, or *relaxations*, are used instead. Particularly useful ones are those based on sum of squares decompositions (see [11, 12] and the references therein). As explained in the cited works, a very useful sufficient condition for nonnegativity is the existence of a sum of squares (SOS) decomposition, i.e., $E(x,y) = \sum_i e_i(x,y)^2$, with the e_i also being multivariate forms. The main reason for this is the fact that, as opposed to nonnegativity, it is possible to efficiently check whether a multivariate form admits a sum of squares decomposition, using semidefinite programming (SDP).

Semidefinite programs (SDP) [17], are a class of convex optimization problems that correspond to the optimization of a linear function, subject to a linear matrix inequality (LMI). The standard SDP problem formulation is:

$$\begin{aligned} \text{minimize} \quad & c^T \mathbf{x} \\ \text{subject to} \quad & F(\mathbf{x}) \geq 0, \end{aligned} \tag{4}$$

where c is a given vector, $\mathbf{x} = (x_1, \ldots, x_m)$, and $F(\mathbf{x}) = F_0 + \sum_i x_i F_i$, for some fixed n-by-n hermitian matrices F_j. The inequality in the second line of (4) means that the matrix $F(\mathbf{x})$ is positive semidefinite. The vector $\mathbf{x}$ is the variable over which the minimization is performed. In the particular instance in which $c = 0$, there is no function to minimize and the problem reduces to whether or not it is possible to find $\mathbf{x}$ such

that $F(\mathbf{x})$ is positive semidefinite. This is termed a feasibility problem. A geometric interpretation of SDP is the minimization of a linear functional, over a convex set defined by the intersection of an affine subspace and the closed cone of positive semidefinite matrices.

To check whether a given multivariate form $E(\mathbf{x})$ can be written as a sum of squares, we try to express it as a quadratic form in a properly chosen set of variables $\mathbf{z}$, i.e.,

$$E(\mathbf{x}) := \mathbf{z}^* Q \mathbf{z}. \tag{5}$$

The choice of auxiliary variables $\mathbf{z}$ will depend on the structure of the form E: for instance, for a bihermitian form such as $E(x, y)$, we would choose as the z_i the monomials of the form $x_i y_j$ and $x_i y_j^*$. In general, the variables z_i will not be algebraically independent, and therefore some quadratic relations (or *syzygies*) will exist among them. This implies the existence of an affine subspace of matrices Q for which (5) holds. This subspace will contain a positive semidefinite matrix if and only if the form E has a sum of squares representation. By the geometric interpretation of SDP outlined earlier, deciding whether E is SOS is equivalent to the solution of a semidefinite program.

Given an affinely parameterized set of multivariate forms, it is also possible to use SDP to search for an element in the family that is a sum of squares. This is exactly what is required in obtaining an entanglement witness W, provided we relax the nonnegativity condition to the sum of squares one, since the form $E(x, y)$ in (3) depends linearly on the parameters W_{ijkl}.

Interestingly enough, it can be shown that the Peres-Horodecki PPT criterion alluded to in the introduction detects the entanglement of only those states that possess entanglement witnesses W for which $E(x, y)$ may be written directly as a sum of squares—the so-called decomposable entanglement witnesses [9] such that $W = P + Q^{T_2}$ for some PSD matrices P and Q.

Furthermore, even if $E(x, y)$ is not a sum of squares, it is possible that after multiplying it by a conveniently chosen positive definite form, the product has the SOS property, therefore establishing nonnegativity. This is the core of the dual side of our approach. Since in the general case there may not be entanglement witnesses W such that (3) is a SOS, we can search over W for which the form is a SOS when multiplied by $\langle x|x\rangle^{k-1}\langle y|y\rangle^{l-1}$ for some $k, l \geq 1$. By duality, this exactly corresponds to the (k, l) separability criterion as presented in Section 3.

We will return to this interpretation after presenting the state extension formulation of our hierarchy of separability tests, the first level of which corresponds exactly to the PPT criterion.

