Entanglement and the truncated moment problem

F. Bohnet-Waldraff,[1,2] D. Braun,[1] and O. Giraud[2]

[1]*Institut für Theoretische Physik, Universität Tübingen, 72076 Tübingen, Germany*
[2]*LPTMS, CNRS, Université Paris-Sud, Université Paris-Saclay, 91405 Orsay, France*

We map the quantum entanglement problem onto the mathematically well-studied truncated moment problem. This yields a necessary and sufficient condition for separability that can be checked by a hierarchy of semidefinite programs. The algorithm always gives a certificate of entanglement if the state is entangled. If the state is separable, typically a certificate of separability is obtained in a finite number of steps and an explicit decomposition into separable pure states can be extracted.

I. INTRODUCTION

The renewed interest that entanglement theory attracted in the last decades has led to a tremendous amount of new results (see the recent reviews [1–4] and references therein). Still, characterization and detection of multipartite entanglement is largely an open question. For quantum states describing a collection of qubits, the size of the Hilbert space, exponential in the number of qubits, makes the problem daunting. A simpler but still challenging problem is to restrict the question of characterizing entanglement to a smaller set of quantum states, such as for instance symmetric states, which are pure states invariant under permutations of constituents, or mixtures thereof. Symmetric states lie in a Hilbert space of size linear in the number of qubits, which makes the investigation more tractable. Once the symmetric case is understood, it can shed light onto the general case. This is the strategy we follow here, first considering the symmetric case, which is easier to handle and to present from a pedagogical point of view, then extending our results to the fully general nonsymmetric case.

Various results on entanglement for symmetric states have been obtained in the literature [5–9]. For instance, criteria for certifying separability in symmetric mixed states of N qubits were found in Ref. [10]. Separable symmetric N-qubit pure states are always fully separable [11]. They are easily characterized, as there is a one-to-one correspondence between these states and points on the Bloch sphere via the Majorana representation [12]. As detailed in the paper, a symmetric state is separable (that is, it can be written as a convex combination of separable pure states) if and only if it can be associated with a probability distribution on the sphere; this measure then gives the positive weights associated with each separable pure state. A convenient representation to describe symmetric states in terms of symmetric tensors was proposed in Ref. [13], generalizing the Bloch sphere picture of spins-1/2. In terms of this tensor representation, decomposing a state into a convex combination of separable pure states amounts to finding a probability distribution whose lowest-order moments are fixed by the tensor entries. In fact, as we see, the generic problem of finding whether an arbitrary (not necessarily symmetric) multipartite state can be decomposed into product states can be cast into the problem of finding a probability distribution whose lowest-order moments are fixed.

The problem of finding a probability distribution from the knowledge of its moments has been extensively studied in the literature. When only a finite number of moments is known,

the problem is to find a probability distribution compatible with these moments. In the case of multivariate distributions, it corresponds to the so-called truncated moment problem: given a truncated moment sequence (TMS), that is, fixing all moments up to a certain order, is there a probability distribution (or, in mathematical terms, a non-negative measure) whose moments coincide with those of the TMS? When it exists, such a measure is called a representing measure of the TMS. Of practical relevance is the closely related K-TMS problem, where the measure reproducing the fixed moments is constrained to be supported on some compact K.

The nontruncated K-moment problem, where all moments are given, was solved in Ref. [14] in the case where the compact K is semialgebraic (i.e., defined by polynomial inequalities). For the K-TMS problem (and for K semialgebraic), Curto and Fialkow [15] obtained a necessary and sufficient condition for a TMS to admit a representing measure (see Theorem 1 below). In Ref. [16], a semidefinite algorithm was introduced, allowing one to find a representing measure (if it exists), and later generalized to situations where only a subset of moments up to a certain order are known [17]. This algorithm was also used in Ref. [18] to test positivity of linear maps and separability of matrices in relation with the entanglement problem. More details on the history of the TMS problem can be found in Ref. [19].

The goal of the present paper is to show how the separability problem for an arbitrary quantum state can be mapped to the K-TMS problem, and to use results from the TMS literature to elucidate some aspects of entanglement detection and characterization of separability. From an analytical point of view, the mapping allows us to make use of theorems providing necessary and sufficient separability conditions. Numerically, semidefinite programming yields an algorithm to obtain an explicit decomposition of separable states.

The idea of using semidefinite programming to test for entanglement was already proposed in Refs. [20–22] by Doherty, Parrilo, and Spedalieri, and independently in Ref. [23]. In Ref. [21] an algorithm was provided which detects entanglement, but this algorithm never stops if the state is separable. Conversely, the algorithm proposed in Ref. [24] detects separable states but does not certify entanglement. The algorithms in Refs. [20–22] use the concept of "extensions"; i.e., states in a larger Hilbert space are considered, such that their partial trace gives back the original state. By going to larger and larger extensions, a hierarchy of semidefinite

programs (SDPs) arises whose infeasibility at any stage signals that the original state ρ_{AB} is entangled. The authors of [20–22] add the request that the extensions have positive partial transpose (i.e., are "PPT") as a necessary criterion for separability. This additional condition can be implemented at little extra cost in the SDP. Furthermore, they search in the space of "N Bose-symmetric extensions," where the extended state ρ_{AB^N} (besides being positive semidefinite and reproducing $\rho_{AB} = \mathrm{tr}_{B^{N-1}}[\rho_{AB^N}]$) is invariant under projection into the symmetric subspace of B^N. These algorithms were further improved in Refs. [25–28].

The algorithm we propose here gives a unifying mathematical framework that also uses semidefinite programming and extensions, but in a somewhat more abstract way, based on a matrix of moments and a theorem in the theory of moment sequences. It provides an elegant solution of the entanglement problem, and in particular provides a certificate of separability, together with an explicit decomposition into product states if the state is separable. Moreover, it applies to arbitrary quantum state with arbitrary number of constituents and arbitrary symmetries between the subparts and easily accommodates missing data, i.e., incompletely specified states.

After setting up the notations, we define the K-TMS problem (Sec. II), explain the procedures and algorithms allowing us to solve it (Sec. III), and then show explicit numerical results (Sec. IV). In Sec. V we show that, conversely, some solutions of the entanglement problems may shed light on a particular TMS problem. A discussion of the advantages and novelties of our treatment compared to previous algorithms is provided in the conclusions.

II. ENTANGLEMENT AND THE TRUNCATED MOMENT PROBLEM

To familiarize the reader with the notations in this paper, we first consider the case of symmetric states of qubits, since in this case the equations are more compact. After that we explain the general case in the following section.

A. Symmetric qubit case

Multiqubit pure states which are invariant under any permutation of the qubits are called symmetric pure states. Symmetric states are mixtures of symmetric pure states. Such states are formally equivalent to spin states with spin quantum number $j = N/2$, where N is the number of qubits. This connection can be made explicit with the Dicke states defined by

$$\left| D_N^{(k)} \right\rangle = \mathcal{N} \sum_\pi | \underbrace{0 \cdots 0}_{k} \underbrace{1 \cdots 1}_{N-k} \rangle, \tag{1}$$

where $\mathcal{N}$ is a normalization constant and the sum runs over all permutations of the qubits. These states with $k \in \{0, \ldots, N\}$ form a basis of the symmetric subspace of the Hilbert space $\mathbb{C}^{2^N}$ of N qubits. We now introduce a convenient way of representing symmetric states as tensors. For a state ρ, let

$$X_{\mu_1 \mu_2 \cdots \mu_N} = \mathrm{tr}\{\rho \, P_s^\dagger \sigma_{\mu_1} \otimes \cdots \otimes \sigma_{\mu_N} P_s\}, \tag{2}$$

with σ_0 the 2×2 identity matrix, $\sigma_1, \sigma_2, \sigma_3$ the three Pauli matrices, and P_s the projector onto the symmetric subspace

spanned by Dicke states (1). Then ρ can be expanded [13] as

$$\rho = \frac{1}{2^N} X_{\mu_1 \mu_2 \cdots \mu_N} P_s^\dagger \sigma_{\mu_1} \otimes \cdots \otimes \sigma_{\mu_N} P_s \tag{3}$$

(with summation over repeated indices). The tensor $X_{\mu_1 \mu_2 \cdots \mu_N}$ is real and invariant under permutation of indices, and verifies

$$X_{0 \cdots 0} = \mathrm{tr}\rho = 1. \tag{4}$$

In this representation, the tensor associated with a pure separable symmetric state $|\psi_{\mathrm{sep}}\rangle$ of N qubits takes the particularly simple form

$$X_{\mu_1 \mu_2 \cdots \mu_N} = n_{\mu_1} \cdots n_{\mu_N} \tag{5}$$

with $n_0 = 1$ and $\mathbf{n} = (n_1, n_2, n_3)$ the Bloch vector of the individual qubit, $n_1^2 + n_2^2 + n_3^2 = 1$. Note that since the state is invariant under the exchange of qubits, a pure state can only be the tensor product of identical qubits (with same Bloch vector $\mathbf{n}$), and a separable pure symmetric state has to be fully separable [29]. As a consequence, a symmetric state is separable if and only if its tensor representation can be written as

$$X_{\mu_1 \mu_2 \cdots \mu_N} = \sum_j w_j n_{\mu_1}^{(j)} \cdots n_{\mu_N}^{(j)}, \tag{6}$$

with $w_j \geqslant 0$, $n_0^{(j)} = 1$, and each Bloch vector $\mathbf{n}^{(j)}$ normalized to 1. This can be equivalently written in an integral form as

$$X_{\mu_1 \mu_2 \cdots \mu_N} = \int_K x_{\mu_1} x_{\mu_2} \cdots x_{\mu_N} \, d\mu(\mathbf{x}), \tag{7}$$

with $K = \{\mathbf{x} \in \mathbb{R}^3 : x_1^2 + x_2^2 + x_3^2 = 1\}$ the unit sphere, $x_0 = 1$, and $d\mu$ a positive measure on K. Indeed, if Eq. (6) holds then the tensor can be written as in Eq. (7) with

$$d\mu(\mathbf{x}) = \sum_j w_j \delta(\mathbf{x} - \mathbf{n}^{(j)}). \tag{8}$$

Conversely, since the system is finite dimensional, Carathéodory's theorem implies that the integral in Eq. (7) can always be reduced to a finite sum as in Eq. (6), so that the positive measure can always be expressed as a sum of δ functions. Expressing Eq. (7) in words, a symmetric state is separable if and only if there exists a positive measure $d\mu$ such that all entries of the tensor $X_{\mu_1 \mu_2 \cdots \mu_N}$ (for all μ_j, $1 \leqslant j \leqslant N$, and $0 \leqslant \mu_i \leqslant 3$) are given by moments of that measure.

