Separability of diagonal symmetric states: a quadratic conic optimization problem

Jordi Tura[1 2], Albert Aloy[1], Rubén Quesada[3], Maciej Lewenstein[1 4], and Anna Sanpera[3 4]

[1]ICFO - Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels (Barcelona), Spain

[2]Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, 85748 Garching, Germany

[3]Departament de Física, Universitat Autònoma de Barcelona, E-08193 Bellaterra, Spain

[4]ICREA, Pg. Lluís Companys 23, E-08010 Barcelona, Spain

December 29, 2017

We study the separability problem in mixtures of Dicke states *i.e.*, the separability of the so-called Diagonal Symmetric (DS) states. First, we show that separability in the case of DS in $\mathbb{C}^d \otimes \mathbb{C}^d$ (symmetric qudits) can be reformulated as a quadratic conic optimization problem. This connection allows us to exchange concepts and ideas between quantum information and this field of mathematics. For instance, copositive matrices can be understood as indecomposable entanglement witnesses for DS states. As a consequence, we show that positivity of the partial transposition (PPT) is sufficient and necessary for separability of DS states for $d \leq 4$. Furthermore, for $d \geq 5$, we provide analytic examples of PPT-entangled states. Second, we develop new sufficient separability conditions beyond the PPT criterion for bipartite DS states. Finally, we focus on N-partite DS qubits, where PPT is known to be necessary and sufficient for separability. In this case, we present a family of almost DS states that are PPT with respect to each partition but nevertheless entangled.

1 Introduction

Entanglement [1] is one of the most striking features of quantum physics, departing entirely from any classical analogy. Furthermore, entanglement is a key resource for quantum information processing tasks, such as quantum cryptography [2] or metrology [3]. Importantly, entanglement is a necessary resource to enable the existence of Bell correlations [4, 5], which are the resource device-independent quantum information processing is built upon [6]. Despite its both fundamental and applied interest, the so-called separability problem (*i.e.*, deciding whether a quantum state is entangled or not, given its description) remains open except for very specific cases. Although this problem has been shown to be, in the general case, NP-hard [7], it remains unclear whether this is also the case for physical systems of interest, where symmetries appear in a natural way.

To tackle the separability problem, simple tests have been put forward, which give a partial characterization of entanglement. The most celebrated entanglement detection criterion is the so-called positivity under partial transposition (PPT) criterion [8]. It states that every state that is not entangled must satisfy the PPT criterion. Therefore, states that break the PPT criterion are entangled. Unfortunately, the converse is true only in very low-dimensional systems [9], such as two qubit [10] or qubit-qutrit systems [11]. Examples of entangled states satisfying the PPT criterion have been found for strictly larger-dimensional systems [12].

Jordi Tura: jordi.tura@mpq.mpg.de

Symmetries are ubiquitous in Nature and they play a fundamental role in finding an efficient description of physical systems. The so-called symmetric states constitute an important class of quantum systems to describe systems of indistinguishable particles [13]. Symmetric states can be mapped to spin systems that are invariant under the exchange of particles and, moreover, they are spanned solely by the largest-spin subspace in the Schur-Weyl duality representation [14]. The Dicke states [15] provide a convenient basis to represent symmetric states. Moreover, Dicke states are also experimentally available [16–18] and they also appear naturally as ground states of physically relevant Hamiltonians, such as the isotropic Lipkin-Meshkov-Glick model [19]. Much theoretical study has been devoted to the characterization of entanglement in qubit symmetric states: 3-qubit symmetric states are separable if, and only if, they satisfy the PPT criterion [13], but this is no longer the case already for $N \geq 4$ [20, 21]. Despite diverse separability criteria exist for symmetric states (see e.g. [22]), the separability problem remains still open.

Mixtures of Dicke states are symmetric states that are diagonal in the Dicke basis. These constitute an important class of quantum states which naturally arise e.g. in dissipative systems such as photonic or plasmonic one-dimensional waveguides [23]. Mixtures of Dicke states form a small subclass of the symmetric states. They are the so-called Diagonal Symmetric (DS) states. In this context, the separability problem has also gained interest. For instance, the best separable approximation (BSA, [24]) has been found analytically for DS states for N-qubits [25]. In [26], it was conjectured that N-qubit DS states are separable if, and only if, they satisfy the PPT criterion with respect to every bipartition. The conjecture was proven by N. Yu in [27] where, moreover, he observed that PPT is a sufficient and necessary condition for bipartite DS states of qudits with dimension 3 and 4, but becomes NP-hard for larger dimensions. Within the N-qubit DS set it has been shown in [28] that there is a family of states that violate the weak Peres conjecture [29]: those states are PPT-bound entangled with respect to one partition, but they violate a family of permutationally invariant two-body Bell inequalities [30–32].

In experiments, PPT-entangled states have also been recently observed. In the multipartite case, the Smolin state has been prepared with four photons, using the polarization degree of freedom for the qubit encoding [33, 34]. Very recently, although bound entanglement is the hardest to detect [35], the Leiden-Vienna collaboration has reported the observation of bound entanglement in the bipartite case with two twisted photons, combining ideas of complementarity [36] and Mutually Unbiased Bases (MUBs) [37].

Here, we independently recover the results of N. Yu [27] by reformulating the problem in terms of optimization in the cone of completely-positive[1] matrices. First, we revisit the problem of determining separability of two DS qudits in arbitrary dimensions. We show that it can be reformulated in terms of a quadratic conic optimization problem [38]. In particular, we show that separability in DS states is equivalent to the membership problem in the set of completely-positive matrices. The equivalence between these two problems allows us to import/export ideas between entanglement theory and non-convex quadratic optimization[2]. Second, we provide examples of entangled PPTDS states and entanglement witnesses detecting them. Third, we give further characterization criteria for separability in DS states in terms of the best diagonal dominant decomposition. Finally, we present a family of N-qubit almost-DS states that are PPT with respect to each bipartition, but nevertheless entangled. The word *almost* here means that by adding an arbitrarily small off-diagonal term (GHZ coherence) to a family of separable DS N-qubits, the state becomes PPT-entangled.

[1] Throughout this paper, the term *completely-positive* corresponds to the definition given in Def. 3.4 and it is not to be confounded with the concept of a completely positive map that arises typically in a quantum information context.

[2] Quadratic conic optimization problems appear naturally in many situations (see [38] and references therein). These include economic modelling [39], block designs [40], maximin efficiency-robust tests [41], even Markovian models of DNA evolution [42]. Recently, they have found their application in data mining and clustering [43], as well as in dynamical systems and control [44, 45].

The paper is organized as follows. In Section 2 we establish the notation and the basic definitions that we are going to use in the next sections. In Section 3 we discuss the separability problem for bipartite DS states of arbitrary dimension, with particular emphasis in their connection to non-convex quadratic optimization problems. In Section 4 we provide sufficient criteria to certify either separability or entanglement. In Section 5 we present a class of PPT-entangled multipartite qubit almost-diagonal symmetric states. In Section 6 we conclude and discuss further research directions. Finally, in the Appendix we present some proofs, examples and counterexamples that complement the results discussed in the text.

2 Preliminaries

In this section we set the notation and define the basic concepts that we are going to use throughout the paper.

2.1 The separability problem

Definition 2.1. *Consider a bipartite quantum state ρ acting on $\mathbb{C}^d \otimes \mathbb{C}^{d'}$. The state ρ is positive semi-definite ($\rho \succeq 0$) and normalized ($\mathrm{Tr}\rho = 1$). A state ρ is separable if it can be written as*

$$\rho = \sum_i p_i \rho_i^A \otimes \rho_i^B, \tag{1}$$

where p_i form a convex combination ($p_i \geq 0$ and $\sum_i p_i = 1$) and ρ_i^A (ρ_i^B) are quantum states acting on Alice's (Bob's) subsystem; i.e., they are positive semidefinite operators of trace one. If a decomposition of ρ of the form of Eq. (1) does not exist, then ρ is entangled.

The separability problem; i.e., deciding whether a quantum state ρ admits a decomposition of the form of Eq. (1) is, in general, an NP-hard problem [7]. However, there exist simple tests that provide sufficient conditions to certify that ρ is entangled [1]. One of the most renowned separability criteria is the positivity under partial transposition (PPT) criterion [8]. It states that, if ρ can be decomposed into the form of Eq. (1), then the state $(\mathbb{1} \otimes T)[\rho]$ must be positive semi-definite, where T is the transposition with respect to the canonical basis of $\mathbb{C}^{d'}$. Such state is denoted ρ^{T_B}, the partial transposition of ρ on Bob's side. Because $(\rho^{T_B})^T = \rho^{T_A}$, the PPT criterion does not depend on which side of the bipartite system the transposition operation is applied on. Breaking PPT criterion is a necessary and sufficient condition for entanglement only in the two qubit [10] and qubit-qutrit [11] cases, and there exist counterexamples for states of strictly higher physical dimension [12].

In the multipartite case, the definition of separability given in Eq. (1) naturally generalizes to N subsystems.

Definition 2.2. *A quantum state ρ acting on $\mathbb{C}^{d_1} \otimes \cdots \otimes \mathbb{C}^{d_N}$ is fully separable if it can be written as*

$$\rho = \sum_i p_i \rho_i^{(A_1)} \otimes \cdots \otimes \rho_i^{(A_N)}, \tag{2}$$

where $\rho_i^{(A_k)}$ are quantum states acting on the k-th subsystem and p_i form a convex combination.

Therefore, the PPT criterion also generalizes to $2^{\lfloor N/2 \rfloor}$ criteria, where $\lfloor \cdot \rfloor$ is the floor function, depending on which subsystems one chooses to transpose.

2.1.1 Entanglement witnesses

Let us denote by $\mathcal{D}_{\mathrm{sep}}$ the set of separable sates (cf. Eqs. (1), (2)). This set is closed and convex. Therefore it admits a dual description in terms of its dual cone, which we denote

$$\mathcal{P} = \{W = W^\dagger \text{ s. t. } \langle W, \rho \rangle \geq 0 \ \forall \rho \in \mathcal{D}_{\mathrm{sep}}\},$$

where the usual Hilbert-Schmidt scalar product $\langle W, \rho\rangle = \mathrm{Tr}(W^\dagger \rho)$ is taken. The elements of $\mathcal{P}$ can be thus viewed as half-spaces containing $\mathcal{D}_{\mathrm{sep}}$. Of course, not every operator in $\mathcal{P}$ is useful to detect entangled states. In order to be non-trivial, one requires that W has at least one negative eigenvalue. Such operators are called *entanglement witnesses* (EW) [46] and they form a non-convex set, denoted $\mathcal{W} = \{W \in \mathcal{P} \text{ s. t. } W \not\succeq 0\}$. A state ρ is then separable if, and only if, $\mathrm{Tr}(W\rho) \geq 0$ for all $W \in \mathcal{W}$.

Among EWs, it is worth to make a distinction that relates them to the PPT criterion: decomposable and indecomposable EWs.

Definition 2.3. *Decomposable EWs (DEWs) in a bipartite quantum system are those $W \in \mathcal{W}$ of the form*

$$W = P + Q^{T_B}, \tag{3}$$

with $P \succeq 0$ and $Q \succeq 0$. Indecomposable EWs (IEWs) are those EWs that are not of the form of Eq. (3).

Although DEWs are easier to characterize [47], they do not detect PPT-entangled states, because

$$\mathrm{Tr}(W\rho) = \mathrm{Tr}(P\rho) + \mathrm{Tr}(Q^{T_B}\rho) = \mathrm{Tr}(P\rho) + \mathrm{Tr}(Q\rho^{T_B}) \geq 0. \tag{4}$$

In Section 4.1 we construct EWs which detect entangled PPTDS states, therefore they correspond to indecomposable witnesses.

3 Separability in diagonal symmetric states acting on $\mathbb{C}^d \otimes \mathbb{C}^d$.

In this section, we characterize the bipartite diagonal symmetric two-qudit states in terms of the separability and the PPT properties. We establish an equivalence between: (i) separability and the PPT property in DS states and (ii) quadratic conic optimization problems and their relaxations, respectively.

We first introduce the Dicke basis in its full generality and then we move to the two particular cases of interest to this paper: the case of N-qubits and the case of 2-qudits. One can think of the space spanned by the Dicke states as the linear subspace of $(\mathbb{C}^d)^{\otimes N}$ containing all permutationally invariant states.

Definition 3.1. *Consider a multipartite Hilbert space $(\mathbb{C}^d)^{\otimes N}$ of N qudits. The Dicke basis in that space consists of all vectors which are equal superpositions of k_0 qudits in the state $|0\rangle$, k_1 qudits in the state $|1\rangle$, etc., where the multiindex variable $\mathbf{k} = (k_0, \ldots, k_{d-1})$ forms a partition of N; i.e., $k_i \geq 0$ and $\sum_{i=0}^{d-1} k_i = N$. They can be written as*

$$|D_{\mathbf{k}}\rangle \propto \sum_{\sigma \in \mathfrak{S}_N} \sigma(|0\rangle^{\otimes k_0}|1\rangle^{\otimes k_1} \cdots |d-1\rangle^{\otimes k_{d-1}}), \tag{5}$$

where σ runs over all permutations of N elements.

The Dicke state has $\binom{N}{\mathbf{k}}$ different elements, where the quantity follows from the multinomial combinatorial quantity

$$\binom{N}{\mathbf{k}} = \frac{N!}{k_0!k_1!\cdots k_{d-1}!}. \tag{6}$$

Finally, recall that there are as many Dicke states as partitions of N into d (possibly empty) subsets; therefore, the dimension of the subspace of $(\mathbb{C}^d)^{\otimes N}$ is given by

$$\dim[\{|D_{\mathbf{k}}\rangle : \mathbf{k} \vdash N\}] = \binom{N+d-1}{d-1}, \tag{7}$$

where $\vdash$ denotes *partition of*.

In this paper, we are particularly interested in the case of N-qubits and 2-qudits:

- $d = 2$. For N-qubit states we shall use the notation $|D_{\mathbf{k}}\rangle \equiv |D_k^N\rangle$, where $k = k_1$ denotes the number of qubits in the excited ($|1\rangle$) state. Mixtures of Dicke states correspond to

$$\rho = \sum_{k=0}^{N} p_k |D_k^N\rangle\langle D_k^N|. \tag{8}$$

- $N = 2$. For bipartite d-level systems, we are going to denote the Dicke states by $|D_{\mathbf{k}}\rangle \equiv |D_{ij}\rangle$, where i and j are the indices (possibly repeated) of the non-zero k_i and k_j. Since the terminology *Dicke states* is often reserved for the multipartite case, we call $|D_{ij}\rangle$ simply *symmetric states*.

In the bipartite case (Sections 3 and 4), we focus on diagonal symmetric states, given by Def. 3.2:

Definition 3.2. *Let ρ be a state acting on a bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B = \mathbb{C}^d \otimes \mathbb{C}^d$. The state ρ is said to be* diagonal symmetric *(DS) if, and only if, ρ can be written in the form*

$$\rho = \sum_{0 \le i \le j < d} p_{ij} |D_{ij}\rangle\langle D_{ij}|, \tag{9}$$

where $p_{ij} \geq 0$, $\sum_{ij} p_{ij} = 1$, $|D_{ii}\rangle := |ii\rangle$ and $|D_{ij}\rangle = (|ij\rangle + |ji\rangle)/\sqrt{2}$.