3 State extensions

In this section we will formulate our hierarchy of semidefinite programs in terms of states. Given ρ as in (1), consider the state $\tilde{\rho}$ defined on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_A$:

$$\tilde{\rho} = \sum p_i |\psi_i\rangle\langle\psi_i| \otimes |\phi_i\rangle\langle\phi_i| \otimes |\psi_i\rangle\langle\psi_i|. \tag{6}$$

Firstly $\mathrm{Tr}[\tilde{\rho}(X \otimes I)] = \mathrm{Tr}[\rho X]$ for any operator X on $\mathcal{H}_A \otimes \mathcal{H}_B$. We say that the state ρ is the *partial trace* of $\tilde{\rho}$ or that $\tilde{\rho}$ is an extension of ρ. Secondly $\tilde{\rho}$ is invariant under interchanging the two copies of $\mathcal{H}_A$. To put this more formally we define the swap operator P such that $P|i\rangle \otimes |k\rangle \otimes |j\rangle = |j\rangle \otimes |k\rangle \otimes |i\rangle$. We have $P^2 = I$, and $\pi = (I + P)/2$ is a projector onto the symmetric subspace. Since $\pi\tilde{\rho}\pi = \tilde{\rho}$ the extension $\tilde{\rho}$ only has support on this subspace. Finally the extension $\tilde{\rho}$ is a tripartite separable state. It will have positive partial transposes with respect to any of the parties, and in particular we have $\tilde{\rho}^{T_1} \geq 0$ and $\tilde{\rho}^{T_2} \geq 0$.

The existence of this extension is a necessary condition for separability. *If the state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable then there is an extension $\tilde{\rho}$ on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_A$ such that $\pi\tilde{\rho}\pi = \tilde{\rho}$, $\tilde{\rho}^{T_1} \geq 0$ and $\tilde{\rho}^{T_2} \geq 0$.* Note that the symmetry of the extension means that if $\tilde{\rho}^{T_1} \geq 0$ then $\tilde{\rho}^{T_3} \geq 0$, so including this would not make a stronger test. We may generalize this criterion to an arbitrary number of copies of both $\mathcal{H}_A$ and $\mathcal{H}_B$. *If the state ρ on $\mathcal{H}_A \otimes \mathcal{H}_B$ is separable then there is an extension $\tilde{\rho}$ with support only on the symmetric subspace of $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B^{\otimes l}$ such that $\tilde{\rho}$ has a positive partial transpose for all partitions of the $k + l$ parties into two groups.* Since the extensions are required to be symmetric, it is only necessary to test the possible partitions into two groups that are not related by permuting copies of $\mathcal{H}_A$ and $\mathcal{H}_B$. Including testing for positivity of the extension itself, there are $\lceil (k + 1)(l + 1)/2 \rceil$ distinct positivity checks to be satisfied by $\tilde{\rho}$.

These results generate a hierarchy of necessary conditions for separability. The first is the usual PPT test for a bipartite density matrix ρ. For PPT states we look for an extension $\tilde{\rho}$ of ρ to three parties such that $\pi\tilde{\rho}\pi = \tilde{\rho}$ that satisfies the PPT test for all possible partial transposes. If no such extension exists, then ρ must be entangled. If such an extension is possible, the state could be separable or entangled, and we need to consider an extension to four parties and so on. As was discussed in [4] each of these tests is at least as powerful as the previous one.

The problem of searching for the required extension is in fact a semidefinite program. We provide here an overview, referring the reader to [4] for the full details. It is possible to construct matrices F_i such that $\mathrm{Tr}[F_0(X \otimes I)] = \mathrm{Tr}[\rho X]$ for an arbitrary operator X on $\mathcal{H}_A \otimes \mathcal{H}_B$, $\mathrm{Tr}[F_0(X \otimes I)] = \mathrm{Tr}[\rho X]$ for $i > 0$ and

$\pi F_i \pi = F_i$ for all i. We also need to include all the available F_i, that is we require that the F_i span the subspace of Hermitian matrices with support on the symmetric subspace of $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B^{\otimes l}$ that have zero partial trace. There will be a linear map Λ from matrices on $\mathcal{H}_A \otimes \mathcal{H}_B$ to matrices on $\mathcal{H}_A^{\otimes k} \otimes \mathcal{H}_B^{\otimes l}$ such that $F_0 = \Lambda(\rho)$. Now all matrices $F(\mathbf{x}) = F_0 + \sum_i x_i F_i$ satisfy the necessary equality constraints on $\tilde{\rho}$ and we wish to vary $\mathbf{x}$ so as to satisfy positivity of $F(\mathbf{x})$ and its partial transposes. Each of these positivity conditions results in a new LMI. If it is feasible to satisfy these simultaneously then an extension of the required form exists. Thus we see that our tests reduce to a semidefinite programming feasibility problem. We can write the LMIs as one by forming a block matrix G where the first block is F and each subsequent block is a partial tranpose of F (defining G_i analogously). In the simplest example, $G = \tilde{\rho} \oplus \tilde{\rho}^{T_1} \oplus \tilde{\rho}^{T_2}$ and so for example $G_0 = F_0 \oplus F_0^{T_1} \oplus F_0^{T_2}$.