In order to prepare for the generalization to arbitrary states in the next section, let us introduce a more compact notation for Eq. (7). For any N-tuple $(\mu_1, \ldots, \mu_N)$ we define a triplet $\alpha = (\alpha_1, \alpha_2, \alpha_3)$ of integers such that

$$x_{\mu_1} x_{\mu_2} \cdots x_{\mu_N} = x^\alpha, \tag{9}$$

where we use the notation $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} x_3^{\alpha_3}$. So, e.g., for $\alpha = (1, 3, 0)$ we have $x^\alpha = x_1 x_2^3$. The degree of the monomial x^α is denoted $|\alpha| \equiv \sum_i \alpha_i$. We also denote the $X_{\mu_1 \mu_2 \cdots \mu_N}$ by y_α, where α corresponds to $(\mu_1 \mu_2 \cdots \mu_N)$ via Eq. (9), so that, e.g., for $N = 6$, $y_{(2,1,0)} = X_{000112}$. With this notation we can rewrite (7) as

$$y_\alpha = \int_K x^\alpha \, d\mu(\mathbf{x}). \tag{10}$$

To test if a symmetric state is separable, a necessary and sufficient condition is therefore that a positive measure $d\mu$

exists that fulfills Eq. (10) for all $|\alpha| \leqslant N$. Problems of this type are known as *truncated K-moment sequence problems* (or *K*-TMS problems), and they can be solved by a semidefinite relaxation procedure. Before we describe this method in Sec. III we generalize the description to arbitrary states of finite-dimensional systems.

B. General case

Consider a multipartite quantum state ρ acting on the tensor product $\mathcal{H} = \mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)} \otimes \cdots \otimes \mathcal{H}^{(d)}$ of Hilbert spaces $\mathcal{H}^{(i)}$. For each i, let $S_\mu^{(i)}$, $0 \leqslant \mu \leqslant t_i$, be a set of $t_i + 1$ Hermitian matrices forming an orthogonal basis (with respect to the scalar product $\text{tr} A^\dagger B$) of the set of bounded linear operators on $\mathcal{H}^{(i)}$, with the choice that $S_0^{(i)}$ is the identity matrix. An orthogonal basis of $\mathcal{H}$ is then given by matrices

$$S_{\mu_1 \mu_2 \cdots \mu_d} = S_{\mu_1}^{(1)} \otimes S_{\mu_2}^{(2)} \otimes \cdots \otimes S_{\mu_d}^{(d)} \qquad (11)$$

and any state can be written as

$$\rho = \mathcal{N} X_{\mu_1 \mu_2 \cdots \mu_d} S_{\mu_1 \mu_2 \cdots \mu_d}, \qquad (12)$$

where summation over repeated indices is understood, and the normalization constant $\mathcal{N} = \prod_{i=1}^d \mathcal{N}_i$, with $\mathcal{N}_i = 1/\sqrt{t_i + 1}$, is chosen so that $X_{0\cdots 0} = 1$. A quantum state ρ_{sep} is said to be separable (over that particular factorization of $\mathcal{H}$) if it can be written as

$$\rho_{\text{sep}} = \sum_j w_j \, \rho_j^{(1)} \otimes \rho_j^{(2)} \otimes \cdots \otimes \rho_j^{(d)} \qquad (13)$$

with $w_j \geqslant 0$, and $\rho_j^{(i)}$ density matrices acting on $\mathcal{H}^{(i)}$ [30]. Any $\rho^{(i)}$ acting on $\mathcal{H}^{(i)}$ can be expanded as $\rho^{(i)} = \mathcal{N}_i \sum_{\mu_i} y_{\mu_i}^{(i)} S_{\mu_i}^{(i)}$, with $y^{(i)}$ a real $(t_i + 1)$-dimensional vector. The condition $\text{tr} \rho^{(i)} = 1$, together with the choice that $S_0^{(i)}$ is the identity matrix and the normalization, implies that $y_0^{(i)} = 1$.

Rewriting condition (13) in terms of average values, we get that a state is fully separable if and only if all averaged basis operators can be expressed as

$$\langle S_{\mu_1 \mu_2 \cdots \mu_d} \rangle_\rho = \sum_j w_j \langle S_{\mu_1}^{(1)} \rangle_{\rho_j^{(1)}} \langle S_{\mu_2}^{(2)} \rangle_{\rho_j^{(2)}} \cdots \langle S_{\mu_p}^{(d)} \rangle_{\rho_j^{(d)}} \qquad (14)$$

with $w_j \geqslant 0$, i.e., the expectation values of all $S_{\mu_1 \mu_2 \cdots \mu_d}$ are convex combinations of the product of local expectation values. This condition can be reexpressed in terms of the coefficients $X_{\mu_1 \mu_2 \cdots \mu_d}$ of ρ_{sep} in expansion (12) and the coefficients $y_{a_i}^{(i;j)}$, $1 \leqslant a_i \leqslant t_i$, in the expansion $\rho_j^{(i)} = \mathcal{N}_i \sum_{\mu_i} y_{\mu_i}^{(i;j)} S_{\mu_i}^{(i)}$, with $y_0^{(i;j)} = 1$. Separability is then equivalent to the existence of $w_j \geqslant 0$ and real numbers $y_{a_i}^{(i;j)}$, $1 \leqslant a_i \leqslant t_i$, such that for all μ_i with $0 \leqslant \mu_i \leqslant t_i$ one has

$$X_{\mu_1 \mu_2 \cdots \mu_d} = \sum_j w_j \, y_{\mu_1}^{(1;j)} y_{\mu_2}^{(2;j)} \cdots y_{\mu_d}^{(d;j)} \qquad (15)$$

and $\sum_{\mu_i} y_{\mu_i}^{(i;j)} S_{\mu_i}^{(i)} \geqslant 0$ for all i and j. This latter condition comes from the fact that each $\rho_j^{(i)} = \mathcal{N}_i \sum_{\mu_i} y_{\mu_i}^{(i;j)} S_{\mu_i}^{(i)}$ appearing in Eq. (13) is a density matrix and thus has to be positive. Since matrices are Hermitian and thus have all their eigenvalues real, one can use the Descartes sign rule to express this positivity condition as inequalities on the coefficients of

the characteristic polynomial of $\rho_j^{(i)}$. Each of these coefficients is a linear combination of traces of powers of $\rho_j^{(i)}$ and, therefore, a polynomial in the variables $y_\mu^{(i;j)}$. Thus, each vector $\mathbf{y}^{(i;j)} = (y_1^{(i;j)}, \ldots, y_{t_i}^{(i;j)})$ is restricted to a certain compact subset $K^{(i)} \subset \mathbb{R}^{t_i}$ defined by some polynomial inequalities. Defining the compact $K = K^{(1)} \times K^{(2)} \times \cdots \times K^{(d)} \subset \mathbb{R}^n$, $n = \sum_i t_i$, and the vector $\mathbf{y}^{(j)} = (\mathbf{y}^{(1;j)}, \mathbf{y}^{(2;j)}, \ldots, \mathbf{y}^{(d;j)}) \in \mathbb{R}^n$, the positivity condition on the partial density matrices amounts to impose that $\mathbf{y}^{(j)} \in K$ with K a compact defined by polynomial inequalities; e.g., for a qubit the polynomial is a quadratic equation of the Bloch vector, restricting its maximal length to 1. Equation (15) can then be rewritten, for $0 \leqslant \mu_i \leqslant t_i$, as

$$X_{\mu_1 \mu_2 \cdots \mu_d} = \int_K x_{\mu_1}^{(1)} x_{\mu_2}^{(2)} \cdots x_{\mu_d}^{(d)} \, d\mu(\mathbf{x}) \qquad (16)$$

with $x_0^{(i)} = 1$, $\mathbf{x} = (\mathbf{x}^{(1)}, \mathbf{x}^{(2)}, \ldots, \mathbf{x}^{(d)}) \in \mathbb{R}^n$, $\mathbf{x}^{(i)} = (x_a^{(i)})_{1 \leqslant a \leqslant t_i} \in \mathbb{R}^{t_i}$, and $d\mu$ the measure over $\mathbb{R}^n$ defined by

$$d\mu(\mathbf{x}) = \sum_j w_j \, \delta(\mathbf{x} - \mathbf{y}^{(j)}). \qquad (17)$$

Equation (16) is the generalization of the symmetric case in Eq. (7), the difference being that each Hilbert space $\mathcal{H}^{(i)}$ has its own set of variables $(x_a^{(i)})_{1 \leqslant a \leqslant t_i}$. As in the symmetric case, the existence of an arbitrary measure $d\mu(\mathbf{x})$ such that Eq. (16) holds is equivalent to the existence of a "discrete" measure of the form in Eq. (17), since one can apply Carathéodory's theorem to our finite-dimensional Hilbert spaces. The separability problem, for a state given by Eq. (12), is thus equivalent to the question whether a positive measure $d\mu$ with support K exists whose moments coincide with the coordinates $X_{\mu_1 \mu_2 \cdots \mu_d}$ of the state.

