


Probing the Geometry of Correlation Matrices with Randomized Measurements

Nikolai Wyderka^{1,*} and Andreas Ketterer²

¹*Institut für Theoretische Physik III, Heinrich-Heine-Universität Düsseldorf, Universitätsstr. 1, Düsseldorf D-40225, Germany*

²*Fraunhofer Institute for Applied Solid State Physics IAF, Tullastr. 72, Freiburg 79108, Germany*

 (Received 14 December 2022; revised 24 February 2023; accepted 6 April 2023; published 10 May 2023)

The generalized Bloch decomposition of a bipartite quantum state gives rise to a correlation matrix whose singular values provide rich information about nonlocal properties of the state, such as the dimensionality of entanglement. While some entanglement criteria based on the singular values exist, a complete understanding of the geometry of admissible correlation matrices is lacking. We provide a deeper insight into the geometry of the singular values of the correlation matrices of limited Schmidt number. First, we provide a link to the framework of randomized measurements and show how to obtain knowledge about the singular values in this framework by constructing observables that yield the same moments as one obtains from orthogonal averages over the Bloch sphere. We then focus on the case of separable states and characterize the boundary of the set of the first two nonvanishing moments by giving explicit constructions for some of the faces and extremal points. These constructions yield a connection between the geometry of the correlation matrices and the existence problems of maximal sets of mutually unbiased bases, as well as symmetric, informationally complete, positive operator-valued measures.

DOI: [10.1103/PRXQuantum.4.020325](https://doi.org/10.1103/PRXQuantum.4.020325)

I. INTRODUCTION

Quantum states exhibit a plethora of nonclassical effects such as entanglement, coherence, and Bell nonlocality that play an integral role in the development of novel quantum technologies. For this reason, the study of fundamental properties of quantum mechanics is a central theme of ongoing research, even almost one hundred years after the initial formulation of quantum theory. Of particular interest in this respect is the nonlocal character of quantum entanglement that acts as a resource for applications like long-range quantum communication [1], metrology [2], and various other quantum information tasks [3].

Nevertheless, the fundamental features of entanglement remain elusive. For example, for states shared between more than two parties, even a unique notion of maximal entanglement does not exist, hinting at the rich underlying structure of multiparticle entanglement. Also, bipartite systems are the subject of active research, given the fact that deciding whether a given state is entangled or not is a NP-hard problem [4]. Especially in the case of bipartite

quantum systems, a large toolchain of criteria exists that allow one to decide (and in some cases quantify) entanglement for some states. Most prominently, the entanglement of bipartite states of joint dimension no greater than six can be efficiently decided by the positive partial transpose criterion [5]. For larger-dimensional systems, however, only sufficient criteria exist.

Some of these entanglement criteria are based directly on the Bloch coefficients of the states: expanding a bipartite quantum state in terms of a local operator basis allows one to represent the state as a $(d^2 \times d^2)$ -dimensional matrix of expansion coefficients. Famous entanglement criteria like the computable crossnorm or realignment criterion (CCNR) [6,7] or the de Vicente criterion [8] (or a mixture of both [9]) are based on norms of the Bloch matrix, or, more specifically, on its singular values. Nevertheless, these criteria have at least three flaws. First of all, it is unclear whether the known criteria are the strongest in terms of those singular values. Second, they only allow one to detect entanglement, but not quantify it. Finally, in order to apply them experimentally, usually a full state tomography is performed that requires a large number of well-defined measurements.

To remedy this last flaw, a connection between the moments of randomized measurement results of certain observables and the singular values of the Bloch matrix has been established recently [10,11]. It allows one to get information on the symmetric polynomials of degrees

*nikolai@wyderka.de

Published by the American Physical Society under the terms of the [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) license. Further distribution of this work must maintain attribution to the author(s) and the published article's title, journal citation, and DOI.

two and four of the singular values by relatively few measurements and mild requirements on the measurement apparatus. However, it was unclear whether observables exist that would yield higher-order polynomials as well, such that the singular values can be uniquely reconstructed.

In the present work we make progress in three main directions. First, we extend the known entanglement criteria that are based on the singular values such that they not only allow us to detect whether a state is entangled or not, but also give lower bounds on the dimensionality of the entanglement via its Schmidt number. Second, we expand the aforementioned connection between randomized measurements and the singular values of the Bloch matrix. We show that in any fixed local dimension d , local observables exist that yield as their moments the even symmetric polynomials of the eigenvalues up to degree d , but no more (except for dimensions $d = 2$ and $d = 3$). This highlights an interesting connection between Bloch sphere averages in $O(d^2 - 1)$ and local unitary averages in $SU(d)$. Third, we give a partial answer to the question of whether stronger entanglement criteria exist when the singular values are known completely, by exploring in detail the landscape spanned by the first two nonvanishing moments of the constructed observables. We show that the margin of potential improvement over the de Vicente criterion is in general very small and might even vanish.

The paper is organized as follows. In Sec. II we introduce the multidimensional Bloch vector representation and present novel criteria for the detection of the dimensionality of two-particle entanglement. Further on, in Sec. III, we introduce the notion of unitary and orthogonal moments and show in Sec. IV how they can be applied to experimentally test the aforementioned criteria. In Sec. V we proceed to discuss the optimality of the entanglement detection by characterizing the boundary of the set of separable states in the space spanned by the two lowest nonvanishing moments. In particular, we highlight connections between these findings and the existence problem of mutually unbiased bases and symmetric, informationally complete, positive operator-valued measures (SIC POVMs) in Sec. VI. In Sec. VII, we simulate the randomized measurement process for the family of isotropic states in order to obtain a guess on the required number of measurements to implement our new criterion experimentally. Finally, we conclude in Sec. VIII.

II. CORRELATION MATRIX AND ENTANGLEMENT DIMENSIONALITY

Throughout this paper, we will be concerned with bipartite quantum states of dimension $d_1 \times d_2$, and we assume without loss of generality that $d_1 \leq d_2$. We decompose this state into terms of local operator bases $\{\lambda_i\}_{i=0}^{d_1^2-1}$, $\{\tilde{\lambda}_i\}_{i=0}^{d_2^2-1}$, which we assume to be orthogonal, such that

$\text{Tr}(\lambda_i \lambda_j^\dagger) = d_1 \delta_{ij}$, $\text{Tr}(\tilde{\lambda}_i \tilde{\lambda}_j^\dagger) = d_2 \delta_{ij}$, and $\lambda_0 = \mathbb{1}_{d_1 \times d_1}$, $\tilde{\lambda}_0 = \mathbb{1}_{d_2 \times d_2}$. This choice guarantees that all other elements of the bases are traceless. Note that all of the results presented here are independent of the specific choice of bases, and popular options are the Hermitian Gell-Mann matrices or the unitary Weyl basis [12].

In this basis, an arbitrary bipartite quantum state ρ can be decomposed as

$$\rho = \frac{1}{d_1 d_2} \left[\mathbb{1} \otimes \mathbb{1} + \sum_{i=1}^{d_1^2-1} \alpha_i \lambda_i \otimes \mathbb{1} + \sum_{j=1}^{d_2^2-1} \beta_j \mathbb{1} \otimes \tilde{\lambda}_j + \sum_{i=1}^{d_1^2-1} \sum_{j=1}^{d_2^2-1} T_{ij} \lambda_i \otimes \tilde{\lambda}_j \right], \quad (1)$$

where we have split the sum according to the occurrence of identity matrices. In this way, the local states are given by $\rho_A = \text{Tr}_B(\rho) = [\mathbb{1} + \sum_i \alpha_i \lambda_i]/d_1$, and likewise for ρ_B , i.e., they are completely determined by the $(d_1^2 - 1)$ -dimensional vectors $\vec{\alpha} = (\alpha_1, \dots, \alpha_{d_1^2-1})^\dagger$ and $\vec{\beta}$, whereas the (classical and quantum) correlations of the state are captured by the $[(d_1^2 - 1) \times (d_2^2 - 1)]$ -dimensional correlation matrix T .

When considering features of the state that are independent of specific local basis choices, such as entanglement, it is useful to note that every local unitary rotation of the quantum state corresponds to an orthogonal rotation of matrix T , i.e., $T \rightarrow O_1 T O_2^T$ [13,14]. As such, many entanglement criteria exist that are based solely on different norms of matrix T [8,11,15,16]. A prominent example of such a criterion is the de Vicente criterion [8], which states that, for separable states,

$$\|T\|_{\text{Tr}} \leq \sqrt{(d_1 - 1)(d_2 - 1)}, \quad (2)$$

where $\|\cdot\|_{\text{Tr}}$ denotes the trace norm, i.e., the sum of the singular values of T . Other examples of nonlocal features that can be decided on the level of the singular values of T include the notion of faithful entanglement, which is linked to the usefulness of a state for a teleportation task [17,18] and whether or not a state constitutes nonlocality that is detectable by a Clauser-Horne-Shimony-Holt-like inequality [19,20].

Given the large evidence for the expressiveness of the singular values of T , it is of great interest to exactly characterize the set of admissible singular values in different subsets of quantum states. Here, we focus on the subsets of states of certain Schmidt numbers, which give information about the dimensionality of the entanglement of the state. The Schmidt number of a pure quantum state is defined by its Schmidt rank, i.e., the number of nonvanishing Schmidt

coefficients in their Schmidt decomposition, given by [5]

$$|\psi\rangle = \sum_{j=1}^r \sqrt{\alpha_j} |a_j\rangle \otimes |b_j\rangle, \quad (3)$$

where $\alpha_j > 0$, $\sum_{j=1}^r \alpha_j = 1$, and r denotes the Schmidt rank $\text{SR}(|\psi\rangle)$. For mixed states, the Schmidt number (SN) is defined via [21]

$$\text{SN}(\rho) = \min \left\{ r: \rho = \sum_i p_i |\psi_i\rangle\langle\psi_i|, \text{ where } \text{SR}(|\psi_i\rangle) \leq r \right\}. \quad (4)$$

The p_i are non-negative numbers summing to 1. The Schmidt number lies between 1 and $\min(d_1, d_2) = d_1$. A special subset are states of Schmidt number 1, which are called separable. They can be decomposed into convex combinations of product states, i.e.,

$$\rho_{\text{sep}} = \sum_i p_i \rho_A^{(i)} \otimes \rho_B^{(i)}, \quad (5)$$

where the p_i constitute a probability distribution.

In order to obtain a criterion for Schmidt numbers based on the singular values, we extend the already introduced de Vicente criterion from Eq. (2).

Lemma 1: *Let ρ_k be a bipartite quantum state as before with Bloch decomposition as in Eq. (1) and $\text{SN}(\rho_k) \leq k$. Then*

$$\|T\|_{\text{Tr}} \leq \sqrt{(d_1 - 1)(d_2 - 1)} + \sqrt{d_1 d_2 (k - 1)}. \quad (6)$$

The proof is given in Appendix A, where a generalization for the family of criteria derived in Ref. [9] for Schmidt number detection is also derived, which includes a bound for the CCNR criterion. Note that, if $d_1 = d_2 = d$, this bound simplifies to $\|T\|_{\text{Tr}} \leq kd - 1$. As a remark, we emphasize that indirect bounds on the Schmidt number using the de Vicente criterion can be obtained via bounds on the concurrence derived in Ref [22]. These are, however, strictly weaker than the bound from Lemma 1. Furthermore, the companion paper [23] reports the same result as our Lemma 1. We would like to stress, however, that their proof is based on bounds for the covariance criterion reported in Ref. [24]. Our proof is independent of this criterion and can be extended to the family of criteria of Ref. [9].

Lemma 1 allows for detection of lower bounds of Schmidt numbers in the following way: if the criterion is violated for a specific choice of k then the state in question must have a Schmidt number of at least $k + 1$.

A complete characterization of the set of occurring singular values in the set of states of certain Schmidt number would yield an optimal criterion for the entanglement dimensionality whenever the singular values are known. Of course, such a criterion would only be useful if the singular values can be obtained experimentally, which is a problem that we address in the following.

III. UNITARY AND ORTHOGONAL MOMENTS

Studying singular values of the correlation matrix is also motivated by the framework of randomized measurements [25–34]. In many of these schemes, one studies moments of the outcome distribution of randomly locally rotated states, i.e., one obtains the quantities

$$\mathcal{R}_A^{(t)}(\rho) := \int dU_A dU_B [\text{Tr}(U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger \mathcal{A} \otimes \mathcal{A})]^t, \quad (7)$$

where \mathcal{A} is some local observable and the integration spans local unitary groups of dimensions d_1 and d_2 with respect to the normalized Haar measures dU_A and dU_B , respectively. For now, we set $d_1 = d_2 \equiv d$ for simplicity.