Using the SDP solver SeDuMi [15], we applied the first criterion ($k = 2, l = 1$) to several examples of PPT entangled states appeared in the literature with $d_A = 2, d_B = 4$ or $d_A = 3, d_B = 3$. On a 500 MHz desktop computer a single state could be tested in under a second for $d_A = 2, d_B = 4$ and in around eight seconds for $d_A = 3, d_B = 3$. We checked 4000 randomly chosen examples of the seven parameter family of PPT entangled states states in [3]. We did not find any PPT entangled state with an extension of the required form, therefore proving (up to numerical error) that they cannot be separable. Very close to the separable states the test was inconclusive due to numerical uncertainties. A specific example, along with the witness certification, is discussed in more detail in Section 5.

4 Duality

For a semidefinite program like (4), the dual problem corresponds to another SDP, that can be written

$$\begin{array}{ll} \text{maximize} & -\mathrm{Tr}[F_0 Z] \\ \text{subject to} & Z \geq 0 \\ & \mathrm{Tr}[F_i Z] = c_i, \end{array} \tag{7}$$

where the matrix Z is hermitian and is the variable over which the maximization is performed. For any feasible solutions of the primal and dual problems we have

$$c^T \mathbf{x} + \mathrm{Tr}[F_0 Z] = \mathrm{Tr}[F(\mathbf{x}) Z] \geq 0, \tag{8}$$

where the last inequality follows from from the fact that both $F(\mathbf{x})$ and Z are positive semidefinite. Then, for the particular case of a feasibility problem ($c = 0$), equation (8) will read $\mathrm{Tr}[F_0 Z] \geq 0$. This result can be used to give a certificate of infeasibility for the primal problem: *if there exists Z such that $Z \geq 0$, $\mathrm{Tr}[F_i Z] = 0$, that satisfies $\mathrm{Tr}[F_0 Z] < 0$, then the primal problem must be infeasible.*

If the primal SDP constructed in Section 3 is infeasible (which means that the state ρ must be entangled), the solution of its dual SDP will provide a certificate of that infeasibility that can be used to construct an entanglement witness for ρ.

To make these duality ideas concrete, we note that due to the block diagonal structure of the LMI, we can restrict any feasible dual solution Z to have the same structure, i.e., $Z = Z_0 \oplus Z_1^{T_1} \oplus Z_2^{T_2}$ where the Z_i are operators on $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_A$. Then we have that $\mathrm{Tr}[G_0 Z] = \mathrm{Tr}[F_0(Z_0 + Z_1 + Z_2)]$. We defined F_0 as a linear function of ρ so that $F_0 = \Lambda(\rho)$ where Λ is a linear map from $\mathcal{H}_A \otimes \mathcal{H}_B$ to $\mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_A$. We can now define an operator $\tilde{Z}$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ through the adjoint map Λ^* such that $\tilde{Z} = \Lambda^*(Z_0 + Z_1 + Z_2)$ and

$$\mathrm{Tr}[\rho \tilde{Z}] = \mathrm{Tr}[\Lambda(\rho)(Z_0 + Z_1 + Z_2)] = \mathrm{Tr}[G_0 Z]. \tag{9}$$

We proceed to show how our scheme allows us to construct an entanglement witness. If ρ_{sep} is any separable state, we know that the primal problem is feasible (the extension $\tilde{\rho}$ exists). As a result there is a feasible value of $\mathbf{x}$ for which G is positive. Consider any dual-feasible Z ($Z \geq 0$, $\mathrm{Tr}[F_i Z] = 0$), then we have $\mathrm{Tr}[G_0 Z] = \mathrm{Tr}[GZ] \geq 0$. Using (9), we have $\mathrm{Tr}[\rho_{sep} \tilde{Z}] \geq 0$ for *any* $\tilde{Z}$ obtained from a dual feasible solution. Note that the dual problem is strictly feasible ($Z = I$ is dual feasible for example). As a result, we are guaranteed that if the primal problem is not feasible (and so ρ is an entangled state), then there exists a feasible dual solution Z_{EW} that satisfies $\mathrm{Tr}[G_0 Z_{EW}] < 0$. Using (9) we can see that the corresponding operator $\tilde{Z}_{EW}$ satisfies $\mathrm{Tr}[\rho \tilde{Z}_{EW}] < 0$ which together with $\mathrm{Tr}[\rho_{sep} \tilde{Z}_{EW}] \geq 0$ means that $\tilde{Z}_{EW}$ is an entanglement witness for ρ.