We now rewrite Eq. (16) in a more compact form. Let us relabel the entries of $\mathbf{x}$ as $\mathbf{x} = (x_1, x_2, \ldots, x_n)$ and introduce the notation $x^\alpha \equiv \prod_{i=1}^n x_i^{\alpha_i}$, where $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a vector of integers. For instance for two qubits we have $\mathbf{x} = (x_1^{(1)}, x_2^{(1)}, x_3^{(1)}, x_1^{(2)}, x_2^{(2)}, x_3^{(2)}) = (x_1, x_2, \ldots, x_6)$. For any given tuple $(\mu_1, \ldots, \mu_d)$, there exists an index α such that

$$x_{\mu_1}^{(1)} x_{\mu_2}^{(2)} \cdots x_{\mu_d}^{(d)} = x^\alpha. \qquad (18)$$

Thus, α_1 counts the number of $x_1^{(1)}$ in the monomial $x_{\mu_1}^{(1)} x_{\mu_2}^{(2)} \cdots x_{\mu_p}^{(d)}$, α_2 counts the number of $x_2^{(1)}$, and so on until α_d, which counts the number of $x_{t_d}^{(d)}$. For instance for a bipartite state of $d = 2$ qubits, $(\mu_1, \mu_2) = (2,3)$ corresponds to $\alpha = (0,1,0,0,0,1)$ or to the monomial $x_2^{(1)} x_3^{(2)}$, while $(\mu_1, \mu_2) = (1,0)$ corresponds to $\alpha = (1,0,0,0,0,0)$ or to the monomial $x_1^{(1)}$. As each monomial $x_{\mu_1}^{(1)} x_{\mu_2}^{(2)} \cdots x_{\mu_d}^{(d)}$ contains at most one variable of each type $x^{(i)}$, the vector α is such that each tuple $(\alpha_1, \ldots, \alpha_{t_1})$, $(\alpha_{t_1+1}, \ldots, \alpha_{t_1+t_2})$, etc., contains at most one 1. For instance for qubits, where $t_i = 3$, each triplet $(\alpha_{3i+1}, \alpha_{3i+2}, \alpha_{3i+3})$ must therefore contain at most one 1.

If we denote $X_{\mu_1 \mu_2 \cdots \mu_d}$ by y_α, where α is the index corresponding to the tuple $(\mu_1, \ldots, \mu_d)$ via Eq. (18), then Eq. (16) can be simply rewritten as

$$y_\alpha = \int_K x^\alpha \, d\mu(\mathbf{x}). \qquad (19)$$

Hence, a state is separable if and only if all its coordinates y_α can be written as in Eq. (19), with $d\mu$ a positive measure.

C. Examples and special cases

The general setting of the previous section allows one to test separability for a given fixed partition. For example, in order to check full separability for a three-qubit state ρ one has to consider $d = 3$ sets of variables $x_{a_i}^{(i)}$, each set being associated with a qubit (and thus with $1 \leqslant a_i \leqslant 3$), with K being the product of three Bloch spheres. One then relabels the coordinates $X_{\mu_1\mu_2\mu_3}$ of ρ as y_α and the variables as $(x_1, \ldots, x_n)$ with $n = 9$, in order to get Eq. (19). Among all 9-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$, only the 64 values which correspond to some triplet (μ_1, μ_2, μ_3) for $0 \leqslant \mu_i \leqslant 3$ via Eq. (18) have to be considered. The state ρ is separable if and only if there exists a measure $d\mu$ such that Eq. (19) is fulfilled for all these α.

However, if one is only interested in the question of entanglement of the first two qubits with respect to the third one, one would have to take the first two qubits as a four-level system. There would then be two sets of variables in Eq. (16), the first one with $t_1 = 15$ variables (characterizing the density matrix of a four-level system), and the second with $t_2 = 3$ variables (characterizing a mixed qubit state). Thus one has $d = 2$ and $n = 18$ variables. Finding whether or not Eq. (19) can be solved answers the question whether or not the third qubit is entangled with the first two, while ignoring any entanglement between the first two qubits.

It is instructive to see how the symmetric case of Sec. II A can be recovered from the general case. As we saw in Sec. II A, the problem of finding whether a symmetric N-qubit state is fully separable can be cast into the form of Eq. (10), with K the 2-sphere and α running over triplets of integers with $|\alpha| \leqslant N$. Applying the general case to the N-qubit case implies $d = N$ parties, and the Hilbert space $\mathcal{H}$ is decomposed as $\mathcal{H} = \mathcal{H}^{(1)} \otimes \mathcal{H}^{(2)} \otimes \cdots \otimes \mathcal{H}^{(N)}$. Each Hilbert space $\mathcal{H}^{(i)}$ has its own set of variables $x_{a_i}^{(i)}$, $1 \leqslant a_i \leqslant 3$, appearing in the right-hand side of Eq. (16). The basis $S_\mu^{(i)}$ in the decomposition $\rho^{(i)} = \frac{1}{2} \sum_\mu y_\mu^{(i)} S_\mu^{(i)}$ is the Pauli basis, the vectors $(y_a^{(i)})_{1 \leqslant a \leqslant 3}$ are the Bloch vectors, and the compact $K^{(i)}$ such that $\sum_\mu y_\mu^{(i)} S_\mu^{(i)}$ is positive is the Bloch sphere. Symmetry then implies that the variables corresponding to each Hilbert space are not independent but equal, so that one has to require $x_\mu^{(i)} = x_\mu$ for all i and μ, and replace the compact $K^{(1)} \times K^{(2)} \times \cdots \times K^{(d)}$ by $K = K^{(1)}$, a single Bloch sphere. To account for the fact that the different sets of variables should no longer be distinguished, the n-tuple α in Eq. (19) should be replaced by the triplet $(\sum_i \alpha_{3i+1}, \sum_i \alpha_{3i+2}, \sum_i \alpha_{3i+3})$, giving the multiplicities of x_1, x_2, x_3. The entries of the triplet can now take values larger than 1. Since Eqs. (19) and (10) coincide, the symmetric and the general cases are in essence the same problem: the difference between them lies only in the definition of the compact K supporting the measure, and also in the set of tuples α considered.

The general formalism (19) allows us in fact to play with any kind of constraint, just by adjusting the sets of variables and α vectors accordingly. The symmetric case explained above is just one example, but this method is general. For instance if one wants to impose a symmetry between two of the subsystems

one just has to equate the sets of independent variables. This adjustment can be easily generalized to test for entanglement for any type of partition. The algorithms for the truncated moment problem that we present in Sec. III provide a solution to all these cases.

D. Partial knowledge of a state

An interesting question in practical application is whether or not a partial set of measurement results is compatible with a separable state. If for example a state tomography is not carried to its end, or if only local measurements are available, can one in some instances infer that the state was entangled? Another interesting question is whether the partial traces of a state can be used to show entanglement of the global state even if all the reduced states are separable [31].

Such problems of partial knowledge can be formulated in the form of Eq. (19) very simply. The only change is the range of tuples over which α varies: since the unknown measurements correspond to unknown y_α, these values of α should not be taken into account as constraints on $d\mu$. If for example only the results of local measurements are known, only averages of the form $\langle S_0^{(1)} \otimes S_0^{(2)} \otimes \cdots \otimes S_\mu^{(i)} \otimes \cdots \otimes S_0^{(d)} \rangle$ are known (recall that $S_0^{(i)}$ is the identity matrix). Therefore, one only knows the values of y_α such that the $\alpha = (\alpha_1, \ldots, \alpha_n)$ have only one nonzero entry. This problem can then be solved in the same way as the general one, just by putting no constraint on the unknown moments.

III. TMS PROBLEMS: DEFINITIONS AND SOLUTIONS

Identifying the entanglement problem with the K-TMS problem allows us to use analytical results and numerical methods from the TMS literature to get insight in entanglement theory. We now introduce the mathematical formalism used to describe and solve the TMS problem.

A. Truncated moment problems

A TMS of degree d is a finite set of numbers $y = (y_\alpha)_{|\alpha| \leqslant d}$ indexed by n-tuples $\alpha = (\alpha_1, \ldots, \alpha_n)$ of integers $\alpha_i \geqslant 0$ such that $|\alpha| = \sum_i \alpha_i \leqslant d$ [17]. The truncated K-moment problem consists in finding conditions under which there exists a (positive) measure $d\mu$ such that each moment y_α with $|\alpha| \leqslant d$ can be represented as an integral of the form

$$y_\alpha = \int_K x^\alpha \, d\mu(\mathbf{x}) \tag{20}$$

with $\mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{R}^n$, $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}$, and $d\mu$ a measure supported on a semialgebraic set

$$K = \{\mathbf{x} \in \mathbb{R}^n | g_1(\mathbf{x}) \geqslant 0, \ldots, g_m(\mathbf{x}) \geqslant 0\} \tag{21}$$

with $g_i(\mathbf{x})$ multivariate polynomials in the variables $x_1, \ldots, x_n$. If such a measure exists it can be written as the sum of δ functions

$$d\mu(\mathbf{x}) = \sum_{j=1}^r w_j \delta(\mathbf{x} - \mathbf{y}^{(j)}) \tag{22}$$

with some finite r, $w_j > 0$, and $\mathbf{y}^{(j)} \in K$. Such a measure is then called a *finitely atomic representing measure*.

Equation (20) is nothing but Eq. (10), where K is the Bloch sphere, $d = N$, and $n = 3$. Therefore, the entanglement problem for symmetric states is a special case of K-TMS problem.

The $\mathcal{A}K$-TMS problem [17] is a generalization of the K-TMS problem in which moments y_α are known only for a finite subset $\mathcal{A} \subset \mathbb{N}^n$ of indices of degree $|\alpha| \leqslant d$. The only difference with the K-TMS problem is that Eq. (20) now has to be fulfilled only for $\alpha \in \mathcal{A}$. This is exactly the situation found in the general case of Sec. II B. Indeed, in that case, we showed that K is defined by polynomial inequalities, so that it is a semialgebraic compact set. Moreover, only indices associated with some tuple $(\mu_1, \ldots, \mu_d)$ for $0 \leqslant \mu_i \leqslant t_i$ do correspond to a certain moment y_α, so that a restriction on indices α is required. This is also the situation encountered in Sec. II D, where the state is only known partially. All these cases therefore correspond to the $\mathcal{A}K$-TMS problem and can in fact be solved in the same way as the K-TMS problem, only with fewer constraints (since fewer moments are fixed).

In all that follows, to ease notations, we only treat the original K-TMS problem where all moments y_α with $|\alpha| \leqslant d$ are known. However, we must stress that the $\mathcal{A}K$-TMS problem is treated in exactly the same way, just by considering $\alpha \in \mathcal{A}$ rather than $|\alpha| \leqslant d$ in all equations involving that restriction.