However, in order to obtain symmetric polynomials of the singular values of T , one would rather be interested in moments resulting from random Bloch sphere rotations:

$$\mathcal{S}^{(t)}(\rho) := \frac{1}{V^2} \int d\vec{\alpha} d\vec{\beta} [\text{Tr}(\rho \vec{\alpha} \cdot \vec{\lambda} \otimes \vec{\beta} \cdot \vec{\lambda})]^t. \quad (8)$$

Here the integration spans $(d^2 - 1)$ -dimensional unit vectors, the surface area of which is given by $V = 2\sqrt{\pi}^{d^2-1} / \Gamma[(d^2 - 1)/2]$, where $\Gamma(z)$ denotes Euler's gamma function with $\Gamma(n) = (n - 1)!$ for positive integer n . In contrast to the unitary moments (7) defined above, we call Eq. (8) orthogonal moments, as they correspond to averaging over orthogonal transformations $\vec{\alpha} \rightarrow O_1 \vec{\alpha}$, $\vec{\beta} \rightarrow O_2 \vec{\beta}$, and $T \rightarrow O_1 T O_2^T$. Indeed, Eq. (8) can be evaluated analytically to be zero for each odd t , and for $t = 2$ and $t = 4$, it yields [11]

$$\mathcal{S}^{(2)}(\rho) = \frac{1}{(d_1^2 - 1)(d_2^2 - 1)} \text{Tr}(TT^\dagger), \quad (9)$$

$$\mathcal{S}^{(4)}(\rho) = \frac{3}{(d_1^4 - 1)(d_2^4 - 1)} [2\text{Tr}(TT^\dagger TT^\dagger) + \text{Tr}(TT^\dagger)^2]. \quad (10)$$

Note that $\text{Tr}(TT^\dagger) = \sum_{i=1}^{d_1^2-1} \sigma_i^2$ and $\text{Tr}(TT^\dagger TT^\dagger) = \sum_{i=1}^{d_1^2-1} \sigma_i^4$ can be written in terms of the singular values $\sigma_1, \dots, \sigma_{d_1^2-1}$ of T . A similar evaluation is possible for general t , and knowledge of the *orthogonal* moments up to order $t = 2d$ allows us to recover the singular values of T completely. However, the orthogonal moments are not

directly accessible in an experiment. Thus, the question arises whether it is possible to choose the observable \mathcal{A} such that the unitary moments in Eq. (7) and the orthogonal moments coincide for all values of t .

The answer to this question depends strongly on the dimension. In Appendix B, we show the following.

Theorem 1: *Let $d \geq 2$ denote the local dimension of an n -partite quantum system. Then there exist unique diagonal operators \mathcal{A}_d such that, for all n -partite quantum states ρ ,*

- (a) $\mathcal{R}_{\mathcal{A}_d}^{(t)}(\rho) = \mathcal{S}^{(t)}(\rho) = 0$ for all odd $t = 1, 3, \dots$,
- (b) $\mathcal{R}_{\mathcal{A}_d}^{(t)}(\rho) = \mathcal{S}^{(t)}(\rho)$ for the subset of even $t = 0, 2, \dots, d$.

If the dimension is small then it additionally follows that

- (a) if $d = 3$, the fourth moment also coincides,
- (b) if $d = 2$, all moments coincide.

The proof as well as some examples can be found in Appendix B. Interestingly, for $d \geq 8$, complex diagonal entries of \mathcal{A}_d are required, making it formally not an observable. However, it can still be measured by assigning complex outcomes to a projective measurement result. Note further that the constructed observables can be easily checked to not yield the correct moments for $t > d$ (for $d > 4$). Thus, these results exclude the existence of observables that recover all moments (except for $d = 2$). We also show that it applies to cases of more than two parties as well.

Finally, we would like to stress that it is possible to explicitly construct low-rank operators that yield matching moments $t = 0, 1, 2, 3, 4$ for all dimensions d . These are given by

$$\mathcal{A}_d^{(4)} = \text{diag}(\pm\kappa_1, \pm\kappa_2, 0, \dots, 0) \quad (11)$$

with

$$\kappa_{1,2} = \frac{1}{2} \sqrt{d \pm \sqrt{d \left(8 - d - \frac{20}{d^2 + 1} \right)}}, \quad (12)$$

and play a central role in the remainder of the manuscript (see Appendix B for further details).

IV. SPACE OF SECOND AND FOURTH MOMENTS

Given the existence of these operators for moments two and four, we aim to obtain the boundaries of the sets of states of different Schmidt numbers in the space spanned by $\mathcal{R}_{\mathcal{A}}^{(2)}$ and $\mathcal{R}_{\mathcal{A}}^{(4)}$. To that end, we minimize and maximize $\mathcal{R}_{\mathcal{A}}^{(4)}$ subject to keeping $\mathcal{R}_{\mathcal{A}}^{(2)}$ constant and some positivity

and Schmidt number constraints, respectively, in terms of the singular values. Of course, we do not know the exact constraints, but we obtain outer approximations to the projected spaces by some necessary conditions, and then try to construct states for each point within the obtained shape to show that in some cases it is actually not an approximation, but a faithful representation of the space.

As a result, we obtain the regions shown in Fig. 1, with $d_1 = d_2 = 3$, for the set of states of Schmidt numbers 1 (i.e., the set of separable states), 2, and 3 (i.e., all states). All in all, the respective regions represent the hierarchical entanglement structure of the space of bipartite quantum states with increasing entanglement dimensionality. In particular, Fig. 1 visualizes the information about the entanglement structure that is gained by combining moments of different orders, as knowledge of the second moment alone detects the entanglement of strictly fewer states. Also, note that we normalize the values of the moments such that $\tilde{\mathcal{R}}_{\mathcal{A}}^{(t)}(|00\rangle) = 1$ for product states, i.e.,

$$\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} := (d_1 + 1)(d_2 + 1)\mathcal{R}_{\mathcal{A}}^{(2)}, \quad (13)$$

$$\tilde{\mathcal{R}}_{\mathcal{A}}^{(4)} := \frac{(d_1 + 1)(d_2 + 1)(d_1^2 + 1)(d_2^2 + 1)}{9(d_1 - 1)(d_2 - 1)}\mathcal{R}_{\mathcal{A}}^{(4)}. \quad (14)$$

With this normalization, the shape of the set of separable states depends only on the smaller of the two dimensions and exhibits $d_1^2 - 2$ kinks along the lower boundary, which can be stated analytically. In the case of the sets of SNs $k = 2$ and $k = 3$, we note that the upper bound presented in Fig. 1 is likely not tight as its derivation is based on the rather weak purity bound of $\text{Tr}(\rho^2) \leq 1$, and we are unable to find states lying on this boundary. The detailed optimization process, as well as the analytical form of the boundaries for all dimensions for the case $k = 1$, can be found in Appendix C.

Let us highlight some important observations for the set of separable states.

- (a) The upper bound of the red, separable set coincides with the upper bound for all states.
- (b) The lower bound of the separable set is a step-wise defined function [Eq. (C3)] with kinks at the positions $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} = 1/(d_1^2 - 1), 1/(d_1^2 - 2), \dots, \frac{1}{3}, \frac{1}{2}$. Thus, switching from d_1 to $d_1 + 1$ changes only some details on the left-hand side of the plot, leaving most of the figure unchanged. Because of our normalization, the difference in the figures for d_1 and $d_1 + 1$ vanishes for large d_1 . As the normalization is dimension dependent, this does not imply that the criterion will be less efficient for larger d_1 .
- (c) States on the lower bound of the separable set are characterized by the fact that the singular values of the correlation matrix are of the form $(0, \dots, 0, l, m, \dots, m)$ with $l \leq m$, and all of them summing up to $\sqrt{(d_1 - 1)(d_2 - 1)}$.

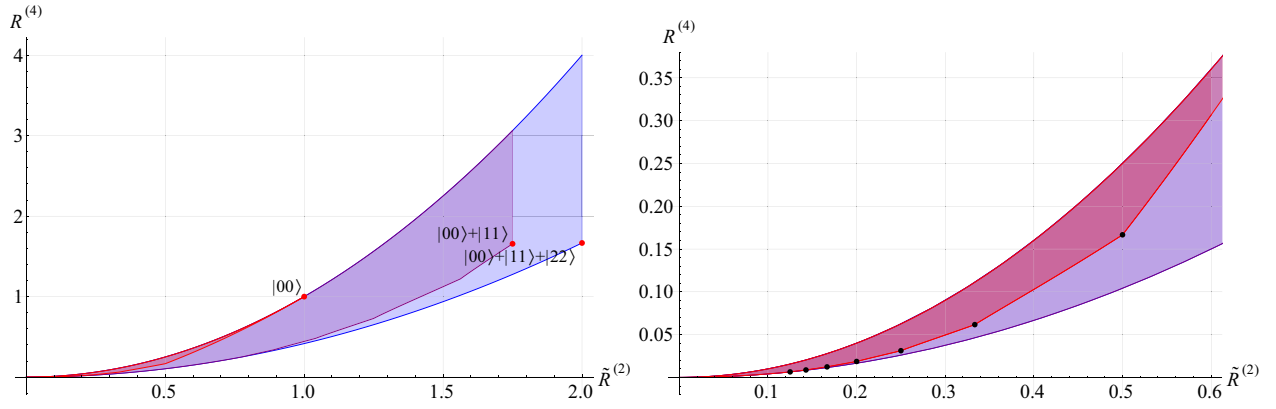


FIG. 1. Left: the space of all states (red, violet, and blue) and the subspaces of states of Schmidt number 2 (violet) and separable states (red) according to the generalized de Vicente criterion in the space spanned by the second and fourth moments given by Eq. (7) for $d_1 = d_2 = 3$. Right: enlarged view of the lower left part of the plot. The lower boundary of the separable set is given by Eq. (C3) and exhibits $d^2 - 2$ kinks (displayed as black dots), which correspond to states with a dichotomous singular value structure.

- (d) States at the kinks are characterized by singular values being $(0, \dots, 0, m, \dots, m)$, summing up to $\sqrt{(d_1 - 1)(d_2 - 1)}$.
- (e) There exist entangled states with $1 < \tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} \leq (d_1 + 1)d_2/d_1(d_2 - 1)$. The maximal value of $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}$ is achieved by the maximally entangled state $|\phi^+\rangle = (1/\sqrt{d_1}) \sum_{i=0}^{d_1-1} |ii\rangle$.
- (f) The lower bound of the set of all states is traced by the isotropic states, $\rho_{\text{iso}} = (1 - p) |\phi^+\rangle\langle\phi^+| + p \mathbb{1}/d_1 d_2$. The lower bound coincides with that of the separable states for $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} \leq 1/(d_1^2 - 1)$, which is exactly the region where ρ_{iso} is separable. Thus, the whole range of entanglement of the isotropic state can be detected.

V. OPTIMALITY OF THE CRITERION

Given that we used a specific entanglement criterion in order to construct the set of separable states in the $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}$ - $\tilde{\mathcal{R}}_{\mathcal{A}}^{(4)}$ plane, the question remains of how tight this criterion really is. Thus, we attempt to construct a separable state for each point within the obtained figure. If this turns out to be possible then this proves that the figure is optimal, i.e., there exists no better, smaller region, and thus that the de Vicente criterion is indeed optimal when given the knowledge of $\sum_i \sigma_i^2$ and $\sum_i \sigma_i^4$.

Note that it suffices to construct separable states on the boundary of the set. All points in the interior can then be reached by mixing the boundary states with white noise in the way detailed below for the states on the upper boundary.

We start by explicitly constructing states for the upper boundary, connecting the pure product states at $(\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}, \tilde{\mathcal{R}}_{\mathcal{A}}^{(4)}) = (1, 1)$ with the origin, where the maximally

mixed state is situated. Considering the family of states

$$\rho_{\text{upper}}(p) = (1 - p) |00\rangle\langle 00| + \frac{p}{d_1 d_2} \mathbb{1}, \quad (15)$$

we note that the correlation matrix of $\rho_{\text{upper}}(p)$ is just a multiple of that of the pure product state, and therefore $\tilde{\mathcal{R}}_{\mathcal{A}}^{(i)}[\rho_{\text{upper}}(p)] = (1 - p)^i$, tracing exactly the upper boundary of the set.

For the lower boundary, we restrict our attention to the case of $d_1 = d_2 \equiv d$.