In the computational basis, a DS ρ is a $d^2 \times d^2$ matrix that is highly sparse. Therefore, it will be useful to associate a $d \times d$ matrix to ρ that captures all its relevant information. We define the M-matrix of ρ to be

Definition 3.3. *To every DS ρ acting on $\mathbb{C}^d \otimes \mathbb{C}^d$, there is an associated $d \times d$ matrix $M(\rho)$, with non-negative entries*

$$M(\rho) := \begin{pmatrix} p_{00} & p_{01}/2 & \cdots & p_{0,d-1}/2 \\ p_{01}/2 & p_{11} & \cdots & p_{1,d-1}/2 \\ \vdots & \vdots & \ddots & \vdots \\ p_{0,d-1}/2 & p_{1,d-1}/2 & \cdots & p_{d-1,d-1} \end{pmatrix}, \tag{10}$$

which arises from the partially transposed matrix ρ^{T_B}.

Notice that, while a DS state ρ is always diagonal in the Dicke basis, its partial transposition (which is defined with respect to the computational basis) scrambles its elements. Then ρ^{T_B} is block-diagonal in the Dicke basis and its blocks are 1×1 elements corresponding to p_{ij} with $i < j$, and $M(\rho)$. One can see the effect of the partial transposition operation on a DS state by inspecting the action of T_B onto the elements $|D_{ij}\rangle\langle D_{ij}|$ that compose Eq. (9):

- If $i = j$, then $(|D_{ii}\rangle\langle D_{ii}|)^{T_B} = |D_{ii}\rangle\langle D_{ii}|$, because $|D_{ii}\rangle = |ii\rangle$.
- If $i \neq j$, the action of the partial transposition is best seen by expanding $|D_{ij}\rangle$ onto the computational basis: $(|D_{ij}\rangle\langle D_{ij}|) = \frac{1}{2}(|ij\rangle\langle ij| + |ij\rangle\langle ji| + |ji\rangle\langle ij| + |ji\rangle\langle ji|)$. Therefore, two of the terms are left invariant and the remaining two are to be mapped as $(|ij\rangle\langle ji| + |ji\rangle\langle ij|)^{T_B} = |ii\rangle\langle jj| + |jj\rangle\langle ii|$.

Thus, $M(\rho)$ is the submatrix corresponding to the elements indexed by $|ii\rangle\langle jj|$ for $0 \leq i, j < d$ of ρ^{T_B}. Because there is no mixing between other rows or columns, we have that ρ^{T_B} decomposes as the direct sum

$$\rho^{T_B} = M(\rho) \bigoplus_{0 \le i \ne j < d} \left(\frac{p_{ij}}{2}\right). \tag{11}$$

Since $p_{ij} = p_{ji}$, we find that the 1×1 blocks appear all with multiplicity 2.

Therefore, each $M(\rho)$ with non-negative entries summing 1 is in one-to-one correspondence to a DS state ρ. In this section we characterize the separability properties of ρ in terms of equivalent properties of $M(\rho)$, which are naturally related to quadratic conic optimization.

In quadratic conic optimization, one is interested in characterizing the so-called completely positive (CP) matrices, which are defined as follows

Definition 3.4. *Let A be a $d \times d$ matrix. A is* completely positive *(CP) if, and only if, it admits a decomposition $A = B \cdot B^T$, where B is a $d \times k$ matrix, for some $k \geq 1$, such that $B_{ij} \geq 0$.*

Matrices which are CP form a proper[3] cone, which is denoted by $\mathcal{CP}_d$. Note that the sum of two CP matrices is a CP matrix and the multiplication of a CP matrix by a non-negative scalar is a CP matrix.

Given a non-convex optimization problem over the simplex, which is NP-hard in general, CP matrices translate the complexity of the problem by reformulating it as a linear problem in matrix variables over $\mathcal{CP}_d$. Therefore, they allow to shift all the difficulty of the original problem into the cone constraint. Precisely, every non-convex quadratic optimization problem over the simplex (LHS of Eq. (12)) has an equivalent CP formulation (RHS of Eq. (12)):

$$\max_{x_i \geq 0,\ \langle u|x\rangle = 1} \langle x|Q|x\rangle = \max_{X \in \mathcal{CP}_d,\ \langle u|X|u\rangle = 1} \mathrm{Tr}(XQ), \tag{12}$$

where $|u\rangle$ is the unnormalized vector of ones and Q is, without loss of generality[4], symmetric and positive semi-definite. Therefore, deciding membership in $\mathcal{CP}_d$ is NP-hard [38].

One can obtain, however, an upper bound on the optimization in Eq. (12) by observing that every CP matrix A is positive semi-definite, because it allows for a factorization $A = B \cdot B^T$. Moreover, it is also entry-wise non-negative: $A_{ij} \geq 0$. This motivates Definition 3.5:

Definition 3.5. *Let A be a $d \times d$ matrix. A is* doubly non-negative *(DNN) if, and only if, $A \succeq 0$ and $A_{ij} \geq 0$.*

We are now ready to introduce the equivalences between the separability problem in DS states and quadratic conic optimization. After producing our results, we learned that these equivalences were independently observed by Nengkun Yu in [27]. We nevertheless prove them in a different way.

Theorem 3.1. *Let ρ be a DS state acting on $\mathbb{C}^d \otimes \mathbb{C}^d$.*

$$\rho \text{ is separable} \iff M(\rho) \text{ is CP.} \tag{13}$$

We prove Theorem 3.1 in Appendix A.

By virtue of Theorem 3.1, we recover the result of [27]: Because it is NP-Hard to decide whether a matrix admits a CP decomposition [38], the separability problem in $\mathbb{C}^d \otimes \mathbb{C}^d$ DS states is NP-Hard.

We remark that the NP-hardness result that we obtain holds under polynomial-time Turing reductions[5], as opposed to poly-time many-one[6] reductions [48]. For instance, this is the case for Gurvits' initial reduction of the weak membership problem[7] in the set of separable states from the NP-complete problem PARTITION[8] [7]. In the case we present here, the reduction holds because the NP-hardness of deciding membership in the $\mathcal{CP}_d$ set follows via a Turing reduction, which is the result we use as our starting point. The part of the reduction that we provide here, however, is many-one.

[3] Closed, convex, pointed and full-dimensional.

[4] Q can be assumed to be symmetric because $\langle x|Q|x\rangle = (\langle x|Q|x\rangle)^T = \langle x|Q^T|x\rangle$. It can be assumed to be positive semi-definite because adding $\mathbb{1}$ to $(Q + Q^T)/2$ does not change the optimal $|x\rangle$; it only adds a bias to the maximum.

[5] Intuitively speaking, a Turing reduction describes how to solve problem A by running an algorithm for a second problem B, possibly multiple times.

[6] A many-one reduction is a special case of a Turing reduction, with the particularity that the algorithm for problem B can be called only one time, and its output is immediately returned as the output of problem A.

[7] Weak in the sense that it allows for error in points at a given Euclidean distance from the border of the set.

[8] The PARTITION problem is a decision problem corresponding to whether a given set of integer numbers can be partitioned into two sets of equal sum. This problem is efficiently solvable with a dynamic programming procedure [49], but becomes NP-hard when the magnitudes of the input integers become exponentially large with the input size.

We here briefly discuss the steps that would be required to make this result completely rigurous from a computer science point of view. One would need to embed the NP-hardness into the formalism of the weak membership problem [7, 50]. This requires, for instance, showing that the convex set of separable DS states has some desirable properties such as being well-bounded or p-centered. We refer the reader to [48] for the technical aspects of these definitions. On the other hand, the completely positive cone is known to be well-bounded and p-centered: in [51] it was proved that the weak membership problem in the completely positive cone is NP-hard. By using the one-to-one correspondence between DS states and CP matrices given by $M(\rho)$ in Def. 3.3, then the result is mapped onto the DS set[9].

Geometrically, the set of separable DS states is convex. Hence, it is fully characterized by its extremal elements (those that cannot be written as a non-trivial convex combination of other separable DS states). Identifying such elements is of great importance towards the characterization of the separability properties of DS states. For instance, in the set of all separable density matrices, the extremal ones are the rank-1 projectors onto product vectors. However, this property may be lost when restricting our search in a subspace: observe that the set of separable DS states states is obtained as the intersection of the subspace of DS states with the convex set of separable density matrices. Therefore, the set of extremal separable DS states states may contain states that are separable, but not extremal in the set of separable density matrices (see Fig. 1). Theorem 3.1 allows us to fully characterize extremality in the set of separable DS states in terms of extremal CP matrices, thus obtaining the following corollary:

Corollary 3.1. *The extremal separable DS states ρ fulfill*

$$p_{ij} = 2\sqrt{p_{ii}p_{jj}}, \qquad i < j. \tag{14}$$

Proof. – Since the extremal rays of the $\mathcal{CP}_d$ cone are the rank-1 matrices $\vec{b}\,\vec{b}^T$ where $b_i \geq 0$ [42], by normalizing and comparing to Eq. (10) we obtain Eq. (14).

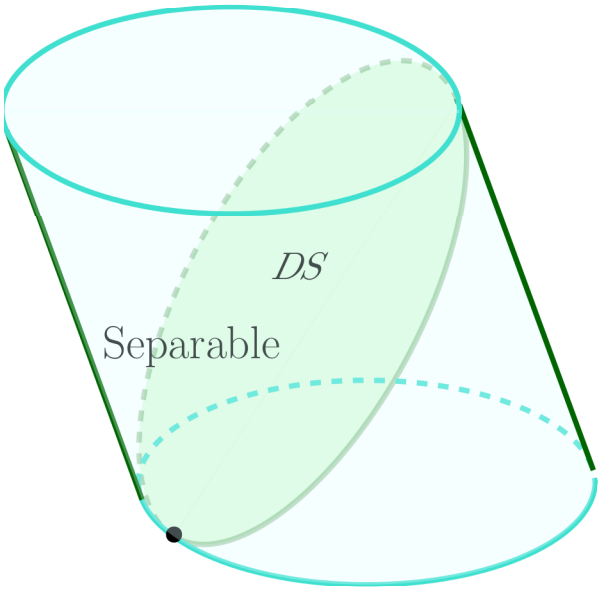

Figure 1: Cartoon picture of the set of separable states SEP (cylinder) and its intersection with the subspace of diagonal symmetric states DS (ellipse). The intersection of the subspace of DS states with the set of separable states gives rise to the set of separable DS states, which is represented by the green ellipse, including its interior. Only the states of the form $|ii\rangle\langle ii|$ are extremal in both sets (represented by the black dot in the figure). However, states that were in the boundary of SEP, could now be extremal when viewed in DS (represented by the border of the green ellipse in the figure).

[9]The technical requirement of full dimensionality [48, 51] depends on the set in which one embeds the problem. Recall that we are interested in solving the separability problem within DS states. The set of DS separable states is of course not full-dimensional when embedded in the whole two-qudit Hilbert space. However, it is full-dimensional when viewed in the DS subspace (cf. Figure 1).

Theorem 3.2. *Let ρ be a DS state acting on $\mathbb{C}^d \otimes \mathbb{C}^d$.*

$$\rho \text{ is PPT} \iff M(\rho) \text{ is DNN.} \tag{15}$$

Proof. – Let us assume that ρ is PPT. Note that the partial transposition of ρ can be written as

$$\rho^\Gamma = \left(\bigoplus_{0 \le a < b < d} \left(\frac{p_{ab}}{2} \right) \oplus \left(\frac{p_{ab}}{2} \right) \right) \oplus M(\rho). \tag{16}$$

Since ρ is PPT, Eq. (16) implies that $M(\rho) \succeq 0$. Since ρ is a valid quantum state, then $p_{ab} \geq 0$ for all $0 \leq a \leq b < d$. Hence, all the entries of $M(\rho)$ are also non-negative. Thus, $M(\rho)$ is DNN.

Conversely, if $M(\rho)$ is DNN then we have that all its entries are non-negative; *i.e.,* $p_{ab} \geq 0$ for $0 \leq a \leq b < d$. These conditions guarantee that $\rho \succeq 0$. Additionally, as $M(\rho) \succeq 0$, these conditions imply that $\rho^\Gamma \succeq 0$. Hence, ρ is PPT.

□

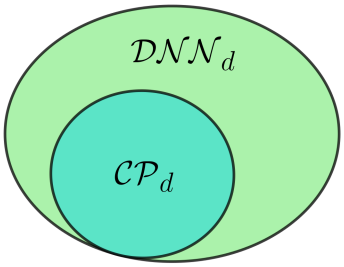

Figure 2: For a two qudit PPTDS state ρ, if its corresponding $M(\rho)$ is in $\mathcal{CP}_d$ then ρ is separable, if $M(\rho)$ is in $\mathcal{DNN}_d$ then ρ is PPT and if $M(\rho)$ is in $\mathcal{DNN}_d$ but not $\mathcal{CP}_d$ then ρ is PPT but entangled.

Recall (cf. Definitions 3.4 and 3.5, also Fig. 2) that $\mathcal{CP}_d \subseteq \mathcal{DNN}_d$. However, the inclusion is strict for $d \geq 5$: It is known that $\mathcal{CP}_d = \mathcal{DNN}_d$ for $d \leq 4$ and $\mathcal{CP}_d \subsetneq \mathcal{DNN}_d$ for $d \geq 5$ [38]. This yields a full characterization of the bipartite separable DS states in terms of the PPT criterion:

Theorem 3.3. *Let ρ be a DS state acting on $\mathbb{C}^d \otimes \mathbb{C}^d$, with $d \leq 4$.*

$$\rho \text{ is separable} \iff \rho \text{ is PPT.} \tag{17}$$

Proof. – The result follows from the identity $\mathcal{CP}_d = \mathcal{DNN}_d$, which holds for $d \leq 4$ [38]. In Example C.1 we provide a constructive proof for $d = 3$.

□

Finally, we end this section by giving a sufficient separability criteria for any d in terms of the ranks of $M(\rho)$.

Theorem 3.4. *Let ρ be a PPTDS state with $M(\rho)$ of rank at most 2. Then, ρ is separable.*

Proof. – Since ρ is PPT, $M(\rho) \succeq 0$. Therefore, it admits a factorization $M(\rho) = VV^T$, where V is a $d \times 2$ or a $d \times 1$ matrix. Geometrically, every row of V can be seen as a vector in $\mathbb{R}^2$ (or a scalar if the rank of $M(\rho)$ is one). Therefore, $M(\rho)$ can be seen as the Gram matrix of those vectors; each element being their scalar product. Since $M(\rho)$ is doubly non-negative, it implies that all these scalar products must be positive; therefore, the angle between each pair of vectors is smaller or equal than $\pi/2$. Thus, the geometrical interpretation is that $M(\rho)$ is CP if, and only if, they can be isometrically embedded into the positive orthant of $\mathbb{R}^k$ for some k. This is always possible to do for $k = 2$ (see Fig. 3), which corresponds to $M(\rho)$ having rank at most 2.

□

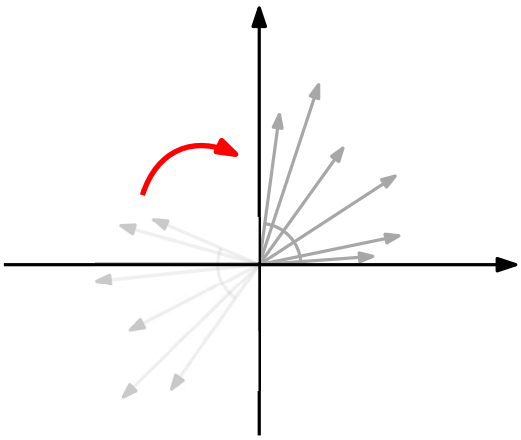

Figure 3: Visual representation of the proof for Theorem 3.4. When the angle between each pair of vectors is smaller or equal than $\pi/2$, meaning that $M(\rho)$ is $\mathcal{CP}_d$, all vectors can be isometrically embedded in the nonnegative orthant.

4 Sufficient criteria for entanglement and separability

In this section we further characterize the bipartite DS states by providing sufficient criteria to certify entanglement by means of Entanglement Witnesses for DS states, and by providing sufficient separability conditions in terms of $M(\rho)$.

