



# The Set of Separable States has no Finite Semidefinite Representation Except in Dimension $3 \times 2$

Hamza Fawzi 

Department of Applied Mathematics and Theoretical Physics, University of Cambridge, Cambridge, UK.  
E-mail: [h.fawzi@damtp.cam.ac.uk](mailto:h.fawzi@damtp.cam.ac.uk)

Received: 22 July 2019 / Accepted: 30 June 2021  
Published online: 31 July 2021 – © The Author(s) 2021

**Abstract:** Given integers  $n \geq m$ , let  $\text{Sep}(n, m)$  be the set of separable states on the Hilbert space  $\mathbb{C}^n \otimes \mathbb{C}^m$ . It is well-known that for  $(n, m) = (3, 2)$  the set of separable states has a simple description using semidefinite programming: it is given by the set of states that have a positive partial transpose. In this paper we show that for larger values of  $n$  and  $m$  the set  $\text{Sep}(n, m)$  has no semidefinite programming description of finite size. As  $\text{Sep}(n, m)$  is a semialgebraic set this provides a new counterexample to the Helton–Nie conjecture, which was recently disproved by Scheiderer in a breakthrough result. Compared to Scheiderer’s approach, our proof is elementary and relies only on basic results about semialgebraic sets and functions.

## 1. Introduction

Entanglement is a fundamental aspect of quantum mechanics. The set of *separable states* (i.e., nonentangled states) on the Hilbert space  $\mathbb{C}^n \otimes \mathbb{C}^m$  is defined as:

$$\text{Sep}(n, m) = \text{conv} \left\{ xx^\dagger \otimes yy^\dagger : x \in \mathbb{C}^n, |x| = 1, y \in \mathbb{C}^m, |y| = 1 \right\}.$$

Here  $x^\dagger = \bar{x}^\top$  indicates conjugate transpose,  $|x|^2 = x^\dagger x = \sum_{i=1}^n |x_i|^2$  and **conv** denotes the convex hull. The set  $\text{Sep}(n, m)$  lives in the space  $\mathbf{H}^{nm}$  of Hermitian matrices of size  $nm \times nm$ , and it is full-dimensional in the subspace of matrices of trace equal to one.

A fundamental computational task in quantum information is to decide membership in the convex set  $\text{Sep}(n, m)$ . One of the first tests designed to check whether a state  $\rho \in \mathbf{H}^{nm}$  is separable is the *Peres-Horodecki criterion* [Per96, HHH96] (also known as the *Positive Partial Transpose (PPT)* criterion). It is based on the observation that for any  $\rho \in \text{Sep}(n, m)$ ,  $(I \otimes \mathbf{T})(\rho)$  is positive semidefinite where  $I$  is the identity map, and  $\mathbf{T}$  the transpose map. Indeed one can easily verify that if  $\rho = xx^\dagger \otimes yy^\dagger$  then

$(I \otimes T)(\rho) = xx^\dagger \otimes (yy^\dagger)^\top = xx^\dagger \otimes \bar{y}\bar{y}^\dagger \geq 0$ . In other words we have the inclusion  $\text{Sep}(n, m) \subseteq \text{PPT}(n, m)$  where

$$\text{PPT}(n, m) = \left\{ \rho \in \mathbf{H}^{nm} : \rho \geq 0, (I \otimes T)(\rho) \geq 0, \text{ and } \text{Tr}[\rho] = 1 \right\}. \tag{1}$$

It is known, from earlier work of Woronowicz [Wor76], that we have equality  $\text{Sep}(n, m) = \text{PPT}(n, m)$  if, and only if  $n + m \leq 5$ . Thus, the smallest cases where  $\text{Sep}(n, m) \neq \text{PPT}(n, m)$  are  $(n, m) = (4, 2)$  and  $(n, m) = (3, 3)$ .

**Semidefinite programming** The description of the set  $\text{PPT}(n, m)$  in Eq. (1) allows us to decide membership, and optimize linear functions on  $\text{PPT}(n, m)$ , via *semidefinite programming*. Semidefinite programming is a fundamental tool in optimization that has played a crucial role in recent developments in quantum information theory. We say that a convex set  $C$  has a *semidefinite representation (also called a semidefinite lift)* of size  $r$  if it can be expressed as

$$C = \pi(S) \tag{2}$$

where  $\pi : \mathbb{R}^D \rightarrow \mathbb{R}^d$  is a linear map and  $S \subset \mathbb{R}^D$  is a convex set defined using a linear matrix inequality

$$S = \{w \in \mathbb{R}^D : M_0 + w_1 M_1 + \dots + w_D M_D \geq 0\} \tag{3}$$

where  $M_0, \dots, M_D$  are Hermitian matrices of size  $r \times r$ . A set  $S$  of the form (3) is known as a *spectrahedron*. In this paper we are most interested in when a semidefinite representation of finite size exists, and call this simply a semidefinite representation throughout. If a convex set  $C$  admits a semidefinite representation, then optimizing a linear function on  $C$  can be cast as a semidefinite program. Equation (1) gives a semidefinite representation of  $\text{PPT}(n, m)$ .

**Horodecki’s criterion** The set of separable states has the following well-known description due to the Horodeckis [HHH96]:

$$\text{Sep}(n, m) = \left\{ \rho \in \mathbf{H}^{nm} : \text{Tr}[\rho] = 1 \text{ and } (I \otimes \Phi)(\rho) \geq 0 \ \forall \Phi : M_m \rightarrow M_n \text{ positive} \right\}. \tag{4}$$

Here  $M_k = \mathbb{C}^{k \times k}$  and a  $\mathbb{C}$ -linear map  $\Phi : M_m \rightarrow M_n$  is *positive* if it is Hermitian preserving and if  $\Phi(X) \geq 0$  for all  $X \geq 0$ . When  $n = m$ , the relaxation  $\text{PPT}(n, m)$  corresponds to having only the identity and transpose maps in Eq. (4), which are both positive. A recent result of Skowronek [Sko16] shows that when  $n = m = 3$ , there is no finite family of positive maps  $\Phi_1, \dots, \Phi_k : M_3 \rightarrow M_3$  such that  $\text{Sep}(3, 3) = \{ \rho \in \mathbf{H}^9 : (I \otimes \Phi_i)(\rho) \geq 0 \ \forall i = 1, \dots, k \}$ . Note that the right-hand side of the previous equation is a specific semidefinite representable set. Thus Skowronek’s result rules out certain specific semidefinite representations for  $\text{Sep}(3, 3)$ .<sup>1</sup>

**DPS hierarchy** In [DPS04], Doherty, Parrilo and Spedalieri proposed a complete hierarchy of approximations to the set of separable states based on semidefinite programming. The first level of the hierarchy coincides with the PPT test, and subsequent levels form tighter and tighter convex relaxations of the set of separable states. If we denote the convex relaxation at level  $k$  by  $\text{DPS}_k(n, m)$  we have (dropping the  $(n, m)$ ):

$$\text{Sep} \subseteq \dots \subseteq \text{DPS}_k \subseteq \text{DPS}_{k-1} \subseteq \dots \subseteq \text{DPS}_1 = \text{PPT}.$$

---

<sup>1</sup> The result of Skowronek is in fact more general than this, and rules any formulation of the form  $\{ \rho : (I \otimes \Phi_i)((I \otimes B)\rho(I \otimes B^\dagger)) \geq 0 \ \forall i = 1, \dots, k, \ \forall B \in M_3 \}$  where  $\Phi_1, \dots, \Phi_k$  is a finite set of positive maps.

The key property of the DPS hierarchy is that each set  $\text{DPS}_k$  has a semidefinite representation of size  $\min(n, m)^{O(k)}$ . The hierarchy is known to be complete, meaning that if  $\rho \notin \text{Sep}$ , then there exists a finite  $k$  such that  $\rho \notin \text{DPS}_k$ . The integer  $k$  however depends on the state  $\rho$  and it is known that, unless  $n + m \leq 5$ , there is no finite  $k$  such that  $\text{DPS}_k(n, m) = \text{Sep}(n, m)$  [DPS04, Section VIII.B].