As noted before, the lower bound for all states is traced by the isotropic state, which becomes separable for $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} \leq 1/(d^2 - 1)$, where the lower bounds of both sets coincide. Thus, we already have separable states for the lower bound in that region. The situation for the rest of the lower bound is more complicated, but simplified by the fact that states at the kinks have a special singular value structure, namely that all of the nonvanishing singular values coincide and sum to $d - 1$.

A. Constructions using equiangular sets

An equiangular set (sometimes called equiangular lines) of size N is a set of N normalized states $\{\psi_i\}_{i=1}^N$, such that $|\langle\psi_i|\psi_j\rangle| = C$ for some constant C if $i \neq j$ [35,36]. A popular example is that of a SIC POVM, where $C = 1/\sqrt{d+1}$. Here, however, we consider sets with $C = 1/\sqrt{d}$, from which states at the kinks can be constructed.

Theorem 2: *Let $\{\psi_i\}_{i=1}^N$ be an equiangular set of normalized vectors in \mathbb{C}^d , with $|\langle\psi_i|\psi_j\rangle| = 1/\sqrt{d}$ if $i \neq j$. Then*

$$\rho = \frac{1}{N} \sum_{i=1}^N |\psi_i\rangle\langle\psi_i| \otimes |\psi_i\rangle\langle\psi_i| \quad (16)$$

lies on the kink at $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}(\rho) = 1/N$.

The proof can be found in Appendix D.

It follows from this theorem that, if there exist $d^2 - 1$ states with distance $1/\sqrt{d}$, we would have a symmetric separable state at each kink. However, the maximal size of such sets is subject to bounds and no systematic constructions are known for arbitrary d [36]. For small d , however, one can construct them explicitly.

For $d = 2$, the vectors $|0\rangle$, $|+\rangle$, and $|+_i\rangle$ form a maximal equiangular set with the correct angle. As $d^2 - 1 = 3$ in this case, this yields states for all of the kinks.

For $d = 3$, one can find a maximal set consisting of four vectors, which is less than eight, the number required to obtain a state for every kink, implying that one needs a different strategy for the rest of the kinks.

In order to obtain a lower bound on the maximal size of equiangular sets with overlap $1/\sqrt{d}$, we can borrow some results from the construction of SIC POVMs. There, one searches for equiangular sets with $C = 1/\sqrt{d+1}$ and it was conjectured by Zauner that the maximal set size is always given by d^2 [37] (concrete SIC POVMs are known for all dimensions $d \leq 193$ [38]). In order to construct sets with overlap $1/\sqrt{d}$, we can take a SIC POVM of dimension $d - 1$ and pad an extra dimension to the vectors. Of course, this procedure might be wasteful, such that it only yields a lower bound, and it relies on Zauner’s conjecture being true. Nevertheless, it implies that we can always find at least $(d - 1)^2$ vectors of the $d^2 - 1$ that we would need.

Note that, with this construction, we can also construct states on the boundary between the kinks.

Corollary 1: *Let $\{\psi_i\}_{i=1}^N \cup \{\psi\}$ be an equiangular set of size $N + 1$ of normalized vectors in \mathbb{C}^d with overlap $1/\sqrt{d}$. Then the family of states*

$$\rho(p) = \frac{p}{N} \sum_{i=1}^N |\psi_i\rangle\langle\psi_i| \otimes |\psi_i\rangle\langle\psi_i| + (1 - p) |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| \quad (17)$$

traces the boundary of the separable set between the kinks at $\tilde{\mathcal{R}}_A^{(2)}[\rho(N/(N + 1))] = 1/(N + 1)$ and $\tilde{\mathcal{R}}_A^{(2)}[\rho(1)] = 1/N$.

The proof is given in Appendix E.

Note that in the limit of large dimension, an increasing percentage of the lower boundary is covered by this construction due to the fact that we find states for each point between $\tilde{\mathcal{R}}_A^{(2)} = 1/(d - 1)^2$ and $\tilde{\mathcal{R}}_A^{(2)} = 1$ (under the assumption that Zauner’s conjecture is true).

The question remains whether the missing kinks can also be covered by separable states. While we cannot answer this question completely, we can find additional states using mutually unbiased bases (MUBs).

B. Constructions using MUBs

A collection of orthonormal bases, $\{|\psi_i^1\rangle\}_{i=0}^{d-1}$, $\{|\psi_i^2\rangle\}_{i=0}^{d-1}, \dots$ is called mutually unbiased if $|\langle\psi_i^k|\psi_j^l\rangle| = 1/\sqrt{d}$ if $k \neq l$. For a fixed dimension d , there are at most $d + 1$ mutually unbiased bases. However, only for prime power dimensions $d = p^m$, constructions of $d + 1$ bases are known (see Ref. [39] and the references therein). For $d = 6$, it is widely believed that only three MUBs exist. Indeed, taking a single vector out of each basis yields an equiangular set of the right overlap for Theorem 2. However, as the maximal size of sets created in this way is given by $d + 1$, this construction is not good enough for our purposes. However, a set of m MUBs can still be used to construct states at some intermediate kinks at $\tilde{\mathcal{R}}_A^{(2)} = 1/l(d - 1)$ for $l = 1, \dots, m$.

Theorem 3: *Consider a set of m MUBs $\{|\psi_j^l\rangle\}_{j=1}^d, \dots, \{|\psi_j^m\rangle\}_{j=1}^d$. Then the state*

$$\rho := \frac{1}{md} \sum_{l=1}^m \sum_{k=1}^d |\psi_k^l\rangle\langle\psi_k^l| \otimes |\psi_k^l\rangle\langle\psi_k^l| \quad (18)$$

lies at the kink at $\tilde{\mathcal{R}}_A^{(2)} = 1/m(d - 1)$.

The proof is given in Appendix F.

With all of these constructions, we are able to construct states for many of the kinks, but not all of them. For example, for $d = 3$, using a maximal equiangular set of size 4, together with the MUB constructions, yields states for the kinks at $K = 1, 2, 3, 4, 6$, and 8; thus, the states at $K = 5$ and $K = 7$ are missing. For $d = 4$, equiangular sets yield states for $K = 1, \dots, 9$, and the MUB construction adds the cases $K = 12$ and $K = 15$, leaving open the cases $K = 10, 11, 13$, and 14. For $d = 6$, the situation is more complex, as only sets of three MUBs are known. The situation is displayed in Fig. 2.

VI. EXISTENCE OF MUBS AND SIC POVMs

It is conjectured that there exist at most three MUBs in $d = 6$. However, there is no proof for this; in fact, there is not even a proof that the number of MUBs is not maximal, i.e., $d + 1 = 7$. We focus here on the question of whether six or seven MUBs in $d = 6$ exist.

According to Theorem 3, the following statements hold.

- (a) If six MUBs exist then there exists a symmetric and homogeneous (meaning $p_i = p_j$) separable state at $\tilde{\mathcal{R}}_A^{(2)} = \frac{1}{30}$ with a correlation matrix being proportional to a projector.
- (b) If seven MUBs exist then there exists a symmetric and homogeneous decomposition of the isotropic

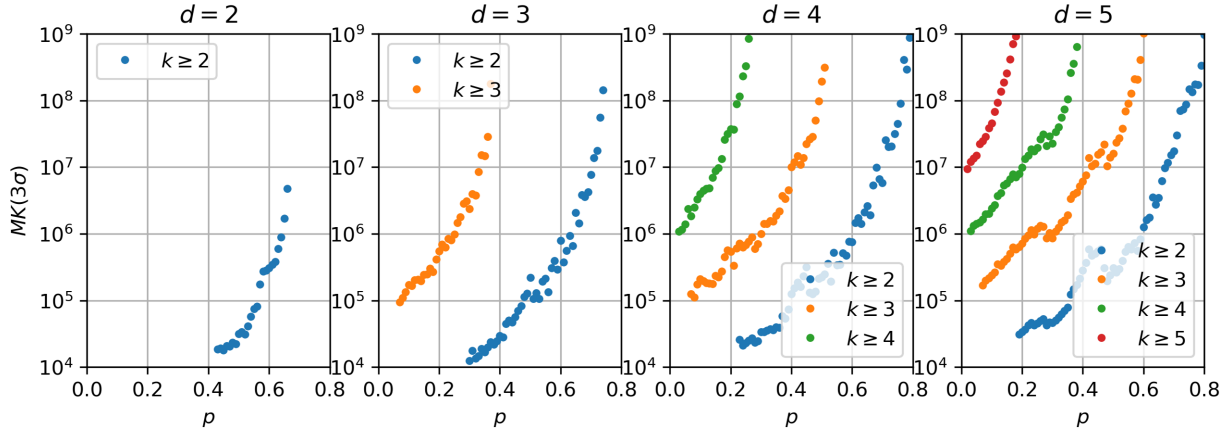


FIG. 2. Estimated number of total measurements MK required to observe a 3σ violation of the criterion in Lemma 1 using randomized measurements for dimensions $d = 2, 3, 4, 5$ for the isotropic state in Eq. (20) as a function of the noise parameter p . For each dimension d , we display the required number of measurements to detect Schmidt numbers of at least $2, \dots, d$. Note that the curves start at some value p_{\min} where our criterion starts to be applicable (for smaller values of p , $\mathcal{R}_{\mathcal{A}}^{(2)}$ alone allows for detection of that Schmidt number), and ends at p_{\max} , where the criterion fails to detect higher Schmidt numbers.

state at $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} = 1/(d^2 - 1) = \frac{1}{35}$ with a correlation matrix being proportional to a projector.

The contraposition states that, if such symmetric, homogeneous separable states do not exist at the given coordinates, then such sets of MUBs do not exist. We do not consider the case of $m = 5$ here, because an equiangular set construction exists at $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} = \frac{1}{25}$, making it unlikely that our trick works.

We can formulate a relaxed version of the existence problem in terms of a convex feasibility problem with rank constraint. For that, we assume without loss of generality that the matrix basis we choose is Hermitian, making the correlation matrix T real valued. Then, the feasibility problem can be stated as

$$\text{find } T \in \mathbb{R}^{(d^2-1) \times (d^2-1)} \quad (19a)$$

$$\text{subject to } T \text{ symmetric, } T \geq 0, \quad (19b)$$

$$\mathbb{1} \otimes \mathbb{1} + \sum_{ij} T_{ij} \lambda_i \otimes \lambda_j \in \text{SEP}, \quad (19c)$$

$$\text{Tr}(T^k) = \frac{d-1}{m^{k-1}} \quad \text{for } k \geq 1. \quad (19d)$$

Here, SEP stands for the set of separable states. If the problem is infeasible then no m MUBs in dimension d exist. Note that the constraints in the feasibility problem are hard to implement, but could be tackled by a combination of two semidefinite programming hierarchies [40,41]. Using the dual representation of this problem, it might be possible to obtain infeasibility certificates that allow one to analytically show the infeasibility of problem (19) [42].

VII. NUMBER OF REQUIRED MEASUREMENTS FOR ENTANGLEMENT DETECTION

To conclude, let us estimate the total number of required measurements for detecting a violation of the criterion in Lemma 1 for the family of isotropic states,

$$\rho_{\text{iso}}(p) = (1-p) |\phi^+\rangle\langle\phi^+| + \frac{p}{d_1 d_2} \mathbb{1}, \quad (20)$$

parameterized by a noise parameter p . To that end, we simulate the measurement process of the two moments $\mathcal{R}_{\mathcal{A}}^{(2)}$ and $\mathcal{R}_{\mathcal{A}}^{(4)}$ for the observable $\mathcal{A}_d^{(4)}$ given in Eq. (11). The total number of measurements is given by MK , where M denotes the number of random local unitaries, whereas K denotes the number of measurements per unitary in order to estimate the trace.

We first simulate the measurement processes for fixed MK while varying M . Looking at the achievable standard deviations of the two moments suggests that always choosing $K \approx 100$ will yield standard deviations close to the minimum. We therefore fix $K = 100$ and simulate the measurement process 100 times for each choice of noise parameter p and dimension $d_1 = d_2 = d \in \{2, 3, 4, 5\}$, and values $M \in \{10, 30, 100, 300, 1000\}$. As expected, the standard deviation of the criterion over the 100 repetitions scales with $1/\sqrt{M}$, which allows us to extrapolate the deviation until we observe a 3σ violation of our criterion for different values of k .