4.1 Entanglement Witnesses for DS states

We begin by introducing the concept of *copositive* matrix:

Definition 4.1. *A matrix A is called* copositive *if, and only if, $\vec{x}^T A\vec{x} \geq 0$ for all $\vec{x}$ with non-negative entries.*

The set of $d \times d$ copositive matrices also forms a proper cone, denoted $\mathcal{COP}_d$. The cones $\mathcal{CP}_d$ and $\mathcal{COP}_d$ are dual to each other with respect to the trace inner product. It is also easy to see that $\mathcal{PSD}_d + \mathcal{N}_d \subseteq \mathcal{COP}_d$, where $\mathcal{PSD}_d$ is the set of positive-semidefinite $d \times d$ matrices and $\mathcal{N}_d$ is the set of symmetric entry-wise non-negative matrix. Actually, we have $\mathcal{DNN}_d = \mathcal{PSD}_d \cap \mathcal{N}_d$ and the observation follows from the inclusion $\mathcal{CP}_d \subseteq \mathcal{DNN}_d$.

Therefore, one can view copositive matrices as EWs for DS states. Furthermore, one could think of $\mathcal{PSD}_d + \mathcal{N}_d$ as the set of DEWs for DS states, in the sense that they do not detect entangled PPTDS states.

In Examples 4.1 and D.1 we provide some $M(\rho) \in \mathcal{DNN}_d \setminus \mathcal{CP}_d$ for $d \geq 5$, therefore corresponding to entangled PPTDS states. The paradigmatic example of a copositive matrix detecting matrices DNN, but not CP, (*i.e.*, PPT, but entangled DS states) is the *Horn* matrix [40], which is defined as

$$H := \begin{pmatrix} 1 & -1 & 1 & 1 & -1 \\ -1 & 1 & -1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 & 1 \end{pmatrix}. \tag{18}$$

It is proven that $H \in \mathcal{COP}_5 \setminus (\mathcal{PSD}_5 + \mathcal{N}_5)$ in [40]. As $\mathrm{Tr}(HM(\rho)) = -1 < 0$, H corresponds to an (indecomposable) entanglement witness for the state corresponding to $M(\rho)$.

Although the boundary of the set of copositive matrices remains uncharacterized for arbitrary dimensions, $\mathcal{COP}_5$ was fully characterized in [51]:

$$\mathcal{COP}_5 = \{DAD : D \text{ is positive diagonal}, A \text{ s. t. } p(A, \vec{x}) \text{ is a sum of squares}\}, \tag{19}$$

where

$$p(A,\vec{x}) := \left(\sum_{i,j} A_{ij} x_i^2 x_j^2\right)\left(\sum_k x_k^2\right).$$

Furthermore, the extremal rays of $\mathcal{COP}_d$ have been fully characterized for $d \leq 5$, divided into classes, but this also remains an open problem for higher d [38].

In Appendix B we discuss exposedness properties of the sets of completely positive and co-positive matrices and their relation to the separability problem and its geometry.

Examples of entangled PPTDS states for $d = 5$. – Let us provide an example of a bipartite PPTDS entangled state for $d = 5$.

$$\tilde{M}(\rho) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 3 \end{pmatrix}. \tag{20}$$

It can be easily seen using the Range criterion, as in Section C.2, that ρ is entangled. By Theorem 3.1, it is equivalent to show [38] that $M(\rho) \in \mathcal{DNN}_5 \setminus \mathcal{CP}_5$.
Finally, it can be appreciated how the Horn matrix can be used as an EW and certify entanglement $\mathrm{Tr}(H\tilde{M}(\rho)) = -1 < 0$.

4.2 Sufficient separability conditions for diagonal symmetric states

In the spirit of best separable approximations (BSA) [24], in this section we provide sufficient separability conditions for bipartite PPTDS states. In the same way that the BSA allows one to express any PPTDS state as a sum of a separable part and an entangled one with maximal weight on the separable one[10]. In this section we introduce Best Diagonal Dominant (BDD) approximations, which give a sufficient criterion to certify that a PPTDS state is separable. The idea is that although checking membership in $\mathcal{CP}_d$ is NP-hard, it is actually easy to (i) characterize the extremal elements in $\mathcal{CP}_d$ (cf. Corollary 3.1) and (ii) check for membership in a subset of $\mathcal{DD}_d \subseteq \mathcal{CP}_d$ that is formed of those matrices $A \in N_d$ that are diagonal dominant. In [52] the inclusion $\mathcal{DD}_d \subseteq \mathcal{CP}_d$ was proven. Therefore, to show that $\mathcal{CP}_d \setminus \mathcal{DD}_d$ is nonempty we study when the decomposition of a potential element in $\mathcal{CP}_d$ as a convex combination of an extremal element of $\mathcal{CP}_d$ and an element of $\mathcal{DD}_d$ is possible (see Figure 4).

Let us start by stating a lemma that gives an explicit separable decomposition of a quantum state.

Lemma 4.1. *Let I be the unnormalized quantum state defined as*

$$I = \sum_{i=0}^{d-1} |ii\rangle\langle ii| + \sum_{0\leq i<j<d} 2|D_{ij}\rangle\langle D_{ji}|, \tag{21}$$

where $|D_{ij}\rangle = (|ij\rangle + |ji\rangle)/\sqrt{2}$. For instance, for $d = 3$,

$$I = \left(\begin{array}{ccc|ccc|ccc} 1 & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \hline \cdot & 1 & \cdot & 1 & \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & 1 & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot \\ \hline \cdot & \cdot & 1 & \cdot & \cdot & \cdot & 1 & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & 1 & \cdot & 1 & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & 1 \end{array}\right). \tag{22}$$

[10] In [25], the BSA was found analytically for N-qubit DS states

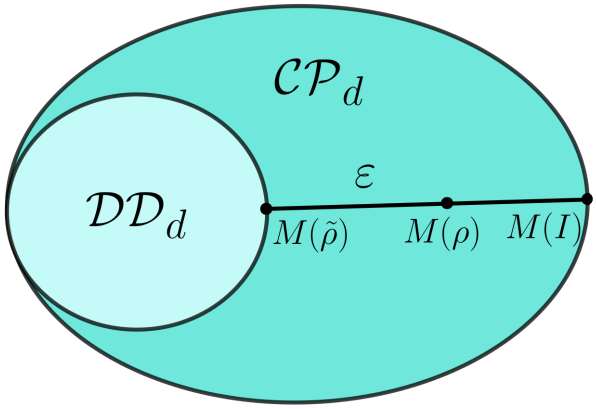

Figure 4: Given a two-qudit PPTDS state ρ, if we can decompose $M(\rho)$ in terms of $M(I)$ (an extremal element of $\mathcal{CP}_d$) and $M(\tilde{\rho})$ (an element of $\mathcal{DD}_d$) we can certify that $M(\rho)$ is in $\mathcal{CP}_d$ and therefore certify that ρ is separable.

Then, I is separable.

Proof. – Let $|e(\vec{\varphi})\rangle = |0\rangle + e^{\mathrm{i}\varphi_1}|1\rangle + \cdots + e^{\mathrm{i}\varphi_{d-1}}|d-1\rangle$. A separable decomposition of I is given by

$$I = \int_{[0,2\pi]^d} \frac{\mathrm{d}\vec{\varphi}}{(2\pi)^d} (|e(\vec{\varphi})\rangle\langle e(\vec{\varphi})|)^{\otimes 2}. \tag{23}$$

Indeed,

$$I = \sum_{ijlk} |ij\rangle\langle kl| \int_{[0,2\pi]^d} \frac{\mathrm{d}\vec{\varphi}}{(2\pi)^d} e^{\mathrm{i}(\varphi_i+\varphi_j-\varphi_k-\varphi_l)} = \sum_{ijlk} |ij\rangle\langle kl|(\delta_{i,k}\delta_{j,l} + \delta_{i,l}\delta_{j,k} - \delta_{i,j,k,l}), \tag{24}$$

where δ is the Kronecker delta function. □

Lemma 4.1 allows us to give a sufficient condition for a state ρ to be separable. The idea is to subtract εI from ρ in such a way that it remains a valid diagonal symmetric state, PPT, and close enough to the interior of the separable set such that it is easy to certify that the state is separable (see Fig. 4).

Theorem 4.1. *Let ρ be a two-qudit PPTDS state with associated $M(\rho)$. If there exists $\varepsilon \geq 0$ such that*

1. *$\varepsilon \leq \rho_{ij}$ for all i, j such that $0 \leq i, j < d$.*
2. *$\varepsilon d \leq (\langle u|\frac{1}{M(\rho)}|u\rangle)^{-1}$ and $|u\rangle \in \mathcal{R}(M(\rho))$, $\mathcal{R}(M(\rho))$ is the range of $M(\rho)$ and $\frac{1}{M(\rho)}$ is the pseudo-inverse of $M(\rho)$. Here $|u\rangle$ is a normalized vector of ones.*
3. *for all i such that $0 \leq i < d$, $\rho_{ii} + \varepsilon(d-2) \geq \sum_{j\neq i} \rho_{ji}$.*

Then, ρ is separable.

See the proof in Appendix D.2.

A few comments are in order: The first condition on Theorem 4.1 ensures that I can be subtracted from ρ and $\tilde{\rho}$ will remain in the DS subspace. The second condition requires that I can be subtracted from ρ while maintaining the PPT property of $\tilde{\rho}$. If $|u\rangle \notin \mathcal{R}(M(\rho))$, then $\tilde{\rho}$ would not be PPT for any $\varepsilon \neq 0$. Therefore, the second condition gives the maximal value of ε that can be subtracted such that $\tilde{\rho}$ remains PPT. Finally, the third condition relies on guaranteeing that $\tilde{\rho}$ is separable, which is ensured by $M(\tilde{\rho})$ to be diagonal dominant. This means that one might need to subtract a minimal amount of I to accomplish such a property (unless ρ is already diagonal dominant).
In Example D.3 we show that $\mathcal{CP}_d \setminus \mathcal{DD}_d \neq \emptyset$ using the approach of Theorem 4.1.

The above result can be now normalized and generalized to any other extremal element I in $\mathcal{CP}_d$:

Lemma 4.2. *Let $\mathbf{x} \in \mathbb{R}^d$ with $x_i \geq 0$ and $||\mathbf{x}|| > 0$. Let $I_{\mathbf{x}}$ be the quantum state defined as*

$$I_{\mathbf{x}} = \frac{1}{||\mathbf{x}||_1^2}\left(\sum_{i=0}^{d-1} x_i^2 |ii\rangle\langle ii| + \sum_{0\leq i<j<d} 2x_i x_j |D_{ij}\rangle\langle D_{ij}|\right).$$

Then, the quantum state $I_{\mathbf{x}}$ is separable.

See the proof in Appendix D.4.

Note that the corresponding $M(I_{\mathbf{x}})$ is given by $|u_{\mathbf{x}}\rangle\langle u_{\mathbf{x}}|$, where $|u_{\mathbf{x}}\rangle = \mathbf{x}/||\mathbf{x}||_1$. The sum of the elements of $M(I_{\mathbf{x}})$ is then one; *i.e.*, $||M(I_{\mathbf{x}})||_1 = 1$.

Lemma 4.2 allows us to give a sufficient condition for a state ρ is separable. This time the idea is to decompose ρ as a convex combination between $I_{\mathbf{x}}$, which is a state that is extremal in the set of separable DS states, and a state $\tilde{\rho}$ which is deep enough in the interior of the set of separable states, such that we can certify its separability by other means (by showing that $M(\tilde{\rho})$ is diagonal dominant and doubly non-negative; therefore completely positive [52]).

Theorem 4.2. *Let ρ be a two-qudit PPTDS state with associated $M(\rho)$. Let $\mathbf{x} \in \mathbb{R}^d$ with $x_i > 0$. If there exists a $\lambda \in [0, 1)$ such that*

1. *$\lambda \leq (M(\rho))_{ij}||\mathbf{x}||_1^2/x_i x_j$ for all i and j,*
2. *$\lambda \leq 1/\langle u_{\mathbf{x}}|\frac{1}{M(\rho)}|u_{\mathbf{x}}\rangle$ and $|u_{\mathbf{x}}\rangle \in \mathcal{R}(M(\rho))$, where $\mathcal{R}(M(\rho))$ is the range of $M(\rho)$ and $\frac{1}{M(\rho)}$ denotes the pseudo-inverse of $M(\rho)$,*
3. *$\lambda x_i(||\mathbf{x}||_1 - 2x_i) \geq ||\mathbf{x}||_1^2\left[\sum_{j\neq i}(M(\rho))_{ij} - (M(\rho))_{ii}\right]$ for all i,*

then ρ is separable. Equivalently, then $M(\rho)$ is completely positive.

See the proof in Appendix D.5 (*i.e.*, write $\rho = (1-\lambda)\tilde{\rho} + \lambda I_{\mathbf{x}}$ and ensure that the associated $M(\tilde{\rho})$ is completely positive).

Notice that Theorem 4.2 provides an advantage over Theorem 4.1 since the parameters of $I_{\mathbf{x}}$ are not fixed which allows to consider a bigger family of decompositions $M(\rho) \in \mathcal{CP}_d$ parametrized by $\mathbf{x}$. In Example 4.2 we attempt to apply both Theorems in order to guarantee separability and illustrate such advantage.

Example. – In this example we provide a PPTDS state with associated $M(\rho) \in \mathcal{CP}_d \setminus \mathcal{DD}_d$ and we show how to apply Theorem 4.2 to guarantee separability. Furthermore, we also apply Theorem 4.1 to illustrate the advantage of Theorem 4.2.

Take the following DS state $\rho \in \mathbb{C}^3$ with associated

$$M(\rho) = \begin{pmatrix} \alpha & \beta & \gamma \\ \beta & \delta & \beta \\ \gamma & \beta & \epsilon \end{pmatrix} = \frac{1}{100}\begin{pmatrix} 19 & 8 & 11.5 \\ 8 & 6.4 & 8 \\ 11.5 & 8 & 19.6 \end{pmatrix}, \tag{25}$$

where it can be checked that the state ρ is normalized. A priori we do not know if this state is separable, the goal is to apply Theorems 4.1 and 4.2 in order to see if separability can be guaranteed. For both Theorems the more restrictive between conditions 1 and 2 provides an upper bound for the corresponding decomposition and condition 3 a lower bound but, as mentioned, Theorem 4.2 offers more flexibility since such bound can be varied by fitting $I_{\mathbf{x}}$. This example illustrates this fact since we will see that Theorem 4.2 guarantees separability but Theorem 4.1 does not.

Lets start with Theorem 4.2. For the given case (25) we want to find if a convex decomposition $M(\rho) = (1-\lambda)M(\tilde{\rho}) + \lambda M(I_{\mathbf{x}})$ exists while fulfilling the conditions of the theorem. For instance, for illustrative purposes we fix $\lambda = 0.8$ and by numerical means we obtain that a possible convex combination would be with an $M(I_{\mathbf{x}}) = |u_{\mathbf{x}}\rangle\langle u_{\mathbf{x}}|$ given by $|u_{\mathbf{x}}\rangle = 1/100(37.46|0\rangle + 25.16|1\rangle + 37.38|2\rangle)$.

Lets proceed to show that the given $M(\rho)$ and $M(I_{\mathbf{x}})$ meet the conditions of Theorem 4.2. Condition 1 provides the more restrictive upper bound given by

$$\lambda \leq \frac{\gamma||\mathbf{x}||_1^2}{x_1 x_3} = 0.8213, \tag{26}$$

while the lower bound will be given by the following case of Condition 3

$$\lambda \geq \frac{||\mathbf{x}||_1^2[2\beta - \delta]}{x_2(||\mathbf{x}||_1 - \delta)} = 0.7681. \tag{27}$$

Therefore, there exists a range of values $\lambda \in [0.7681, 0.8213]$ that satisfy the conditions of Theorem 4.2 and certifies that the state ρ is separable. Notice that, for illustrative purposes, once we found an $M(I_{\mathbf{x}})$ fulfilling the conditions we fixed it to find a range of values for λ but we could have allowed for more freedom and find a bigger range of possible decompositions.