**Contributions** The main result of this paper is

**Theorem 1.** *If  $\text{Sep}(n, m) \neq \text{PPT}(n, m)$  then  $\text{Sep}(n, m)$  has no (finite) semidefinite representation. In other words,  $\text{Sep}(n, m)$  has no semidefinite representation when  $n + m > 5$ .*

*Remark 1.* Some remarks concerning Theorem 1:

- Note that Theorem 1 contains as a special case the fact that whenever  $\text{Sep}(n, m) \neq \text{PPT}(n, m)$ , then there is no representation of  $\text{Sep}(n, m)$  as  $\{\rho \in \mathbf{H}^{nm} : \text{Tr}[\rho] = 1 \text{ and } (I \otimes \Phi_i)(\rho) \geq 0, \forall i = 1, \dots, k\}$  where  $\Phi_1, \dots, \Phi_k : \mathbf{M}_m \rightarrow \mathbf{M}_n$  is a finite family of positive maps. This is because the latter set is semidefinite representable (in fact it is a spectrahedron). Let us mention that if one is only interested in *approximating* the set  $\text{Sep}(n, m)$ , Aubrun and Szarek [AS17b] gave a lower bound on the number  $k$  of positive maps needed.
- Our result also includes as a special case the fact that there is no finite  $k$  such that  $\text{DPS}_k(n, m) = \text{Sep}(n, m)$ , when  $n + m > 5$ . We note that our result is a strict generalization of this fact. Indeed, the failure of the DPS hierarchy to converge in a finite number of levels does not preclude by itself the existence of another semidefinite program that represents  $\text{Sep}(n, m)$  exactly. There are well-known examples of convex sets where the sum-of-squares hierarchy (of which DPS can be seen as a particular instance) is never exact and yet a finite semidefinite representation does exist, see e.g., [NPS10, Example 3.7].
- Observe that if  $\text{Sep}(n, m)$  has no semidefinite representation, then the same is true for  $\text{Sep}(N, m)$  for  $N \geq n$ . This is because  $\text{Sep}(n, m)$  can be realized as a linear section of  $\text{Sep}(N, m)$  as follows:

$$\text{Sep}(n, m) \simeq \{\rho \in \text{Sep}(N, m) : (\text{Tr}_2 \rho)_{ii} = 0 \forall i = n + 1, \dots, N\}$$

where  $\text{Tr}_2 \rho$  is the result of tracing out the second subsystem from  $\rho$ . Indeed, setting  $(\text{Tr}_2 \rho)_{ii} = 0$  implies that in any representation of  $\rho$  as  $\rho = \sum_k p_k x_k x_k^\dagger \otimes y_k y_k^\dagger$ , the vectors  $x_k$  must satisfy  $(x_k)_i = 0$  for all  $i = n + 1, \dots, N$ , i.e., that  $x_k \in \mathbb{C}^n \times \{0\}^{N-n} \simeq \mathbb{C}^n$ . To prove our theorem it thus suffices to prove that  $\text{Sep}(3, 3)$  and  $\text{Sep}(4, 2)$  have no semidefinite representations.

**Helton–Nie conjecture** The question of finding semidefinite representations for convex sets has attracted a lot of attention in the optimization community [Nem06, GPT13]. Helton and Nie [HN09] gave sufficient conditions for a set to have a semidefinite representation, and conjectured that any convex *semialgebraic* set has a semidefinite representation. (A set is semialgebraic set if it can be described using a finite boolean combinations of polynomial equations and inequalities. One can verify that  $\text{Sep}(n, m)$  is a semialgebraic set, see Sect. 2.3.) In his breakthrough paper, Scheiderer [Sch18] disproved this conjecture and exhibited convex semialgebraic sets that have no semidefinite representations.

Our proof of Theorem 1 is inspired from the arguments of Scheiderer. Compared to the paper of Scheiderer the present paper has two main contributions. First, the proof we give simplifies the arguments of Scheiderer and does not rely on any specialized results

from algebraic geometry. We only use basic results from analysis (Taylor expansions), and some standard facts about semialgebraic sets and functions which are elementary to state. The proof should thus be accessible to readers in quantum information and optimization. The second contribution is the application of the method of proof for  $\text{Sep}(n, m)$  which is defined in terms of complex numbers. This turns out to cause certain difficulties as certain standard facts about real polynomials are not true about Hermitian polynomials, particularly on the relation between homogeneous polynomials and their dehomogenizations (see Sect. 5 and Appendix A for more details).

**Main technical result** Our main technical result, Theorem 2 below and of which Theorem 1 is a corollary, gives a general way to construct a convex set with no semidefinite representation from a nonnegative Hermitian polynomial that is not a sum of squares. We recall that a *Hermitian polynomial*  $p(z)$  is a polynomial with complex coefficients in the indeterminates  $(z, \bar{z}) = (z_1, \dots, z_n, \bar{z}_1, \dots, \bar{z}_n)$  such that  $p(z) \in \mathbb{R}$  for all  $z \in \mathbb{C}^n$ . A Hermitian polynomial is a sum of squares if it can be written as a sum of squares of Hermitian polynomials. (More details about Hermitian polynomials are given in Sect. 2.) For the statement of the theorem, we use the monomial notation  $z^u = \prod_{i=1}^n z_i^{u_i}$  for  $u \in \mathbb{N}^n$ .

**Theorem 2 (General theorem).** *Let  $p(z) = \sum_{(u,v) \in A} p_{uv} z^u \bar{z}^v$  be a Hermitian polynomial supported on  $A \subset \mathbb{N}^n \times \mathbb{N}^n$ , and assume that  $p$  is nonnegative on  $\mathbb{C}^n$  but not a sum of squares. Assume furthermore that  $A$  is downward closed, i.e., if  $(u, v) \in A$  then all  $(u', v') \in \mathbb{N}^n \times \mathbb{N}^n$  with  $0 \leq u' \leq u$  and  $0 \leq v' \leq v$  are in  $A$ . Define the monomial map  $\mathbf{m}_A : \mathbb{C}^n \rightarrow \mathbb{C}^{|A|}$ ,  $z \mapsto [z^u \bar{z}^v]_{(u,v) \in A}$  for  $z \in \mathbb{C}^n$ . Then the convex set*

$$\mathcal{C}_A = \mathbf{cl\ conv} \{ \mathbf{m}_A(z) : z \in \mathbb{C}^n \} \tag{5}$$

is not semidefinite representable, where  $\mathbf{cl}$  denotes topological closure.

The set of separable states is of the form (5) for well-chosen set  $A$ . Indeed, dropping the normalization condition and letting  $\mathcal{SEP}(n, m)$  be the convex cone of separable states, we have:

$$\begin{aligned} \mathcal{SEP}(n, m) &= \mathbf{conv} \left\{ [x_i \bar{x}_j y_k \bar{y}_l]_{\substack{1 \leq i, j \leq n \\ 1 \leq k, l \leq m}} : (x, y) \in \mathbb{C}^n \times \mathbb{C}^m \right\} \\ &= \mathbf{conv} \left\{ [x^\alpha \bar{x}^\beta y^\gamma \bar{y}^\delta]_{|\alpha|=|\beta|=|\gamma|=|\delta|=1} : (x, y) \in \mathbb{C}^n \times \mathbb{C}^m \right\} \end{aligned}$$

where for  $\zeta \in \mathbb{N}^k$  we let  $|\zeta| = \sum_{i=1}^k \zeta_i$ . This shows that  $\mathcal{SEP}(n, m) = \mathcal{C}_A$  where

$$A = \{ (\alpha, \beta, \gamma, \delta) \in (\mathbb{N}^n \times \mathbb{N}^n) \times (\mathbb{N}^m \times \mathbb{N}^m) : |\alpha| = |\beta| = |\gamma| = |\delta| = 1 \}. \tag{6}$$

The attentive reader will notice that this set  $A$  is *not* downward closed, and so does not satisfy the condition of Theorem 2. As a matter of fact, to prove Theorem 1 we apply Theorem 2 with a *dehomogenization* of  $A$  which satisfies the downward closed condition, and then homogenize back to get the desired convex cone. The details are explained in Sect. 5.

**Overview of proof** We briefly sketch the main ideas for the proof of Theorem 2.

- We first show that if the set  $\mathcal{C}_A$  has a semidefinite representation, then there exists a finite number of functions  $f_1, \dots, f_r : \mathbb{R}^{2n} \simeq \mathbb{C}^n \rightarrow \mathbb{R}$  such that any nonnegative Hermitian polynomial supported on  $A \cup \{(\mathbf{0}, \mathbf{0})\}$  can be written as a sum of squares from  $\text{span}_{\mathbb{R}}(f_1, \dots, f_r)$ . This characterization of semidefinite representations via sums of squares is not new: it follows from the factorization theorem of Gouveia, Parrilo and Thomas [GPT13] and its sum-of-squares interpretation see e.g., [Faw16]. We note that a similar characterization is also used in Scheiderer’s paper, see [Sch18, Theorem 3.4].
- One of the main observations needed to prove Theorem 2 is to note that the functions  $f_1, \dots, f_r$  can be chosen to be *semialgebraic*. (We recall the precise definition of semialgebraic functions in Sect. 2.) One key property of such functions that turns out to be particularly important is that they are smooth almost everywhere. Combining this property with a simple observation regarding smooth sum of squares decompositions of homogeneous polynomials allows us to prove Theorem 2 already in the special case where  $p$  is a homogeneous polynomial. This allows us to prove that  $\text{Sep}(n, m)$  is not semidefinite representable when  $(n, m) = (5, 3)$  or  $(4, 4)$ . The complete proof of Theorem 2 which allows us to cover the cases  $(n, m) = (4, 2)$  and  $(3, 3)$  for separable states, requires an additional technical argument using Puiseux expansions for univariate continuous semialgebraic functions.