B. Moment matrices

Let us now present the mathematical setting for the K-TMS problem defined by Eq. (20). Let $y = (y_\alpha)_{|\alpha| \leqslant d}$ be a TMS of degree d, with $\alpha = (\alpha_1, \ldots, \alpha_n)$ being n-tuples of integers. The integrand on the right-hand side of Eq. (20) is a monomial in n variables $(x_1, \ldots, x_n)$ of degree less than d. Any polynomial of degree less than d can be written as a vector in the basis of monomials ordered in degree-lexicographic order (that is, monomials are sorted by order and within each order in a lexicographic order). For instance for $n = 3$ and $d = 2$ the monomial basis is $\{1, x_1, x_2, x_3, x_1^2, x_1 x_2, x_1 x_3, x_2^2, x_2 x_3, x_3^2\}$, and a polynomial such as, e.g., $p(\mathbf{x}) = 7x_3 - 3x_2^2 + 2$ would be written as the vector $(2, 0, 0, 7, 0, 0, 0, -3, 0, 0)$. The components of the vector representing $p(\mathbf{x})$ are coefficients p_α such that $p(\mathbf{x}) = \sum_\alpha p_\alpha x^\alpha$.

For any integer $k \leqslant d/2$, let $M_k(y)$ be the matrix defined by

$$M_k(y)_{\alpha\beta} = y_{\alpha+\beta}, \quad |\alpha|, |\beta| \leqslant k. \tag{23}$$

It is called the *moment matrix* of order k associated with the TMS y. A necessary condition for a TMS to admit a representing measure as in Eq. (20) is that the moment matrix of any order is positive semidefinite. Indeed, if Eq. (20) holds, then for any vector $p = (p_\alpha)_{|\alpha| \leqslant k}$ representing a polynomial $p(\mathbf{x})$ of degree k or less we have

$$p^T M_k(y) p = \sum_{|\alpha|, |\beta| \leqslant k} p_\alpha y_{\alpha+\beta} p_\beta$$

$$= \sum_{|\alpha|, |\beta| \leqslant k} p_\alpha p_\beta \int_K x^{\alpha+\beta} d\mu(\mathbf{x})$$

$$= \int_K p(\mathbf{x})^2 d\mu(\mathbf{x}) \geqslant 0, \tag{24}$$

so that $M_k(y)$ a is positive-semidefinite matrix [15,16].

Other necessary conditions can be obtained from the polynomial constraints $g_i(\mathbf{x}) \geqslant 0$ which define the set K in Eq. (21). Let us now suppose that the degree d is even. For any polynomial g of degree $\deg(g) \geqslant 1$, one can define a "shifted TMS" of degree $d - \deg(g)$ as

$$(g \star y)_\alpha = \sum_{|\gamma| \leqslant \deg(g)} g_\gamma y_{\alpha+\gamma}, \quad |\alpha| \leqslant d - \deg(g). \tag{25}$$

Let $d_g = \lceil \deg(g)/2 \rceil$ (we denote by $\lceil x \rceil$ the smallest integer larger than or equal to x and by $\lfloor x \rfloor$ the largest integer smaller than or equal to x). Applying definition (23), one can define the $(k - d_g)$th moment matrix of $g \star y$, for any integer k such that $0 \leqslant k - d_g \leqslant (d - \deg(g))/2$, by $M_{k-d_g}(g \star y)_{\alpha\beta} = (g \star y)_{\alpha+\beta}$. This matrix is called the kth-order *localizing matrix* of g [16], defined for even d. In explicit form, it reads

$$M_{k-d_g}(g \star y)_{\alpha\beta} = \sum_{|\gamma| \leqslant \deg(g)} g_\gamma y_{\alpha+\beta+\gamma}, \quad |\alpha|, |\beta| \leqslant k - d_g. \tag{26}$$

Using the fact that $\lfloor (d - \deg(g))/2 \rfloor = d/2 - d_g$, we have that the kth-order localizing matrix is defined for any integer k such that $d_g \leqslant k \leqslant d/2$ (the definition of d_g has been precisely chosen in such a way that the upper bound $k \leqslant d/2$ is the same as that for the kth-order moment matrix). If a TMS admits a representing measure then any kth-order localizing matrix is necessarily positive semidefinite: indeed for any vector $p = (p_\alpha)_{|\alpha| \leqslant k-d_g}$ representing a polynomial $p(\mathbf{x})$ with degree $k - d_g$ or less we have

$$p^T M_{k-d_g}(g \star y) p = \sum_{|\alpha|, |\beta| \leqslant k-d_g} p_\alpha p_\beta \sum_{|\gamma| \leqslant \deg(g)} g_\gamma y_{\alpha+\beta+\gamma}$$

$$= \int_K g(\mathbf{x}) p(\mathbf{x})^2 d\mu(\mathbf{x}) \geqslant 0, \tag{27}$$

which is positive because g is positive on K by definition (21). Another way of seing that is to observe that if y admits a positive representing measure then so does the shifted TMS $g \star y$.

As moment matrices of order k' are submatrices of matrices of order k if $k' \leqslant k$ it suffices to consider the largest possible value for k to get the strongest necessary conditions. For a TMS y of degree d, the above analysis leads to the necessary condition $M_{\lfloor d/2 \rfloor}(y) \geqslant 0$. If the degree d is even and the compact K is defined as in Eq. (21) by polynomial inequalities, the localizing matrices for each polynomial g_i, $1 \leqslant i \leqslant m$, have to be positive, namely, $M_{d/2-d_{g_i}}(g_i \star y) \geqslant 0$, $d_{g_i} = \lceil \deg(g_i)/2 \rceil$.

C. A necessary and sufficient condition

The above conditions are only necessary conditions. A sufficient condition was obtained in [15] for even-degree TMS. We formulate it following Theorem 1.1 of [16]. Namely, if a TMS z of even degree $2k$ is such that its kth-order moment matrix and all kth-order localizing matrices are positive, and if additionally

$$\text{rank} M_k(z) = \text{rank} M_{k-d_0}(z) \tag{28}$$

with $d_0 = \max_{1 \leqslant i \leqslant m}\{1, \lceil \deg(g_i)/2 \rceil\}$, then the TMS z admits a representing measure composed of $r = \text{rank} M_k(z)$ δ functions.

Note that the rank condition already appeared in Ref. [25] under the name rank-loop, using a result from [32].

As the above condition is only sufficient, a TMS y admitting a representing measure does not necessarily fulfill Eq. (28). However, one can search for an extension z of y which fulfills it. An extension of a TMS y of degree d is defined as any TMS z of degree $2k$ with $2k > d$, such that $z_\alpha = y_\alpha$ for all $|\alpha| \leqslant d$. A extension z is called flat if it satisfies Eq. (28). If z verifies the sufficient conditions above, then it has a representing measure, and so does y as a restriction of z. This allows us to formulate the following necessary and sufficient condition for the existence of a representing measure.

Theorem 1 ([15]; see also Theorem 1.2 of [16]). A TMS $(y_\alpha)_{|\alpha| \leqslant d}$ admits a representing measure supported by K if and only if there exists a flat extension $(z_\beta)_{|\beta| \leqslant 2k}$ with $2k > d$ such that $M_k(z) \geqslant 0$, $M_{k-d_{g_i}}(g_i \star z) \geqslant 0$ for $i = 1, \ldots, m$.

This theorem can be implemented as a semidefinite program as shown in Sec. III D. It has been extended to an arbitrary $\mathcal{A}K$ TMS in proposition 3.3 in Ref. [17]. With the identifications made in Sec. II between the entanglement and the TMS problem, these results can be reformulated as a necessary and sufficient condition for separability of an arbitrary quantum state:

Theorem 2. A state ρ is separable if and only if its coordinates $X_{\mu_1 \mu_2 \cdots \mu_d}$ defined in Eq. (12) are mapped to a TMS $(y_\alpha)_{\alpha \in \mathcal{A}}$ such that there exists a flat extension $(z_\beta)_{|\beta| \leqslant 2k}$ with $2k > d$, $M_k(z) \geqslant 0$, and $M_{k-d_{g_i}}(g_i \star z) \geqslant 0$ for $i = 1, \ldots, m$.

D. Semidefinite program and the entanglement problem

For a given TMS $(y_\alpha)_{|\alpha| \leqslant d}$, finding an extension $(z_\beta)_{|\beta| \leqslant 2k}$ as in the theorem above amounts to constructing a positive matrix $M_k(z)_{\alpha\beta} = z_{\alpha+\beta}$ with some entries given, namely, $z_\alpha = y_\alpha$ for $|\alpha| \leqslant d$, and constraints of positivity of moment matrices and localizing matrices, which are linear in the z_α. This type of problem corresponds to what is known in numerical analysis as semidefinite program (SDP) problems. Here, the variables of the SDP are the z_β for $|\beta| \leqslant 2k$. The smallest extension order is $k_0 = \lfloor d/2 \rfloor + 1$. All the constraints of Theorem 1 can be directly implemented in the SDP apart from the flatness condition [Eq. (28)]. If also the flatness condition could be implemented efficiently then $P = NP$ [19]. To take into account the flatness condition, the idea [17] is to consider the SDP

$$\min_z \sum_{\alpha, |\alpha| \leqslant k_0} R_\alpha z_\alpha \tag{29}$$

such that

$$M_k(z) \geqslant 0, \tag{30}$$

$$M_{k-d_i}(g_i \star z) \geqslant 0 \quad \text{for } i = 1, \ldots, m, \tag{31}$$

$$z_\alpha = y_\alpha \quad \text{for } |\alpha| \leqslant d. \tag{32}$$

The coefficients R_α are chosen randomly, but in order to ensure that $\sum_{\alpha, |\alpha| \leqslant k_0} R_\alpha z_\alpha$ has indeed a global minimum, the polynomial $R(\mathbf{x}) = \sum_\alpha R_\alpha x^\alpha$ is taken as a sum-of-squares polynomial of degree $2k_0$. When the order of the extension k is increased, the polynomial is kept the same, so that minimization is realized only on the z_β with $|\beta| \leqslant 2k_0$.