Now lets see what happens with Theorem 4.1. In this case the most restrictive upper bound is given by Condition 2

$$\varepsilon \leq (\langle u|\frac{1}{M(\rho)}|u\rangle)^{-1} = 0.06, \tag{28}$$

while the most restrictive lower bound will be given by the following case of Condition 3

$$\varepsilon \geq 2\beta - \delta = 0.096. \tag{29}$$

Thus, for this case there does not exist an ε satisfying the conditions for Theorem 4.1, while there exists a range of λ satisfying conditions for Theorem 4.2 and therefore illustrating its advantage by being able to certify separability.

5 A class of PPT-entangled quasi-DS states

In this Section, we introduce a uni-parametric class of N-qubit PPTESS, for an odd number of qubits. As it has been shown in [27, 28], N-qubit PPTDS states are fully separable. The class we introduce can be seen as a N-qubit PPTDS state with slight GHZ coherences. Surprisingly, in the family of states we provide, an arbitrarily small weight on the non-diagonal elements (in the Dicke basis) allows the state to be genuinely multipartite entangled while maintaining the PPT property.

The procedure we have chosen to derive this class of states is based on the iterative algorithm for finding extremal PPT symmetric states [20, 21] (see also [53]), which we briefly recall here in the interest of completeness. One starts with an initial symmetric state ρ_0 that is fully separable; for instance, the symmetric completely mixed state. Then, one picks a random direction σ_0 in the set of quantum states and subtracts it from the initial state while preserving the PPT property, therefore obtaining $\rho_0 - x_0\sigma_0$, $x_0 > 0$. One necessarily finds a critical x_0^* such that one arrives at the boundary of the PPT set, where the rank of $\rho_0 - x_0^*\sigma_0$ or one of its partial transpositions must have decreased. Hence, at least one new vector appears in the kernel of the state or in the kernel of some of its partial transpositions. This state with lower ranks is set as the initial state for the next iteration $\rho_1 = \rho_0 - x_0^*\sigma_0$. The new direction σ_1 is chosen such that it preserves all the vectors present in the kernels of both the state and its partial transpositions. This process is repeated until no new improving direction can be found, yielding an extremal state ρ_k in the PPT set. As the PPT set contains all separable states, we note that if the rank of such extremal PPT state is greater than one, then it cannot be extremal in the set of separable states (because these are pure product vectors, which have rank one), therefore it must be entangled. The study carried out in [20, 21] looked for typical extremal PPT states by exploring random directions every time. However, by carefully picking these directions, one can look for classes of states of different forms, such as the ones presented in Theorem 5.1.

In Example E.1 we present a 4-qubit PPT-entangled symmetric state whose density matrix is sparse with real entries when represented in the computational basis and has a closed analytical form.

The class of states we are going to present is furthermore symmetric with respect to the $|0\rangle \leftrightarrow |1\rangle$ exchange and, to simplify our proof and take advantage of this symmetry, we shall consider only an odd number of qubits $N = 2K + 1$, with $K > 1$.

Theorem 5.1. *Let $N = 2K + 1$ with $K \in \mathbb{N}$ and $K > 1$. Let $Z \in (0, \infty)$ and $\sigma = \pm 1$. We define the sequence $\{f_k(Z)\}_{k\in\mathbb{Z}}$ through the recurrence relation $f_{k+2}(Z) = (2 + Z)f_{k+1}(Z) - f_k(Z)$ and the initial conditions $f_0(Z) = 1$ and $f_1(Z) = 1 + Z$. We also define $\lambda_k(Z) := f_{K-k}(Z)$. The diagonal part of the state is defined as*

$$d(Z) := \sum_{k=0}^{N} \binom{N}{k} \lambda_k(Z) |D_N^k\rangle\langle D_N^k|, \tag{30}$$

and the off-diagonal part as

$$o(\sigma) := \sigma(|D_N^0\rangle\langle D_N^N| + |D_N^N\rangle\langle D_N^0|). \tag{31}$$

Then, the N-qubit symmetric state

$$\rho(Z) := \frac{d(Z) + o(\sigma)}{2(4 + Z)^K}, \tag{32}$$

is PPT with respect to every bipartition, has ranks $(N + 1, 2N, 2N, \ldots, 2N, 2N - 1)$ and is extreme in the PPT set (therefore, it is entangled).

We split the proof into several lemmas, for better readability and intuition on the above definitions.

Proof. –

Let us start with some general considerations on the structure of $\rho(Z)$. In order to efficiently apply the partial transposition operation with respect to m subsystems, we need to express $\rho(Z)$ acting on $\mathbb{C}^{m+1} \otimes \mathbb{C}^{N-m+1}$.

Lemma 5.1. *Let $\lambda'_k = \binom{N}{k}\lambda_k$. Let ρ be an N-qubit PPTDS state with diagonal elements $\{\lambda'_k\}_{k=0}^N$ and GHZ coherences $o(\sigma)$. Its partial transposition with respect to m subsystems ρ^{Γ_m}, acting on $\mathbb{C}^{m+1} \otimes \mathbb{C}^{N-m+1}$, block-diagonalizes as*

$$\rho^{\Gamma_m} = \begin{pmatrix} \lambda_m & \sigma \\ \sigma & \lambda_{N-m} \end{pmatrix} \bigoplus \left(\bigoplus_{n=-m+1}^{N-m-1} A_n^{(m)} \right), \tag{33}$$

where $A_n^{(m)} := D_n^{(m)} H_n^{(m)} D_n^{(m)}$. $A_n^{(m)}$ is a square matrix of size $\min\{m, N - m + n\} - \max\{0, n\} + 1$ elements, which decomposes as a product of the diagonal matrix $D_n^{(m)}$, with diagonal elements

$$\left\{ \sqrt{\binom{m}{k}\binom{N-m}{k-n}} \right\}_{k=\max\{0,n\}}^{\min\{m,N-m+n\}}, \tag{34}$$

and the Hankel matrix

$$H_n^{(m)} = (\lambda_{i+k-n})_{\max\{0,n\}\le i,k\le \min\{m,N-m+n\}}. \tag{35}$$

See the Proof in Appendix E.2.

In what follows we are going to argue the construction of our class of states. Having a state with ranks as low as possible tremendously simplifies the analysis of PPT entanglement [12]. It is the main idea we are going to follow in defining all the elements of our class. Therefore, we first study the condition for which the block of ρ^{Γ_m} that contains σ has zero determinant. This gives the condition $\lambda_m \lambda_{N-m} = \sigma^2 = 1$. In particular, if we impose this condition for $m = K$, we obtain $\lambda_K^2 = 1$, which means (by definition) that $f_0 = 1$.

Now we focus on the block $n = -m + 1$ with $m = K$. The determinant of the n-th block is

$$|A_{-K+1}^{(K)}| = K(N-K)|B_{-K+1}^{(K)}| = K(N-K)\begin{vmatrix} \lambda_{K-1} & \lambda_K \\ \lambda_K & \lambda_{K+1} \end{vmatrix} = K(N-K)(f_1 f_0 - f_0^2) = K(N-K)(f_1 - 1). \tag{36}$$

By imposing the determinant of $B^{(K)}_{-K+1}$ to be $Z > 0$ we obtain the condition $f_1 = 1 + Z$ with $Z > 0$. This choice is arbitrary and is the one that characterizes our class.

Finally, we move to the 3×3 block determinants, which we shall make 0. These are

$$|B^{(m)}_{-m+2}| = \begin{vmatrix} \lambda_{m-2} & \lambda_{m-1} & \lambda_m \\ \lambda_{m-1} & \lambda_m & \lambda_{m+1} \\ \lambda_m & \lambda_{m+1} & \lambda_{m+2} \end{vmatrix} = 0. \tag{37}$$

This condition reads

$$\lambda_{m+2}(\lambda_m\lambda_{m-2} - \lambda^2_{m-1}) = \lambda^3_m - 2\lambda_{m-1}\lambda_m\lambda_{m+1} + \lambda_{m-2}\lambda^2_{m+1}. \tag{38}$$

We want to determine a recursive form for the λ_m that satisfies Eq. (38). This is an equation in differences which is nonlinear. It is in general extremely hard to solve these kind of equations. Nevertheless, despite the appearance of Eq. (38), one can exploit some properties: for instance, it is immediate to check that it is homogeneous of degree 3, its coefficients sum zero on each side of the equation and the indices of each monomial sum $3m$ for all the terms. This suggests that the equation admits a solution of the form $\lambda_{m+1} \propto \lambda_m$. Indeed, any sequence of the form $\lambda_{m+1} = c\lambda_m$ with $c \in \mathbb{R}$ is a solution. More generally, one can show that *any* sequence $\lambda_{m+2} + c_1\lambda_{m+1} + c_0\lambda_m = 0$ is a solution, for all $c_0, c_1 \in \mathbb{R}$. We are going to find a solution of this form, so we have to determine c_0 and c_1.

Thanks to the symmetry $\lambda_m = \lambda_{N-m}$ we can find the coefficients c_0 and c_1: Indeed, by taking $m = K$ and $m = K - 1$ we have the equations

$$\begin{cases} \lambda_{K+2} + c_0\lambda_{K+1} + c_0\lambda_K = f_1 + c_0 f_0 + c_1 f_0 = 0 \\ \lambda_{K+1} + c_0\lambda_K + c_0\lambda_{K-1} = f_0 + c_0 f_0 + c_1 f_1 = 0 \end{cases}, \tag{39}$$

which give $c_0 = 1$ and $c_1 = -2(1 + Z)$ as the unique solutions.

Let us note that one can find the expression for f_m in a non-recursive form, with the aid of the Z-transform:

$$f_{m+2} + c_1 f_{m+1} + c_0 f_m = 0 \leftrightarrow F(z) = \frac{z(1 + Z + c_1 + z)}{z^2 + zc_1 + c_0}. \tag{40}$$

By undoing the Z-transform, we obtain the explicit expression for f_m:

$$f_m = \frac{\alpha - 1}{\alpha - \beta}\alpha^m - \frac{\beta - 1}{\alpha - \beta}\beta^m, \tag{41}$$

where $\alpha := (2 + Z + \sqrt{Z(4 + Z)})/2$ and $\beta := (2 + Z - \sqrt{Z(4 + Z)})/2$.

Lemma 5.2. *Let λ_m be defined as in (41). The blocks $B^{(m)}_n$ are positive semidefinite and their rank is 2. Therefore, ρ is PPT and its ranks are $(N + 1, 2N....2N, 2N - 1)$.*

See the proof in Appendix E.3.

Lemma 5.3. *The trace of ρ is $2(4 + Z)^K$.*

See the proof in Appendix E.4.

Lemma 5.4. *The state ρ is extremal in the PPT set.*

Proof of Lemma 5.4. – To prove extremality, we use the following theorem from [54]: ρ is extremal in the PPT set if, and only if, every Hermitian matrix H satisfying $\mathcal{R}(H^{\Gamma_m}) \subseteq \mathcal{R}(\rho^{\Gamma_m})$ is proportional to ρ. Note that by taking $H \propto \rho$ we always find a solution satisfying the above conditions, but we have to show that no other exists. Let us consider the subspace E of the $(N + 1) \times (N + 1)$ Hermitian matrices spanned by the following matrices:

$$E = \left[|D^0_N\rangle\langle D^0_N|, \ldots, |D^N_N\rangle\langle D^N_N|, \frac{1}{\sqrt{2}}(|D^N_N\rangle\langle D^0_N| + |D^0_N\rangle\langle D^N_N|) \right]. \tag{42}$$

Let us argue that we can assume that H has to live in the same subspace as ρ. Since $\mathcal{R}(\rho) \subseteq E$, H has to be of the form

$$H = \sum_{k=0}^{N} h_k |D_N^k\rangle\langle D_N^k| + h\frac{1}{\sqrt{2}}(|D_N^N\rangle\langle D_N^0| + |D_N^0\rangle\langle D_N^N|), \tag{43}$$

where h_k and h are real parameters.

The condition $\mathcal{R}(H^{\Gamma_m}) \subseteq \mathcal{R}(\rho^{\Gamma_m})$ means that the vectors spanning H^{Γ_m} must be orthogonal to (at least) the vectors in the kernel of ρ^{Γ_m}. Fortunately, we have calculated the block-decomposition of ρ^{Γ_m}:

$$\rho^{\Gamma_m} = \begin{pmatrix} \lambda_m & \sigma \\ \sigma & \lambda_{N-m} \end{pmatrix} \bigoplus \left(\bigoplus_{n=-m+1}^{N-m-1} A_n^{(m)} \right), \tag{44}$$

As a side-comment let us observe that $(D_n^{(m)})^{-1}|v\rangle \in \ker A_n^{(m)} \iff |v\rangle \in \ker B_n^{(m)}$. Anyway, being orthogonal to $\ker {B_n}^{(m)}$ implies that the coefficients h_m must satisfy a recurrence relation of the form

$$h_{m+2} - (2+Z)h_{m+1} + h_m = 0, \tag{45}$$

which fixes $h_m \propto f_m$. Finally, we fix the value of h by looking at the kernel of the block that goes alone in ρ^{Γ_K}, which is spanned by $(\sigma, -1)^T$. Hence, we have that $h_K\sigma - h = 0$, which implies that $h = \sigma h_K$. Hence, $H = h_K\rho \propto \rho$ is the only solution to $\mathcal{R}(H^{\Gamma_m}) \subseteq \mathcal{R}(\rho^{\Gamma_m})$, proving that ρ is extremal. □

Since all the states in the PPT set which are separable and extremal have ranks $r(\rho^{\Gamma_m}) = 1$, an extremal PPT state with a rank $r(\rho^{\Gamma_m}) > 1$ cannot be separable. Hence, $\rho(Z)$ is a uni-parametric family of PPT-entangled states for all $Z \in (0, \infty)$.

6 Conclusions and Outlook

In this work we have studied the separability problem for diagonal symmetric states that are positive under partial transpositions. In the bipartite case, we have explored its connection to quadratic conic optimization problems, which naturally appear in a plethora of situations. Via this equivalence, we have been able to translate results from quantum information to optimization and vice-versa. For instance, we have characterized the extremal states of the set of separable DS states, defined entanglement witnesses for PPTDS states in terms of copositive matrices and we have rediscovered that the separability problem is NP-hard even in this highly symmetric and simplified case. We have shown that PPT is equivalent to separability in this context only for states of physical dimension not greater than 4. We have complemented our findings with a series of analytical examples and counterexamples. Furthermore, the state of the art in quadratic conic optimization allows us to see which are going to be the forthcoming challenges, in which insights developed within the quantum information community might contribute in advancing the field.

Second, we have provided a set of tools to certify separability of a bipartite PPTDS state in arbitrary dimensions, by decomposing it as a combination of an extremal DS state and a diagonal dominant DS state.. A natural further research direction is to study whether more sophisticated decompositions are possible, in terms of various extremal elements in $\mathcal{CP}_d$ and by understanding how the facial structure of $\mathcal{CP}_d$ plays a role in this problem.

