Entanglement detection via mutually unbiased bases

Christoph Spengler,1,* Marcus Huber,1,2 Stephen Brierley,2 Theodor Adaktylos,1 and Beatrix C. Hiesmayr1,3

1Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria
2Department of Mathematics, University of Bristol, Bristol BS8 1TW, United Kingdom
3Institute of Theoretical Physics and Astrophysics, Masaryk University, Kotlářská 2, 61137 Brno, Czech Republic

(Received 2 May 2012; published 9 August 2012)

We investigate correlations among complementary observables. In particular, we show how to take advantage of mutually unbiased bases for the efficient detection of entanglement in arbitrarily high-dimensional, multipartite, and continuous-variable quantum systems. The introduced entanglement criteria are relatively easy to implement experimentally since they require only a few local measurement settings. In addition, we establish a link between the separability problem and the maximum number of mutually unbiased bases—opening an additional avenue in this long-standing open problem.

DOI: 10.1103/PhysRevA.86.022311 PACS number(s): 03.67.Mn, 03.65.Ud, 03.65.Ta, 03.65.Aa

I. INTRODUCTION

A key feature of quantum theory is the prediction of correlations that have no classical analog, i.e., correlations that differ fundamentally from Bertlmann’s socks [1]. Whereas such quantum correlations were initially considered to be an artifact of the theory, it was later confirmed in several experiments that they actually exist in nature. They are a manifestation of the fact that composite quantum systems can be entangled, in the sense that they are not exclusively separable.

Nowadays, it is widely known that quantum entanglement enables numerous applications ranging from quantum cryptography to quantum computing. Although the theory of entanglement has been extensively studied within recent decades (for recent reviews, consult Refs. [2,3]), it is still an evolving research field with many open problems. One of these problems concerns the reliable and efficient detection of entanglement in experiments [4,5]. While for bipartite two-level systems it is possible to experimentally verify the presence of entanglement by making a few joint local measurements, the number of measurements needed for entanglement detection generally scales rather disadvantageously with the size of the system. The main challenge for high-dimensional multipartite systems is not only to develop mathematical tools for entanglement detection, but to find schemes whose experimental implementation requires minimal effort. In other words, the aim is to verify entanglement with as few measurements as possible, specifically without resorting to full state tomography.

Another fundamental concept of quantum theory is complementarity, which states that there exist observables that cannot be measured simultaneously. In the mathematical formalism, complementarity expresses itself through the fact that there are pairs of observables for which no common eigenbasis can be found. Consequently, if two observables are complementary then it is impossible to prepare a system such that the outcome of both is predictable with certainty. The extreme case of complementarity is when the eigenbases of two observables form a pair of mutually unbiased bases (MUBs) [6]. This is when all (normalized) eigenvectors of one observable have the same overlap with all eigenvectors of the other observable. Thus, if a system is in an eigenstate of a particular basis, then the measurement result in a corresponding mutually unbiased basis is completely random.

The question of how many MUBs exist for a given Hilbert space has been a lively topic of research (see [7] for a recent review). Although it is been known since 1989 [8] that for \( \mathcal{H} = \mathbb{C}^d \) the number of MUBs is at most \( d + 1 \) and that such a complete set of MUBs exists whenever \( d \) is a prime power, the maximal number of MUBs remains open for all other dimensions. Even for the smallest non-prime-power dimension \( d = 6 \), the existence of a complete set remains an open problem, and current numerical [9–11] and analytical [12–16] evidence suggests that it is likely that there is none.

It is currently unclear if the (non)existence of a complete set of MUBs in non-prime-power dimensions has fundamental reasons or consequences. However, one should also look at MUBs from a pragmatic perspective; or as phrased by Bengts- son [17]: “the real MUB problem is not how many MUBs we can find. The real MUB problem is to find out what we can do with those that exist.” Existing applications of MUBs are quantum state tomography [8,18–20], cryptographic protocols [21,22], and the mean king’s problem [23,24]. In short, they are generally useful for finding and hiding (quantum) information. In this paper, we present a different application of mutually unbiased bases. Namely, we link the concept of MUBs with the separability problem. We show that one can exploit the properties of MUBs to derive powerful entanglement detection criteria for arbitrarily high-dimensional systems. These criteria are well suited for the experimental verification of entanglement as they are experimentally accessible through measuring correlations between only a few local observables. In contrast to a full state tomography where the experimental effort can grow exponentially with the system size [25], our approach enables optimal entanglement detection using a number of measurement settings which scales only linearly with the dimensionality of the local subsystems. In fact, we also show that even two local MUB settings, in general, suffice for a comparably robust entanglement test. Furthermore, by considering the noise thresholds of our criteria we find an interesting theoretical connection between the separability of density matrices and the maximum number of MUBs. In
particular, we provide an alternative proof that there cannot be more than $d + 1$ MUBs in any dimension. We also consider extensions of our methodology for continuous variables and multipartite systems. These are discussed by the example of the two-mode squeezed state and the Aharonov state.

II. PRELIMINARIES

A set of orthonormal bases $\{B_k\}$ for a Hilbert space $\mathcal{H} = \mathbb{C}^d$ where $B_k = \{|i_k\rangle\} = \{|0_k\rangle, \ldots, |d - 1_k\rangle\}$ is called mutually unbiased if and only if

$$
|i_k \rangle \langle j_i| = \frac{1}{d}, \quad \forall \: i, j \in \{0, \ldots, d - 1\}, \quad (1)
$$

holds for all basis vectors $|i_k\rangle$ and $|j_i\rangle$ that belong to different bases, i.e., $\forall \: k \neq l$. If two bases are mutually unbiased, their corresponding observables are complementary—a measurement of one of these observables reveals no information about the outcome of the other.