**Real version of Theorem 2** We note that one can state an analogue of Theorem 2 dealing with real polynomials instead of Hermitian polynomials. The proof is similar, and we state it below just for convenience and for future reference.

**Theorem 3** (Main theorem for real polynomials). *Let  $p(x) = \sum_u p_u x^u \in \mathbb{R}[x]$  where  $A \subset \mathbb{N}^n$  finite, be a real polynomial that is nonnegative on  $\mathbb{R}^n$  but not a sum of squares. Assume furthermore that  $A$  is downward closed, i.e., if  $u \in A$  then all  $u' \in \mathbb{N}^n$  with  $0 \leq u' \leq u$  are in  $A$ . Define the monomial map  $\mathbf{m}_A(x) = [x^u]_{u \in A}$  for  $x \in \mathbb{R}^n$ . Then the convex set*

$$\text{cl conv } \{ \mathbf{m}_A(x) : x \in \mathbb{R}^n \}$$

*is not semidefinite representable.*

The theorem above can be used to recover the result of Scheiderer [Sch18, Corollary 4.25], that the cone  $P_{n,2d}$  of nonnegative (real) forms in  $n$  variables of degree  $2d$  is not semidefinite representable when it is distinct from  $\Sigma_{n,2d}$ , the cone of sums of squares. Indeed, it suffices to take  $p$  in Theorem 3 to be a dehomogenization of a nonnegative form that is not a sum of squares, and to use the well-known fact that a convex set has a semidefinite representation if and only if its dual has one.

**Organization** The paper is organized as follows. In Sect. 2 we set some of the notations and present some background material on Hermitian polynomials, sums of squares, and semialgebraic sets and functions that are useful for the proof of the main theorem. In Sect. 3 we review the connection between the existence of semidefinite programming representations, and sums of squares. The proof of Theorem 2 is in Sect. 4 and the proof of Theorem 1 in Sect. 5.

## 2. Preliminaries

We recall in this section some results on Hermitian polynomials, the duality  $\text{Sep}/\text{nonnegative polynomials}$  and  $\text{PPT}/\text{sums of squares}$  and semialgebraic sets and functions.

**2.1. Hermitian polynomials.** For  $z \in \mathbb{C}^n$ , we denote the elementwise complex conjugate of  $z$  by  $\bar{z} = (\bar{z}_1, \dots, \bar{z}_n)$ . If  $u \in \mathbb{N}^n$  we define the monomial  $z^u = z_1^{u_1} \dots z_n^{u_n}$ . A Hermitian polynomial  $p(z)$  is a polynomial in  $z$  and  $\bar{z}$  of the form

$$p(z) = \sum_{(u,v) \in A} p_{uv} z^u \bar{z}^v \quad (A \subset \mathbb{N}^n \times \mathbb{N}^n) \tag{7}$$

such that  $p(z) \in \mathbb{R}$  for all  $z \in \mathbb{C}^n$ . This is equivalent to saying that  $p_{uv} = \overline{p_{vu}}$  for all  $u, v$ . The *support* of  $p$  is  $\text{supp}(p) = \{(u, v) : p_{uv} \neq 0\} \subset \mathbb{N}^n \times \mathbb{N}^n$ . The Hermitian polynomial  $p$  is *nonnegative* if  $p(z) \geq 0$  for all  $z \in \mathbb{C}^n$ . Further, we say that  $p$  is a *sum of squares* if we can write

$$p = \sum_k q_k^2 \tag{8}$$

for Hermitian polynomials  $q_k$ . If  $p(z)$  is a Hermitian polynomial we will often consider the *real* polynomial  $P(a, b) = p(a + ib)$  in  $\mathbb{R}[a_1, \dots, a_n, b_1, \dots, b_n]$ . One can check that  $p$  is a sum-of-squares if and only if  $P$  is a sum-of-squares of real polynomials.

*Remark 2* (Sums of squares for Hermitian polynomials). Another common definition of a Hermitian polynomial  $p(z)$  being a sum-of-squares is that  $p$  can be written as  $p(z) = \sum_k |g_k(z)|^2$  where  $g_k$  are (holomorphic) polynomials in  $z$  *only* (and not in  $\bar{z}$ ). Clearly if  $p$  has such a representation then it is a sum-of-squares in the sense (8) since then  $p = \sum_k \text{Re}[g_k]^2 + \text{Im}[g_k]^2$  and  $\text{Re}[g_k]$  and  $\text{Im}[g_k]$  are both Hermitian polynomials. The converse however is not true. It is possible that a polynomial  $p$  has a representation (8) and cannot be written as a sum of modulus squares of holomorphic polynomial mappings. See e.g., [DP09] for more on this distinction. In this paper we only work with the definition (8) of sums of squares.

**2.2. Sep, PPT, nonnegative polynomials, and sums of squares.** For convenience, we will work in this paper with the *cone* of separable states, where we drop the normalization condition:

$$\mathcal{SEP}(n, m) = \text{conv} \left\{ xx^\dagger \otimes yy^\dagger : x \in \mathbb{C}^n, y \in \mathbb{C}^m \right\}.$$

One can verify that  $\text{Sep}(n, m)$  is the compact slice  $\text{Sep}(n, m) = \mathcal{SEP}(n, m) \cap \{\rho : \text{Tr } \rho = 1\}$ .<sup>2</sup> Let also  $\mathcal{PPT}$  be the cone of states that have positive partial transpose, i.e.,

$$\mathcal{PPT}(n, m) = \{\rho \in \mathbf{H}^{nm} : \rho \geq 0 \text{ and } (I \otimes \mathbf{T})(\rho) \geq 0\}$$

so that  $\text{PPT}(n, m) = \mathcal{PPT}(n, m) \cap \{\rho : \text{Tr } \rho = 1\}$ .

**Dual of Sep** For any integer  $k$ , let  $M_k = \mathbb{C}^{k \times k}$ . A  $\mathbb{C}$ -linear map  $\Phi : M_n \rightarrow M_m$  that is Hermitian preserving is *positive* if  $\Phi(\rho) \geq 0$  whenever  $\rho \geq 0$ . Equivalently,  $\Phi$  is positive if the degree-four Hermitian polynomial  $p(x, y) = y^\dagger \Phi(xx^\dagger)y$  is nonnegative on  $\mathbb{C}^{n+m} \simeq \mathbb{C}^n \times \mathbb{C}^m$ . It is well-known that the dual of  $\mathcal{SEP}(n, m)$  can be identified, via

<sup>2</sup> Indeed if  $\rho = \sum_i p_k x_k x_k^\dagger \otimes y_k y_k^\dagger$  with  $\text{Tr } \rho = 1$  and  $p_k \geq 0$ , then by redefining  $p_k \leftarrow p_k |x_k|^2 |y_k|^2$  we can assume without loss of generality that  $|x_k| = |y_k| = 1$ . Taking the trace on both sides of  $\rho = \sum_i p_k x_k x_k^\dagger \otimes y_k y_k^\dagger$  tells us that  $1 = \sum_k p_k$  since  $\text{Tr } \rho = 1$ , i.e.,  $\rho \in \text{Sep}(n, m)$ .

the Choi isomorphism<sup>3</sup>, with the cone of positive maps  $M_n \rightarrow M_m$  (see e.g., [AS17a, Table 2.2]). Equivalently, the dual of  $\mathcal{SEP}(n, m)$  can be identified with nonnegative degree-four Hermitian polynomials of the form

$$p(x, y) = \sum_{\substack{1 \leq i, j \leq n \\ 1 \leq k, l \leq m}} p_{ijkl} x_i \bar{x}_j y_k \bar{y}_l \quad (x \in \mathbb{C}^n, y \in \mathbb{C}^m) \tag{9}$$

where  $p_{ijkl} = \Phi(E_{ij})_{lk}$ . Polynomials of the form (9) have a *biquadratic* structure: they are quadratic independently in each block of variables  $x$  and  $y$ . The duality between  $\mathcal{SEP}$  and nonnegative polynomials of the form (9) is in fact immediate from the definition of  $\mathcal{SEP}$ .

**Dual of PPT** Using the identification above, it turns out that the dual of  $\mathcal{PPT}(n, m)$  corresponds to polynomials  $p(x, y)$  that are *sums of squares*. Indeed, it is well-known (see again [AS17a, Table 2.2]) that the dual cone of  $\mathcal{PPT}(n, m)$  can be identified, via the Choi isomorphism, with the cone of maps  $\Phi : M_n \rightarrow M_m$  that are *decomposable*, i.e., that can be written  $\Phi = S_1 + S_2 \circ \mathbb{T}$  where  $S_1$  and  $S_2$  are two *completely positive maps*, and  $\mathbb{T}$  is the transpose map. Recall that a map  $S : M_n \rightarrow M_m$  is completely positive if there exist matrices  $V_t$  such that  $S(X) = \sum_t V_t^* X V_t$ . One can verify that a map  $\Phi$  is decomposable if and only if, the associated Hermitian polynomial (9) is a sum of squares. We did not find any reference for this equivalence, so we include a proof here. (The proofs we found in the literature are only for the direction  $\Rightarrow$  in Proposition 1. The proof of Proposition 1 is a special case of a more general result in [FF20], joint with Kun Fang, where it is shown that the dual of  $\text{DPS}_k$  can be identified with a sum-of-squares condition of degree  $k$ .)