We display the estimated number of measurements MK to obtain a 3σ violation of the criterion as a function of the noise parameter p in Fig. 3. The results suggest that entanglement detection (i.e., detecting Schmidt number $k \geq 2$) in the regime where our criterion applies is possible starting from roughly 2×10^4 measurements for lower values of

parameter p , regardless of the dimensions, whereas detection of higher Schmidt numbers requires at least 10^5 (for $k \geq 3$) or 10^6 (for $k \geq 4$) measurements. Note that, for increasing values of the noise parameter p , the number of required measurements also increases.

VIII. CONCLUSIONS

In this paper, we generalized entanglement criteria based on norms of correlation matrices of bipartite quantum states in order to detect their Schmidt numbers and connected them to moments of randomized measurements. We constructed observables whose random moments coincide with orthogonal moments for $t \leq d$, such that their measurement gives direct insight into the singular values of the correlation matrix of a quantum state. Furthermore, we provided explicit low-rank observables that yield the second and fourth moments, i.e., knowledge of the sum of squares and the sum of quarts of the singular values of the underlying state.

Further on, we explored the landscape of the second and fourth moments for arbitrary dimension d . In particular, we showed how to express the introduced Schmidt number criterion in this language and we showed that at least in the case of $d = 2$ (and in the limit of large dimensions, provided that Zauner's conjecture is true), the subset of separable states predicted by the de Vicente criterion is optimal. To do so, we constructed separable states for each point in the set resulting from the de Vicente criterion by exploiting the existence of SIC POVMs and sets of mutually unbiased bases in specific dimensions. In this way, we shed light onto the question of whether a given vector of singular values exists in a (separable) quantum state.

An immediate future research direction in this context would be a similar analysis for the subset of higher Schmidt numbers: here, the question of whether our generalized criterion is optimal is even less clear. Nevertheless, the additional knowledge of higher moments $\tilde{\mathcal{R}}_A^{(t)}$ for $t > 4$ allows one to reconstruct the singular values of the correlation matrix more precisely and would eventually allow one to detect all states that violate our criterion.

In principle, it should even be possible to detect all states of a certain Schmidt number using randomized measurements, as the tool allows one to measure all polynomial local unitary invariants [43]. Identifying the most relevant ones for bounding the Schmidt number of a state is a challenging task for further studies.

Given the connection between the existence of MUBs and SIC POVMs to the present geometrical problem of characterizing the set of separable quantum states, it seems fruitful to fully understand the geometry of sets of singular values existing in states of limited Schmidt numbers. However, solving this task could be as demanding as solving the aforementioned existence problems directly.

Our findings pose the more general question of generalizations of known entanglement criteria to the detection of entanglement dimensionality. It has been known before that the reduction map criterion can be generalized to detect the Schmidt number [21], and recently, it was shown that the covariance matrix criterion can also be extended in this direction [24]. The same question could be investigated for other criteria as well.

Finally, we assessed the experimental feasibility of the randomized measurement scheme to detect Schmidt numbers using our criterion and found that a reasonable number of total measurements of around 10^6 would suffice to detect Schmidt numbers of at least 2, 3, and 4. This implies that the measurement scheme could be implemented in optical setups as well as relatively slow trapped ion experiments, where preparation and entangling gate times in the range of microseconds to milliseconds are usually limiting the repetition rate [44]. In all of these setups, however, the implementation of Haar random local unitary gates could be challenging, and a thorough analysis of the impacts of deviating distributions on the results of randomized measurements would be advantageous for real-world implementations.

ACKNOWLEDGMENTS

We thank Felix Huber for fruitful discussion. N.W. acknowledges support from the QuantERA project QuICHE via the German Ministry of Education and Research (BMBF Grant No. 16KIS1119K). A.K. acknowledges funding from the Ministry of Economic Affairs, Labour and Tourism Baden-Württemberg, under the project QORA.

Note added.—Recently, we became aware that related results were derived in Ref. [23]. While they derived the same criterion as our Lemma 1, their proof is completely different and makes use of the covariance matrix criterion. Furthermore, they proceeded by comparing the criterion to fidelity-based Schmidt rank witnesses and discussed generalizations to multipartite states, whereas we focus on the optimality and experimental implementability.

APPENDIX A: PROOF OF LEMMA 1 AND GENERALIZATIONS

First, we prove the statement of Lemma 1 in the main text. After that, we generalize the statement to the whole family of entanglement criteria presented in Ref. [9].

Lemma 2: *Let ρ_k be a bipartite quantum state as before with Bloch decomposition as in Eq. (1) and $\text{SN}(\rho_k) \leq k$. Then*

$$\|T\|_{\text{Tr}} \leq \sqrt{(d_1 - 1)(d_2 - 1)} + \sqrt{d_1 d_2}(k - 1). \quad (\text{A1})$$

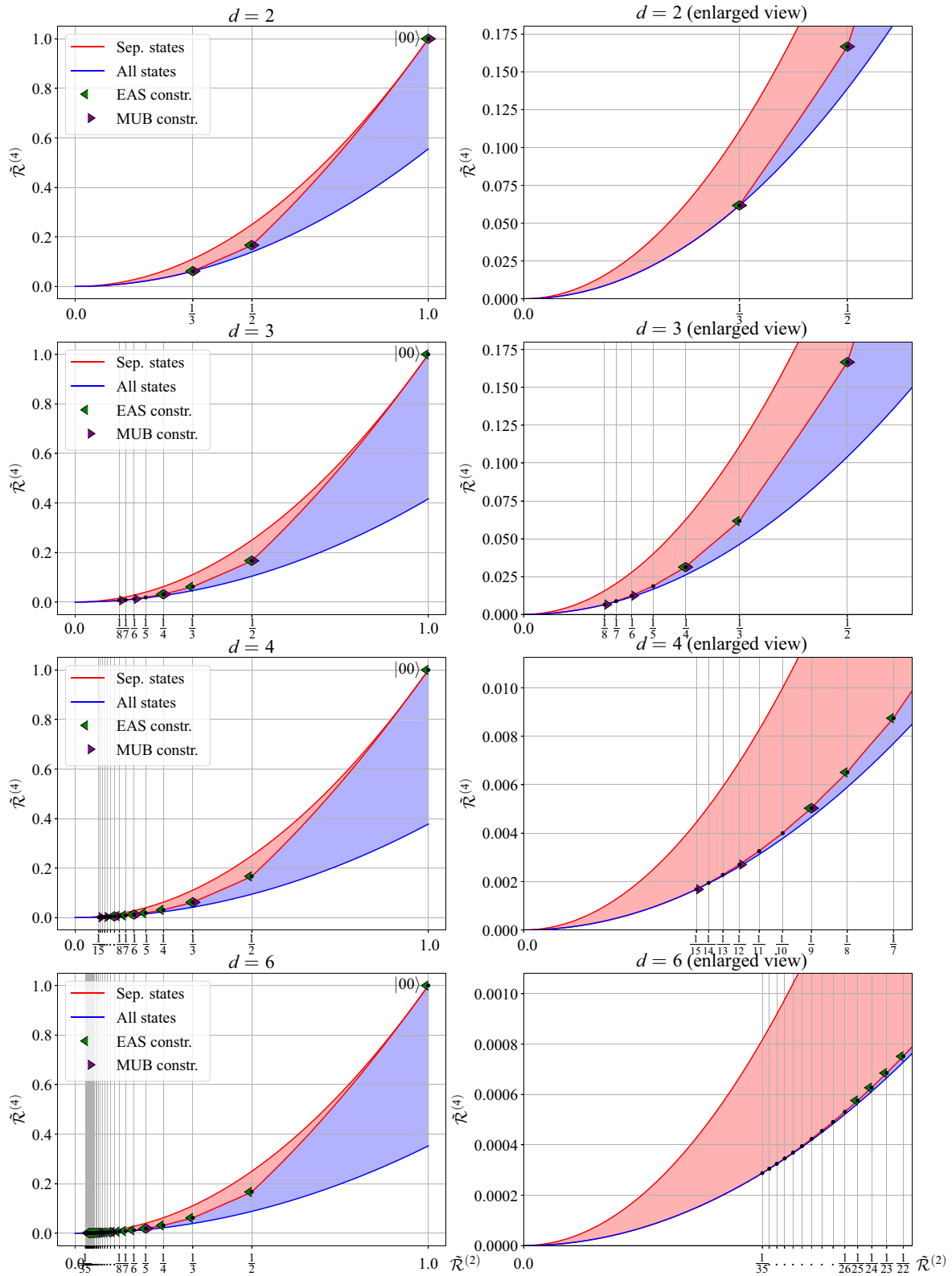


FIG. 3. The moment landscape of the second and fourth moments. Displayed is the set of all states (red and blue) and the subset of separable states (red) together with its kinks on the lower boundary for $d = 2, 3, 4,$ and 6 . The markers labeled MUB (mutually unbiased basis) and EAS (equiangular set) indicate that a separable state at the corresponding point can be constructed by one of our methods.

Proof. Let $\rho_k = \sum_i p_i |\psi_i\rangle\langle\psi_i|$ with $\text{SR}(|\psi_i\rangle) \leq k$. Then, $\|T\|_{\text{Tr}} \leq \sum_i p_i \|T(|\psi_i\rangle\langle\psi_i|)\|_{\text{Tr}}$. For some fixed i , we explicitly write

$$|\psi_i\rangle\langle\psi_i| = \sum_{m,n=1}^r \sqrt{q_m q_n} |a_m\rangle\langle a_n| \otimes |b_m\rangle\langle b_n|, \quad (\text{A2})$$

where $r \leq k$. Each of the objects $|a_m\rangle\langle a_n|$ and $|b_m\rangle\langle b_n|$ can be decomposed into the operator bases $\{\lambda_i\}$, $\{\tilde{\lambda}_i\}$, respectively, such that

$$|a_m\rangle\langle a_n| = \frac{1}{d_1} \left[\delta_{mn} \mathbb{1} + \sum_{l=1}^{d_1-1} \alpha_l^{(m,n)} \lambda_l \right], \quad (\text{A3})$$

$$|b_m\rangle\langle b_n| = \frac{1}{d_2} \left[\delta_{mn} \mathbb{1} + \sum_{l=1}^{d_2-1} \beta_l^{(m,n)} \tilde{\lambda}_l \right]. \quad (\text{A4})$$

Note that the fact that the $|a_m\rangle$ and $|b_m\rangle$ are orthonormal fixes the constant in front of the identity.

Using this decomposition, we get

$$\begin{aligned} \|T(|\psi_i\rangle\langle\psi_i|)\|_{\text{Tr}} &= \left\| \sum_{m,n=1}^r \sqrt{q_m q_n} \vec{\alpha}^{(m,n)} \vec{\beta}^{(m,n)\dagger} \right\|_{\text{Tr}} \\ &\leq \sum_{m,n=1}^r \sqrt{q_m q_n} \|\vec{\alpha}^{(m,n)}\| \|\vec{\beta}^{(m,n)}\|, \end{aligned} \quad (\text{A5})$$

where we exploit the usual properties of the trace norm. Finally, we upper bound the Bloch vectors $\vec{\alpha}^{(m,n)}$ and $\vec{\beta}^{(m,n)}$. To that end, we write

$$1 = \text{Tr}(|a_m\rangle\langle a_n| |a_n\rangle\langle a_m|) = \frac{1}{d_1} (\delta_{mn} + \|\vec{\alpha}^{(m,n)}\|^2), \quad (\text{A6})$$

and likewise for $\beta^{(m,n)}$. Therefore,

$$\begin{aligned} \|T(|\psi_i\rangle\langle\psi_i|)\|_{\text{Tr}} &\leq \sum_{m,n=1}^r \sqrt{q_m q_n} \sqrt{d_1 - \delta_{mn}} \sqrt{d_2 - \delta_{mn}} \\ &= \sum_{m=1}^r q_m \sqrt{d_1 - 1} \sqrt{d_2 - 1} + \\ &\quad + 2 \sum_{m < n=1}^r \sqrt{q_m q_n} \sqrt{d_1 d_2} \\ &\leq \sqrt{d_1 - 1} \sqrt{d_2 - 1} + \sqrt{d_1 d_2} (r - 1), \end{aligned} \quad (\text{A7})$$

as the maximal value of the sum is attained when $q_m = q_n = 1/r$. Finally, using $r \leq k$, we obtain the claim. \blacksquare