It is not hard to show that all of the witnesses generated by Eqn. (9) satisfy the relation

$$\begin{aligned} \langle xyx | Z \otimes I | xyx \rangle &= \langle xyx | (Z_0 + Z_1 + Z_2) | xyx \rangle \\ &= \langle xyx | Z_0 | xyx \rangle + \langle x^* yx | Z_1^{T_1} | x^* yx \rangle \\ &\quad + \langle xy^* x | Z_2^{T_2} | xy^* x \rangle. \end{aligned} \tag{10}$$

Since $Z_0, Z_1^{T_1}$ and $Z_2^{T_2}$ are positive by construction the biquadratic hermitian form $E(x,y)\langle x|x\rangle$ has a decomposition as a sum of squared magnitudes (SOS). This guarantees that the form $E(x,y)$ in (3) is positive semidefinite.

The reformulation of our separability tests as a search for SOS decompositions of the forms $E(x,y)$ provides connections with existing results in real algebra (see [12] for a discussion of the SDP-based approach in a general setting). By Artin's positive solution to

Hilbert's 17th problem, for any real PSD form $f(\mathbf{x})$ there exists a SOS form $h(\mathbf{x})$, such that the product $f(\mathbf{x})h(\mathbf{x})$ is SOS [14]. Finding such an $h(\mathbf{x})$ and SOS decomposition proves that f is PSD. For a fixed SOS form $h(x,y)$, we may write a SDP that attempts to find EWs such that $h(x,y)E(x,y)$ is SOS. In our hierarchy of criteria the form h is restricted to be $\langle x|x\rangle^{k-1}\langle y|y\rangle^{l-1}$. While it is conceivable that every positive semidefinite bihermitian form is SOS when multiplied by appropriate factors of this kind, this is currently an open question.

5 Example

We present next an example illustrating the presented methodology. Consider the state described in [6, Section 4.6], given by:

$$\rho_\alpha = \frac{2}{7}|\psi_+\rangle\langle\psi_+| + \frac{\alpha}{7}\sigma_+ + \frac{5-\alpha}{7}P\sigma_+P, \qquad (11)$$

with $0 \leq \alpha \leq 5$, $|\psi_+\rangle = \frac{1}{\sqrt{3}}\sum_{i=0}^{2}|ii\rangle$, $\sigma_+ = \frac{1}{3}(|01\rangle\langle 01| + |12\rangle\langle 12| + |20\rangle\langle 20|)$. Notice that ρ_α is invariant under the simultaneous change of $\alpha \to 5-\alpha$ and interchange of the parties. The state is separable for $2 \leq \alpha \leq 3$ and not PPT for $\alpha > 4$ and $\alpha < 1$. Numerically entanglement witnesses could be constructed for ρ_α in the range $3+\epsilon < \alpha \leq 4$ (and $1 \leq \alpha < 2-\epsilon$) with $\epsilon \geq 10^{-8}$. A witness for $\alpha > 3$ can be extracted from these by inspection:

$$\begin{aligned} Z_{EW} \;=\; & 2\left(|00\rangle\langle 00| + |11\rangle\langle 11| + |22\rangle\langle 22|\right) + \\ & + |02\rangle\langle 02| + |10\rangle\langle 10| + |21\rangle\langle 21| - 3|\psi_+\rangle\langle\psi_+|. \end{aligned}$$

This observable is nonnegative on separable states:

$$\begin{aligned} 2\langle xy|Z_{EW}|xy\rangle\langle x|x\rangle \;=\; & |2\,x_0x_1y_2^* - x_2x_0y_1^* - x_1x_2y_0^*|^2 \\ & + |2x_0x_0^*y_0 - 2x_1x_0^*y_1 + x_1x_1^*y_0 - x_2x_0^*y_2|^2 \\ & + |2x_0x_0^*y_2 - 2x_1x_2^*y_1 + x_2x_2^*y_2 - x_0x_2^*y_0|^2 \\ & + |2x_0x_1^*y_0 - 2x_2x_2^*y_1 + x_2x_1^*y_2 - x_1x_1^*y_1|^2 \\ & + 3\,|x_2x_0y_1^* - x_1x_2y_0^*|^2 + 3\,|x_1x_1^*y_0 - x_2x_0^*y_2|^2 \\ & + 3\,|x_2x_2^*y_2 - x_0x_2^*y_0|^2 + 3\,|x_2x_1^*y_2 - x_1x_1^*y_1|^2 \geq 0. \end{aligned}$$

The expected value on the original state is $\mathrm{Tr}[Z_{EW}\rho_\alpha] = \frac{1}{7}(3-\alpha)$, demonstrating entanglement for all $\alpha > 3$.