**Proposition 1.** *A map  $\Phi : M_n \rightarrow M_m$  is decomposable if, and only if, the Hermitian polynomial  $p(x, y) = y^\dagger \Phi(x x^\dagger) y$  is a sum of squares.*

*Proof.* If  $S(\rho) = \sum_t V_t \rho V_t^\dagger$  is a completely positive map then  $y^\dagger S(x x^\dagger) y = \sum_t y^\dagger V_t x x^\dagger V_t^\dagger y = \sum_t |\bar{y}^\top V_t x|^2$  is a sum-of-squares. Also for the transpose map  $\mathbb{T}$ , we have  $y^\dagger (S \circ \mathbb{T})(x x^\dagger) y = y^\dagger S(\bar{x} \bar{x}^\dagger) y = \sum_t |y^\top \bar{V}_t \bar{x}|^2$  is also a sum-of-squares. It follows that if  $\Phi$  is decomposable then  $p(x, y) = y^\dagger \Phi(x x^\dagger) y$  is a sum-of-squares.

We now prove the converse. Assume  $p(x, y) = y^\dagger \Phi(x x^\dagger) y$  is a sum-of-squares, i.e.,  $p(x, y) = \sum_t q_t(x, y)^2$  for some Hermitian polynomials  $q_t$ . We need to show that  $\Phi$  is decomposable. Because of the biquadratic structure of  $p$  we see that  $q_t$  cannot have monomials  $x_i^2, \bar{x}_i^2, x_i x_j, \bar{x}_i \bar{x}_j, x_i \bar{x}_j$  or  $\bar{x}_i x_j$  and similarly for the  $y$ 's. Thus this means that  $q_t$  must have the form

$$q_t(x, y) = \underbrace{x^\top M_t y}_{g_t} + \underbrace{\bar{x}^\top \bar{M}_t \bar{y}}_{\bar{g}_t} + \underbrace{x^\top N_t \bar{y}}_{h_t} + \underbrace{\bar{x}^\top \bar{N}_t y}_{\bar{h}_t}$$

where  $M \in \mathbb{C}^{n \times n}$  and  $N \in \mathbb{C}^{m \times m}$ . Squaring  $q_t$  we get

$$q_t^2 = g_t^2 + 2|g_t|^2 + 2g_t h_t + 2g_t \bar{h}_t + \bar{g}_t^2 + 2\bar{g}_t h_t + 2\bar{g}_t \bar{h}_t + h_t^2 + 2|h_t|^2 + \bar{h}_t^2.$$

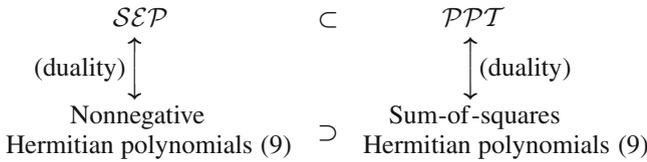
<sup>3</sup> The Choi isomorphism associates with a channel  $\Phi : M_n \rightarrow M_m$  the state  $C(\Phi) = \sum_{1 \leq i, j \leq n} E_{ij} \otimes \Phi(E_{ij}) \in \mathbb{C}^{nm \times nm}$  where  $E_{ij}$  is the matrix with a 1 in entry  $(i, j)$  and zero elsewhere. The state  $C(\Phi)$  satisfies for any  $x \in \mathbb{C}^n$  and  $y \in \mathbb{C}^m$  the identity  $\text{Tr}[C(\Phi) x x^\dagger \otimes y y^\dagger] = y^\dagger \Phi(\bar{x} \bar{x}^\dagger) y$ .

When summing  $\sum_k q_i^2$  we see that the only terms that can produce monomials of the form  $x_i \bar{x}_j y_k \bar{y}_l$  (the monomials that appear in  $p$ ) are the terms  $2|g_t|^2$  and  $2|h_t|^2$ . The sum of all the other terms must thus be equal to 0. At the end we get (including the constant 2 in  $M_t$  and  $N_t$ ):

$$p = \sum_t |x^\top M_t y|^2 + |x^\top N_t \bar{y}|^2.$$

From here it easily follows that  $\Phi = S_1 + S_2 \circ \mathbb{T}$  where  $S_1(\rho) = \sum_t N_t \rho N_t^\dagger$  and  $S_2(\rho) = \sum_t \bar{M}_t \rho \bar{M}_t^\dagger$ . □

The following diagram summarizes the discussion above.



**2.3. Semialgebraic sets and functions. Semialgebraic sets** A semialgebraic subset of  $\mathbb{R}^n$  is a subset that can be defined by a finite boolean combination of polynomial equations ( $P = 0$ ) and inequalities ( $P > 0$ ) where  $P \in \mathbb{R}[x_1, \dots, x_n]$ . For example a set of the form  $\{w \in \mathbb{R}^D : M_0 + w_1 M_1 + \dots + w_D M_D \geq 0\}$  is semialgebraic since the condition that a matrix is positive semidefinite can be expressed by a finite number of polynomial inequalities. The set of separable states can be shown to be semialgebraic. One can prove this using the celebrated and powerful result of Tarski stating that the projection of a semialgebraic set is semialgebraic. A consequence of Tarski’s theorem is that the *convex hull* of a semialgebraic set  $S \subset \mathbb{R}^n$  is semialgebraic. Indeed this is because we can write  $\mathbf{conv}(S)$  as the projection on the  $x$  component of the following semialgebraic set

$$\left\{ (x, \lambda, s_1, \dots, s_{n+1}) \in \mathbb{R}^n \times \mathbb{R}^{n+1} \times (\mathbb{R}^n)^{n+1} : \right. \\
 \left. \lambda_1, \dots, \lambda_{n+1} \geq 0, s_1, \dots, s_{n+1} \in S, x = \sum_{i=1}^{n+1} \lambda_i s_i \text{ and } \sum_{i=1}^{n+1} \lambda_i = 1 \right\}.$$

(Note that, by Carathéodory theorem any element in  $\mathbf{conv}(S)$  is a convex combination of at most  $n + 1$  points in  $S$ .) To see why the set  $\text{Sep}(n, m)$  is a semialgebraic subset of  $\mathbf{H}^{nm} \simeq \mathbb{R}^{2(nm)^2}$  first note that the following set

$$\left\{ (\rho, x, y) \in \mathbf{H}^{nm} \times \mathbb{C}^n \times \mathbb{C}^m \text{ s.t. } \rho = x x^\dagger \otimes y y^\dagger \text{ and } |x|^2 = |y|^2 = 1 \right\} \tag{10}$$

is a semialgebraic subset of  $\mathbf{H}^{nm} \times \mathbb{C}^n \times \mathbb{C}^m \simeq \mathbb{R}^{2(nm)^2} \times \mathbb{R}^{2n} \times \mathbb{R}^{2m}$  since the equations can all be written as real polynomial equations in the real and imaginary components. By Tarski’s theorem it follows that the projection of (10) on the  $\mathbf{H}^{nm}$  component, which is precisely the set of pure product states, is semialgebraic. Thus  $\text{Sep}$  is semialgebraic as the convex hull of a semialgebraic set.

**Semialgebraic functions** A function  $f : \mathbb{R}^n \rightarrow \mathbb{R}^m$  is called *semialgebraic* if its graph  $\{(x, f(x)) : x \in \mathbb{R}^n\} \subseteq \mathbb{R}^n \times \mathbb{R}^m$  is a semialgebraic set. Even though semialgebraic

functions form a very broad class of functions, they are tame and possess nice regularity properties. Examples of semialgebraic functions are polynomials, rational functions, or power functions (with rational exponent). Functions that are not semialgebraic are e.g.,  $\exp(x)$ , or the indicator function of the rationals in  $\mathbb{R}$ . We state two basic results about semialgebraic functions that will be crucial for us.

**Theorem 4** (Almost everywhere smoothness of semialgebraic functions). *Let  $f : \mathbb{R}^n \rightarrow \mathbb{R}$  be a semialgebraic function. Then  $f$  is smooth ( $C^\infty$ ) everywhere except possibly on the zero set of a polynomial  $P \in \mathbb{R}[x_1, \dots, x_n] \setminus \{0\}$ .*

*Proof.* See e.g., [HP16, Theorem 1.7]. □

Clearly Theorem 4 is not true for general functions, cf. the indicator function of the rationals in  $\mathbb{R}$ . The second result that we will need concerns semialgebraic functions in one variable.