Corollary 2: Let ρ_k be a bipartite quantum state as before with Bloch decomposition as in Eq. (1) and $\text{SN}(\rho_k) \leq k$. Let $x, y \geq 0$. Then

$$\begin{aligned} \|D_x C D_y\|_{\text{Tr}} &\leq \sqrt{(d_1 - 1 + x^2)(d_2 - 1 + y^2)} \\ &\quad + \sqrt{d_1 d_2} (k - 1), \end{aligned} \quad (\text{A8})$$

where $D_x = \text{diag}(x, 1, \dots, 1)$, $D_y = \text{diag}(y, 1, \dots, 1)$, and

$$C = \begin{pmatrix} 1 & \vec{\beta}^\dagger \\ \vec{\alpha} & T \end{pmatrix}.$$

Proof. The proof follows the same lines as the proof of Lemma 1. Instead of considering the correlation matrix T , we calculate the trace norm of $D_x C D_y$ as defined above. In this case, however,

$$\begin{aligned} \|D_x C(|\psi_i\rangle\langle\psi_i|) D_y\|_{\text{Tr}} &\leq \sum_{m,n=1}^r \sqrt{q_m q_n} \sqrt{x^2 \delta_{mn} + \|\vec{\alpha}^{(m,n)}\|^2} \\ &\quad \sqrt{y^2 \delta_{mn} + \|\vec{\beta}^{(m,n)}\|^2}. \end{aligned}$$

The rest of the proof remains the same, yielding the claim. \blacksquare

APPENDIX B: EQUIVALENCE OF ORTHOGONAL AND UNITARY MOMENTS

In this appendix, we are going to construct observables \mathcal{A}_d such that the unitary moments $\mathcal{R}_{\mathcal{A}_d}^{(t)}(\rho)$ coincide with the orthogonal moments $\mathcal{S}^{(t)}(\rho)$ for all n -partite quantum states of local dimension d and for as many moments t as possible. The outline of the argument is as follows. First, we describe the n -partite case in general, then we show that, for \mathcal{A}_d to yield the correct moments in this case, it is necessary that it does so already on a single-particle level. Then we show that, for single particles, the spectrum of \mathcal{A}_d is already fixed by the constraints that it should yield the same moments for all odd t , as well as the even moments $t \leq d$. Next, we show that this fixed spectrum also yields these coinciding moments for n -partite states. Finally, we construct a specific simple rank-4 observable that leads to coinciding second and fourth moments.

1. Moments for n -partite states

For a multipartite quantum state ρ of local dimension d , we choose a local, Hermitian basis $\{\lambda_0, \dots, \lambda_{d^2-1}\}$ with

$\lambda_0 = \mathbb{1}$, $\text{Tr}(\lambda_i \lambda_j) = d\delta_{ij}$ to write

$$\rho = \frac{1}{d^n} \sum_{i_1, \dots, i_n=0}^{d^2-1} \alpha_{i_1 \dots i_n} \lambda_{i_1} \otimes \dots \otimes \lambda_{i_n}. \quad (\text{B1})$$

To start, we define two different moments. First, we choose a local observable A and write the moments of the distribution of measurement results under local unitary rotations, which map

$$\rho \rightarrow \rho_U = U_1 \otimes \dots \otimes U_n \rho U_1^\dagger \otimes \dots \otimes U_n^\dagger \quad (\text{B2})$$

as

$$\begin{aligned} \mathcal{R}_{\mathcal{A}d}^{(t)}(\rho) &= \int dU_1 \dots dU_n \langle A \otimes \dots \otimes A \rangle_{\rho_U}^t \\ &= \int dU_1 \dots dU_n \langle U_1^\dagger \mathcal{A}_d U_1 \otimes \dots \otimes U_n^\dagger \mathcal{A}_d U_n \rangle_{\rho}^t. \end{aligned} \quad (\text{B3})$$

Second, we instead rotate the Bloch vectors locally, i.e.,

$$\begin{aligned} \rho \rightarrow \rho_O &= \frac{1}{d^n} \sum_{\substack{i_1, \dots, i_n \\ j_1, \dots, j_n}} (O_1)_{i_1 j_1} \dots (O_n)_{i_n j_n} \alpha_{j_1 \dots j_n} \lambda_{i_1} \otimes \lambda_{i_n} \\ &= \frac{1}{d^n} \sum_{i_1, \dots, i_n} \alpha_{i_1 \dots i_n} [O_1^T \vec{\lambda}]_{i_1} \otimes \dots \otimes [O_n^T \vec{\lambda}]_{i_n}, \end{aligned} \quad (\text{B4})$$

where the O_i are orthogonal matrices of size d^2 , but the upper left entry is chosen to be 1 in order to preserve the property of the basis that $\lambda_0 = \mathbb{1}$. Thus, effectively,

$$O_i = \begin{pmatrix} 1 & \vec{0}^T \\ \vec{0} & \tilde{O}_i \end{pmatrix} \quad (\text{B5})$$

with $\tilde{O}_i \in O(d^2 - 1)$. Then, we arbitrarily choose one of the traceless basis elements to measure, e.g., λ_1 , and define the moments with respect to random local Bloch bases as

$$\begin{aligned} \mathcal{S}^{(t)}(\rho) &= \int d\tilde{O}_1 \dots d\tilde{O}_n \langle \lambda_1 \otimes \dots \otimes \lambda_1 \rangle_{\rho_O}^t \\ &= \int d\tilde{O}_1 \dots d\tilde{O}_n \langle (O_1 \vec{\lambda})_1 \otimes \dots \otimes (O_n \vec{\lambda})_1 \rangle_{\rho}^t \\ &= \frac{1}{V^n} \int d\vec{\alpha}_1 \dots d\vec{\alpha}_n \langle \vec{\alpha}_1 \cdot \vec{\lambda} \otimes \dots \otimes \vec{\alpha}_n \cdot \vec{\lambda} \rangle_{\rho}^t, \end{aligned} \quad (\text{B6})$$

where the integration spans all $(d^2 - 1)$ -dimensional unit vectors $\vec{\alpha}_i$, $\vec{\lambda} = (\lambda_1, \dots, \lambda_{d^2-1})^T$, and $V = 2\sqrt{\pi}^{d^2-1} / \Gamma[(d^2 - 1)/2]$ is the surface of the unit sphere in $d^2 - 1$ dimensions.

While the orthogonal moments $\mathcal{S}^{(t)}$ do not depend on the specific choice of observable, the unitary moments $\mathcal{R}_{\mathcal{A}}^{(t)}$ do depend on \mathcal{A} . We aim to answer the question: for a fixed local dimension d , can one choose \mathcal{A} such that $\mathcal{S}^{(t)}(\rho) = \mathcal{R}_{\mathcal{A}}^{(t)}(\rho)$ for all states ρ ?

2. Reduction to single qudits

Before answering the question for n -partite states, we consider the following necessary condition: if $\mathcal{S}^{(t)}(\rho) = \mathcal{R}_{\mathcal{A}}^{(t)}(\rho)$ for all ρ then it will be true for $\rho_1^{\otimes n}$, where ρ_1 is some single-qudit state, implying that $\mathcal{S}^{(t)}(\rho_1) = \mathcal{R}_{\mathcal{A}}^{(t)}(\rho_1)$ on the single-particle level.

In order to find conditions for \mathcal{A} in this case, we first evaluate the orthogonal moments for a general single-qudit state

$$\rho = \frac{1}{d} \left(\mathbb{1} + \sum_{i=1}^{d^2-1} \alpha_i \lambda_i \right). \quad (\text{B7})$$

We get

$$\begin{aligned} \mathcal{S}^{(t)}(\rho) &= \frac{1}{V} \int d\vec{\beta} \langle \vec{\beta} \cdot \vec{\lambda} \rangle_{\rho}^t \\ &= \frac{1}{V} \int d\vec{\beta} \left(\sum_{i=1}^{d^2-1} \alpha_i \beta_i \right)^t. \end{aligned} \quad (\text{B8})$$

We choose $(d^2 - 1)$ -dimensional spherical coordinates and set, without loss of generality, $\vec{\alpha} = (0, \dots, 0, \alpha)^T$, such that $\vec{\alpha} \cdot \vec{\beta} = |\alpha| \cos(\phi_1)$. Thus,

$$\begin{aligned} \mathcal{S}^{(t)}(\rho) &= \frac{|\alpha|^t}{V} \int_0^\pi d\phi_1 \dots \int_0^\pi d\phi_{d^2-3} \int_0^{2\pi} d\phi_{d^2-2} \\ &\quad \times \cos(\phi_1)^t \sin(\phi_1)^{d^2-3} \prod_{k=2}^{d^2-3} \sin(\phi_{d^2-1-k})^{k-1} \\ &= \frac{2\pi |\alpha|^t}{V} \delta_{t, \text{even}} \frac{\Gamma[(d^2 - 2)/2] \Gamma[(t + 1)/2]}{\Gamma[(d^2 - 1 + t)/2]} \\ &\quad \prod_{k=2}^{d^2-3} \left[\frac{\sqrt{\pi} \Gamma(k/2)}{\Gamma[(k + 1)/2]} \right] \\ &= \frac{2\sqrt{\pi}^{d^2-2} |\alpha|^t}{V} \delta_{t, \text{even}} \frac{\Gamma[(t + 1)/2]}{\Gamma[(d^2 - 1 + t)/2]} \\ &= \frac{|\alpha|^t \Gamma[(d^2 - 1)/2] \Gamma[(t + 1)/2]}{\sqrt{\pi} \Gamma[(d^2 - 1 + t)/2]} \delta_{t, \text{even}}. \end{aligned} \quad (\text{B9})$$

It will later become useful to express the Bloch length $|\alpha|^t$ in terms of the purity of ρ via $|\alpha|^2 = d\text{Tr}(\rho^2) - 1$ for the

case of even t :

$$\begin{aligned} \mathcal{S}^{(t)}(\rho) &= \frac{\Gamma[(d^2 - 1)/2]\Gamma[(t + 1)/2]}{\sqrt{\pi}\Gamma[(d^2 - 1 + t)/2]} (d\text{Tr}(\rho^2) - 1)^{t/2} \\ &= \frac{\Gamma[(d^2 - 1)/2]\Gamma[(t + 1)/2]}{\sqrt{\pi}\Gamma[(d^2 - 1 + t)/2]} \\ &\quad \sum_{j=0}^{t/2} \binom{t/2}{j} (-1)^{t/2-j} d^j \text{Tr}(\rho^2)^j. \end{aligned} \quad (\text{B10})$$

Now, we turn to the evaluation of $\mathcal{R}_A^{(t)}(\rho)$. To that end, we first write

$$\begin{aligned} \mathcal{R}_A^{(t)}(\rho) &= \int dU \text{Tr}(U\rho U^\dagger \mathcal{A})^t \\ &= \text{Tr}\left(\rho^{\otimes t} \int dU (U^\dagger \mathcal{A} U)^{\otimes t}\right) \\ &= \text{Tr}(\rho^{\otimes t} \tilde{A}^{(t)}), \end{aligned} \quad (\text{B11})$$

where $\tilde{A}^{(t)}$ is the t -twirled operator A . As it is invariant under unitaries $U^{\otimes t}$, using Schur-Weyl duality, it can be written as

$$\tilde{A}^{(t)} = \sum_{\pi \in S_t} a_\pi^{(t)} V_\pi, \quad (\text{B12})$$

where S_t denotes the set of permutations of size t and V_π is its unitary representation, i.e.,

$$V_\pi = \sum_{i_1 \dots i_t=0}^{d-1} |i_{\pi_1} \dots i_{\pi_t}\rangle \langle i_1 \dots i_t|. \quad (\text{B13})$$

The coefficients $a_\pi^{(t)}$ are rather restricted. First, note that

$$\text{Tr}(\rho^{\otimes t} \tilde{A}^{(t)}) = \sum_{\pi} a_\pi^{(t)} \text{Tr}(V_\pi \rho^{\otimes t}). \quad (\text{B14})$$

The trace with the product of the ρ will produce products of $\text{Tr}(\rho^k)$ according to the cycle type of π . For example, if $t = 4$ and $\pi = (12) \equiv (12)(3)(4)$, meaning that 1 is mapped to 2, 2 is mapped to 1, and 3 and 4 remain unchanged, then $\text{Tr}(V_\pi \rho^{\otimes 4}) = \text{Tr}(\rho^2)$. As we set this equal to Eq. (B10), which contains only terms of $\text{Tr}(\rho)$ and $\text{Tr}(\rho^2)$, $a_\pi^{(t)} = 0$ whenever π contains a cycle of length 3 or longer. We can therefore write

$$\tilde{A}^{(t)} = a_0^{(t)} \mathbb{1} + \sum_{i < j} a_{(ij)}^{(t)} V_{(ij)} + \sum_{\substack{i < j, k < l, i < k \\ j \neq l, j \neq k}} a_{(ij)(kl)}^{(t)} V_{(ij)(kl)} + \dots \quad (\text{B15})$$

As $\tilde{A}^{(t)}$ is invariant under exchange of any of the t systems, we get $a_{(ij)}^{(t)} = a_{(kl)}^{(t)}$, etc. Thus, the coefficients depend only

on the cycle type, and, as there are only cycles of length 2 (and identities), only on the number of two cycles,

$$\begin{aligned} \tilde{A}^{(t)} &= a_0^{(t)} \mathbb{1} + a_1 \sum_{i < j} V_{(ij)} + a_2 \sum_{\substack{i < j, k < l, i < k \\ j \neq l, j \neq k}} V_{(ij)(kl)} + \dots \\ &= a_0^{(t)} \mathbb{1} + \sum_{k=1}^{t/2} a_k^{(t)} \sum_{(i_1 j_1) \dots (i_k j_k)} V_{(i_1 j_1) \dots (i_k j_k)}, \end{aligned} \quad (\text{B16})$$

where the sum over the two cycles only runs over proper two cycles, i.e., no index occurs twice and $i_l < j_l$ for all l . In this sum, there are $\binom{t}{2k} (2k - 1)!!$ terms.