Third, we have shown that, although N-qubit DS states are separable if, and only if, they are PPT with respect to every bipartition, just adding a new GHZ-like coherence can entangle the state while mantaining the PPT property for every bipartition. We have characterized analytically this class and we have shown that its ranks are much lower than those typically found in previous numerical studies [21]. In this search, we have also found an analytical example of a 4-qubit PPT-entangled symmetric state, whose density matrix is sparse with real entries, when expressed in the computational basis, contrary to previous numerical examples [20]. A natural following research direction is to connect the recently developed concept of coherence [55] to the Dicke basis, and to explore further its connection to

PPT-entangled symmetric states. Furthremore, it seems plausible that one can find further connections between the properties of $M(\rho)$ and those of MUBs since it has been shown that one can construct EWs based on MUBs that are capable of detecting bound entangled states (See [56] for a recent construction or [57] for an application to magic simplex states in an experimentally feasible way). Whether there is a clear connection between EWs from MUBs and EWs for bound entangled DS states in terms of the properties of $M(\rho)$ remains an open research direction.

Acknowledgements

We acknowledge financial support from the Spanish MINECO (SEVERO OCHOA grant SEV-2015-0522, FISICATEAMO FIS2016-79508-P, FIS2013-40627-P and FIS2016-86681-P AEI/FEDER EU), ERC AdG OSYRIS (ERC-2013-ADG No. 339106), Generalitat de Catalunya (2014-SGR-874, 2014-SGR-966 and the CERCA Programme), and Fundació Privada Cellex. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 748549. R. Q. acknowledges the Spanish MECD for the FPU Fellowship (No. FPU12/03323). We thank S. Gharibian and two anonymous reviewers for insightful comments on the manuscript.

References

[1] Ryszard Horodecki, Paweł Horodecki, Michał Horodecki, and Karol Horodecki, "Quantum entanglement," Rev. Mod. Phys. **81**, 865–942 (2009).

[2] Artur K. Ekert, "Quantum cryptography based on Bell's theorem," Phys. Rev. Lett. **67**, 661–663 (1991).

[3] Christian Gross, Tilman Zibold, Eike Nicklas, Jerome Esteve, and Markus K Oberthaler, "Nonlinear atom interferometer surpasses classical precision limit," Nature **464**, 1165–1169 (2010).

[4] John S Bell, "On the Einstein Podolsky Rosen paradox," Physics **1**, 195–200 (1964).

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

[6] Antonio Acín, Nicolas Brunner, Nicolas Gisin, Serge Massar, Stefano Pironio, and Valerio Scarani, "Device-independent security of quantum cryptography against collective attacks," Physical Review Letters **98**, 230501 (2007).

[7] Leonid Gurvits, "Classical deterministic complexity of Edmonds' problem and quantum entanglement," in *Proceedings of the Thirty-fifth Annual ACM Symposium on Theory of Computing*, STOC '03 (ACM, New York, NY, USA, 2003) pp. 10–19.

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

[9] Michał Horodecki, Paweł Horodecki, and Ryszard Horodecki, "Separability of mixed states: necessary and sufficient conditions," Physics Letters A **223**, 1 – 8 (1996).

[10] Erling Størmer, "Positive linear maps of operator algebras," Acta Math. **110**, 233–278 (1963).

[11] S.L. Woronowicz, "Positive maps of low dimensional matrix algebras," Reports on Mathematical Physics **10**, 165 – 183 (1976).

[12] Pawel Horodecki, "Separability criterion and inseparable mixed states with positive partial transposition," Physics Letters A **232**, 333 – 339 (1997).

[13] K. Eckert, J. Schliemann, D. Bruß, and M. Lewenstein, "Quantum correlations in systems of indistinguishable particles," Annals of Physics **299**, 88 – 127 (2002).

[14] Roe Goodman and Nolan R Wallach, *Symmetry, representations, and invariants*, Vol. 255 (Springer, 2009).

[15] R. H. Dicke, "Coherence in spontaneous radiation processes," Phys. Rev. **93**, 99–110 (1954).

[16] Robert McConnell, Hao Zhang, Jiazhong Hu, Senka Ćuk, and Vladan Vuletić, "Entanglement with negative Wigner function of almost 3,000 atoms heralded by one photon," Nature **519**, 439–442 (2015).

[17] Witlef Wieczorek, Roland Krischek, Nikolai Kiesel, Patrick Michelberger, Géza Tóth, and Harald Weinfurter, "Experimental entanglement of a six-photon symmetric Dicke state," Phys. Rev. Lett. **103**, 020504 (2009).
[18] Chao-Yang Lu, Xiao-Qi Zhou, Otfried Gühne, Wei-Bo Gao, Jin Zhang, Zhen-Sheng Yuan, Alexander Goebel, Tao Yang, and Jian-Wei Pan, "Experimental entanglement of six photons in graph states," Nature Physics **3**, 91–95 (2007).
[19] José I. Latorre, Román Orús, Enrique Rico, and Julien Vidal, "Entanglement entropy in the Lipkin-Meshkov-Glick model," Phys. Rev. A **71**, 064101 (2005).
[20] J. Tura, R. Augusiak, P. Hyllus, M. Kuś, J. Samsonowicz, and M. Lewenstein, "Four-qubit entangled symmetric states with positive partial transpositions," Phys. Rev. A **85**, 060302 (2012).
[21] R. Augusiak, J. Tura, J. Samsonowicz, and M. Lewenstein, "Entangled symmetric states of n qubits with all positive partial transpositions," Phys. Rev. A **86**, 042316 (2012).
[22] Jordi Tura i Brugués, *Characterizing Entanglement and Quantum Correlations Constrained by Symmetry* (Springer International Publishing, 2017).
[23] Alejandro González-Tudela and Diego Porras, "Mesoscopic entanglement induced by spontaneous emission in solid-state quantum optics," Phys. Rev. Lett. **110**, 080502 (2013).
[24] Maciej Lewenstein and Anna Sanpera, "Separability and entanglement of composite quantum systems," Phys. Rev. Lett. **80**, 2261–2264 (1998).
[25] Ruben Quesada and Anna Sanpera, "Best separable approximation of multipartite diagonal symmetric states," Physical Review A **89**, 052319 (2014).
[26] Elie Wolfe and S. F. Yelin, "Certifying separability in symmetric mixed states of n qubits, and superradiance," Phys. Rev. Lett. **112**, 140402 (2014).
[27] Nengkun Yu, "Separability of a mixture of Dicke states," Phys. Rev. A **94**, 060101 (2016).
[28] Ruben Quesada, Swapan Rana, and Anna Sanpera, "Entanglement and nonlocality in diagonal symmetric states of n qubits," Physical Review A **95**, 042128 (2017).
[29] Asher Peres, "All the Bell inequalities," Foundations of Physics **29**, 589–614 (1999).
[30] J. Tura, R. Augusiak, A. B. Sainz, T. Vértesi, M. Lewenstein, and A. Acín, "Detecting nonlocality in many-body quantum states," Science **344**, 1256–1258 (2014).
[31] J. Tura, R. Augusiak, A.B. Sainz, B. Lücke, C. Klempt, M. Lewenstein, and A. Acín, "Nonlocality in many-body quantum systems detected with two-body correlators," Annals of Physics **362**, 370 – 423 (2015).
[32] Matteo Fadel and Jordi Tura, "Bounding the set of classical correlations of a many-body system," Phys. Rev. Lett. **119**, 230402 (2017).
[33] Elias Amselem and Mohamed Bourennane, "Experimental four-qubit bound entanglement," Nature Physics **5**, 748 EP – (2009), article.
[34] Jonathan Lavoie, Rainer Kaltenbaek, Marco Piani, and Kevin J. Resch, "Experimental bound entanglement in a four-photon state," Phys. Rev. Lett. **105**, 130501 (2010).
[35] Joonwoo Bae, Markus Tiersch, Simeon Sauer, Fernando de Melo, Florian Mintert, Beatrix Hiesmayr, and Andreas Buchleitner, "Detection and typicality of bound entangled states," Phys. Rev. A **80**, 022317 (2009).
[36] Beatrix C Hiesmayr and Wolfgang Löffler, "Complementarity reveals bound entanglement of two twisted photons," New Journal of Physics **15**, 083036 (2013).
[37] Christoph Spengler, Marcus Huber, Stephen Brierley, Theodor Adaktylos, and Beatrix C. Hiesmayr, "Entanglement detection via mutually unbiased bases," Phys. Rev. A **86**, 022311 (2012).
[38] Avi Berman, Mirjam Dur, and Naomi Shaked-Monderer, "Open problems in the theory of completely positive and copositive matrices," Electronic Journal of Linear Algebra **29**, 46–58 (2015).
[39] Leonard J Gray and David G Wilson, "Nonnegative factorization of positive semidefinite nonnegative matrices," Linear Algebra and its Applications **31**, 119–127 (1980).
[40] Marshall Hall and Morris Newman, "Copositive and completely positive quadratic forms," Mathematical Proceedings of the Cambridge Philosophical Society **59**, 329–339 (1963).

[41] Sudip Bose and Eric Slud, "Maximin efficiency-robust tests and some extensions," Journal of statistical planning and inference **46**, 105–121 (1995).
[42] A. Berman and N. Shaked-Monderer, *Completely Positive Matrices* (World Scienfic, 2003).
[43] Chris Ding, Xiaofeng He, and Horst D Simon, "On the equivalence of nonnegative matrix factorization and spectral clustering," in *Proceedings of the 2005 SIAM International Conference on Data Mining* (SIAM, 2005) pp. 606–610.
[44] Abraham Berman, Christopher King, and Robert Shorten, "A characterisation of common diagonal stability over cones," Linear and Multilinear Algebra **60**, 1117–1123 (2012).
[45] Oliver Mason and Robert Shorten, "On linear copositive lyapunov functions and the stability of switched positive linear systems," IEEE Transactions on Automatic Control **52**, 1346–1349 (2007).
[46] Barbara M. Terhal, "Bell inequalities and the separability criterion," Physics Letters A **271**, 319 – 326 (2000).
[47] R Augusiak, J Tura, and M Lewenstein, "A note on the optimality of decomposable entanglement witnesses and completely entangled subspaces," Journal of Physics A: Mathematical and Theoretical **44**, 212001 (2011).
[48] Sevag Gharibian, "Strong np-hardness of the quantum separability problem," Quantum Information & Computation **10**, 343–360 (2010).
[49] Michael R. Garey and David S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-Completeness* (W. H. Freeman & Co., New York, NY, USA, 1979).
[50] Martin Grötschel, László Lovász, and Alexander Schrijver, *Geometric algorithms and combinatorial optimization*, Vol. 2 (Springer Science & Business Media, 2012).
[51] Peter J. C. Dickinson, Mirjam Dür, Luuk Gijben, and Roland Hildebrand, "Scaling relationship between the copositive cone and parrilo's first level approximation," Optimization Letters **7**, 1669–1679 (2013).
[52] M. Kaykobad, "On nonnegative factorization of matrices," Linear Algebra and its Applications **96**, 27 – 33 (1987).
[53] Jon Magne Leinaas, Jan Myrheim, and Per Øyvind Sollid, "Numerical studies of entangled positive-partial-transpose states in composite quantum systems," Phys. Rev. A **81**, 062329 (2010).
[54] Remigiusz Augusiak, Janusz Grabowski, Marek Kuś, and Maciej Lewenstein, "Searching for extremal PPT entangled states," Optics Communications **283**, 805 – 813 (2010), quo vadis Quantum Optics?
[55] T. Baumgratz, M. Cramer, and M. B. Plenio, "Quantifying coherence," Phys. Rev. Lett. **113**, 140401 (2014).
[56] Dariusz Chruściński, Gniewomir Sarbicki, and Filip Wudarski, "Entanglement witnesses from mutually unbiased bases," arXiv preprint arXiv:1708.05181 (2017).
[57] Beatrix C Hiesmayr and Wolfgang Löffler, "Mutually unbiased bases and bound entanglement," Physica Scripta **2014**, 014017 (2014).
[58] Gábor Pataki, "Strong duality in conic linear programming: Facial reduction and extended duals," in *Computational and Analytical Mathematics: In Honor of Jonathan Borwein's 60th Birthday*, edited by David H. Bailey, Heinz H. Bauschke, Peter Borwein, Frank Garvan, Michel Théra, Jon D. Vanderwerff, and Henry Wolkowicz (Springer New York, New York, NY, 2013) pp. 613–634.
[59] Peter J.C. Dickinson, "Geometry of the copositive and completely positive cones," Journal of Mathematical Analysis and Applications **380**, 377 – 395 (2011).
[60] Gábor Pataki, "The geometry of semidefinite programming," in *Handbook of Semidefinite Programming: Theory, Algorithms, and Applications*, edited by Henry Wolkowicz, Romesh Saigal, and Lieven Vandenberghe (Springer US, Boston, MA, 2000) pp. 29–65.
[61] P. Sonneveld, J.J.I.M. van Kan, X. Huang, and C.W. Oosterlee, "Nonnegative matrix factorization of a correlation matrix," Linear Algebra and its Applications **431**, 334 – 349 (2009).

A Proof of Theorem 3.1

Proof. Let us assume that ρ is separable. Since it is symmetric, it admits a convex decomposition into product vectors of the following form:

$$\rho = \sum_i \lambda_i |e_i\rangle|e_i\rangle\langle e_i|\langle e_i|, \tag{46}$$

where λ_i form a convex combination and $|e_i\rangle := \sum_{j=0}^{d-1} e_{ij}|j\rangle$, $e_{ij} \in \mathbb{C}$. It follows that we have the identity

$$\rho = \sum_{i,x_1,x_2,y_1,y_2} \lambda_i e_{i,x_1} e_{i,x_2} e^*_{j,y_1} e^*_{j,y_2} |x_1\rangle|x_2\rangle\langle y_1|\langle y_2| = \sum_{0\le a\le b<d} p_{ab}|D_{ab}\rangle\langle D_{ab}|. \tag{47}$$

By projecting Eq. (47) onto the Dicke basis we obtain the following conditions[11]:

$$\begin{aligned} \langle rr|\rho|rr\rangle &= p_{rr} = \sum_i \lambda_i |e_{ir}|^4 \\ \langle D_{rs}|\rho|D_{rs}\rangle &= p_{rs} = \sum_i \lambda_i 2|e_{ir}|^2|e_{is}|^2. \end{aligned} \tag{48}$$

We can now construct $M(\rho)$, which has the form

$$M(\rho) = \sum_i \lambda_i \begin{pmatrix} |e_{i0}|^4 & |e_{i0}|^2|e_{i1}|^2 & \cdots & |e_{i,0}|^2|e_{i,d-1}|^2 \\ |e_{i0}|^2|e_{i1}|^2 & |e_{i1}|^4 & \cdots & |e_{i,1}|^2|e_{i,d-1}|^2 \\ \vdots & \vdots & \ddots & \vdots \\ |e_{i0}|^2|e_{i,d-1}|^2 & |e_{i1}|^2|e_{i,d-1}|^2 & \cdots & |e_{i,d-1}|^4 \end{pmatrix}. \tag{49}$$

It is clear from Eq. (49) that $M(\rho)$ is CP, as it admits a factorization $M(\rho) = \sum_i \vec{b_i} \cdot \vec{b_i}^T$, where $\vec{b_i}$ is a vector with components

$$\vec{b_i} := \lambda_i^{1/2} \begin{pmatrix} |e_{i0}|^2 & |e_{i1}|^2 & \cdots & |e_{i,d-1}|^2 \end{pmatrix}^T. \tag{50}$$

Clearly, we see from Eq. (50) that $M(\rho)$ is a convex combination of CP matrices, as $b_{ij} \ge 0$. Since CP matrices form a convex cone, $M(\rho)$ is CP. Actually, we can write $M(\rho) = B \cdot B^T$, where $\vec{b_i}$ are the columns of B.