According to the theorems above, finding a representing measure, or finding a decomposition into a mixture of separa-
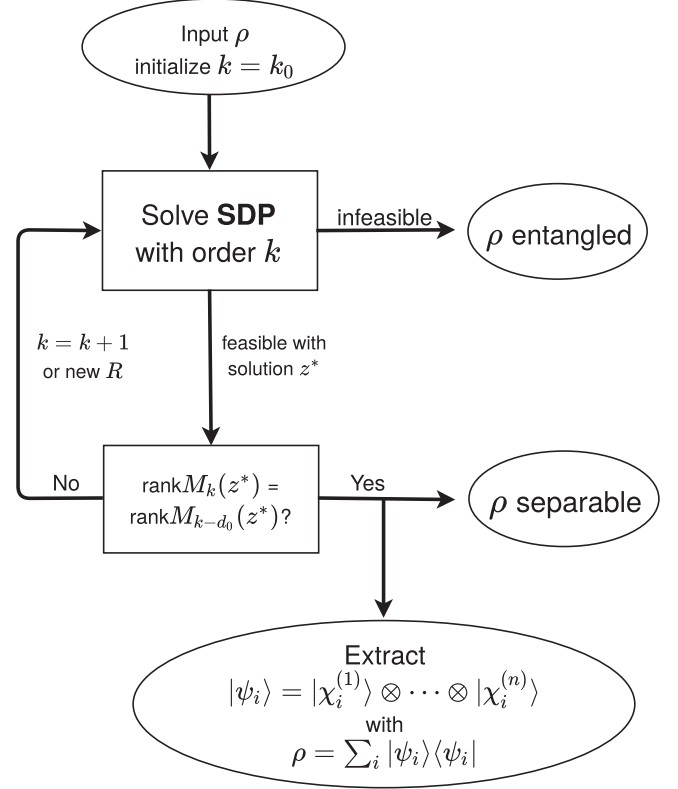

FIG. 1. Flow diagram to visualize the algorithm. "Solve SDP" refers to Eqs. (29)–(32).

ble product states, amounts to finding an extension z that fulfills constraints (30)–(32), i.e., such that the SDP is "feasible," and that also fulfills rank condition (28). We can now propose an algorithm which, for any entangled state, provides a certificate of entanglement, and for a separable state usually halts at the first iteration $k = k_0$ and provides a decomposition into pure product states. This algorithm is illustrated in Fig. 1. One runs the algorithm by starting from the lowest possible extension order $k = k_0$ and increasing k. If there exists an order k such that the SDP is infeasible, then the TMS y admits no representing measure. In terms of entanglement, this means that the quantum state whose coordinates are given by the y_α is entangled. If, on the contrary, the SDP problem is feasible at some order k (i.e., if all constraints can be met) and if for that value of k the extension obtained fulfills Eq. (28), then the TMS y admits a representing measure, and the corresponding quantum state is separable with respect to the multipartite factorization of the Hilbert space considered. The algorithm remains inconclusive as long as the SDP remains feasible but with an extension which is not flat. In such a case, one can either repeat the SDP with the same k and a different R, or increase the order k by 1. As soon as the rank condition is met, or the SDP becomes infeasible, the algorithm stops and gives a certificate of separability, or entanglement. The only situation where the algorithm does not give an answer in a finite number of steps is the case where extensions are found for any k and all choices of R, but are never flat.

When the algorithm stops with a feasible flat extension z it is possible to extract a representing measure as a sum

of rank$[M_k(z)]$ δ functions [16], which provides an explicit factorization of the separable quantum state. Indeed, suppose the algorithm stops at order k and gives an extension $z = z^*$ which optimizes Eq. (29) and fulfills rank condition (28). If the moment matrix of the optimal solution $M_k(z^*)$ has rank r, then it is possible to calculate an explicit decomposition of the form

$$M_k(z^*)_{\alpha\beta} = \sum_{j=1}^{r} w_j \, x^*(j)^\alpha x^*(j)^\beta, \quad |\alpha|, |\beta| \leqslant k, \quad (33)$$

with $w_j \geqslant 0$, $\sum_j w_j = 1$, and $\mathbf{x}^*(j) \in K$, with the methods described in Ref. [33] and implemented in the MATLAB package GLOPTIPOLY3 [34] (see Appendix A). These r vectors yield r δ functions in the decomposition of the representing measure, and for a separable quantum state they yield an explicit decomposition as a sum of r factorized states.

IV. IMPLEMENTATION AND NUMERICAL RESULTS

A. Two-qubit symmetric states

We now apply this TMS approach to some concrete examples of entanglement detection, starting with the simplest case of two-qubit symmetric states. Any state ρ can be expanded as in Eq. (3) with $N = 2$. The TMS problem is given by Eq. (10) with $d = N = 2$ and $n = 3$ variables. We can choose to obtain a decomposition of the state either into mixed states, in which case the compact K should be taken as the

unit ball, or into pure states, where K has to be the unit sphere. Here we consider the pure state decomposition, so that we define $K = \{\mathbf{x} \in \mathbb{R}^3 | g(\mathbf{x}) = 0\}$ with $g(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 - 1$ [equality $g(x) = 0$ obviously means that K is semialgebraic and defined by the two polynomials $g \geqslant 0$ and $-g \geqslant 0$]. The measure $d\mu$ must satisfy constraints such as

$$y_{110} = \int_{||\mathbf{x}||=1} x_1 x_2 \, d\mu(\mathbf{x}) \quad \text{or} \quad y_{002} = \int_{||\mathbf{x}||=1} x_3^2 \, d\mu(\mathbf{x}), \quad (34)$$

where $||\mathbf{x}||^2 = x_1^2 + x_2^2 + x_3^2$ and the y_α are the entries corresponding to the $X_{\mu_1\mu_2}$.

The necessary condition given in Sec. III B is positivity of the moment matrix of order $d/2 = 1$, that is, $M_1(y) \geqslant 0$, with

$$M_1(y) = \begin{pmatrix} y_{000} & y_{100} & y_{010} & y_{001} \\ y_{100} & y_{200} & y_{110} & y_{101} \\ y_{010} & y_{110} & y_{020} & y_{011} \\ y_{001} & y_{101} & y_{011} & y_{002} \end{pmatrix}. \quad (35)$$

Solving the entanglement problem in this case amounts to constructing a TMS $(z_\beta)_{|\beta|\leqslant 2k}$ which is a flat extension of y. Since $k_0 = 2$, the lowest-order moment matrix of the extension is $M_2(z)$, which is a 10×10 matrix whose upper left 4×4 block is matrix (35). The conditions of Theorem 1 imply that we look for an extension such that $M_2(z) \geqslant 0$ and $M_1(g * z) \geqslant 0$, where

$$M_1(g * z) = \begin{pmatrix} z_{000} - z_{200} - z_{020} - z_{002} & z_{100} - z_{300} - z_{120} - z_{102} & z_{010} - z_{210} - z_{030} - z_{012} & z_{001} - z_{201} - z_{021} - z_{003} \\ z_{100} - z_{300} - z_{120} - z_{102} & z_{200} - z_{400} - z_{220} - z_{202} & z_{110} - z_{310} - z_{130} - z_{112} & z_{101} - z_{301} - z_{121} - z_{103} \\ z_{010} - z_{210} - z_{030} - z_{012} & z_{110} - z_{310} - z_{130} - z_{112} & z_{020} - z_{220} - z_{040} - z_{022} & z_{011} - z_{211} - z_{031} - z_{013} \\ z_{001} - z_{201} - z_{021} - z_{003} & z_{101} - z_{301} - z_{121} - z_{103} & z_{011} - z_{211} - z_{031} - z_{013} & z_{002} - z_{202} - z_{022} - z_{004} \end{pmatrix} \quad (36)$$

is the 4×4 localizing matrix of z. The SDP is then to find $\min_z \sum_\alpha R_\alpha z_\alpha$, with R an arbitrary given list of coefficients so that $\sum_\alpha R_\alpha z_\alpha$ is positive and bounded, under the constraints that $M_2(z) \geqslant 0$, $M_1(g * z) \geqslant 0$, and $z_\alpha = y_\alpha$ for $|\alpha| \leqslant 2$.

The point of this section was to illustrate the different ingredients of our algorithm. In fact, in this case, the necessary condition $M_1(y) \geqslant 0$ is necessary and sufficient. Indeed, $M_1(y)$ is exactly the 4×4 matrix $(X_{\mu\nu})_{0\leqslant\mu,\nu\leqslant3}$, which was proven in Ref. [29] to be similar to the partial transpose matrix of ρ up to a factor of $1/2$. It is well known that the partial transpose criterion is a necessary and sufficient separability condition for two qubits [35,36]; hence positivity of $M_1(y)$ suffices to prove separability.

In Theorem 4.7 of [37] the authors solved the K-TMS problem of degree 2 in the case where K is defined by a single quadratic equality by direct proof rather than using the above theorems on generic TMS. The key point is a result from [38]. Using the mapping between the TMS problem and the separability problem, the theorem of [37] directly yields a necessary and sufficient condition for separability of a symmetric two-qubit state. Actually, this problem also coincides with the problem of characterizing the convex hull of spin coherent states. For spin-1, a necessary and sufficient criterion

was established in terms of positivity of a matrix [39]. Again, this criterion coincides with the result of Theorem 4.7 of [37]. Moreover, it was shown in Ref. [40] that any separable symmetric two-qubit state could be decomposed as a mixture of four pure product states. The above method provides a concise constructive proof of the same fact. In Appendix B we present a simple derivation of this result using the TMS language.

B. N-qubit symmetric states

The case of an N-qubit symmetric state ρ can be mapped onto the TMS problem of Eq. (10) where $\mathbf{x} = (x_1, x_2, x_3)$ is a vector of $\mathbb{R}^3$. We define $K = \{x \in \mathbb{R}^3 | g(\mathbf{x}) = 0\}$, with $g(\mathbf{x}) = x_1^2 + x_2^2 + x_3^2 - 1$ as in the two-qubit case. The highest degree of the monomial x^α in Eq. (10) is the total number of indices of the tensor $X_{\mu_1\cdots\mu_N}$, i.e., $d = N$. The degree of the polynomial defining K is 2, and therefore $d_0 = 1$.