3. Evaluating the $a_k^{(t)}$

Let us now try to fix the coefficients $a_k^{(t)}$. To that end, we evaluate, using Eq. (B16),

$$\begin{aligned} \mathcal{R}_A^{(t)} &= \text{Tr}(\tilde{A}^{(t)} \rho^{\otimes t}) \\ &= a_0^{(t)} + \sum_{k=1}^{t/2} a_k^{(t)} \binom{t}{2k} (2k - 1)!! \text{Tr}(\rho^2)^k, \end{aligned} \quad (\text{B17})$$

which we set equal to Eq. (B10) and compare the coefficients. We get

$$\begin{aligned} a_k^{(t)} &= \frac{(-1)^{t/2-k} d^k \Gamma[(d^2 - 1)/2] (t - 1)!! \binom{t/2}{k}}{2^{t/2} \Gamma[(d^2 - 1 + t)/2] (2k - 1)!! \binom{t}{2k}} \\ &= (-1)^{t/2-k} d^k \frac{(d^2 - 3)!! (t - 2k - 1)!!}{(d^2 - 3 + t)!!} \end{aligned} \quad (\text{B18})$$

for $k = 0, \dots, t/2$ [we use the convention that $(-1)!! = 1$]. Thus, operator $\tilde{A}^{(t)}$ is completely fixed, and all that remains is to translate it back into observable A .

4. Evaluating $\text{Tr}(\mathcal{A}^t)$

After all of these preparations, we can now tackle the task of obtaining \mathcal{A} . Of course, \mathcal{A} is only fixed up to unitary rotations, which means that we can only hope to fix its eigenvalues. Equivalently, we fix $\text{Tr}(\mathcal{A}^t)$ for all t , from which the eigenvalues can be recovered. Let us start with odd powers, and restart from the expression of the unitary moment, but this time we twirl state ρ , yielding $\tilde{\rho}^{(t)} = \int dU (U\rho U^\dagger)^{\otimes t} = \sum_{\pi \in S_t} r_\pi V_\pi$. This yields

$$\mathcal{R}_A^{(t)} = \sum_{\pi \in S_t} r_\pi \text{Tr}(V_\pi \mathcal{A}^{\otimes t}), \quad (\text{B19})$$

where $\text{Tr}(V_\pi \mathcal{A}^{\otimes t})$ is again a product of traces of powers of \mathcal{A} . As t is odd, each of these terms has to contain the trace of an odd power of \mathcal{A} , and the permutations corresponding to single cycles of length t all yield $\text{Tr}(\mathcal{A}^t)$.

Now, starting with $t = 1$, we directly get $0 = \mathcal{R}_{\mathcal{A}}^{(1)}(\rho) = \text{Tr}(\mathcal{A})$. From $t = 3$, we get expressions with $\text{Tr}(\mathcal{A})$, which vanish, and a contribution of $\text{Tr}(\mathcal{A}^3)$, which therefore has to vanish as well. By induction, we conclude that

$$\text{Tr}(\mathcal{A}^t) = 0 \quad (\text{B20})$$

for t odd. This implies that the eigenvalues of \mathcal{A} must come in pairs $\pm x$.

Now, let us turn to the case of even t . In this case, we evaluate

$$\begin{aligned} \text{Tr}(\tilde{\mathcal{A}}^{(t)} V_{(1,2,\dots,t)}) &= \int dU \text{Tr}[(U^\dagger \mathcal{A} U)^{\otimes t} V_{(1,2,\dots,t)}] \\ &= \int dU \text{Tr}[(U^\dagger \mathcal{A} U)^t] \\ &= \text{Tr}(\mathcal{A}^t). \end{aligned} \quad (\text{B21})$$

On the other hand, inserting Eq. (B16) and using the fact that $\text{Tr}(V_\pi) = d^{\#\text{cycles}(\pi)}$ yields

$$\begin{aligned} \text{Tr}(\tilde{\mathcal{A}}^{(t)} V_{(1,2,\dots,t)}) &= a_0^{(t)} d + \sum_{k=1}^{t/2} a_k^{(t)} \sum_{(i_1 j_1) \dots (i_k j_k)} \text{Tr}(V_{(i_1 j_1) \dots (i_k j_k)} V_{(1,2,\dots,t)}). \end{aligned} \quad (\text{B22})$$

Now, the difficulty lies in evaluating the trace on the right-hand side. In fact, we find

$$\begin{aligned} \sum_{(i_1 j_1) \dots (i_k j_k)} \text{Tr}(V_{(i_1 j_1) \dots (i_k j_k)} V_{(1,2,\dots,t)}) &= \binom{t}{2k} \sum_{g=0}^{\lfloor k/2 \rfloor} a(k, g) d^{k+1-2g}, \end{aligned} \quad (\text{B23})$$

where the numbers $a(n, g)$ denote the number of ways to glue sides of a $2n$ -gon so as to produce a surface of genus g ; they are available online [45]. We can now insert the expressions for $a_k^{(t)}$ from Eq. (B18) and explicitly evaluate, for fixed dimension d , $\text{Tr}(\mathcal{A}^t)$ for $t \leq d$. Finally, from knowledge of the traces, we can uniquely infer the eigenvalues of \mathcal{A} .

5. Examples

We construct the observables for $d \leq 7$. For $d > 8$, we need to allow for complex eigenvalues. We have

$$\mathcal{A}_2 = \text{diag}(1, -1), \quad (\text{B24})$$

$$\mathcal{A}_3 = \text{diag}(\sqrt{3/2}, 0, -\sqrt{3/2}) \approx \text{diag}(1.225, 0, -1.225), \quad (\text{B25})$$

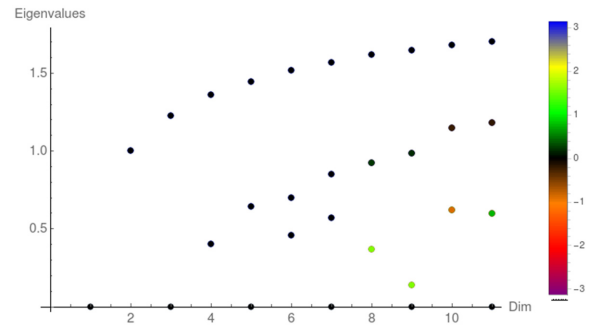


FIG. 4. The absolute values of the eigenvalues of the observable A that reproduces orthogonal moments up to order d as a function of the dimension d . Note that starting from $d = 8$, complex-valued eigenvalues are needed. Their complex phases are indicated by the color.

$$\begin{aligned} \mathcal{A}_4 &= \text{diag}\left(\sqrt{1 + 2\sqrt{3/17}}, \sqrt{1 - 2\sqrt{3/17}}, \right. \\ &\quad \left. -\sqrt{1 - 2\sqrt{3/17}}, -\sqrt{1 + 2\sqrt{3/17}}\right) \\ &\approx \text{diag}(1.357, 0.400, -0.400, -1.357), \end{aligned} \quad (\text{B26})$$

$$\mathcal{A}_5 \approx \text{diag}(1.444, 0.644, 0, -0.644, -1.444), \quad (\text{B27})$$

$$\mathcal{A}_6 \approx \text{diag}(1.518, 0.695, 0.459, -0.459, -0.695, -1.518), \quad (\text{B28})$$

$$\begin{aligned} \mathcal{A}_7 &\approx \text{diag}(1.567, 0.851, 0.567, 0, -0.567, -0.851, \\ &\quad -1.567). \end{aligned} \quad (\text{B29})$$

The solutions are displayed in Fig. 4.

While these operators yield matching moments for $t \leq d$, they fail to do so in general for larger t , as can be readily checked by comparing $\text{Tr}(\mathcal{A}_d^t)$ with Eq. (B22) for some $t > d$. Only in the case of $d = 2$ do they match for all t , and for $d = 3$, they match up to $t = 4$. Otherwise, they differ.

If we just want an observable that reproduces moments $t = 1, 2, 3, 4$ with as few nonvanishing eigenvalues as possible, we can construct them by setting equal Eqs. (B17) and (B10) just for $t \leq 4$. This fixes the $a_k^{(t)}$ for these t , and via Eq. (B21) also $\text{Tr}(\mathcal{A}^t)$ for $t \leq 4$. This yields an explicit solution for $d \geq 2$:

$$\mathcal{A}_d^{(4)} = \text{diag}(\pm\kappa_1, \pm\kappa_2, 0, \dots, 0) \quad (\text{B30})$$

with

$$\kappa_{1,2} = \frac{1}{2} \sqrt{d \pm \sqrt{d \left(8 - d - \frac{20}{d^2 + 1} \right)}}. \quad (\text{B31})$$

Note that these solutions in general can only reproduce moments up to order $t = d$, as the unique solutions for the eigenvalues fail to match $\text{Tr}(\mathcal{A}^t)$ for $t > d$. However,

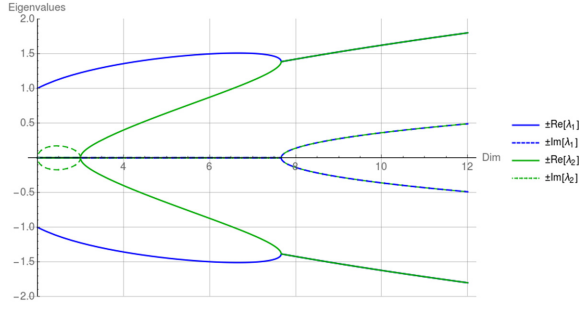


FIG. 5. The (up to) four nonvanishing eigenvalues of the observable A that reproduces orthogonal moments up to order four.

there are two exceptions. First, for $d = 2$, all moments match, as $\text{Tr}(A^t) = 2$ for all even t . Second, for $d = 3$, $t = 4$ is also magically reproduced. The eigenvalues for these fourth-moment observables are displayed in Fig. 5.

6. Generalization to n -partite states

The last missing step is to argue that the solutions obtained for single particles also provide solutions to the n -partite case. To that end, note that

$$\mathcal{S}^{(t)}(\rho_n) = \text{Tr}[\rho_n^{\otimes t} \tilde{S}^{(t)\otimes n}], \quad (\text{B32})$$

where $\tilde{S}^{(t)} = \int d\vec{\alpha} (\vec{\alpha} \cdot \vec{\lambda})^{\otimes t}$ and, likewise

$$\mathcal{R}_A^{(t)}(\rho_n) = \text{Tr}[\rho_n^{\otimes t} \tilde{A}^{(t)\otimes n}]. \quad (\text{B33})$$

Now, thanks to the fact that $SU(d)$ is a proper subgroup of the special orthogonal group $SO(d^2 - 1)$ for every unitary rotation $U \in SU(d)$, there exists an orthogonal rotation $O \in SO(d^2 - 1)$, such that $U\vec{\alpha} \cdot \vec{\lambda}U^\dagger = (O\vec{\alpha}) \cdot \vec{\lambda}$, implying that $\tilde{S}^{(t)}$ is invariant under local unitary transformations $U^{\otimes t}$, just like $\tilde{A}^{(t)}$. Using the Schur-Weyl duality once more, this implies that $\tilde{S}^{(t)} = \sum_{\pi \in S_t} s_\pi V_\pi$, and comparing with Eq. (B10) fixes $\tilde{S}^{(t)} = \tilde{A}^{(t)}$ for all t . Thus, Eqs. (B33) and (B32) must coincide for all n , if they coincide for $n = 1$.