**Theorem 5.** (Puiseux expansion for one-dimensional semialgebraic functions) *Assume  $f : (0, \eta) \rightarrow \mathbb{R}$  where  $\eta > 0$ , is a semialgebraic continuous function that is bounded. Then  $f$  can be extended by continuity to the interval  $[0, \eta)$ . Additionally, there exists an integer  $m$  such that the map  $t \mapsto f(t^m)$  is  $C^\infty$  on  $[0, \epsilon)$  for some  $0 < \epsilon < \eta$ .*

*Proof.* See [BPR06, Section 3.3]. □

We note that the theorem above is not true for arbitrary functions. For example the function  $x \mapsto \sin(1/x)$  is bounded and continuous on any interval  $(0, \eta)$  but cannot be extended by continuity at 0. We finally record the following result which will also be needed for our proof. It simply says that any linear map, restricted to a semialgebraic set always admits a semialgebraic inverse.

**Theorem 6.** *Let  $S \subset \mathbb{R}^N$  be a semialgebraic set and let  $\pi : \mathbb{R}^N \rightarrow \mathbb{R}^n$  be a linear map. Then there exists a semialgebraic function  $F : \pi(S) \rightarrow S$  that satisfies  $\pi(F(x)) = x$  for all  $x \in \pi(S)$ .*

*Proof.* See [HP16, Lemma 1.5]. □

### 3. Semidefinite Programming Lifts

We are now ready to start the proof of Theorem 2 (and thus of Theorem 1 too). The first thing we need is a necessary condition for the existence of a semidefinite representation for a given convex set  $C$ . The condition we state in Theorem 7 below is very similar to [GPT13, Theorem 1]<sup>4</sup>. Recall that, for  $A \subset \mathbb{N}^n \times \mathbb{N}^n$  we denote by  $\mathbf{m}_A(z)$  the monomial map:

$$\mathbf{m}_A(z) = [z^u \bar{z}^v]_{(u,v) \in A}.$$

We also denote by  $\mathbf{cl} S$  the (topological) closure of a set  $S$ .

**Theorem 7.** *Let  $A \subset \mathbb{N}^n \times \mathbb{N}^n$ . Assume that*

$$C_A = \mathbf{cl} \mathbf{conv} \{ \mathbf{m}_A(z) : z \in \mathbb{C}^n \}$$

*has a semidefinite representation of size  $k$ . Then there exists  $2k^2 + 1$  semialgebraic functions  $f_j : \mathbb{C}^n \rightarrow \mathbb{R} (j = 1, \dots, 2k^2 + 1)$  such that any nonnegative Hermitian polynomial*

---

<sup>4</sup> The given condition is also sufficient, but we will only need necessity here.

$p$  supported on  $A \cup \{(\mathbf{0}, \mathbf{0})\}$  is a sum-of-squares from  $V = \text{span}_{\mathbb{R}}(f_1, \dots, f_{2k^2+1})$ , i.e.,  $p = \sum_j h_j^2$  for some  $h_j \in V$ . Furthermore, the magnitude of the coefficients expressing the  $h_j$  in terms of the basis  $(f_1, \dots, f_{2k^2+1})$  are all bounded by  $\phi(\|p\|)$  where  $\|p\|$  is the largest magnitude of the coefficients of  $p$ , and  $\phi$  is some polynomial that only depends on the semidefinite representation of  $\mathcal{C}_A$ .

The main difference between the statement above and the one in [GPT13] (see also [Faw16, Theorem 5, Chapter 2]) is that here the functions  $f_1, \dots, f_{2k^2+1}$  are *semialgebraic*. (We say that a function  $f : \mathbb{C}^n \rightarrow \mathbb{R}$  is semialgebraic if the function  $F : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$  defined by  $F(a, b) = f(a + ib)$  is semialgebraic.) This observation will be crucial to us. We note that a statement similar to the theorem above appears as Theorem 3.4 in [Sch18]. Instead of working with semialgebraic functions, Scheiderer works with polynomial functions on an algebraic variety  $X$ .

*Proof.* Assume that  $\mathcal{C}_A = \pi(S)$  where  $S$  is a spectrahedron defined using a linear matrix inequality of size  $k \times k$ :

$$S = \left\{ w \in \mathbb{R}^N : M(w) := M_0 + M_1 w_1 + \dots + M_N w_N \succeq 0 \right\}.$$

We can assume without loss generality that  $S$  has nonempty interior in  $\mathbb{R}^N$ . This in turn implies, using standard results about spectrahedra, that there exists  $\tilde{w} \in S$  such that  $M(\tilde{w})$  is positive definite (possibly after changing  $M$ , see e.g., [RG95, Section 2.4]).

For any  $z \in \mathbb{C}^n$  there exists  $w(z) \in S$  such that  $\pi(w(z)) = \mathbf{m}_A(z)$ . Since  $M(w(z)) \succeq 0$  we can find  $F(z) \in \mathbb{C}^{k \times k}$  such that  $M(w(z)) = F(z)F(z)^\dagger$ . Furthermore, by Theorem 6, the function  $z \in \mathbb{C}^n \mapsto F(z) \in \mathbb{C}^{k \times k}$  can be taken to be semialgebraic.

Let  $p(z)$  be a Hermitian polynomial supported on  $A \cup \{(\mathbf{0}, \mathbf{0})\}$ , i.e.,  $p(z) = \langle \tilde{p}, \mathbf{m}_A(z) \rangle + c$  for some  $c \in \mathbb{R}$ , where  $\tilde{p}$  denotes the coefficients of the polynomial  $p(z)$  in the monomial basis. Since  $p \geq 0$  we get  $\langle \tilde{p}, \mathbf{m}_A(z) \rangle + c \geq 0$  for all  $z \in \mathbb{C}^n$ . This implies that  $\langle \tilde{p}, \sigma \rangle + c \geq 0$  for all  $\sigma \in \mathcal{C}_A$ . We can lift this linear inequality to an inequality on the spectrahedron  $S$ , i.e., we have  $\langle \tilde{p}, \pi(w) \rangle + c \geq 0$  for all  $w \in S$ , in other words

$$\langle \pi^*(\tilde{p}), w \rangle + c \geq 0 \quad \forall w \in \mathbb{R}^N \text{ s.t. } M(w) \succeq 0.$$

By Farkas' lemma/duality for SDPs, this means that there exists  $B \succeq 0$  and  $b \geq 0$  such that

$$\langle \pi^*(\tilde{p}), w \rangle + c = \langle B, M(w) \rangle + b \quad \forall w \in \mathbb{R}^N. \tag{11}$$

Plugging  $w = w(z)$  we get

$$\langle \tilde{p}, \pi(w(z)) \rangle + c = \langle B, M(w(z)) \rangle + b = \langle B, F(z)F(z)^\dagger \rangle + b.$$

Since  $\pi(w(z)) = \mathbf{m}_A(z)$  and  $\langle \tilde{p}, \mathbf{m}_A(z) \rangle = p(z)$  we get finally that  $p(z) + c = \langle B, F(z)F(z)^\dagger \rangle + b$  for all  $z \in \mathbb{C}^n$ . Factorizing  $B = DD^\dagger$  we get

$$\begin{aligned} p(z) + c &= \text{Tr} \left[ DD^\dagger F(z)F(z)^\dagger \right] + b = \sum_{ij=1}^k |D^\dagger F(z)|_{ij}^2 + b \\ &= \sum_{ij=1}^k \text{Re}[(D^\dagger F(z))_{ij}]^2 + \text{Im}[(D^\dagger F(z))_{ij}]^2 + b. \end{aligned}$$

If we define the  $2k^2 + 1$  semialgebraic functions to be the constant function and the  $z \mapsto \operatorname{Re}[F_{ij}(z)]$  and  $z \mapsto \operatorname{Im}[F_{ij}(z)]$ , we get the desired claim.

For the last statement of the theorem, we show that the coefficients of  $B$  (and thus of  $D$ ) are bounded by a polynomial in the coefficients of  $p$ . To get this, we can simply plug the value  $w = \tilde{w}$  that makes  $M(w)$  positive definite in (11). If we denote by  $\lambda > 0$  the smallest eigenvalue of  $M(\tilde{w})$  we get  $\langle \pi^*(\tilde{p}), \tilde{w} \rangle + c = \langle B, M(\tilde{w}) \rangle + b \geq \lambda \operatorname{Tr}[B] + b \geq \lambda \|B\| + b$ , thus  $\max(\|B\|, b) \leq (\langle \pi^*(\tilde{p}), \tilde{w} \rangle + c) / \min(\lambda, 1) \leq O(\max\{\|p\|, |c|\})$ .  $\square$

#### 4. Proof of Theorem 2

We are now ready to prove our main theorem, Theorem 2. We first recall a piece of notation that we will use throughout the proof: for any function  $f : \mathbb{C}^n \rightarrow \mathbb{R}$  we associate the function of real variables  $F : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$ , denoted by a capital letter, defined by  $F(a, b) = f(a + ib)$ . We will also sometimes think of a vector  $z \in \mathbb{C}^n$  as  $z \in \mathbb{R}^{2n}$  and write for instance  $F(z)$ .