To numerically investigate the algorithm for an N-qubit symmetric state we have to solve a SDP with degree $d = N$ and flatness condition rank$M_k(z) = $ rank$M_{k-1}(z)$. If the state is entangled (ρ_{ent}), the SDP [Eqs. (29)–(32)] should prove infeasible at some value of k, but this usually happens already at the lowest order $k = k_0$. When the state is separable (ρ_{sep}),

TABLE I. Timing of the algorithm in seconds for N-qubit symmetric states as function of N, averaged over 100 random states, when run on a standard desktop PC. The first row corresponds to random states drawn from the uniform Haar measure (following [41]), which are usually entangled. They are typically detected by the condition $M_k(y) \geqslant 0$. The second row corresponds to random separable states created by randomly mixing random pure separable states. The timing can vary depending on the separable state tested and the randomly generated functional R in Eq. (29). Up to six different R are tested before moving to the next order.

States \ N	2	3	4	5	6	7	8	9	10	11	12
ρ_{ent}	0.2	0.2	0.4	0.6	1.0	2.1	5.2	11.6	26.8	54.6	170.5
ρ_{sep}	0.7	0.4	0.6	1.0	2.0	4.2	10.2	20.8	66.9	94.5	716.3

the algorithm has to find a flat extension for some k, which may require to run the SDP for more than one R, or to increase the values of k. Hence, the run time is typically longer than in the case of an entangled state, as can be seen in Table I. Usually we found a flat extension either at the lowest order $k = k_0$ or at order $k = k_0 + 1$.

C. Physical interpretation of the positivity of $M_k(y)$

Consider a $2k$-qubit symmetric state ρ. The necessary condition $M_k(y) \geqslant 0$ of Sec. III B turns out to be equivalent to the positivity of the partial transpose of ρ with respect to the k first qubits. Indeed, let T be the real symmetric matrix defined by

$$T_{\boldsymbol{\mu}, \boldsymbol{\nu}} = X_{\mu_1 \cdots \mu_k \nu_1 \cdots \nu_k} \tag{37}$$

in terms of the coordinates $X_{\mu_1 \mu_2 \cdots \mu_{2k}}$ of ρ [see Eq. (3)], where matrix indices $\boldsymbol{\mu}$ and $\boldsymbol{\nu}$ are multi-indices $\boldsymbol{\mu} = (\mu_1, \ldots, \mu_k)$ and $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_k)$, with $0 \leqslant \mu_i, \nu_i \leqslant 3$. Then, up to a constant numerical factor, the matrix T is similar to the partial transpose of the density matrix in the computational basis for the partition into two sets of k qubits each [29]. Moreover, T has some recurring rows and columns, which when removed yield exactly the moment matrix $M_k(y)$. A symmetric matrix is positive semidefinite if and only if all principal minors, i.e., the determinants of all submatrices, are non-negative. The determinant of a matrix which has a recurring column or row is equal to zero, so only the submatrices with nonrecurring rows and columns have to be considered. Therefore, T, and thus the partial transpose, is positive semidefinite if and only if the matrix $M_k(y)$ is positive semidefinite. So the necessary condition $M_k(y) \geqslant 0$ is equivalent to the positive partial transpose criterion of a symmetric state of $2k$ qubits with equal-size partitions. Since for a separable N-qubit state ρ any reduced density matrix of $2k$ qubits has to be separable, the necessary conditions $M_k(y) \geqslant 0$ with $k \leqslant N/2$ can be interpreted as positivity of the partial transpose of the reduced density matrices of ρ. This provides an interesting interpretation of the physical meaning of the positivity of the moment matrix.

D. The example of four-qubit symmetric states

One of the best-known results from entanglement theory is the Peres-Horodecki criterion, which states that 2×2 and 2×3 systems are separable if and only if the partial transpose is positive [35,36] (PPT criterion). In the case of N-qubit symmetric

states, where separable states are always fully separable, this PPT criterion suffices to detect separability for $N = 2$ and $N = 3$. The first nontrivial case is thus $N = 4$ (note that even for $N = 2$ or 3, decomposing explicitly the state as a mixture of product states is not trivial; see Sec. IV E and Appendix B).

Our approach has several advantages over algorithms such as QETLAB [42]. First, in the case of symmetric states, our algorithm is particularly suited to take advantage of the symmetry. The QETLAB toolbox embeds the state in the full exponentially large Hilbert space even if the state is symmetric, while the way we implement it via the tensor representation allows us to directly exploit the smaller size of Hilbert space. For $N = 4$, the TMS problem corresponds to finding a measure $d\mu$ whose moments $\int_K x^\alpha d\mu(\mathbf{x})$ are fixed by the y_α up to degree $d = 4$. The algorithm looks for an extension $(z_\beta)_{|\beta| \leqslant 2k}$ with $k \geqslant k_0 = \lfloor d/2 \rfloor + 1 = 3$. At its first step $k = 3$, the SDP contains the constraint that the matrix $M_3(z)_{\alpha\beta} = z_{\alpha+\beta}$ be positive, and that $z_\alpha = y_\alpha$ for $|\alpha| \leqslant 4$. As a consequence, the matrix $M_2(y)$ appears as the upper-left block of $M_3(z) \geqslant 0$, so that it is also constrained to be positive. As we mentioned in the previous section, $M_2(y) \geqslant 0$ is equivalent to having positive partial transpose of the initial state with respect to two qubits; thus the PPT criterion (with transpose over two qubits) is embedded in the first step of the algorithm. It is anyway easy to check both PPT criteria (with transpose over one or two qubits) on the initial state before running the algorithm.

Our approach has the additional advantage over the QETLAB toolbox in that it yields an explicit decomposition into a convex combination of product state. We give an explicit example to illustrate this extra feature of our approach. Consider for example the four-qubit state

$$\rho = \frac{1}{2\pi} \int_0^{2\pi} d\varphi \left| \frac{\pi}{2}, \varphi \right\rangle \left\langle \frac{\pi}{2}, \varphi \right|, \tag{38}$$

which by construction is separable. Our algorithm yields a decomposition into five separable symmetric states arranged as a rotated pentagram on the equator, as

$$\rho = \sum_{j=1}^5 \frac{1}{5} \left| \frac{\pi}{2}, \varphi_j \right\rangle \left\langle \frac{\pi}{2}, \varphi_j \right| \tag{39}$$

with $\varphi_j = -0.2213 + 0.4j$. If we consider a mixture $\rho = 0.09 |\psi_{QQ}\rangle\langle\psi_{QQ}| + 0.91\rho_0$ of the most quantum four-qubit state $|\psi_{QQ}\rangle = \sqrt{\frac{1}{3}} |D_4^{(0)}\rangle + \sqrt{\frac{2}{3}} |D_4^{(3)}\rangle$ and the maximally mixed state $\rho_0 = \frac{1}{5} \sum_{k=0}^4 |D_4^{(k)}\rangle\langle D_4^{(k)}|$, the algorithm yields a decomposition into ten states as follows:

w	ϕ	θ	
0.1149	-2.0533	5.2439	
0.0771	-2.95	5.0379	
0.1251	-2.1878	3.1092	
0.0425	-1.1868	5.3285	
0.1183	-0.9663	4.3268	(40)
0.1245	-2.2363	1.0639	
0.0784	-1.1732	3.2701	
0.1174	-0.9454	6.2323	
0.0761	-1.2474	0.9776	
0.1258	-0.9623	2.0945	

As we see in the next section, the minimal number of separable symmetric states required to decompose a randomly generated four-qubit state is 9, obtained for 1% of the states generated. The question of the number of separable symmetric states needed generically is still an open one, which our algorithm should allow one to investigate.

E. Minimal number of pure product states needed

If a quantum state is separable it can be written as a convex sum of pure product states. Replacing each product state by its eigenvalue-eigenvector decomposition we obtain a decomposition of the initial quantum state as a convex sum of pure product states. What is the minimal number r_{min} of pure product states required to decompose an arbitrary separable state?

The answer is unknown in the general case. For symmetric states, pure states in the decomposition have to be symmetric themselves (see, e.g., Theorem 1 in Ref. [29]). As Appendix B shows, and as was obtained in Ref. [40], in the case of two qubits, four states are sufficient to represent any separable symmetric state.

The above algorithm yields $\mathrm{rank} M_k(z) = r$ as an upper bound to the number of pure states required to decompose a given quantum state. In order to investigate systematically the number of states required, we generated symmetric separable states by mixing a large number m of random separable symmetric pure states with random weights as

$$\rho_{\mathrm{sep,sym}} = \sum_{i=1}^{m} w_i (|\psi_i\rangle\langle\psi_i|)^{\otimes N}, \qquad (41)$$

with $\sum_i w_i = 1$, and applied the algorithm to the resulting mixed states. When our algorithm stops with a flat extension z such that $\mathrm{rank} M_k(z) = r$, then r is an upper bound on the true minimal number of separable states required to express $\rho_{\mathrm{sep,sym}}$. Indeed, since the extension depends on the random choice of R_α there may be extensions with a smaller rank, as the algorithm does not minimize this rank. Therefore, every number $r < m$ obtained should give an upper bound to the actual generic value for r_{min}. In practice we generated a large list of separable symmetric states with a value of $m = 25$ for $N \leqslant 6$ and $m = 45$ for $N > 6$ and found a flat extension for each one. The smallest numbers found are reported in Table II.

TABLE II. The smallest value of r found, which gives an upper bound on the true value r_{min} of the minimal number of pure states needed to generate every separable symmetric state. The third column gives the number of states for which the value $\min r$ has been reached among the states tested.

N	Min r	No. of states min reached	No. of states tested
2	4	37 304	61 494
3	6	2 410	60 641
4	9	1 104	174 011
5	12	17	174 193
6	17	408	153 081
7	22	18	16 129
8	29	12	16 030
9	35	2	10 000
10	42	1	10 000

V. A NEW SOLUTION TO A PARTICULAR TMS PROBLEM

The mapping presented above not only helps in solving the separability problem, but it can also, conversely, shed light on particular TMS problems by using results from entanglement theory. We now give an example of such a situation.