6 Conclusions

We discussed a hierarchy of SDP-based separability tests, introduced in [4], that are strictly stronger than the standard PPT criterion. The tests have complementary interpretations, both in terms of state extensions and sums of squares decompositions of real-valued complex forms. It is the duality between these two formulations that leads to a construction of entanglement witnesses for states that fail any separability test in the sequence.

The first step in the hierarchy of tests is exactly equivalent to the well-known PPT criterion. Only the second step in this sequence was required to detect the entanglement of a wide class of known PPT entangled states taken from the literature. The numerical results can also be very helpful in finding analytical expressions for the entanglement witness, as was illustrated in the example of Section 5.

Acknowledgments: It is a pleasure to acknowledge conversations with Hideo Mabuchi, John Doyle, John Preskill and Patrick Hayden. This work was supported by the Caltech MURI Center for Quantum Networks, the NSF Institute for Quantum Information and the Caltech MURI Center for Uncertainty Management for Complex Systems.

References

[1] J. S. Bell. On the Einstein-Podolsky-Rosen paradox. *Physics*, 1:195–200, 1964.

[2] S. L. Braunstein, C. M. Caves, R. Jozsa, N. Linden, S. Popescu, and R. Schack. Separability of very noisy mixed states and implications for NMR quantum computing. *Phys. Rev. Lett.*, 83(5):1054–1057, 1999.

[3] D. Bruss and A. Peres. Construction of quantum states with bound entanglement. *Phys. Rev. A*, 61:030301(R), 2000.

[4] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri. Distinguishing separable and entangled states. *Phys. Rev. Lett.*, 88(18):187904–1–4, May 2002.

[5] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A*, 223:1, 1996.

[6] M. Horodecki, P. Horodecki, and R. Horodecki. Mixed-state entanglement and quantum communication. quant-ph/0109124, 2001.

[7] P. Horodecki. Separability criterion and inseparable mixed states with positive partial transpose. *Phys. Lett. A*, 232:233, 1997.

[8] M. Lewenstein, D. Bruss, J. I. Cirac, B. Kraus, M. Kus, J. Samsonowicz, A. Sanpera, and R. Tarrach. Separability and distillability in composite quantum systems -a primer-. *J. Mod. Opt.*, 47:2841, 2000.

[9] M. Lewenstein, B. Kraus, J. I. Cirac, and P. Horodecki. Optimization of entanglement witnesses. *Phys. Rev. A*, 62:052310, 2000.

[10] M. N. Nielsen and I. L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[11] P. A. Parrilo. *Structured Semidefinite Programs and Semialgebraic Geometry Methods in Robustness and Optimization*. PhD thesis, California Institute of Technology, May 2000. Available at `http://www.cds.caltech.edu/~pablo/`.

[12] P. A. Parrilo. Semidefinite programming relaxations for semialgebraic problems. To appear in *Mathematical Programming*, available at `http://www.control.ethz.ch/~parrilo/pubs/`, 2001.

[13] A. Peres. Separability criterion for density matrices. *Phys. Rev. Lett.*, 77(8):1413–1415, 1996.

[14] B. Reznick. Some concrete aspects of Hilbert's 17th problem. In *Contemporary Mathematics*, volume 253, pages 251–272. American Mathematical Society, 2000.

[15] J. F. Sturm. Using SeDuMi 1.02, a MATLAB toolbox for optimization over symmetric cones. *Optimization Methods and Software*, 11–12:625–653, 1999. Available at `http://fewcal.kub.nl/sturm/software/sedumi.html`.

[16] B. M. Terhal. Bell inequalities and the separability criterion. *Phys. Lett. A*, 271(5–6):319–326, 2000.

[17] L. Vandenberghe and S. Boyd. Semidefinite programming. *SIAM Review*, 38(1):49–95, 1996.

[18] R. F. Werner. Quantum states with Einstein-Podolsky-Rosen correlations admitting a hidden-variable model. *Phys. Rev. A*, 40(8):4277–4281, 1989.