Assume that  $\mathcal{C}_A$  has an SDP representation. Then, from Theorem 7 there exist semialgebraic functions  $f_1, \dots, f_r : \mathbb{C}^n \rightarrow \mathbb{R}$  such that the following is true:

$$\begin{aligned} \text{Any nonnegative Hermitian polynomial supported on } A \cup \{(\mathbf{0}, \mathbf{0})\} \\ \text{is a sum-of-squares of functions from } \operatorname{span}_{\mathbb{R}}(f_1, \dots, f_r). \end{aligned} \tag{*}$$

We will now prove that the functions  $f_i$  can be taken to be smooth at the origin. (By this we mean that the associated functions  $F_i : \mathbb{R}^n \times \mathbb{R}^n \rightarrow \mathbb{R}$  are smooth at  $(0, 0)$ .) This will follow from our assumption that  $A$  is downward closed. Since the  $F_i$  are semialgebraic we know from Theorem 4 that each  $F_i$  is smooth almost everywhere. Thus we can find a common point  $z_0 = (a_0, b_0) \in \mathbb{R}^n \times \mathbb{R}^n$  such that all functions  $F_i$  are smooth at  $z_0$ . Now let  $\tilde{f}_i(z) = f_i(z - z_0)$  for all  $i \in \{1, \dots, r\}$ . We claim that these semialgebraic functions still satisfy the property (\*). Indeed if  $q$  is a nonnegative Hermitian polynomial supported on  $A \cup \{(\mathbf{0}, \mathbf{0})\}$  then  $q(z + z_0)$  is nonnegative and is also supported on  $A$ , since  $A$  is downward closed. It follows that  $q(z + z_0)$  is a sum-of-squares from  $\operatorname{span}_{\mathbb{R}}(f_1, \dots, f_r)$ . But this implies that  $q(z)$  is a sum-of-squares from  $\operatorname{span}_{\mathbb{R}}(\tilde{f}_1, \dots, \tilde{f}_r)$ .

In the rest of the proof we will thus assume that the  $F_1, \dots, F_r$  are smooth at the origin. If  $p$  is homogeneous we are almost done by the following simple observation: if  $P$  is a real homogeneous polynomial and  $P = \sum_j H_j^2$  for some functions  $H_j : \mathbb{R}^m \rightarrow \mathbb{R}$  that are smooth at the origin, then  $P$  is a sum-of-squares of *polynomials*. This can be proved by a simple Taylor expansion; for example by applying the following proposition to the identity  $t^{2k} P(z) = P(tz) = \sum_j H_j(tz)^2$  and observing that  $\left. \frac{d^k}{dt^k} H_j(tz) \right|_{t=0}$  is a degree  $k$  polynomial in  $z \in \mathbb{R}^{2n}$  (it is the  $k$ 'th term in the Taylor expansion of  $H_j$  at  $z$ ).

**Proposition 2.** *Assume that  $g_j : [0, \eta) \rightarrow \mathbb{R}$  are smooth functions<sup>5</sup> and that there exists  $a \in \mathbb{R}$  such that  $at^{2k} = \sum_j g_j(t)^2$  for all  $t \in [0, \eta)$ . Then  $a = \sum_j \left( \frac{g_j^{(k)}(0)}{k!} \right)^2$ .*

*Proof.* If we Taylor expand the  $g_j$  at 0 we get  $at^{2k} = \sum_j (g_j(0) + tg'_j(0) + \dots + t^k g_j^{(k)}(0)/k! + o(t^k))^2$ . By equating powers of  $t$  we get that  $g_j(0) = \dots = g_j^{(k-1)}(0) = 0$  and that  $a = \sum_j (g_j^{(k)}(0)/k!)^2$  as desired.  $\square$

<sup>5</sup> Smoothness at 0 is smoothness on the right.

The case where  $p$  is not necessarily homogeneous requires an additional argument. The following argument is inspired from [Sch18, Proposition 4.18]. Let  $2d = \deg p$ , and for any  $t \in \mathbb{R}$  consider the Hermitian polynomial  $p_t(z) = t^{2d} p(z/t)$ . This Hermitian polynomial is nonnegative and is also supported on  $A$ . Thus we know from property (\*) that there exist real coefficients  $a_j(t) \in \mathbb{R}^r$  s.t.

$$P_t(z) = \sum_j \left( a_j(t)^\top F(z) \right)^2 \quad \forall z \in \mathbb{R}^{2n} \tag{12}$$

where we let  $F(z) = (F_1(z), \dots, F_r(z))$ . The functions  $a_j(t)$  are defined by a semialgebraic relation and so can be taken to be semialgebraic. As such the  $a_j$  must be continuous on some  $(0, \eta)$  for  $\eta > 0$ . From the last part of the statement of Theorem 7 we also know that the  $a_j$  must be bounded on  $(0, \eta)$ . Thus, by Theorem 5 we know that the  $a_j$  can be extended by continuity to  $[0, \eta)$  and that for large enough  $m$ ,  $a_j(t^m)$  is smooth on  $[0, \eta')$  for some  $0 < \eta' < \eta$ . From (12) we get:

$$P_{t^m}(t^m z) = \sum_j (a_j(t^m)^\top F(t^m z))^2.$$

But note that  $P_{t^m}(t^m z) = t^{2dm} P(z)$ . Thus

$$t^{2dm} P(z) = \sum_j (a_j(t^m)^\top F(t^m z))^2.$$

If we let  $g_j(t) = a_j(t^m)^\top F(t^m z)$  we know that the  $g_j$  are smooth on  $[0, \eta')$ , since the  $F$  are smooth at the origin. We can apply the observation of Proposition 2 to get that

$$P(z) = \sum_j \left( \frac{g_j^{(dm)}(0)}{(dm)!} \right)^2.$$

But from the definition of  $g_j$ ,  $g_j^{(dm)}(0)$  is a polynomial of degree  $d$  in  $z$  (this can be seen e.g., by considering a Taylor expansion of  $F$  at the origin and of  $t \mapsto a_j(t^m)$  at  $t = 0$ ). This contradicts the assumption that  $p(z)$  is not a sum of squares of polynomials.

### 5. Proof of Theorem 1

**The case Sep(3, 3):** We prove that  $\mathcal{SEP}(3, 3)$  has no semidefinite representation. Define the Choi polynomial [Cho75] by

$$\begin{aligned} p(x, y) &= |x_1|^2 |y_1|^2 + |x_2|^2 |y_2|^2 + |x_3|^2 |y_3|^2 \\ &\quad - 2(\operatorname{Re}[x_1 \bar{x}_2 y_1 \bar{y}_2] + \operatorname{Re}[x_2 \bar{x}_3 y_2 \bar{y}_3] + \operatorname{Re}[x_1 \bar{x}_3 y_1 \bar{y}_3]) \\ &\quad + 2(|x_1|^2 |y_2|^2 + |x_2|^2 |y_3|^2 + |x_3|^2 |y_1|^2). \end{aligned}$$

It was shown in [Cho75] (see also [Cho80, Appendix B]) that  $p(x, y) \geq 0$  for all  $(x, y) \in \mathbb{C}^3 \times \mathbb{C}^3$ , and yet  $p(x, y)$  is not a sum of squares. In fact the *real* polynomial  $p(x, y)$  when  $(x, y) \in \mathbb{R}^3 \times \mathbb{R}^3$  is not a sum of squares. It follows, by a simple homogenization

argument, that the Hermitian polynomial  $\hat{p}(x_1, x_2, y_1, y_2) = p(x_1, x_2, 1, y_1, y_2, 1)$  is not a sum of squares. Note that the support of  $\hat{p}$  satisfies

$$\text{supp } \hat{p} \subset \hat{A} = \left\{ (\alpha, \beta, \gamma, \delta) \in (\mathbb{N}^2 \times \mathbb{N}^2) \times (\mathbb{N}^2 \times \mathbb{N}^2) : |\alpha| \leq 1, |\beta| \leq 1, |\gamma| \leq 1, |\delta| \leq 1 \right\}.$$