As mentioned in Sec. IV D, the PPT criterion provides a necessary and sufficient separability condition when $N = 2$ or 3. It has been generalized to the following two statements: If ρ is supported on $\mathbb{C}^2 \times \mathbb{C}^N$ and the rank $r(\rho) = N$ then ρ is separable (Theorem 1 of [43]) and can be written as a convex sum of projectors on N product vectors (Corollary 3a of [43]).

When ρ is fully symmetric, the above characterizations yield the following result:

Theorem 3 [44]. Let ρ be a symmetric N-qubit state with positive partial transpose with respect to the first qubit. If $N = 2$ or 3, or if $N > 3$ and $r(\rho) \leqslant N$, then ρ is fully separable.

Note that for four qubits there exist entangled symmetric states with a positive partial transpose [45]. As shown in Ref. [29], the PPT conditions can be expressed as linear matrix inequalities involving the entries of the tensor $X_{\mu_1 \mu_2 \cdots \mu_N}$, or equivalently the y_α. Rewriting the above theorem for $N = 3$ in the language of K-TMS problems yields a theorem for a special case of a TMS. Even more, by using the fact that 2×3 systems are separable if and only if they are PPT, we directly get a necessary and sufficient condition for a TMS problem of degree $d = 3$ to admit a representing measure supported on the unit sphere of $\mathbb{R}^3$. This condition reads

$$
\begin{pmatrix}
y_{000} + y_{001} & y_{100} - iy_{010} & y_{100} + y_{101} & y_{200} - iy_{110} & y_{010} + y_{011} & y_{110} - iy_{020} & y_{001} + y_{002} & y_{101} - iy_{011} \\
y_{100} + iy_{010} & y_{000} - y_{001} & y_{200} + iy_{110} & y_{100} - y_{101} & y_{110} + iy_{020} & y_{010} - y_{011} & y_{101} + iy_{011} & y_{001} - y_{002} \\
y_{100} + y_{101} & y_{200} - iy_{110} & y_{200} + y_{201} & y_{300} - iy_{210} & y_{110} + y_{111} & y_{210} - iy_{120} & y_{101} + y_{102} & y_{201} - iy_{111} \\
y_{200} + iy_{110} & y_{100} - y_{101} & y_{300} + iy_{210} & y_{200} - y_{201} & y_{210} + iy_{120} & y_{110} - y_{111} & y_{201} + iy_{111} & y_{101} - y_{102} \\
y_{010} + y_{011} & y_{110} - iy_{020} & y_{110} + y_{111} & y_{210} - iy_{120} & y_{020} + y_{021} & y_{120} - iy_{030} & y_{011} + y_{012} & y_{111} - iy_{021} \\
y_{110} + iy_{020} & y_{010} - y_{011} & y_{210} + iy_{120} & y_{110} - y_{111} & y_{120} + iy_{030} & y_{020} - y_{021} & y_{111} + iy_{021} & y_{011} - y_{012} \\
y_{001} + y_{002} & y_{101} - iy_{011} & y_{101} + y_{102} & y_{201} - iy_{111} & y_{011} + y_{012} & y_{111} - iy_{021} & y_{002} + y_{003} & y_{102} - iy_{012} \\
y_{101} + iy_{011} & y_{001} - y_{002} & y_{201} + iy_{111} & y_{101} - y_{102} & y_{111} + iy_{021} & y_{011} - y_{012} & y_{102} + iy_{012} & y_{002} - y_{003}
\end{pmatrix} \geqslant 0.
$$

$$(42)$$

(see the expression of [29] which explicitly gives the PPT criterion for three qubits). This result does not appear to have been known previously in the TMS literature.

While Eq. (42) is a necessary and sufficient condition in the case $N = 3$, Theorem 3 also provides us with a sufficient condition for arbitrary N. Indeed, suppose one wants to know whether a given TMS y of degree $N > 3$ admits a representing measure on the unit sphere. Using the mapping inverse to the one in Sec. IV B one can construct the density matrix ρ associated with the TMS via Eq. (3). If ρ is PPT and has rank $r(\rho) \leqslant N$, then there exists a representing measure.

VI. CONCLUSIONS

We have proposed an elegant solution of the entanglement problem by mapping it to the truncated K-moment problem. Benefiting from the mathematically well-developed field of the theory of moments, we provide an algorithm that for an entangled state certifies its entanglement in a finite number of steps. If the state is separable, it usually halts at the first iteration ($k = k_0$ in Fig. 1) and then returns an explicit decomposition of the state into a convex sum of product states. Similarly to previous algorithms, our algorithm makes use of semidefinite programming and "extensions," but there are a number of conceptual differences that allow us to express and solve the problem very elegantly and adapt it easily to different physical situations, including subsystems of different dimensions or symmetries, or incomplete data.

In our approach, rather than working directly with the density matrix, the semidefinite optimization problem is based on moment matrices and localizing matrices, where the latter incorporate the constraints of the states of the subspaces. This is possible as long as these states in the subspaces are restricted to compact sets characterized by polynomial constraints, as is the case, e.g., for individual spins-1/2 in terms of their Bloch spheres. Both the moment matrix and the localizing matrices must be positive semidefinite for a state to be separable. Extensions are extensions of the moment matrix, and we need not impose a particular symmetry on such an extension, nor positivity of the partial transpose of the state, since this is taken care of by positivity of the moment matrix (see Sec. IV C). In particular, the first step of the algorithm, for $k = k_0$, precisely corresponds to the PPT necessary separability criterion.

Our algorithm contains in addition a crucial element, namely the idea of "flat extensions": if at a given order k of the extension the SDP is feasible, one checks whether the rank of the extended moment matrix is the same as the one at order $k - d_0$ [with d_0 related to the largest degree of the constraint polynomials; see after Eq. (28)]. If so, the state is separable and one obtains its explicit convex decomposition into product states. This is an improvement over known entanglement detection packages such as QETLAB [42]. In Ref. [25] it was already noted that when PPT is imposed on the extensions in the algorithm by Doherty *et al.* [20–22], *sometimes* separability can be concluded in a finite number of steps by checking

whether the rank of the found extension of the density matrix has not increased compared to the original state, a situation called rank loop. The sufficiency of a rank loop for separability follows here from a theorem due to Horodecki *et al.* [32], according to which a PPT state is separable if its rank is smaller than or equal to the rank of the reduced state. In our case, the implementation of the flat-extension query is a decisive part of the algorithm, based on Theorem 1.

Formulating the entanglement as a truncated K-TMS problem also has the advantage that the algorithm readily accepts incomplete data from an experiment. Indeed, since for multipartite systems fully determining the state requires an effort that grows exponentially with the number of subsystems, fully specifying or experimentally determining the state becomes at some point impossible in practice. Since our algorithm is based from the very beginning on a truncated sequence of moments (that can be chosen to be expectation values of Hermitian operators that *were* measured), we can leave open additional moments that were not measured and still run the algorithm. Using the algorithm in this way should allow one to determine how many and which moments one should measure in order to still be able to prove that a state is entangled.

Finally, as symmetric states of N qubits coincide with spin-j states with $N = 2j$, separable symmetric states can be identified with classical spin-j states (see, e.g., [39]). The latter, defined in Ref. [39], are convex combinations of spin-coherent states and can be considered the quantum states which are closest to having a classical behavior in the sense of minimal quantum fluctuations [13,29,46]. Applying the algorithm presented here to symmetric states of N qubits also allows one to check whether a spin-j state is classical.

APPENDIX A: MATLAB IMPLEMENTATION

Here we give a MATLAB implementation of the easiest case of the symmetric state of two qubits (or a spin-1 state [47]). The quantum state ρ is given as in Eq. (2) as

$$X_{\mu_1\mu_2} = \mathrm{tr}\big\{\rho \, P_s^\dagger \sigma_{\mu_1} \otimes \sigma_{\mu_2} P_s\big\}, \qquad (A1)$$

with P_s the projector onto the symmetric states. The following implementation uses MATLAB and the programs GLOPTIPOLY3 [34] and the solver SEDUMI [48]. To increase the probability of finding a flat extension, the semidefinite solver should use the highest possible accuracy in the calculation of the minimal

value of the SDP:

```
1    mpol x 3
2    xMom=[1 x(1) x(2) x(3) x(1)² x(1)*x(2) x(1)*x(3) x(2)²
        x(2)*x(3) x(3)²];
3    y=[X(1,1) X(1,2) X(1,3) X(1,4) X(2,2) X(2,3) X(2,4) X(3,3)
        X(3,4) X(4,4)];
4    con=[mom(xMom)==y];
5    K = [x(1)²+x(2)²+x(3)²−1==0];
6    G = randn(length(xMom));
7    R = xMom*(G'*G)*xMom';  k=2;
8    P = msdp(min(mom(R)) ,K, con, k);
9    pars.eps=0; mset(pars);
10   [status] =msol(P);
```

Line 3 is given by Eq. (A1), line 4 corresponds to Eq. (10), K fixes the variables to Bloch vectors of length 1, and R is the arbitrary positive bounded polynomial which should be minimized. In line 8, "msdp" formulates the problem in the language of SDPs (construction of moment matrices and localizing matrices). Line 9 sets the accuracy of the SDP solver to its highest value. In line 10, "msol" solves the SDP.

(1) If the problem is detected as infeasible (status = -1) the state is entangled.

(2) If there is no flat extension found (status = 0), one can rerun the program with a different R, or increase the rank by 1.

(3) If the state is separable and a flat extension is found (status = 1) the solution can be extracted with the command "sol=double(x)." Then "sol" contains a list of Bloch vectors of the pure states that give a decomposition into separable states as in Eq. (6). The vector of weights w_i can then be easily calculated.

This implementation can be extended to a larger number of qubits by adapting the monomial basis in line 2 to a higher degree and line 3 to contain all entries of the tensor $X_{\mu_1 \cdots \mu_N}$ [Eq. (2)]. The generalization to nonsymmetric states is also possible, but the number of variables increases. For example, two qubits would require one independent Bloch vector for each subsystem, so one would need six variables in total.