Conversely, let us assume that $M(\rho)$ is CP. Note that, as ρ is DS, $M(\rho)$ is in one-to-one correspondence with ρ. Since $M(\rho)$ is CP, we can write $M(\rho) = B \cdot B^T$, with B being a $d \times k$ matrix fulfilling $B_{ij} \ge 0$. We have to give a separable convex combination of the form of Eq. (46) that produces the DS ρ matching the given $M(\rho)$. As we shall see, this separable decomposition is by no means unique. We begin by writing

$$M(\rho) = \sum_{i=1}^{k} \vec{b_i} \cdot \vec{b_i}^T, \tag{51}$$

where $\vec{b_i}$ are the columns of B, so all the coordinates of $\vec{b_i}$ are non-negative. Let $\{z_{ij}\}_{ij}$ be a set of complex numbers satisfying $|z_{ij}|^2 = (\vec{b_i})_j \ge 0$ and let us define

$$|z_i\rangle := \sum_{0\le j<d} z_{ij}|j\rangle. \tag{52}$$

Note that if we naively make the convex combination Eq. (46) with the vectors introduced in Eq. (52), we shall produce a state with the corresponding $M(\rho)$, but it will not be DS in general. In order

[11] There are, of course, more conditions that follow from Eq. (47), such as $\sum_i \lambda_i (e_{ir})^2 (e^*_{is})^2 = 0$, but we do not need them for this implication.

to ensure that the ρ we are going to construct is DS we have to build it in a way that we eliminate all unwanted coherences. To this end, let us consider the more general family of vectors

$$|\zeta_{i,j,\mathbf{k}}\rangle := \sum_{0\leq l<d} (-1)^{k_l}\omega^{jl} z_{il}|l\rangle, \qquad 0\leq j<d, \quad 0\leq \mathbf{k}<2^d, \tag{53}$$

where k_l is the l-th digit of $\mathbf{k}$ in base 2 and ω is a primitive $2d-$th root of the unity (for instance, $\omega = \exp(2\pi\mathbb{i}/2d)$). Let us now construct the (unnormalized) quantum state

$$\rho_i = \sum_{0\leq j<d}\sum_{0\leq \mathbf{k}<2^d} |\zeta_{i,j,\mathbf{k}}\rangle|\zeta_{i,j,\mathbf{k}}\rangle\langle\zeta_{i,j,\mathbf{k}}|\langle\zeta_{i,j,\mathbf{k}}|. \tag{54}$$

By expanding Eq. (54) we obtain

$$\rho_i = \sum_{j,\mathbf{k},l_1,l_2,l_3,l_4} (-1)^{k_{l_1}+k_{l_2}+k_{l_3}+k_{l_4}}\omega^{j(l_1+l_2-l_3-l_4)} z_{i,l_1}z_{i,l_2}z^*_{i,l_3}z^*_{i,l_4}|l_1,l_2\rangle\langle l_3,l_4|, \tag{55}$$

which we can rewrite as

$$\rho_i = \sum_{0\leq l_1,l_2,l_3,l_4<d} z_{i,l_1}z_{i,l_2}z^*_{i,l_3}z^*_{i,l_4}|l_1,l_2\rangle\langle l_3,l_4| \left(\sum_{0\leq\mathbf{k}<2^d}(-1)^{k_{l_1}+k_{l_2}+k_{l_3}+k_{l_4}}\right)\left(\sum_{0\leq j<d}\omega^{j(l_1+l_2-l_3-l_4)}\right). \tag{56}$$

Let us inspect the possible values for the sums in parenthesis in Eq. (56). The expression involving $\mathbf{k}$ will be zero whenever l_1, l_2, l_3, l_4 are all different (half of the sum will come with a plus sign and the other half with a minus sign). If only two of them are equal, the expression is still zero by the same argument. If two of the indices are equal to the other two, then the value of the expression is 2^d. Hence, we have that

$$\sum_{0\leq\mathbf{k}<2^d}(-1)^{k_{l_1}+k_{l_2}+k_{l_3}+k_{l_4}} = 2^d\left(\delta_{l_1-l_2}\delta_{l_3-l_4}+\delta_{l_1-l_3}\delta_{l_2-l_4}+\delta_{l_1-l_4}\delta_{l_2-l_3}-2\delta_{l_1-l_2}\delta_{l_2-l_3}\delta_{l_3-l_4}\right), \tag{57}$$

where δ_x is the Kronecker Delta function (note that the last term prevents that the case $l_1=l_2=l_3=l_4$ is counted more than once). The second parenthesis in Eq. (56) is a geometrical series, so we have that it is d if, and only if, $l_1+l_2\equiv l_3+l_4 \mod 2d$ (because ω is taken to be primitive); otherwise it is 0. As $0\leq l_1+l_2, l_3+l_4<2d$, this can only happen if $l_1+l_2=l_3+l_4$. Thus,

$$\sum_{0\leq j<d}\omega^{(l_1+l_2-l_3-l_4)j} = d\delta_{l_1+l_2-(l_3+l_4)}. \tag{58}$$

By inserting Eqs. (57, 58) into Eq. (56), we have that the only possible values for (l_1,l_2,l_3,l_4) are (l_1,l_1,l_1,l_1), (l_1,l_2,l_1,l_2) and (l_1,l_2,l_2,l_1) (with $l_1\neq l_2$). Note that Eq. (58) forbids the combination (l_1,l_1,l_2,l_2) if $l_1\neq l_2$. This leads to

$$\rho_i = d2^d\sum_{0\leq l_1\neq l_2<d}|z_{i,l_1}|^2|z_{i,l_2}|^2(|l_1,l_2\rangle\langle l_1,l_2|+|l_1,l_2\rangle\langle l_2,l_1|)+d2^d\sum_{0\leq l_1<d}|z_{i,l_1}|^4|l_1,l_1\rangle\langle l_1,l_1|. \tag{59}$$

By expressing Eq. (59) in the Dicke basis, we have that ρ_i is DS:

$$\rho_i = d2^d\sum_{0\leq x<y<d}2|z_{i,x}|^2|z_{i,y}|^2|D_{xy}\rangle\langle D_{xy}|+d2^d\sum_{0\leq x<d}|z_{i,x}|^4|D_{xx}\rangle\langle D_{xx}|. \tag{60}$$

Eq. (60) implies that $M(\rho_i)$ is

$$M(\rho_i) = d2^d\vec{b_i}\cdot\vec{b_i}^T. \tag{61}$$

Therefore, the convex combination that we seek is

$$\rho = \frac{1}{d2^d||M(\rho)||_1}\sum_{0\leq j<d}\sum_{0\leq\mathbf{k}<2^d}|\zeta_{i,j,\mathbf{k}}\rangle^{\otimes 2}\langle\zeta_{i,j,\mathbf{k}}|^{\otimes 2}, \tag{62}$$

where $||.||_1$ is the entry-wise 1-norm (the sum of the absolute values of all the matrix entries). If $M(\rho)$ comes from a quantum state, then $||M(\rho)||_1=1$. Eq. (62) proves that the state ρ corresponding to $M(\rho)$ is separable.

□

B Exposedness

Convex sets are completely determined by their extremal elements (those that cannot be written as a proper convex combination of other elements in the set). An important step in characterizing the extremal elements of convex sets is understanding their facial structure.

Definition B.1. *Given a convex cone $\mathcal{K}$, a face of $\mathcal{K}$ is a subset $\mathcal{F} \subseteq \mathcal{K}$ such that every line segment in the cone with an interior point in $\mathcal{F}$ must have both endpoints in $\mathcal{F}$.*

Note that every extreme ray of $\mathcal{K}$ is a one-dimensional face. To understand the facial structure of cones, one is interested in learning whether $\mathcal{K}$ is facially exposed. Facial exposedness is an important property that is exploited in optimization, allowing to design facial reduction algorithms [58].

Definition B.2. *Let $\mathcal{K}$ be a cone in the space of real, symmetric matrices and let $\mathcal{F} \subseteq \mathcal{K}$ be a non-empty face. $\mathcal{F}$ is defined as an exposed face of $\mathcal{K}$ if, and only if, there exists a non-zero real symmetric matrix A such that*

$$\mathcal{K} \subseteq \{X \ s.\ t.\ X \in M_{\mathbb{R}}(d,d),\ X = X^T,\ \langle A, X\rangle \geq 0\} \tag{63}$$

and

$$\mathcal{F} = \{X \in \mathcal{K} \ s.\ t.\ \langle A, X\rangle = 0\}. \tag{64}$$

Hence, a face is exposed if it is the intersection of the cone with a non-trivial supporting hyperplane.

A cone is facially exposed if all of its faces are exposed. Although every extreme ray of $\mathcal{CP}_d$ is exposed [59], it remains unknown whether $\mathcal{CP}_d$ is facially exposed. In the case of $\mathcal{COP}_d$, the extreme rays corresponding to $|ii\rangle\langle ii|$ are not exposed [59], implying that $\mathcal{PSD}_d + \mathcal{N}_d$ (the set of DEWs for PPTDS states) is not facially exposed. However, the set $\mathcal{DNN}_d$ of PPTDS states is facially exposed, because both $\mathcal{PSD}_d$ and $\mathcal{N}_d$ are facially exposed [60] and the intersection of facially exposed cones is facially exposed.

C Examples and counterexamples

C.1 Every PPTDS state acting on $\mathbb{C}^3 \otimes \mathbb{C}^3$ is separable

In this example, we prove that every PPTDS state ρ acting on $\mathbb{C}^3 \otimes \mathbb{C}^3$ is separable. This follows from Theorem 3.3, which is usually proven [27] invoking results from quadratic non-convex optimization [38]. We prove it here using quantum information tools solely: by building a convex separable decomposition of ρ of the form of Eq. (1). We do this in two steps. First, we provide a three-parameter class of PPTDS states that are separable. Then, by performing a Cholesky decomposition of ρ^Γ we see that ρ can be expressed as a convex combination of the family we introduced, for some parameters. The PPT conditions directly relate to the existence of such a Cholesky decomposition.

Recall that ρ is written as

$$\rho = \sum_{0\leq i\leq j<3} p_{ij} |D_{ij}\rangle\langle D_{ij}|, \tag{65}$$

where $|D_{ii}\rangle = |ii\rangle$ and $|D_{ij}\rangle = (|ij\rangle + |ji\rangle)/\sqrt{2}$ if $i < j$. Short algebra shows that ρ and its partial transpose ρ^Γ have the form

$$\rho = \bigoplus_{0\leq i\leq j<3} (p_{ij})\,, \tag{66}$$

and

$$\rho^\Gamma = \left(\frac{p_{01}}{2}\right) \oplus \left(\frac{p_{01}}{2}\right) \oplus \left(\frac{p_{02}}{2}\right) \oplus \left(\frac{p_{02}}{2}\right) \oplus \left(\frac{p_{12}}{2}\right) \oplus \left(\frac{p_{12}}{2}\right) \oplus M, \tag{67}$$

where

$$M = \begin{pmatrix} p_{00} & p_{01}/2 & p_{02}/2 \\ p_{01}/2 & p_{11} & p_{12}/2 \\ p_{02}/2 & p_{12}/2 & p_{22} \end{pmatrix}. \tag{68}$$

Lemma C.1. *Let $x, y, z \in \mathbb{C}$. Let ω be a primitive third root of the unity: $\omega^3 = 1$. Let us denote $P_{x,y,z} := |\psi_{x,y,z}\rangle\langle\psi_{x,y,z}|$, where $|\psi_{x,y,z}\rangle := x|0\rangle + y|1\rangle + z|2\rangle$ (we do not normalize $|\psi_{x,y,z}\rangle$). Let us further define*

$$Q_{x,y,z} := P^{\otimes 2}_{x,y,z} + P^{\otimes 2}_{x,\omega y,\omega^2 z} + P^{\otimes 2}_{x,\omega^2 y,\omega z}. \tag{69}$$

Then, the unnormalized quantum state

$$\sigma_{x,y,z} := \frac{1}{12}\left(Q_{x,y,z} + Q_{-x,y,z} + Q_{x,-y,z} + Q_{x,y,-z}\right) \tag{70}$$

is diagonal symmetric. (Obviously it is PPT, as it is separable). Furthermore, its expression in Eq. (65) corresponds to

$$\begin{cases} p_{00} &= |x|^4 \\ p_{01} &= 2|x|^2|y|^2 \\ p_{02} &= 2|x|^2|z|^2 \\ p_{11} &= |y|^4 \\ p_{12} &= 2|y|^2|z|^2 \\ p_{22} &= |z|^4 \end{cases}, \tag{71}$$

where $|\cdot|$ denotes the complex modulus.

Proof. The proof follows from expressing $\sigma_{x,y,z}$ in the computational basis. After some elementary algebra, one arrives at the form of Eq. (65).

□

The following Lemma allows us to find a decomposition of a positive semi-definite matrix A of the form $A = B \cdot B^T$. To this end, we apply Cholesky's decomposition.

Lemma C.2. *Let A be a real, symmetric, positive-semidefinite 3×3 matrix given by*

$$A = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}. \tag{72}$$

Then, A's Cholesky decomposition can be written as

$$\begin{aligned} A = \frac{1}{a}(a,b,c)^T(a,b,c) + \frac{1}{a\begin{vmatrix} a & b \\ b & d \end{vmatrix}} \left(0, \begin{vmatrix} a & b \\ b & d \end{vmatrix}, \begin{vmatrix} a & c \\ b & e \end{vmatrix}\right)^T \left(0, \begin{vmatrix} a & b \\ b & d \end{vmatrix}, \begin{vmatrix} a & c \\ b & e \end{vmatrix}\right) \\ + \frac{1}{\begin{vmatrix} a & b \\ b & d \end{vmatrix} \det A}(0,0,\det A)^T(0,0,\det A). \end{aligned} \tag{73}$$

Proof. The idea of the proof is to use the rank-1 matrix $A_1 := (a,b,c)^T(a,b,c)/a$ to fix the elements of A that lie on the first column and first row. Then, the second summand will adjust the elements of the second row, second column of A and the last summand will fix the bottom-right element of A. Therefore, we have

$$A_1 = \begin{pmatrix} a & b & c \\ b & \cdot & \cdot \\ c & \cdot & \cdot \end{pmatrix}, \tag{74}$$

where the $\cdot$ are terms that are not yet fixed. When we add the second term to A_1 we have

$$A_2 = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & \cdot \end{pmatrix}, \tag{75}$$

and adding the last term to A_2 we recover A.

□

Now we have the tools to prove that every DNN 3×3 matrix is CP:

Lemma C.3. *If A is a 3×3 positive-semidefinite matrix, and it is entry-wise non-negative, then there exists a Cholesky decomposition of A with non-negative vectors (i.e., the vectors' coordinates are non-negative).*

Proof. The only problematic term in Eq (73) is $\begin{vmatrix} a & c \\ b & e \end{vmatrix}$ as all the other expressions are either principal minors of A or entries of A, so they are non-negative. Recall that the Cholesky decomposition of A picks an order of rows, but this is arbitrary; it could be done in any order. Just to illustrate it, if we reorder the columns and rows of A then we have that all the possibilities are

$$\left\{ \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}, \begin{pmatrix} a & c & b \\ c & f & e \\ b & e & d \end{pmatrix}, \begin{pmatrix} d & b & e \\ b & a & c \\ e & c & f \end{pmatrix}, \begin{pmatrix} d & e & b \\ e & f & c \\ b & c & a \end{pmatrix}, \begin{pmatrix} f & c & e \\ c & a & b \\ e & b & d \end{pmatrix}, \begin{pmatrix} f & e & c \\ e & d & b \\ c & b & a \end{pmatrix} \right\}. \tag{76}$$

Hence, the corresponding minors that could be negative are

$$\left\{ \begin{vmatrix} a & c \\ b & e \end{vmatrix}, \begin{vmatrix} d & e \\ b & c \end{vmatrix}, \begin{vmatrix} f & e \\ c & b \end{vmatrix} \right\}. \tag{77}$$

If any of the numbers in (77) is non-negative, then we can pick the Cholesky decomposition for that particular order and we obtain the result. The alternative is that all of them are strictly negative. We are going to see now that this would contradict the fact that $A \succeq 0$.