Since  $\hat{A}$  is downward closed it follows from Theorem 2 that

$$\begin{aligned} \mathcal{C}_{\hat{A}} &= \mathbf{cl\ conv} \left\{ \mathbf{m}_{\hat{A}}(x, y) : (x, y) \in \mathbb{C}^2 \times \mathbb{C}^2 \right\} \\ &= \mathbf{cl\ conv} \left\{ [x^\alpha y^\beta \bar{x}^\gamma \bar{y}^\delta]_{|\alpha| \leq 1, |\beta| \leq 1, |\gamma| \leq 1, |\delta| \leq 1} : (x, y) \in \mathbb{C}^2 \times \mathbb{C}^2 \right\} \end{aligned} \tag{13}$$

does not have a semidefinite representation. To conclude that  $\mathcal{SEP}(3, 3)$  has no semidefinite representation, it remains to note that  $\mathcal{C}_{\hat{A}}$  is a hyperplane section of  $\mathcal{SEP}(3, 3)$ . Indeed, first recall that  $\mathcal{SEP}(3, 3)$  can be written as

$$\mathcal{SEP}(3, 3) = \mathbf{cl\ conv} \left\{ \mathbf{m}_A(x, y) : (x, y) \in \mathbb{C}^3 \times \mathbb{C}^3 \right\}$$

where

$$A = \left\{ (\alpha, \beta, \gamma, \delta) \in (\mathbb{N}^3 \times \mathbb{N}^3) \times (\mathbb{N}^3 \times \mathbb{N}^3) : |\alpha| = 1, |\beta| = 1, |\gamma| = 1, |\delta| = 1 \right\}.$$

It is easy to see that there is a one-to-one correspondence between  $\hat{A}$  and  $A$ . In terms of the monomial map  $\mathbf{m}$  this simply means that  $\mathbf{m}_A$  is the homogenization of  $\mathbf{m}_{\hat{A}}$ . For example under an appropriate ordering of the monomials we have  $\mathbf{m}_A(x_1, x_2, x_3, y_1, y_2, y_3) = |x_3|^2 |y_3|^2 \mathbf{m}_{\hat{A}}\left(\frac{x}{x_3}, \frac{y}{y_3}\right)$  where we let  $x = (x_1, x_2)$  and  $y = (y_1, y_2)$ . It thus follows that  $\mathcal{SEP}(3, 3)$  can be written as

$$\mathcal{SEP}(3, 3) = \mathbf{cl\ conv} \left\{ |x_3|^2 |y_3|^2 \mathbf{m}_{\hat{A}}\left(\frac{x}{x_3}, \frac{y}{y_3}\right) : (x, y) \in \mathbb{C}^3 \times \mathbb{C}^3 \right\}.$$

It can then be readily verified that  $\mathcal{C}_{\hat{A}}$  is a hyperplane section of  $\mathcal{SEP}(3, 3)$  where the appropriate coordinate (corresponding to the monomial  $|x_3|^2 |y_3|^2$ ) is set to 1.

**The case Sep(4, 2):** Following the same approach as above, we need to exhibit a Hermitian polynomial  $\hat{p}(x_1, x_2, x_3, y)$  supported on

$$\hat{A} = \left\{ (\alpha, \beta, \gamma, \delta) \in (\mathbb{N}^3 \times \mathbb{N}) \times (\mathbb{N}^3 \times \mathbb{N}) : |\alpha| \leq 1, |\beta| \leq 1, |\gamma| \leq 1, |\delta| \leq 1 \right\} \tag{14}$$

that is nonnegative but not a sum-of-squares. Since  $\text{Sep}(4, 2) \neq \text{PPT}(4, 2)$  we know that there exists a Hermitian *homogeneous* polynomial  $p(x, y)$  on  $(x, y) \in \mathbb{C}^4 \times \mathbb{C}^2$  of the form

$$p(x, y) = \sum_{ijkl} p_{ijkl} x_i \bar{x}_j y_k \bar{y}_l \quad (x \in \mathbb{C}^4, y \in \mathbb{C}^2)$$

that is nonnegative but not a sum of squares. Note that such a  $p$  satisfies  $p(\lambda x, \mu y) = |\lambda|^2 |\mu|^2 p(x, y)$  for any  $(\lambda, \mu) \in \mathbb{C}^2$ . To get the desired polynomial  $\hat{p}$  it would suffice to dehomogenize the polynomial  $p$  by setting one of the  $x$  variables to 1, and one of the  $y$  variables to 1. It turns out, however, that one cannot guarantee in general that this dehomogenized polynomial is not a sum of squares. (We give an explicit example in Appendix A.) The reason we could dehomogenize the Choi polynomial in the (3, 3)

case was that the Choi polynomial is not a sum of squares when the variables are *real*. One cannot expect this to be true for our polynomial in (4,2) variables as it is known that any biquadratic *real* polynomial in  $(n, 2)$  variables *is* a sum of squares [Cal73]. Nevertheless we show in Appendix A that by choosing an appropriate polynomial  $p$ , and an appropriate dehomogenization we can get a polynomial  $\hat{p}(x, y)$  supported on  $\hat{A}$  of Eq. (14) that is not a sum-of-squares. This implies that  $\mathcal{C}_{\hat{A}}$  is not semidefinite representable. Using a similar argument as for the (3, 3) case we get that  $\mathcal{SEP}(4, 2)$  is not semidefinite representable.

*Acknowledgements.* I would like to thank Omar Fawzi for his encouragements and for helpful comments on the paper. I would also like to thank Claus Scheiderer for useful discussions and exchanges related to the material of this paper, and James Saunderson for comments that helped improved the exposition.

**Open Access** This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article’s Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article’s Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

**Publisher’s Note** Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

### A. The Case Sep(4, 2)

In this section we exhibit a nonnegative Hermitian polynomial  $\hat{p}(x_1, x_2, x_3, y)$  supported on  $\hat{A}$ , defined in Eq. (14), that is not a sum of squares.

Consider the following map  $\Phi : M_2 \rightarrow M_4$  studied in [HK16]:

$$\Phi \left( \begin{bmatrix} x & y \\ z & w \end{bmatrix} \right) = \begin{bmatrix} 3w + 4x - 2y - 2z & 2z - 2x & 0 & 0 \\ 2y - 2x & 2x & z & 0 \\ 0 & y & 2w & -w - 2z \\ 0 & 0 & -w - 2y & 2w + 4x \end{bmatrix}.$$

It is shown in [HK16] that the map  $\Phi$  is positive but not decomposable. We associate to  $\Phi$  the Hermitian polynomial

$$\mathbf{W}(x, y) = x^\dagger \Phi(yy^\dagger)x \quad x \in \mathbb{C}^4, y \in \mathbb{C}^2.$$

Then we know from Proposition 1 that  $\mathbf{W}$  is positive but not a sum of squares. The purpose of this section is to prove the following:

**Proposition 3** *The (nonhomogeneous) Hermitian polynomial  $\mathbf{W}(1, x_2, x_3, x_4, 1, y_2)$  is not a sum of squares.*

The proof of this proposition involves some computations, and we use the specific properties of  $\mathbf{W}$  (its zeros) which have been studied in [HK16]. We note that there are other dehomogenizations of  $\mathbf{W}$  that *are* sums of squares. For example, we show later that  $\mathbf{W}(x_1, x_2, -6, x_4, 1, y_2)$  is a sum of squares.

*Proof of Proposition 3.* To lighten the notation we let  $y_2 = \alpha$ . In [HK16], the zeros of the polynomial  $\mathbf{W}$  were identified. Namely it was shown that

$$\mathbf{W}(x_1(\alpha), x_2(\alpha), x_3(\alpha), x_4(\alpha), 1, \alpha) = 0 \quad \forall \alpha \in \mathbb{C} \tag{15}$$

where

$$x(\alpha) := \left( 2\alpha(1 - \alpha), \alpha \left[ 4 - 2(\alpha + \bar{\alpha}) + 3|\alpha|^2 \right], -4 - 2|\alpha|^2, -\bar{\alpha}(2 + \alpha) \right) \in \mathbb{C}^4.$$

Let  $p(x_2, x_3, x_4, \alpha) = \mathbf{W}(1, x_2, x_3, x_4, 1, \alpha)$ . The explicit formula of  $p$  is

$$\begin{aligned} p(x_2, x_3, x_4, \alpha) &= 2|\alpha|^2|x_3|^2 + 2|\alpha|^2|x_4|^2 - x_3\bar{x}_4|\alpha|^2 - \bar{x}_3x_4|\alpha|^2 \\ &\quad + \bar{x}_2x_3\alpha + x_2\bar{x}_3\bar{\alpha} - 2\bar{x}_3x_4\alpha - 2x_3\bar{x}_4\bar{\alpha} \\ &\quad + 3|\alpha|^2 + 2|x_2|^2 + 4|x_4|^2 + 2x_2\alpha + 2\bar{x}_2\bar{\alpha} \\ &\quad - 2x_2 - 2\bar{x}_2 - 2\alpha - 2\bar{\alpha} + 4. \end{aligned}$$