APPENDIX B: MINIMAL RANK FOR SYMMETRIC TWO-QUBIT STATES

Theorem 4.7 of [37] states that a TMS y of degree 2 admits a representing measure supported by K if and only if $M_1(y)$ is positive and $y_{000} - y_{200} - y_{020} - y_{002} = 0$. We therefore obtain that a two-bit symmetric state ρ is separable if and only if it is associated with a TMS such that $M_1(y)$ is positive and $y_{000} - y_{200} - y_{020} - y_{002} = 0$. These two conditions in fact coincide respectively with the PPT criterion and with

the condition that $X_{00} = \sum_{a=1}^{3} X_{aa}$ (see Sec. IV C). The latter condition itself is a consequence of properties of the projections of tensor products of Pauli matrices over the symmetric subspace, as was shown in Ref. [13].

The proof of the fact that if and only if $M_1(y)$ is positive and $y_{000} - y_{200} - y_{020} - y_{002} = 0$ then ρ is separable into a mixture of only four separable states can be simplified by using the TMS formalism. Let us derive the necessary and sufficient condition above in our language. The "necessary" direction is obvious. The proof for the "sufficient" direction goes as follows. Let us assume that the coordinates $X_{\mu\nu}$ form a positive rank-r matrix $M_1(y)$. Since the state is symmetric, $M_1(y)$ is a real symmetric 4×4 matrix and hence $r \leqslant 4$. Then $M_1(y)$ can be decomposed into a sum of r projectors on orthogonal vectors $u^{(k)}$ as

$$X_{\mu\nu} = \sum_{k=1}^{r} u_\mu^{(k)} u_\nu^{(k)}. \tag{B1}$$

Let $\Delta_u = (u_0)^2 - \sum_{a=1}^{3}(u_a)^2$ for any 4-vector u. Since $X_{\mu\nu}$ verify $X_{00} = \sum_{a=1}^{3} X_{aa}$ we have $\sum_{i=1}^{r} \Delta_{u^{(i)}} = 0$. Whenever $\Delta_{u^{(i)}} = 0$, one has $u_0^{(i)} \neq 0$ [otherwise the whole vector $u^{(i)}$ vanishes and does not contribute to the sum (B1)], so that the corresponding projector can be rewritten

$$u_\mu^{(i)} u_\nu^{(i)} = \left(u_0^{(i)}\right)^2 n_\mu^{(i)} n_\nu^{(i)} \tag{B2}$$

with $n^{(i)} = (1, \mathbf{n})$ and $|\mathbf{n}| = 1$. If all $\Delta_{u^{(i)}} = 0$ then Eqs. (B1) and (B2) immediately yield a sum over r separable pure states. If not, then since $\sum_i \Delta_{u^{(i)}} = 0$ there must be two indices i and j with $\Delta_{u^{(i)}} < 0$ and $\Delta_{u^{(j)}} > 0$. Let $v(t) = tu^{(i)} + (1-t)u^{(j)}$. Then $\Delta_{v(0)} > 0$ and $\Delta_{v(1)} < 0$, so that there has to be a $t_c \in]0, 1[$ such that $\Delta_{v(t_c)} = 0$. The vector $v'(t) = -(1-t)u^{(i)} + tu^{(j)}$ is then such that

$$u_\mu^{(i)} u_\nu^{(i)} + u_\mu^{(j)} u_\nu^{(j)} = \frac{v(t_c)_\mu v(t_c)_\nu + v'(t_c)_\mu v'(t_c)_\nu}{t_c^2 + (1-t_c)^2}. \tag{B3}$$

Then subtracting a projector on $v(t_c)$ yields

$$X_{\mu\nu} - \frac{v(t_c)_\mu v(t_c)_\nu}{t_c^2 + (1-t_c)^2} = \sum_{k=1}^{r-1} \tilde{u}_\mu^{(k)} \tilde{u}_\nu^{(k)}, \tag{B4}$$

where $\tilde{u}^{(k)}$ are the orthogonal states $u^{(k')}$ ($k' \neq i, j$) and $v'(t_c)$. Because of the definition of t_c and using Eq. (B2), the projector on $v(t_c)$ is proportional to a projector representing a separable pure state, and the remaining sum is such that $\sum_{k=1}^{r-1} \Delta_{\tilde{u}^{(k)}} = 0$. We are therefore back to the form (B1) but with the rank reduced by 1. The same procedure can be applied repeatedly to further reduce the rank down to 1; the last projector is then necessarily of the form (B2). In the end, ρ is written as a sum of $r \leqslant 4$ projectors on separable pure states.

---

[1] D. Bruss, J. Math. Phys. **43**, 4237 (2002).

[2] M. B. Plenio and S. Virmani, Quantum Inf. Comput. **7**, 1 (2007).

[3] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Rev. Mod. Phys. **81**, 865 (2009).

[4] O. Gühne and G. Tóth, Phys. Rep. **474**, 1 (2009).

[5] A. R. Usha Devi, R. Prabhu, and A. K. Rajagopal, Phys. Rev. Lett. **98**, 060501 (2007).

[6] R. Hübener, M. Kleinmann, T.-C. Wei, C. González-Guillén, and O. Gühne, Phys. Rev. A **80**, 032324 (2009).

[7] G. Tóth and O. Gühne, Phys. Rev. Lett. **102**, 170503 (2009).

[8] R. Augusiak, J. Tura, J. Samsonowicz, and M. Lewenstein, Phys. Rev. A **86**, 042316 (2012).

[9] D. Baguette, T. Bastin, and J. Martin, Phys. Rev. A **90**, 032314 (2014).

[10] E. Wolfe and S. F. Yelin, Phys. Rev. Lett. **112**, 140402 (2014).

[11] T. Ichikawa, T. Sasaki, I. Tsutsui, and N. Yonezawa, Phys. Rev. A **78**, 052105 (2008).

[12] E. Majorana, Nuovo Cimento **9**, 43 (1932).

[13] O. Giraud, D. Braun, D. Baguette, T. Bastin, and J. Martin, Phys. Rev. Lett. **114**, 080401 (2015).

[14] K. Schmüdgen, Math. Ann. **289**, 203 (1991).

[15] R. E. Curto and L. A. Fialkow, J. Oper. Theory **54**, 189 (2005).

[16] J. W. Helton and J. Nie, Found. Comput. Math. **12**, 851 (2012).

[17] J. Nie, Found. Comput. Math. **14**, 1243 (2014).

[18] J. Nie and X. Zhang, SIAM J. Optim. **26**, 1236 (2016).

[19] M. Laurent, in *Emerging Applications of Algebraic Geometry*, edited by M. Putinar and S. Sullivant (Springer, New York, 2009), pp. 157–270.

[20] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. Lett. **88**, 187904 (2002).

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

[22] A. C. Doherty, P. A. Parrilo, and F. M. Spedalieri, Phys. Rev. A **71**, 032333 (2005).

[23] J. Eisert, P. Hyllus, O. Gühne, and M. Curty, Phys. Rev. A **70**, 062317 (2004).

[24] F. Hulpke and D. Bruß, J. Phys. A **38**, 5573 (2005).

[25] M. Navascués, M. Owari, and M. B. Plenio, Phys. Rev. A **80**, 052306 (2009).

[26] B. Jungnitsch, T. Moroder, and O. Gühne, Phys. Rev. Lett. **106**, 190502 (2011).

[27] A. W. Harrow, A. Natarajan, and X. Wu, Commun. Math. Phys. **352**, 881 (2017).

[28] J. Chen, Z. Ji, D. Kribs, N. Lütkenhaus, and B. Zeng, Phys. Rev. A **90**, 032318 (2014).

[29] F. Bohnet-Waldraff, D. Braun, and O. Giraud, Phys. Rev. A **94**, 042343 (2016).

[30] R. F. Werner, Phys. Rev. A **40**, 4277 (1989).

[31] N. Miklin, T. Moroder, and O. Gühne, Phys. Rev. A **93**, 020104 (2016).

[32] P. Horodecki, M. Lewenstein, G. Vidal, and I. Cirac, Phys. Rev. A **62**, 032310 (2000).

[33] D. Henrion and J.-B. Lasserre, in *Positive Polynomials in Control*, edited by D. Henrion and A. Garulli (Springer, Berlin, 2005), pp. 293–310.

[34] D. Henrion, J. B. Lasserre, and J. Loefberg, Optim. Methods Softw. **24**, 761 (2009); see also http://homepages.laas.fr/henrion/software/gloptipoly/

[35] A. Peres, Phys. Rev. Lett. **77**, 1413 (1996).

[36] M. Horodecki, P. Horodecki, and R. Horodecki, Phys. Lett. A **223**, 1 (1996).

[37] L. Fialkow and J. Nie, J. Funct. Anal. **258**, 328 (2010).

[38] J. Sturm and S. Zhang, Math. Oper. Res. **28**, 246 (2003).

[39] O. Giraud, P. Braun, and D. Braun, Phys. Rev. A **78**, 042112 (2008).

[40] M. Kuś and I. Bengtsson, Phys. Rev. A **80**, 022319 (2009).

[41] K. Życzkowski, K. A. Penson, I. Nechita, and B. Collins, J. Math. Phys. **52**, 062201 (2011).

[42] http://www.qetlab.com/Main_Page

[43] B. Kraus, J. I. Cirac, S. Karnas, and M. Lewenstein, Phys. Rev. A **61**, 062302 (2000).

[44] K. Eckert, J. Schliemann, D. Bruss, and M. Lewenstein, Ann. Phys. **299**, 88 (2002).

[45] J. Tura, R. Augusiak, P. Hyllus, M. Kuś, J. Samsonowicz, and M. Lewenstein, Phys. Rev. A **85**, 060302(R) (2012).

[46] O. Giraud, P. Braun, and D. Braun, Phys. Rev. A **85**, 032101 (2012).

[47] F. Bohnet-Waldraff, D. Braun, and O. Giraud, Phys. Rev. A **93**, 012104 (2016).

[48] J. Sturm, Optim. Meth. Softw. **11**, 625 (1999).