$f_{\text{lb}}(\tilde{\mathcal{R}}_A^{(2)})$

$$= \begin{cases} \frac{d_1^2 + 1}{3(d_1^2 - 1)} (\tilde{\mathcal{R}}_A^{(2)})^2, & 0 \leq \tilde{\mathcal{R}}_A^{(2)} \leq 1/(d^2 - 1), \\ \frac{1}{3} (\tilde{\mathcal{R}}_A^{(2)})^2 + \frac{2}{3(d_1^2 - m)^4} \left[\left(\sqrt{v(\tilde{\mathcal{R}}_A^{(2)}, m)} - 1 \right)^4 + \frac{\left(\sqrt{v(\tilde{\mathcal{R}}_A^{(2)}, m)} + d_1^2 - m - 1 \right)^4}{(d_1^2 - m - 1)^3} \right], & 1/(d_1^2 - m) \leq \tilde{\mathcal{R}}_A^{(2)} \leq 1/ \\ & (d_1^2 - m - 1), \\ & m = 1, \dots, d_1^2 - 2, \end{cases} \quad (\text{C3})$$

APPENDIX C: OPTIMIZATION OF THE MOMENT LANDSCAPE

In order to find optimized entanglement criteria using the second and fourth moments, we express them in terms of the local unitary invariants $\text{Tr}(TT^\dagger)$ and $\text{Tr}(TT^\dagger TT^\dagger)$, as

$$\tilde{\mathcal{R}}_A^{(2)} = \frac{1}{(d_1 - 1)(d_2 - 1)} \text{Tr}(TT^\dagger), \quad (\text{C1})$$

$$\tilde{\mathcal{R}}_A^{(4)} = \frac{1}{3(d_1 - 1)^2(d_2 - 1)^2} [2\text{Tr}(TT^\dagger TT^\dagger) + \text{Tr}(TT^\dagger)^2]. \quad (\text{C2})$$

Here, T denotes the $[(d_1^2 - 1) \times (d_2^2 - 1)]$ -dimensional correlation matrix of the quantum state as defined in the main text.

We assume without loss of generality that $d_1 \leq d_2$ and we denote the singular values of T as $(\sigma_1, \dots, \sigma_{d_1^2 - 1})$. Then, $\text{Tr}(TT^\dagger) = \sum_i \sigma_i^2$ and $\text{Tr}(TT^\dagger TT^\dagger) = \sum_i \sigma_i^4$. We now minimize and maximize $\text{Tr}(TT^\dagger TT^\dagger)$ for a fixed value of $\text{Tr}(TT^\dagger)$ under the constraint dictated by the generalized de Vicente criterion for states of Schmidt number k from Lemma 1, namely, $\sum_i \sigma_i \leq \sqrt{(d_1 - 1)(d_2 - 1)} + \sqrt{d_1 d_2}(k - 1)$, yielding the optimization problem

$$\min/\max_{\{\sigma_i\}} \sum_i \sigma_i^4$$

subject to $\sigma_i \geq 0$,

$$\sum_i \sigma_i^2 = (d_1 - 1)(d_2 - 1) \tilde{\mathcal{R}}_A^{(2)},$$

$$\sum_i \sigma_i \leq \sqrt{(d_1 - 1)(d_2 - 1)} + \sqrt{d_1 d_2}(k - 1).$$

The optimization can be solved analytically using the standard Lagrange multiplier method with slack variables to implement the upper bound. This readily reveals that the lower bound is given by arrangements of singular values that either vanish or are equal, except for one singular value that is allowed to take different values.

For the case of separable states, i.e., $k = 1$, we find the analytical expression $f_{\text{lb}}(\tilde{\mathcal{R}}_A^{(2)}) \leq \tilde{\mathcal{R}}_A^{(4)} \leq f_{\text{ub}}(\tilde{\mathcal{R}}_A^{(2)})$ with

where $v(\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}, m) = (d_1^2 - m)(d_1^2 - m - 1)(\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} - 1 / (d_1^2 - m))$. The upper bound in the case of $k = 1$ is simply given by

$$f_{\text{ub}}(\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}) = (\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)})^2. \quad (\text{C4})$$

For $k \geq 2$, the maximal value of $\tilde{\mathcal{R}}_{\mathcal{A}}^{(4)}$ depends on the maximal value that a single singular value can take. To the best of our knowledge, this upper bound is not known, and the best bound that we could find is dictated by the purity bound $\text{Tr}(\rho^2) \leq 1$, which translates to a bound on the Frobenius norm of T ,

$$\|T\|_{\text{Fr}} = \sum_{ij} |T_{ij}|^2 \leq d_1 d_2 + 1 - \frac{d_1 + d_2}{k}, \quad (\text{C5})$$

which can be derived by rewriting $\text{Tr}(\rho^2) = (d_1 \text{Tr}(\rho_{\mathcal{A}}^2) + d_2 \text{Tr}(\rho_{\mathcal{B}}^2) + \|T\|_{\text{Fr}} - 1) / d_1 d_2$ and maximizing over pure states of Schmidt rank k . The upper bound is then given by Eq. (C4) as well, as long as

$$\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} \leq 1 + \frac{k-1}{k} \frac{d_1 + d_2}{(d_1 - 1)(d_2 - 1)},$$

as values larger than this are incompatible with Schmidt number k states. However, the upper bound is probably not tight, except for the case $k = 1$.

The resulting picture is displayed for the case of $d_1 = d_2 = 3$ in Fig. 1.

The lower bound for the whole set of states is traced by the isotropic state, and is given by

$$g_{\text{lb}}(\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}) = \frac{d_1^2 + 1}{3(d_1^2 - 1)} (\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)})^2. \quad (\text{C6})$$

APPENDIX D: PROOF OF THEOREM 2

Here, we prove Theorem 2 from the main text.

Theorem 4: Let $\{\psi_i\}_{i=1}^N$ be an equiangular set of normalized vectors in \mathbb{C}^d , with $|\langle \psi_i | \psi_j \rangle| = 1/\sqrt{d}$ if $i \neq j$. Then

$$\rho = \frac{1}{N} \sum_{i=1}^N |\psi_i\rangle\langle\psi_i| \otimes |\psi_i\rangle\langle\psi_i| \quad (\text{D1})$$

lies on the kink at $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)}(\rho) = 1/N$.

Proof. As noted before, lying on the kink at $\tilde{\mathcal{R}}_{\mathcal{A}}^{(2)} = 1/N$ is equivalent to the singular values of the correlation matrix being $(0, \dots, 0, (d-1)/N, \dots, (d-1)/N)$, summing up

to $d-1$. The elements of the correlation matrix are given by

$$\begin{aligned} T_{ij} &= \text{Tr}(\lambda_i \otimes \lambda_j \rho) \\ &= \frac{1}{N} \sum_{k=1}^N \langle \psi_k | \lambda_i | \psi_k \rangle \langle \psi_k | \lambda_j | \psi_k \rangle \\ &= \vec{k}_i \cdot \vec{k}_j \end{aligned} \quad (\text{D2})$$

with the N -dimensional vectors $\vec{k}_i = (\langle \psi_1 | \lambda_i | \psi_1 \rangle / \sqrt{N}, \dots, \langle \psi_N | \lambda_i | \psi_N \rangle / \sqrt{N})^T$. This implies that T is a $(d^2 - 1)$ -dimensional Gramian matrix of rank N , implying that it is positive semidefinite and its eigenvalues coincide with the singular values. Thus, if we show that $T^2 = (d-1)T/N$ and $\text{Tr}(T) = d-1$, we are done. We calculate

$$\begin{aligned} (T^2)_{ij} &= \sum_a T_{ia} T_{aj} \\ &= \frac{1}{N^2} \sum_{a,k,l} \langle \psi_k | \lambda_i | \psi_k \rangle \langle \psi_k | \lambda_a | \psi_k \rangle \langle \psi_l | \lambda_a | \psi_l \rangle \\ &\quad \langle \psi_l | \lambda_j | \psi_l \rangle \\ &= \frac{1}{N^2} \sum_{k,l} \langle \psi_k | \lambda_i | \psi_k \rangle \langle \psi_l | \lambda_j | \psi_l \rangle \\ &\quad \times \langle \psi_k | \langle \psi_l | \sum_a \lambda_a \otimes \lambda_a | \psi_k \rangle | \psi_l \rangle \\ &= \frac{1}{N^2} \sum_{k,l} \langle \psi_k | \lambda_i | \psi_k \rangle \langle \psi_l | \lambda_j | \psi_l \rangle \\ &\quad \times \langle \psi_k | \langle \psi_l | (dV - \mathbb{1} \otimes \mathbb{1}) | \psi_k \rangle | \psi_l \rangle \\ &= \frac{1}{N^2} \sum_{k,l} \langle \psi_k | \lambda_i | \psi_k \rangle \langle \psi_l | \lambda_j | \psi_l \rangle [(d-1)\delta_{kl} + 1 - 1] \\ &= \frac{d-1}{N} \vec{k}_i \cdot \vec{k}_j \\ &= \frac{d-1}{N} T_{ij}, \end{aligned} \quad (\text{D3})$$

where V denotes the swap operator, given by $V = \sum_{i,j=0}^{d-1} |ij\rangle\langle ji|$, and we use the well-known relation $dV = \sum_{a=0}^{d^2-1} \lambda_a \otimes \lambda_a$. The trace can be evaluated analogously. ■

APPENDIX E: PROOF OF COROLLARY 1

Here, we prove Corollary 1 from the main text.

Corollary 3: Let $\{\psi_i\}_{i=1}^N \cup \{|\psi\rangle\}$ be an equiangular set of size $N+1$ of normalized vectors in \mathbb{C}^d with overlap $1/\sqrt{d}$.

Then the family of states

$$\rho(p) = \frac{p}{N} \sum_{i=1}^N |\psi_i\rangle\langle\psi_i| \otimes |\psi_i\rangle\langle\psi_i| + (1-p) |\psi\rangle\langle\psi| \otimes |\psi\rangle\langle\psi| \quad (\text{E1})$$

traces the boundary of the separable set between the kinks at $\tilde{\mathcal{R}}_A^{(2)}[\rho(N/(N+1))] = 1/(N+1)$ and $\tilde{\mathcal{R}}_A^{(2)}[\rho(1)] = 1/N$.

Proof. The proof follows similar lines as the proof of Theorem 2. We can write the correlation matrix explicitly as

$$T_{ij} = \frac{p}{N} \sum_k \langle\psi_k|\lambda_i|\psi_k\rangle \langle\psi_k|\lambda_j|\psi_k\rangle + (1-p) \langle\psi|\lambda_i|\psi\rangle \langle\psi|\lambda_j|\psi\rangle, \quad (\text{E2})$$

which can, again, be written as an inner product, implying that T is a Gramian matrix. As noted before, lying on the boundary of the set of separable states between the kinks at $\tilde{\mathcal{R}}_A^{(2)} = 1/N$ and $\tilde{\mathcal{R}}_A^{(2)} = 1/(N+1)$ is equivalent to the singular values of T being given by $(0, \dots, 0, l, m, \dots, m)$ with $0 \leq l \leq m$ and the singular value m appearing N times. Furthermore, the sum of the singular values must equal $d-1$.

As the eigenvalues of the Gramian matrix T coincide with its singular values, the claim is therefore equivalent to showing that

$$T^2 = mT + (l^2 - ml) |v_l\rangle\langle v_l|, \quad (\text{E3})$$

where $|v_l\rangle$ is the eigenvector of T with eigenvalue l . Similar calculations as before and making use of $\sum_{a=1}^{d^2-1} \lambda_a \otimes \lambda_a = dV - \mathbb{1}$ reveal

$$(T^2)_{ij} = \sum_a T_{ia} T_{aj} = \frac{(d-1)p}{N} T_{ij} + (d-1)^2 \left[(1-p)^2 - \frac{p(1-p)}{N} \right] \langle\psi|\lambda_i|\psi\rangle \langle\psi|\lambda_j|\psi\rangle. \quad (\text{E4})$$

Indeed, the last term in Eq. (E4) can be interpreted as an element of a rank-one matrix. Comparing Eq. (E4) with

Eq. (E3), we read off

$$m = \frac{(d-1)p}{N}, \quad (\text{E5})$$

$$l = (d-1)(1-p), \quad (\text{E6})$$

$$|v_l\rangle = \frac{1}{\sqrt{d-1}} (\langle\psi|\lambda_1|\psi\rangle, \dots, \langle\psi|\lambda_{d^2-1}|\psi\rangle)^T. \quad (\text{E7})$$

Finally, we have to check two things. First, the sum of the singular values, $l + Nm$, must sum to $d-1$, which is easily confirmed. Second, we have to ensure that $|v_l\rangle$ is the eigenvector of T with eigenvalue l . To that end, we insert T_{ij} into

$$\begin{aligned} \langle v_l|T|v_l\rangle &= \frac{1}{d-1} \sum_{ij} \langle\psi|\lambda_i|\psi\rangle \langle\psi|\lambda_j|\psi\rangle T_{ij} \\ &= (d-1)(1-p) \\ &= l. \end{aligned} \quad (\text{E8})$$

This concludes the proof. ■

APPENDIX F: PROOF OF THEOREM 3

Here, we prove Theorem 3 from the main text.