Note that all the numbers in (77) being strictly negative imply that $d > 0$. Otherwise, if $d = 0$, since $A \succeq 0$, this would imply that $b = e = 0$. Then, all the numbers in (77) would be zero. Therefore, d must be strictly positive. Similarly, $b > 0$. Otherwise, if $b = 0$, then we would have $cd < 0$ and $ae < 0$, contradicting the fact that A is entry-wise non-negative. Therefore, $b > 0$.

It is sufficient to find a contradiction just with a subset of the conditions given by (77): Let us assume that $ae < bc$ and $cd < be$. Then, we have that

$$aed < bcd < b^2 e, \tag{78}$$

where we used $ae < bc$ and $d > 0$ in the first inequality and $cd < be$ and $b > 0$ in the second. Therefore, $aed < b^2 e$. Hence, it must be that $e > 0$ (otherwise we would have $0 < 0$). Then, we deduce that $ad < b^2$, but this directly contradicts $A \succeq 0$, as the latter implies $ad \geq b^2$.

□

Now we have the necessary tools to prove the result claimed in the example.

Consider ρ to be a PPTDS state. Then, we have that $p_{ij} \geq 0$ and $M \succeq 0$. We want to write ρ as a convex combination of some elements $\sigma_{x,y,z}$ introduced in Lemma C.1 by appropriately picking x, y, z as functions of p_{ij}. Observe that for all $x, y, z \in \mathbb{C}$, the entries of $\sigma_{x,y,z}$ will be non-negative. Moreover, the matrix M associated to $\sigma_{x,y,z}$ is

$$M_\sigma = \begin{pmatrix} |x|^4 & |x|^2|y|^2 & |x|^2|z|^2 \\ |x|^2|y|^2 & |y|^4 & |y|^2|z|^2 \\ |x|^2|z|^2 & |y|^2|z|^2 & |z|^4 \end{pmatrix}, \tag{79}$$

which has rank 1, and it is generated as $M_\sigma = (|x|^2, |y|^2, |z|^2)^T (|x|^2, |y|^2, |z|^2)$. Hence, the idea is to relate M_σ to each element of the Cholesky decomposition Eq. (73) so that their sum gives the

original M. If we recover the given M, we automatically recover ρ and we have a separable convex decomposition of it. This can be done if, and only if, the components of the vectors appearing in Eq. (73) are non-negative, because we can always find numbers $x, y, z \in \mathbb{C}$ realizing them.

Let us then apply Lemma C.2 to M_σ: We want to generate $\rho = \lambda_0 \sigma_{x_0,y_0,z_0} + \lambda_1 \sigma_{x_1,y_1,z_1} + \lambda_2 \sigma_{x_2,y_2,z_2}$. We begin by picking

$$\lambda_0 = \frac{1}{p_{00}}, \qquad (x_0, y_0, z_0) = (\sqrt{p_{00}}, \sqrt{p_{01}/2}, \sqrt{p_{02}/2}).$$

All the components are non-negative by hypothesis. Let us now move to (x_1, y_1, z_1). We now pick

$$\lambda_1 = \frac{1}{p_{00}(p_{00}p_{11} - p_{01}^2/4)}, \qquad (x_1, y_1, z_1) = \left(0, \sqrt{p_{00}p_{11} - p_{01}^2/4}, \sqrt{p_{00}p_{12}/2 - p_{01}p_{02}/4}\right).$$

In this case $p_{00}p_{11} - p_{01}^2/4 \geq 0$ because it is a principal minor of M. So, $\lambda_1 \geq 0$ and $y_1 \geq 0$. However, z_1 might need to be negative. We deal with this case at the end.

Finally, we consider (x_2, y_2, z_2). Now we have

$$\lambda_2 = \frac{1}{(p_{00}p_{11} - p_{01}^2/4)\det M}, \qquad (x_2, y_2, z_2) = \left(0, 0, \sqrt{\det M}\right).$$

Here it is easy to see that $\lambda_2 \geq 0$ and $z_2 \geq 0$.

The proof is finished if we can argue that z_1 can be taken to be a positive number. This is guaranteed by Lemma C.3, which tells us that there exists always a relabeling of the computational basis elements $|0\rangle$, $|1\rangle$ and $|2\rangle$ such that the Cholesky decomposition of M is done with non-negative vectors.

C.2 An example of a PPTDS entangled state acting on $\mathbb{C}^6 \otimes \mathbb{C}^6$.

We now present an example for $d = 6$ that constitutes an unnormalized PPTDS entangled state. This is based on a counterexample that appeared in the context of financial engineering [61].

Let $p_{ii} = 2, p_{i,i+1} = 3, p_{i,i+2} = 1, p_{i,i+3} = 0, p_{i,i+4} = 1, p_{i,i+5} = 3$. This means that the matrix M takes the form

$$M = \begin{pmatrix} 2 & 3/2 & 1/2 & 0 & 1/2 & 3/2 \\ 3/2 & 2 & 3/2 & 1/2 & 0 & 1/2 \\ 1/2 & 3/2 & 2 & 3/2 & 1/2 & 0 \\ 0 & 1/2 & 3/2 & 2 & 3/2 & 1/2 \\ 1/2 & 0 & 1/2 & 3/2 & 2 & 3/2 \\ 3/2 & 1/2 & 0 & 1/2 & 3/2 & 2 \end{pmatrix}. \tag{80}$$

Observe that M is a circulant matrix. More importantly, M factorizes as $M = Z^T \cdot Z$, where

$$Z = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & \sqrt{3}/2 & \sqrt{3}/2 & 0 & -\sqrt{3}/2 & -\sqrt{3}/2 \\ 1 & 1/2 & -1/2 & -1 & -1/2 & 1/2 \end{pmatrix}. \tag{81}$$

Note that this proves that ρ is PPT. The matrix M does not admit a non-negative matrix factorization [61], so we cannot apply the separable decomposition of the $3 \otimes 3$ case.

The matrix M has rank 3 and its kernel is given by three vectors orthogonal to Z, which are

$$\begin{pmatrix} 1 & 0 & 0 & -1 & 2 & -2 \\ 0 & 1 & 0 & -2 & 3 & -2 \\ 0 & 0 & 1 & -2 & 2 & -1 \end{pmatrix}. \tag{82}$$

Now we can apply the range criterion to ρ. So, if ρ is separable, there will exist $|\psi\rangle = |\zeta\rangle_A|\zeta\rangle_B$ in the range of ρ such that $|\psi^c\rangle = |\zeta\rangle_A|\zeta^*\rangle_B$ is in the range of ρ^Γ (I assume the same vector $|\zeta\rangle$ on A and B as ρ acts on the symmetric space). As a vector belongs to the range iff it is orthogonal to the kernel, the range criterion implies that, if ρ is separable, then the system of equations imposed by $|\psi\rangle \perp \ker\rho$ and $|\psi^c\rangle \perp \ker\rho^\Gamma$ has a non-trivial solution.

Let us parametrize $|\zeta\rangle = \sum_{0\leq i<6} z_i|i\rangle$. Then we have that

$$|\psi\rangle = \sum_{0\leq i,j<6} z_i z_j |ij\rangle \tag{83}$$

and

$$|\psi^c\rangle = \sum_{0\leq i,j<6} z_i z_j^* |ij\rangle. \tag{84}$$

The kernel of ρ is spanned by $|D_{03}\rangle, |D_{14}\rangle$ and $|D_{25}\rangle$, because $p_{i,i+3} = 0$. This gives the equations

$$z_0 z_3 = z_1 z_4 = z_2 z_5 = 0. \tag{85}$$

The kernel of ρ^Γ is given by the vectors $|i, i+3\rangle$ and $|i+3, 3\rangle$, and the vectors in the kernel of M, in the appropriate basis. The first ones introduce redundant equations

$$z_0 z_3^* = z_1 z_4^* = z_2 z_5^* = 0. \tag{86}$$

So all the important information comes from the kernel of M. This means that

$$\begin{aligned}
(\langle 00| - \langle 33| + 2\langle 44| - 2\langle 55|)|\psi^c\rangle = 0 \\
(\langle 11| - 2\langle 33| + 3\langle 44| - 2\langle 55|)|\psi^c\rangle = 0 \\
(\langle 22| - 2\langle 33| + 2\langle 44| - \langle 55|)|\psi^c\rangle = 0
\end{aligned} \tag{87}$$

It follows that the above system can be compacted as

$$\begin{pmatrix} |z_0|^2 \\ |z_1|^2 \\ |z_2|^2 \end{pmatrix} = \begin{pmatrix} 1 & -2 & 2 \\ 2 & -3 & 2 \\ 2 & -2 & 1 \end{pmatrix} \begin{pmatrix} |z_3|^2 \\ |z_4|^2 \\ |z_5|^2 \end{pmatrix}. \tag{88}$$

There are a few cases to consider now, to include the conditions $z_0 z_3 = z_1 z_4 = z_2 z_5 = 0$:

- If $z_3 = z_4 = z_5 = 0$, then the above system implies $z_0 = z_1 = z_2 = 0$.
- Conversely, as the 3×3 matrix in Eq. (88) is invertible (actually, it is its own inverse), if $z_0 = z_1 = z_2 = 0$, then the above system implies $z_3 = z_4 = z_5 = 0$.
- If two of the numbers in $\{z_3, z_4, z_5\}$ are zero (then one number in $\{z_0, z_1, z_2\}$ is also zero) we have that the system becomes of the following form (for instance, for the case $z_0 = z_4 = z_5 = 0$)

$$\begin{pmatrix} 0 \\ |z_1|^2 \\ |z_2|^2 \end{pmatrix} = |z_3|^2 \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix}. \tag{89}$$

  This also implies that $z_3 = 0$, which implies that $z_1 = z_2 = 0$.
- The remaining case is that one of the numbers in $\{z_3, z_4, z_5\}$ are zero and two of the numbers of $\{z_0, z_1, z_2\}$ are zero. By inverting Eq. (88), this reduces to the previous case.

Hence, the only solution to the above system of equations is that $z_0 = z_1 = z_2 = z_3 = z_4 = z_5 = 0$. This does not give a valid quantum state. Hence, there does not exist a quantum state ψ with the properties required by the range criterion. Consequently, ρ is entangled.

D Proofs and examples for Section 4

D.1 Example of an entangled PPTDS state for $d = 5$.

Example for $d = 5$ would be [42]

$$\hat{M}(\rho) = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 2 & 1 & 0 & 0 \\ 0 & 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 2 & 1 \\ 1 & 0 & 0 & 1 & 6 \end{pmatrix}. \tag{90}$$

In this case, $\ker \hat{M}(\rho) = \{\vec{0}\}$, so to apply the Range criterion one needs to subtract some rank-1 projectors, which are $3/16\vec{v_1}\vec{v_1}^T + 1/16\vec{v_2}\vec{v_2}^T$, where $\vec{v_1}^T = (1, 0, 0, 0, 1)$ and $\vec{v_2} = (1, 0, 0, 0, 9)$. Equivalently, we can use the Horn matrix as an EW to certify entanglement $\mathrm{Tr}(H(\hat{M}(\rho) - 3/16\vec{v_1}\vec{v_1}^T - 1/16\vec{v_2}\vec{v_2}^T)) = -1 < 0$.

D.2 Proof of Theorem 4.1

Proof. Let us rewrite $\rho = \tilde{\rho} + \varepsilon I$, where $\tilde{\rho} = \rho - \varepsilon I$. Let us make the following observations:

1. $\tilde{\rho}$ is a legitimate DS matrix: $\tilde{\rho}_{ij} \geq 0$. This comes from the fact that $\tilde{\rho}_{ij} = \rho_{ij} - \varepsilon$ and the first hypothesis is precisely $\rho_{ij} - \varepsilon \geq 0$.

2. $\tilde{\rho}$ is PPT. Since $\tilde{\rho}_{ij} \geq 0$, the only remaining condition to prove is that $\tilde{M}(\rho) \succeq 0$. Note that $\tilde{M}(\rho) = M(\rho) - d\varepsilon|u\rangle\langle u|$. We want to prove that, for any vector $|v\rangle$, we have that $\langle v|(M - \varepsilon d|u\rangle\langle u|)|v\rangle \geq 0$. Note that, since $|u\rangle \in \mathcal{R}(M(\rho))$, there exists $|\Psi\rangle$ such that $|u\rangle = M(\rho)|\Psi\rangle$. Therefore, we can write $\langle v|u\rangle\langle u|v\rangle = |\langle v|\sqrt{M(\rho)}\frac{1}{\sqrt{M(\rho)}}|u\rangle|^2$ and, by virtue of Cauchy-Schwarz inequality, $\langle v|u\rangle\langle u|v\rangle \leq \langle v|M(\rho)|v\rangle\langle u|\frac{1}{M(\rho)}|u\rangle$. Note that the positive semi-definiteness of $M(\rho)$ allows us to pick a square root such that $\sqrt{M(\rho)} \succeq 0$. Thus, we have that

$$\langle v|M(\rho)|v\rangle \geq \langle v|u\rangle\langle u|v\rangle(\langle u|\frac{1}{M(\rho)}|u\rangle)^{-1} \geq \langle v|u\rangle\langle u|v\rangle d\varepsilon, \tag{91}$$

   which yields the result $\langle v|\tilde{M}(\rho)|v\rangle \geq 0$ for all $|v\rangle$.

3. A sufficient condition for a real symmetric non-negative matrix to be completely positive is that it is diagonally dominant [52]. Therefore, if we prove that $\tilde{M}(\rho)$ is diagonally dominant, the associated $\tilde{\rho}$ will be a DS separable state. This is guaranteed by the third hypothesis:

$$\tilde{\rho}_{ii} = \rho_{ii} - \varepsilon \geq \sum_{j \neq i} \rho_{ji} - (d-1)\varepsilon = \sum_{j \neq i} \tilde{\rho}_{ji}.$$

   Hence, ρ is separable.

□

D.3 An example for Theorem 4.1

Let us construct an example to show that $\mathcal{CP}_d \setminus \mathcal{DD}_d \neq \emptyset$ and then show how to guarantee separability using Theorem 4.1.

Consider the case of a DS state ρ that takes the form

$$\rho = \sum_{i=0}^{d-1} \alpha|ii\rangle\langle ii| + \sum_{0 \leq i < j < d} 2\beta|D_{ij}\rangle\langle D_{ij}| \tag{92}$$

and coefficients $\alpha, \beta \in \mathbb{R}_{\geq 0}$. Normalization imposes the constraint $d\alpha + d(d-1)\beta = 1$.
Let us choose α and β in such a way that $M(\rho)$ lies in the line segment between $M(I)$ and $M(\tilde{\rho})$; *i.e.*, it is a convex combination of the following form:

$$M(\rho) = \lambda M(\tilde{\rho}) + (1-\lambda)M(I) \text{ for } 0 \leq \lambda \leq 1, \tag{93}$$

where $M(I)$ is an extremal of $\mathcal{CP}_d$, with the rank-1 state I defined as in Lemma 4.1, and $M(\tilde{\rho})$ has the same form as $M(\rho)$ but with coefficients $\tilde{\alpha}, \tilde{\beta}$ chosen as $\tilde{\alpha} = (d-1)\tilde{\beta}$ which corresponds to the limit where $M(\rho)$ becomes $\mathcal{DD}_d$. Together with the normalization constraint, one obtains $\tilde{\alpha} = (2d)^{-1}$ and $\tilde{\beta} = (2d(d-1))^{-1}$.

Therefore, by construction, any choice of $\lambda \in [0, 1)$ will yield a state with associated $M(\rho)$ being $\mathcal{CP}_d \setminus \mathcal{DD}_d$.