Assume that  $p = \sum_i g_i^2$  where  $g_i$  are Hermitian polynomials in  $x_2, x_3, x_4, \alpha$ . Since  $p$  has no terms  $|x_3|^2$  we see that the  $g_i$  cannot contain monomials  $x_3$  or  $\bar{x}_3$ . Similarly  $p$  does not have a term  $|\alpha|^2|x_2|^2$  and so the  $g_i$  cannot contain monomials  $\alpha x_2, \bar{\alpha}x_2, \alpha\bar{x}_2$  or  $\bar{\alpha}\bar{x}_2$ . It follows that each  $g_i$  must be a linear combination of the monomials

$$1, \alpha, x_2, x_4, \alpha x_3, \alpha x_4, \bar{\alpha}x_3, \bar{\alpha}x_4$$

and their conjugates. In other words, each  $g_i$  is of the form:

$$\begin{aligned} g_i(x_2, x_3, x_4, \alpha) &= a_i + b_i\alpha + c_i x_2 + d_i x_4 + e_i \alpha x_3 + f_i \alpha x_4 + g_i \bar{\alpha} x_3 + h_i \bar{\alpha} x_4 \\ &\quad + \bar{b}_i \bar{\alpha} + \bar{c}_i \bar{x}_2 + \bar{d}_i \bar{x}_4 + \bar{e}_i \bar{\alpha} \bar{x}_3 + \bar{f}_i \bar{\alpha} \bar{x}_4 + \bar{g}_i \bar{\alpha} \bar{x}_3 + \bar{h}_i \bar{\alpha} \bar{x}_4 \end{aligned} \tag{16}$$

where  $a_i, b_i, \dots, h_i \in \mathbb{C}$ . We will now use the information about the zeros of  $\mathbf{W}$  (and thus of  $p$ ) to deduce relations about these coefficients and reach a contradiction. Since  $\mathbf{W}$  is bihomogeneous in the first set of variables, we have (dividing by  $|x_1(\alpha)|^2$ ) from (15) that

$$p \left( \frac{x_2(\alpha)}{x_1(\alpha)}, \frac{x_3(\alpha)}{x_1(\alpha)}, \frac{x_4(\alpha)}{x_1(\alpha)}, \alpha \right) = 0, \quad \forall \alpha \in \mathbb{C} \setminus \{0, 1\}.$$

Since  $p = \sum_i g_i^2$  we get that for all  $i$ ,

$$g_i \left( \frac{x_2(\alpha)}{x_1(\alpha)}, \frac{x_3(\alpha)}{x_1(\alpha)}, \frac{x_4(\alpha)}{x_1(\alpha)}, \alpha \right) = 0, \quad \forall \alpha \in \mathbb{C} \setminus \{0, 1\}. \tag{17}$$

We can clear denominators in (17) by multiplying the expression by  $|x_1(\alpha)|^2$ . As a result we get that

$$|x_1(\alpha)|^2 g_i \left( \frac{x_2(\alpha)}{x_1(\alpha)}, \frac{x_3(\alpha)}{x_1(\alpha)}, \frac{x_4(\alpha)}{x_1(\alpha)}, \alpha \right) = 0, \quad \forall \alpha \in \mathbb{C}. \tag{18}$$

The left-hand side of (18) is a Hermitian polynomial in  $\alpha$  that is identically zero. Hence all its coefficients must be equal to 0. This allows us to derive conditions on the coefficients of  $g_i$  in (16). More precisely:

- The coefficient of  $\alpha^4$  is  $4\bar{h}_i$ . Setting  $4\bar{h}_i$  to zero yields  $h_i = 0$ .

- The coefficient of  $\alpha^4 \bar{\alpha}$  is  $4\bar{g}_i + 2\bar{h}_i$ . Setting to zero we get  $g_i = 0$ .
- The coefficient of  $\alpha^2$  is  $-4d_i - 8\bar{g}_i$ . Setting to zero we get  $d_i = 0$ .

This gives a contradiction: indeed the coefficient of  $|x_4|^2$  in  $p$  is  $4 > 0$  and yet  $\sum_i |d_i|^2 = 0$ . □

We conclude this appendix by proving, as promised, that there is another dehomogenization of  $\mathbf{W}$  that is a sum of squares. Let:

$$q(x_1, x_2, x_4, \alpha) = \mathbf{W}(x_1, x_2, -6, x_4, 1, \alpha).$$

Let

$$A = \begin{pmatrix} 36 & 0 & -3 & 0 & 0 & 0 \\ 0 & 2 & -1 & 0 & -1 & 0 \\ -3 & -1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & -1 & 1 & 0 & \frac{3}{2} & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 & 0 & 6 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 6 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 3 & -1 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

One can verify that  $A - B \succeq 0$  and  $A + B \succeq 0$ , i.e., that  $\begin{bmatrix} A & B \\ B & A \end{bmatrix} \succeq 0$ . Let  $m(x_1, x_2, x_4, \alpha) = (\alpha, x_1, x_2, x_4, \bar{\alpha}x_1, \bar{\alpha}x_4)$ . Then one can check that we have the following sum of squares decomposition of  $q$ :

$$q(x_1, x_2, x_4, \alpha) = \begin{bmatrix} m(x, \alpha) \\ \bar{m}(x, \alpha) \end{bmatrix}^\dagger \begin{bmatrix} A & B \\ B & A \end{bmatrix} \begin{bmatrix} m(x, \alpha) \\ \bar{m}(x, \alpha) \end{bmatrix}.$$

**References**

[AS17a] Aubrun, G., Szarek, S.: Alice and Bob Meet Banach: The Interface of Asymptotic Geometric Analysis and Quantum Information Theory, vol. 223. American Mathematical Society, New York (2017)

[AS17b] Aubrun, G., Szarek, S.: Dvoretzky’s theorem and the complexity of entanglement detection. *Discrete Anal.* (2017)

[BPR06] Basu, S., Pollack, R., Roy, M.F.: Algorithms in Real Algebraic Geometry. Springer, New York (2006)

[Cal73] Calderón, A.P.: A note on biquadratic forms. *Linear Algebra Appl.* **7**(2), 175–177 (1973)

[Cho75] Choi, M.D.: Positive semidefinite biquadratic forms. *Linear Algebra Appl.* **12**(2), 95–100 (1975)

[Cho80] Choi, M.D.: Some assorted inequalities for positive linear maps on  $C^*$ -algebras. *J. Oper. Theory* 271–285 (1980)

[DP09] D’Angelo, J.P., Putinar, M.: Polynomial optimization on odd-dimensional spheres. In: *Emerging Applications of Algebraic Geometry*, pp. 1–15. Springer (2009)

[DPS04] Doherty, A.C., Parrilo, P.A., Spedalieri, F.M.: Complete family of separability criteria. *Phys. Rev. A* **69**(2), 022308 (2004)

[Faw16] Fawzi, H.: Power and limitations of convex formulations via linear and semidefinite programming lifts. PhD thesis, Massachusetts Institute of Technology (2016)

[FF20] Fang, K., Fawzi, H.: The sum-of-squares hierarchy on the sphere and applications in quantum information theory. *Math. Program.* (2020)

[GPT13] Gouveia, J., Parrilo, P.A., Thomas, R.R.: Lifts of convex sets and cone factorizations. *Math. Oper. Res.* **38**(2), 248–264 (2013)

[HHH96] Horodecki, M., Horodecki, P., Horodecki, R.: Separability of mixed states: necessary and sufficient conditions. *Phys. Lett. A* **223**(1), 1–8 (1996)

[HK16] Ha, K.C., Kye, S.H.: Construction of exposed indecomposable positive linear maps between matrix algebras. *Linear Multilinear Algebra* **64**(11), 2188–2198 (2016)

[HN09] Helton, J.W., Nie, J.: Sufficient and necessary conditions for semidefinite representability of convex hulls and sets. *SIAM J. Optim.* **20**(2), 759–791 (2009)

- [HP16] Hà, H.V., Pham, T.S.: *Genericity in Polynomial Optimization*, vol. 3. World Scientific, Singapore (2016)
- [Nem06] Nemirovski, A.: *Advances in convex optimization: conic programming*. In: *Proceedings of the International Congress of Mathematicians (ICM 2006)* (2006)
- [NPS10] Netzer, T., Plaumann, D., Schweighofer, M.: Exposed faces of semidefinitely representable sets. *SIAM J. Optim.* **20**(4), 1944–1955 (2010)
- [Per96] Peres, A.: Separability criterion for density matrices. *Phys. Rev. Lett.* **77**(8), 1413 (1996)
- [RG95] Ramana, M., Goldman, A.J.: Some geometric results in semidefinite programming. *J. Glob. Optim.* **7**(1), 33–50 (1995)
- [Sch18] Scheiderer, C.: Spectrahedral shadows. *SIAM J. Appl. Algebra Geom.* **2**(1), 26–44 (2018)
- [Sko16] Skowronek, L.: There is no direct generalization of positive partial transpose criterion to the three-by-three case. *J. Math. Phys.* **57**(11), 112201 (2016)
- [Wor76] Stanislaw, L.W.: Positive maps of low dimensional matrix algebras. *Rep. Math. Phys.* **10**(2), 165–183 (1976)

Communicated by H-T. Yau