Theorem 5: Consider a set of m MUBs $\{|\psi_j^1\rangle\}_{j=1}^d, \dots, \{|\psi_j^m\rangle\}_{j=1}^d$. Then the state

$$\rho := \frac{1}{md} \sum_{l=1}^m \sum_{k=1}^d |\psi_k^l\rangle\langle\psi_k^l| \otimes |\psi_k^l\rangle\langle\psi_k^l| \quad (\text{F1})$$

lies at the kink at $\tilde{\mathcal{R}}_A^{(2)} = 1/m(d-1)$.

Proof. We again show that the correlation matrix is a multiple of a projector, i.e., $T^2 = (d-1)T/K$. To that end, we note that $|\langle\psi_k^l|\psi_{k'}^{l'}\rangle|^2 = \delta_{ll'}\delta_{kk'} + (1-\delta_{ll'})/d$ and explicitly write

$$T_{ij} = \frac{1}{md} \sum_{l=1}^m \sum_{k=1}^d \langle\psi_k^l|\lambda_i|\psi_k^l\rangle \langle\psi_k^l|\lambda_j|\psi_k^l\rangle \quad (\text{F2})$$

and

$$\begin{aligned} T_{ij}^2 &= \frac{1}{m^2 d^2} \sum_{a=1}^{d^2-1} \sum_{l,l'=1}^m \sum_{k,k'=1}^d \langle\psi_k^l|\lambda_i|\psi_k^l\rangle \langle\psi_{k'}^{l'}|\lambda_j|\psi_{k'}^{l'}\rangle \langle\psi_k^l|\lambda_a|\psi_k^l\rangle \langle\psi_{k'}^{l'}|\lambda_a|\psi_{k'}^{l'}\rangle \\ &= \frac{1}{m^2 d^2} \sum_{l,l'=1}^m \sum_{k,k'=1}^d \langle\psi_k^l|\lambda_i|\psi_k^l\rangle \langle\psi_{k'}^{l'}|\lambda_j|\psi_{k'}^{l'}\rangle \langle\psi_k^l|\psi_{k'}^{l'}\rangle \langle\psi_{k'}^{l'}|\psi_k^l\rangle \langle dV - \mathbb{1} | \psi_k^l\rangle\langle\psi_{k'}^{l'}| \end{aligned}$$

$$\begin{aligned}
 &= \frac{1}{m^2 d^2} \sum_{l,l'=1}^m \sum_{k,k'=1}^d \langle \psi_k^l | \lambda_i | \psi_k^l \rangle \langle \psi_{k'}^{l'} | \lambda_j | \psi_{k'}^{l'} \rangle (d \delta_{ll'} \delta_{kk'} + (1 - \delta_{ll'}) - 1) \\
 &= \frac{1}{m^2 d^2} \sum_{l=1}^m \sum_{k=1}^d \left[d \langle \psi_k^l | \lambda_i | \psi_k^l \rangle \langle \psi_k^l | \lambda_j | \psi_k^l \rangle - \sum_{k'=1}^d \langle \psi_k^l | \lambda_i | \psi_k^l \rangle \langle \psi_{k'}^l | \lambda_j | \psi_{k'}^l \rangle \right] \\
 &= \frac{d}{m^2 d^2} \sum_{l=1}^m \sum_{k=1}^d \langle \psi_k^l | \lambda_i | \psi_k^l \rangle \langle \psi_k^l | \lambda_j | \psi_k^l \rangle \\
 &= \frac{1}{m} T_{ij}.
 \end{aligned} \tag{F3}$$

Rearranging $1/m = (d - 1)/K$ yields $K = m(d - 1)$. ■

-
- [1] S. Muralidharan, L. Li, J. Kim, N. Lütkenhaus, M. D. Lukin, and L. Jiang, Optimal architectures for long distance quantum communication, *Sci. Rep.* **6**, 20463 (2016).
 - [2] G. Tóth, Multipartite entanglement and high-precision metrology, *Phys. Rev. A* **85**, 022322 (2012).
 - [3] N. Friis, G. Vitagliano, M. Malik, and M. Huber, Entanglement certification from theory to experiment, *Nat. Rev. Phys.* **1**, 72 (2019).
 - [4] S. Gharibian, Strong NP-hardness of the quantum separability problem, *Quantum Inf. Comput.* **10**, 343 (2010).
 - [5] O. Gühne and G. Tóth, Entanglement detection, *Phys. Rep.* **474**, 1 (2009).
 - [6] O. Rudolph, Further results on the cross norm criterion for separability, *Quantum Inf. Process.* **4**, 219 (2005).
 - [7] K. Chen and L.-A. Wu, A matrix realignment method for recognizing entanglement, *Quantum Inf. Comput.* **3**, 193 (2003).
 - [8] J. I. de Vicente, Separability criteria based on the bloch representation of density matrices, *Quantum Inf. Comput.* **7**, 624 (2007).
 - [9] G. Sarbicki, G. Scala, and D. Chruściński, Family of multipartite separability criteria based on a correlation tensor, *Phys. Rev. A* **101**, 012341 (2020).
 - [10] A. Ketterer, N. Wyderka, and O. Gühne, Characterizing Multipartite Entanglement with Moments of Random Correlations, *Phys. Rev. Lett.* **122**, 120505 (2019).
 - [11] S. Imai, N. Wyderka, A. Ketterer, and O. Gühne, Bound Entanglement from Randomized Measurements, *Phys. Rev. Lett.* **126**, 150501 (2021).
 - [12] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States* (Cambridge University Press, Cambridge, 2006).
 - [13] R. Horodecki and M. Horodecki, Information-theoretic aspects of inseparability of mixed states, *Phys. Rev. A* **54**, 1838 (1996).
 - [14] W. Thirring, *Lehrbuch der Mathematischen Physik* (Springer Vienna, Vienna, 1980).
 - [15] P. Badziag, C. Brukner, W. Laskowski, T. Paterek, and M. Żukowski, Experimentally Friendly Geometrical Criteria for Entanglement, *Phys. Rev. Lett.* **100**, 140403 (2008).
 - [16] J. I. de Vicente and M. Huber, Multipartite entanglement detection from correlation tensors, *Phys. Rev. A* **84**, 062306 (2011).
 - [17] M. Horodecki, P. Horodecki, and R. Horodecki, General teleportation channel, singlet fraction, and quasidistillation, *Phys. Rev. A* **60**, 1888 (1999).
 - [18] O. Gühne, Y. Mao, and X.-D. Yu, Geometry of Faithful Entanglement, *Phys. Rev. Lett.* **126**, 140503 (2021).
 - [19] R. Horodecki, P. Horodecki, and M. Horodecki, Violating Bell inequality by mixed states: Necessary and sufficient condition, *Phys. Lett. A* **200**, 340 (1995).
 - [20] F. Verstraete and M. M. Wolf, Entanglement versus Bell Violations and Their Behavior Under Local Filtering Operations, *Phys. Rev. Lett.* **89**, 170401 (2002).
 - [21] B. M. Terhal and P. Horodecki, Schmidt number for density matrices, *Phys. Rev. A* **61**, 040301(R) (2000).
 - [22] J. I. de Vicente, Lower bounds on concurrence and separability conditions, *Phys. Rev. A* **75**, 052320 (2007).
 - [23] S. Liu, Q. He, M. Huber, O. Gühne, and G. Vitagliano, Characterizing Entanglement Dimensionality from Randomized Measurements, *PRX Quantum* **4**, 020324 (2023).
 - [24] S. Liu, M. Fadel, Q. He, M. Huber, and G. Vitagliano, (2022), Preprint [ArXiv:2208.04909](https://arxiv.org/abs/2208.04909).
 - [25] J. Emerson, R. Alicki, K. Życzkowski, and J. Opt. B, Scalable noise estimation with random unitary operators, *Quantum Semiclass. Opt.* **7**, S347 (2005).
 - [26] E. Knill, D. Leibfried, R. Reichle, J. Britton, R. B. Blakestad, J. D. Jost, C. Langer, R. Ozeri, S. Seidelin, and D. J. Wineland, Randomized benchmarking of quantum gates, *Phys. Rev. A* **77**, 012307 (2008).
 - [27] S. T. Flammia and Y.-K. Liu, Direct Fidelity Estimation from Dew Pauli Measurements, *Phys. Rev. Lett.* **106**, 230501 (2011).
 - [28] S. Aaronson, The learnability of quantum states, *Proc. R. Soc. A* **463**, 3089 (2007).
 - [29] H.-Y. Huang, R. Kueng, and J. Preskill, Predicting many properties of a quantum system from very few measurements, *Nat. Phys.* **16**, 1050 (2020).
 - [30] J. Morris and B. Dakić, (2019), Preprint [ArXiv:1909.05880](https://arxiv.org/abs/1909.05880).

- [31] D. S. França, F. G. L. Brandão, and R. Kueng, in *16th Conference on the Theory of Quantum Computation, Communication and Cryptography (TQC 2021)*, Leibniz International Proceedings in Informatics, Vol. 197 (Dagstuhl, Germany, 2021), p. 7:1–7:13, doi:10.4230/LIPIcs.TQC.2021.7.
- [32] Y.-C. Liang, N. Harrigan, S. D. Bartlett, and T. Rudolph, Nonclassical Correlations from Randomly Chosen Local Measurements, *Phys Rev. Lett.* **104**, 050401 (2010).
- [33] J. J. Wallman and S. D. Bartlett, Observers can always generate nonlocal correlations without aligning measurements by covering all their bases, *Phys. Rev. A* **85**, 024101 (2012).
- [34] P. Shadbolt, T. Vértesi, Y.-C. Liang, C. Branciard, N. Brunner, and J. L. O’Brien, Guaranteed violation of a Bell inequality without aligned reference frames or calibrated devices, *Sci. Rep.* **2**, 470 (2012).
- [35] L. Welch, Lower bounds on the maximum cross correlation of signals (corresp.), *IEEE Trans. Inf. Theory* **20**, 397 (1974).
- [36] J. A. Tropp, in *Wavelets XI*, Vol. 5914 (SPIE, 2005), p. 591401.
- [37] G. Zauner, Quantum designs: Foundations of a noncommutative design theory, *Int. J. Quantum Inf.* **09**, 445 (2011).
- [38] M. Grassl, “SIC-POVMs,” <http://sicpovm.markus-grassl.de/>, accessed: 2022-11-10.
- [39] I. Bengtsson, in *AIP Conference Proceedings*, Vol. 889 (American Institute of Physics, 2007), p. 40.
- [40] M. Navascués, S. Pironio, and A. Acín, A convergent hierarchy of semidefinite programs characterizing the set of quantum correlations, *New J. Phys.* **10**, 073013 (2008).
- [41] X.-D. Yu, T. Simnacher, H. C. Nguyen, and O. Gühne, Quantum-Inspired Hierarchy for Rank-Constrained Optimization, *PRX Quantum* **3**, 010340 (2022).
- [42] L. Vandenberghe and S. Boyd, Semidefinite programming, *SIAM Rev.* **38**, 49 (1996).
- [43] N. Wyderka, A. Ketterer, S. Imai, J. L. Bönsel, D. E. Jones, B. T. Kirby, X.-D. Yu, and O. Gühne, (2022), Preprint [ArXiv:2212.07894](https://arxiv.org/abs/2212.07894).
- [44] C. D. Bruzewicz, J. Chiaverini, R. McConnell, and J. M. Sage, Trapped-ion quantum computing: Progress and challenges, *Appl. Phys. Rev.* **6**, 021314 (2019).
- [45] <https://oeis.org/A035309>.