Now let's proceed to show how to guarantee separability of ρ by virtue of Theorem 4.1 given a two-qudit PPTDS state ρ. Take, for instance, (93) with $\lambda = 1/2$ resulting in $M(\rho) = 1/2(M(\tilde{\rho}) + M(I))$ (which is in $\mathcal{CP}_d \setminus \mathcal{DD}_d$ by construction. To guarantee separability using Theorem 4.1, we are going to find a decomposition $\rho = \tilde{\rho} + \epsilon I$ showing that there exists an ε that fulfils the conditions of the theorem (we are going to assume $d \geq 5$).
Condition 1 gives an upper bound given by $\varepsilon \leq \min\{\alpha, \beta\} = \alpha = \frac{d+2}{4d^2}$. Condition 2 gives a more restrictive upper bound

$$\varepsilon \leq \frac{1}{d}(\langle u| \frac{1}{M(\rho)} |u\rangle)^{-1} = \frac{\alpha + (d-1)\beta}{d} = 1/d^2, \tag{94}$$

where the pseudoinverse can be found via the Sherman-Morrison formula (because of the particular form of Eq. (92)). Finally condition 3 gives the lower bound

$$\varepsilon \geq \frac{\beta(d-1) - \alpha}{(d-2)} = \frac{d-1}{4d^2(d-2)}. \tag{95}$$

Therefore, we have certified the separability of ρ since we can find the desired decomposition $\rho = \tilde{\rho} + \epsilon I$ for all $\varepsilon \in [\frac{d-1}{4d^2(d-2)}, \frac{1}{d^2}]$.

D.4 Proof of Lemma 4.2

Proof. Let $|e(\vec{\varphi})\rangle = \sum_{i=0}^{d-1} \sqrt{x_i/||\mathbf{x}||_1} e^{\mathrm{i}\varphi_i} |i\rangle$. A separable decomposition of $I_{\mathbf{x}}$ is given by

$$I_{\mathbf{x}} = \int_{[0,2\pi]^d} \frac{\mathrm{d}\vec{\varphi}}{(2\pi)^d} (|e(\vec{\varphi})\rangle\langle e(\vec{\varphi})|)^{\otimes 2}. \tag{96}$$

Indeed, note that

$$\begin{aligned} I_{\mathbf{x}} &= \sum_{ijkl} |ij\rangle\langle kl| \int_{[0,2\pi]^d} \frac{\mathrm{d}\vec{\varphi}}{(2\pi)^d} \frac{\sqrt{x_i x_j x_k x_l}}{||\mathbf{x}||_1^2} e^{\mathrm{i}(\varphi_i + \varphi_j - \varphi_k - \varphi_l)} \\ &= \sum_{ijkl} |ij\rangle\langle kl| \frac{\sqrt{x_i x_j x_k x_l}}{||\mathbf{x}||_1^2} (\delta_{i,k}\delta_{j,l} + \delta_{i,l}\delta_{j,k} - \delta_{i,j,k,l}), \end{aligned} \tag{97}$$

where δ is the Kronecker delta function. □

D.5 Proof of Theorem 4.2

Proof. We write $\rho = (1-\lambda)\tilde{\rho} + \lambda I_{\mathbf{x}}$. Therefore, we have that

$$M(\tilde{\rho}) = \frac{1}{1-\lambda}(M(\rho) - \lambda M(I_{\mathbf{x}})). \tag{98}$$

Our goal is to prove that $M(\tilde{\rho})$ is completely positive. Therefore, $M(\rho)$ will also be completely positive and ρ will be a separable quantum state.

1. We start by showing that $M(\tilde{\rho})$ is non-negative component-wise. Indeed, we have that

$$(M(\tilde{\rho}))_{ij} = \frac{1}{1-\lambda}((M(\rho))_{ij} - \lambda(M(I_{\mathbf{x}}))_{ij}) \geq \frac{1}{1-\lambda}((M(\rho))_{ij} - \frac{(M(\rho))_{ij}||\mathbf{x}||_1^2}{x_i x_j}(M(I_{\mathbf{x}}))_{ij}) = 0, \tag{99}$$

because $(M(I_{\mathbf{x}}))_{ij} = \frac{x_i x_j}{||\mathbf{x}||_1^2}$.

2. Now we show that $M(\tilde{\rho})$ is positive semi-definite. This means that $\langle v|M(\tilde{\rho})|v\rangle \geq 0$ for every $|v\rangle$. Since we assume that $1-\lambda > 0$, it suffices to check that $\langle v|(M(\rho) - \lambda M(I_{\mathbf{x}}))|v\rangle \geq 0$ holds. Recall that $\langle v|M(I_{\mathbf{x}})|v\rangle = |\langle v|u_{\mathbf{x}}\rangle|^2$. Since $|u_{\mathbf{x}}\rangle \in \mathcal{R}(M(\rho))$, it means that $\langle u_{\mathbf{x}}|M(\rho)|u_{\mathbf{x}}\rangle > 0$ and therefore $\langle u_{\mathbf{x}}|\frac{1}{M(\rho)}|u_{\mathbf{x}}\rangle > 0$. Therefore, we can apply the Cauchy-Schwarz inequality to $\langle v|M(I_{\mathbf{x}})|v\rangle$ and obtain

$$\langle v|u_{\mathbf{x}}\rangle\langle u_{\mathbf{x}}|v\rangle = |\langle v|\sqrt{M(\rho)}\frac{1}{\sqrt{M(\rho)}}|u_{\mathbf{x}}\rangle|^2 \leq \langle v|M(\rho)|v\rangle\langle u_{\mathbf{x}}|\frac{1}{M(\rho)}|u_{\mathbf{x}}\rangle. \tag{100}$$

Note that the positive semi-definiteness of $M(\rho)$ enables us to choose a square root branch of $M(\rho)$ such that $\sqrt{M(\rho)} \succeq 0$. Therefore, we have that

$$\langle v|(M(\rho) - \lambda M(I_{\mathbf{x}}))|v\rangle \geq \langle v|M(\rho)|v\rangle(1 - \lambda\langle u_{\mathbf{x}}|\frac{1}{M(\rho)}|u_{\mathbf{x}}\rangle) \geq \langle v|M(\rho)|v\rangle(1-1) = 0. \tag{101}$$

3. At this point we have proved that conditions 1 and 2 of the theorem guarantee that $M(\tilde{\rho})$ is doubly non-negative. The third condition will guarantee that it is diagonal dominant. In order to show

$$(M(\tilde{\rho}))_{ii} - \sum_{j\neq i}(M(\tilde{\rho}))_{ij} \geq 0 \tag{102}$$

for all i, we note that this can be rewritten as

$$(M(\rho))_{ii} - \sum_{j\neq i}(M(\rho))_{ij} - \lambda\left(\frac{x_i^2}{||\mathbf{x}||_1^2} - \sum_{j\neq i}\frac{x_i x_j}{||\mathbf{x}||_1^2}\right) \geq 0. \tag{103}$$

By adding and subtracting x_i^2 to the parenthesis, we can rearrange the condition we want to prove as

$$(M(\rho))_{ii} - \sum_{j\neq i}(M(\rho))_{ij} - \frac{\lambda x_i}{||\mathbf{x}||_1^2}(2x_i - ||\mathbf{x}||_1) \geq 0, \tag{104}$$

which from this form, the result follows immediately from the fact that our assumption is $\lambda x_i(||\mathbf{x}||_1 - 2x_i) \geq ||\mathbf{x}||_1^2\left[\sum_{j\neq i}(M(\rho))_{ij} - (M(\rho))_{ii}\right]$ for all i.

Therefore, the conditions of the theorem guarantee that we have a diagonal dominant $M(\tilde{\rho})$ that is also doubly non-negative. Since every real symmetric non-negative matrix that is diagonally dominant is completely positive [52], the associated $\tilde{\rho}$ is a separable DS state. Therefore, ρ can be written as a convex combination of separable states; therefore ρ is separable.

□

E Proofs and examples for Section 5

E.1 A four-qubit PPT-entangled symmetric state with a closed analytical form

Following the procedure described in the beginning of Section 5, we have been able to find an example of a four-qubit PPT-entangled symmetric state.

$$\rho = \frac{1}{50\sqrt{7}} \begin{pmatrix} 7\sqrt{7} & & & & \\ & 12\sqrt{7} & & & -2\sqrt{15} \\ & & 12\sqrt{7} & & \\ & & & 12\sqrt{7} & \\ & -2\sqrt{15} & & & 7\sqrt{7} \end{pmatrix}. \tag{105}$$

This state has the same typical ranks as the ones found numerically in [20, 21]; *i.e.*, the rank of ρ is 5, the rank of ρ^{T_A} is 7 (there is one vector in its kernel) and the rank of $\rho^{T_{AB}}$ is 8 (there is another vector in its kernel).

E.2 Proof Lemma 5.1

Proof. Let us start by recalling that a symmetric diagonal state ρ with diagonal elements $\{\lambda'_k\}_{k=0}^N$ and GHZ coherences $o(\sigma)$ is expressed as follows, when acting on $\mathbb{C}^{m+1} \otimes \mathbb{C}^{n-m+1}$:

$$\rho_{k,l}^{i,j} = \lambda_{i+j} s_{n,m}(i,j;k,l)\delta_{i+j=k+l} + \sigma(\delta_{(i,j)=(m,n-m)}\delta_{(k,l)=(0,0)} + \delta_{(i,j)=(0,0)}\delta_{(k,l)=(m,n-m)}), \tag{106}$$

where $\rho_{k,l}^{i,j} = \langle i,j|\rho|k,l\rangle$ and

$$s_{n,m}(i,j;k,l) = \sqrt{\binom{m}{i}\binom{n-m}{j}\binom{m}{k}\binom{n-m}{l}}. \tag{107}$$

Hence, the partial transposition on m qubits is

$$(\rho^{\Gamma_m})_{k,l}^{i,j} = \lambda_{i+l} s_{n,m}(i,l;k,j)\delta_{j-i=l-k} + \sigma(\delta_{(i,j)=(0,n-m)}\delta_{(k,l)=(m,0)} + \delta_{(i,j)=(m,0)}\delta_{(k,l)=(0,n-m)}). \tag{108}$$

The partially transposed state ρ^{Γ_m} decomposes into a direct sum of different blocks, which we shall index by the parameter n. Note that there are $N+1$ solutions to the equation $n = j-i$ with $0 \leq i \leq m$ and $0 \leq j \leq N-m$. Hence, n ranges from $-m$ to $N-m$. The effect of the coherences with strength σ only interferes the $-m$-th and $(N-m)$-th blocks (which would be 1×1 if $\sigma = 0$) joining them into a 2×2 block. This proves Eq. (33). □

E.3 Proof of Lemma 5.2

Proof. With the assumption that the λ_m form a sequence satisfying the above recurrence, we can now easily span the kernel of $B_n^{(m)}$ for $-m+2 \leq n \leq N-m-2$:

$$(\ 0\ \ \ldots\ \ 0\ \ 1\ \ c_1\ \ c_0\ \ 0\ \ \ldots\ \ 0\ )^T \in \ker B_n^{(m)}. \tag{109}$$

Hence, $B_n^{(m)}$ has rank at most 2. Now we prove its rank is 2 and ρ is PPT. We do this by constructing a Cholesky decomposition (or a Gram decomposition) of $B_n^{(m)}$:

Let us define $I_{a,b} := f_m \cdot f_{m+a+b} - f_{m+a}\cdot f_{m+b}$. Let us note that $I_{a,b}$ is independent of m:

$$I_{a,b} = \frac{(\alpha-1)(\beta-1)}{(\alpha-\beta)^2}\alpha^m\beta^m(\alpha^a-\beta^a)(\alpha^b-\beta^b),$$

but let us observe that $\alpha\beta = 1$. Hence,

$$I_{a,b} = \frac{(\alpha-1)(\beta-1)}{(\alpha-\beta)^2}(\alpha^a - \beta^a)(\alpha^b - \beta^b),$$

Since $Z \geq 0$ by definition, we have that $\alpha \geq \beta > 0$. Hence, $I_{a,b} \geq 0$. Furthermore, $I_{a,b} = \sqrt{I_{a,a}I_{b,b}}$.

It now follows that $B_n^{(m)}$ has rank 2 whenever $m > 0$ and it is positive semidefinite, admitting the following Cholesky decomposition $B_n^{(m)} = L_n^{(m)} \cdot (L_n^{(m)})^T$, where

$$(L_n^{(m)})^T = \frac{1}{\sqrt{f_p}} \begin{pmatrix} f_p & f_{p+1} & f_{p+2} & f_{p+3} & \cdots & f_{p+q} \\ \sqrt{I_{0,0}} & \sqrt{I_{1,1}} & \sqrt{I_{2,2}} & \sqrt{I_{3,3}} & \cdots & \sqrt{I_{q,q}} \end{pmatrix}, \tag{110}$$

with $p = 2\max\{0, n\} - n$ and $q = 2(\min\{m, N-m+n\} - \max\{0, n\}) - n$.

We observe that the element on the a-th row, b-th column of $B_n^{(m)}$ corresponds to

$$\begin{aligned}(B_n^{(m)})_b^a &= \frac{1}{f_p}(f_{p+a}f_{p+b} - \sqrt{I_{a,a}I_{b,b}}) = \frac{1}{f_p}(f_{p+a}f_{p+b} - I_{a,b}) \\ &= \frac{1}{f_p}(f_{p+a}f_{p+k} + f_p f_{p+a+b} - f_{p+a}f_{p+b}) = f_{p+a+b} = f_{a+b-n}.\end{aligned} \tag{111}$$

Observe that the property that $I_{a,b}$ is independent of p becomes crucial. □

E.4 Proof of Lemma 5.3

Proof. To calculate the trace of ρ, it will be very useful to note the following identity: $f_p = f_{-p-1}$. Indeed, one can show that

$$f_p - f_{-p-1} = \frac{(1-\alpha)\alpha^{-1-p} + (\alpha-1)\alpha^p + (\beta-1)\beta^{-1-p} + (1-\beta)\beta^p}{\alpha-\beta} = 0,$$

where the last identity easily follows from the property that $\alpha\beta = 1$. Hence, the trace of ρ reduces to the sum

$$\mathrm{Tr}(\rho) = \sum_{k=0}^{2K+1} \binom{2K+1}{k} \lambda_k = \sum_{k=0}^{2K+1} \binom{2K+1}{k} f_{K-k} \tag{112}$$

Let us note the following identity (it easily follows from Newton's binomial and $\beta = \alpha^{-1}$):

$$\sum_{k=0}^{2K+1} \binom{2K+1}{k} \alpha^{K-k} = \alpha^K (1+\beta)^{2K+1}. \tag{113}$$

This allows us to calculate

$$\mathrm{Tr}(\rho) = \sum_{k=0}^{2K+1} \binom{2K+1}{k} \left(\frac{\alpha-1}{\alpha-\beta}\alpha^{K-k} - \frac{\beta-1}{\alpha-\beta}\beta^{K-k}\right) = \frac{\alpha-1}{\alpha-\beta}\alpha^K(1+\beta)^{2K+1} - \frac{\beta-1}{\alpha-\beta}\beta^K(1+\alpha)^{2K+1}. \tag{114}$$

Since $\alpha\beta = 1$, we can express the trace of ρ in terms of α and α^{-1}:

$$\mathrm{Tr}(\rho) = (1+\alpha^{-1})^{2K}\alpha^K + (\alpha^{-1})^K(1+\alpha)^{2K} = 2\alpha^{-K}(1+\alpha)^{2K} = 2[(1+\alpha)(1+\alpha^{-1})]^K = 2[2+\alpha+\alpha^{-1}]^K. \tag{115}$$

Hence, we arrive at the expression we wanted to prove:

$$\mathrm{Tr}(\rho) = 2(2+\alpha+\beta)^K = 2(4+Z)^K. \tag{116}$$

□