In dimension $d = 2$, a set of three mutually unbiased bases is readily obtained from the eigenvectors of the three Pauli matrices $\sigma_x, \sigma_y,$ and $\sigma_z$:

$B_1 = \{|01\rangle, |10\rangle\} = \{|0\rangle, |1\rangle\}$,

$B_2 = \{|02\rangle, |12\rangle\} = \left\{ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle), \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right\}$,

$B_3 = \{|03\rangle, |13\rangle\} = \left\{ \frac{1}{\sqrt{2}} (|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}} (|0\rangle - i|1\rangle) \right\}$.

These three bases constitute a complete set since it is impossible to find an additional basis that is mutually unbiased to all of them.

In general, for prime-power dimensions $d = p^n$, there are several explicit methods to construct a complete set of $d + 1$ MUBs making use of finite fields $[8, 26]$, the Heisenberg-Weyl group $[27]$, generalized angular momentum operators $[28]$, and identities from number theory $[29]$. For the special cases $d = 2^n$ and $d = p^2$, it was shown that such sets can be constructed in a rather simple and experimentally accessible way $[30, 31]$.

The concept of mutually unbiased bases can also be extended to continuous-variable (CV) systems $[7, 32]$. Here, the bases given by the (generalized) eigenstates of position and momentum operators provide a well-known example of MUBs. If one allows the right-hand side of Eq. (1) to vary between each pair of bases, a continuum of MUBs is available $[7]$. Requiring that all pairwise overlaps have the same modulus leads to a symmetric set of three MUBs for CV systems $[32]$.

First, in order to relate MUBs with the separability problem, let us specify how correlations can be quantified. Consider a bipartite system where measurements on each of the two subsystems $A$ and $B$ have $d$ different outcomes $\{0, \ldots, d - 1\}$. If we can predict with certainty the outcome of a measurement on $A$ when we know the outcome of a measurement on $B$ (or vice versa) we call a system fully correlated. On the other hand, we call a system completely uncorrelated if the outcome of a measurement of one party tells us nothing about the other party, i.e., when the outcomes are completely random. Following this notion, it is possible to construct a correlation function for any two observables $a, b$ on $A, B$. We denote the joint probability that the outcome of $a$ is $i$ and the outcome of $b$ is $j$ by $P_{a,b}(i,j)$.

We define the correlation function

$$
C_{a,b} = \sum_{i=0}^{d-1} P_{a,b}(i,i), \quad (2)
$$

which we call the mutual predictability. It can be used to quantify the probability of predicting the measurement results of $a$ knowing the outcome of $b$, and vice versa. Namely, if the observables $a$ and $b$ are fully correlated then the outcomes $\{i\} = \{0, \ldots, d - 1\}$ can always be labeled in a way such that $C_{a,b} = 1$. It is noteworthy that labels in general have no physical meaning. Thus, it is up to us what outcome we declare unbiased if and only if $C_{a,b} = 1$. It is noteworthy that labels in general have no physical meaning. Thus, it is up to us what outcome we declare unbiased if and only if $C_{a,b} = 1$. It is noteworthy that labels in general have no physical meaning. Thus, it is up to us what outcome we declare unbiased if and only if $C_{a,b} = 1$. It is noteworthy that labels in general have no physical meaning. Thus, it is up to us what outcome we declare unbiased if and only if $C_{a,b} = 1$. It is noteworthy that labels in general have no physical meaning. Thus, it is up to us what outcome we declare unbiased if and only if $C_{a,b} = 1$.

In the quantum case, each observable $a, b$ corresponds to an orthonormal basis $\{|i\rangle\}$ and $\{|j\rangle\}$ where we have $P_{a,b}(i,j) = \langle i|a\rho|j\rangle$ where $\rho$ is the state of the system, and thus the mutual predictability reads $C_{a,b} = \sum_{i,j} P_{a,b}(i,i) = \sum_{i,j} |\langle i|a\rho|j\rangle|^2$. Again, one obtains $C_{a,b} = 1$ for fully correlated states when $\{|i\rangle\}$ and $\{|j\rangle\}$ are chosen appropriately with respect to $\rho$, and $C_{a,b} = 1/d$ for completely uncorrelated states, independent of the chosen bases.

III. ENTANGLEMENT DETECTION: BIPARTITE QUDIT SYSTEMS

For a particular state $\rho$ and measurement settings $a, b$ the quantity $C_{a,b}$ tells us nothing about the separability of a state. For instance, we can have $C_{a,b} = 1$ for all entangled pure states $|\psi\rangle$ which directly follows from the Schmidt decomposition. Any entangled state may be written in the form $|\psi\rangle = \sum_{i=0}^{r} \lambda_i |i\rangle |\tilde{i}\rangle \otimes |\tilde{i}\rangle |\tilde{i}\rangle$ with $1 \leq r \leq d - 1$ using the orthonormal Schmidt bases $\{|\tilde{i}\rangle\}$ and $\{|\tilde{i}\rangle\}$. Using observables $a$ and $b$ that correspond to these bases, we obviously obtain $C_{a,b} = 1$. However, we also obtain $C_{a,b} = 1$ for a classically correlated separable state $\rho_{CC} = \sum_{i=0}^{d-1} |\tilde{i}\rangle \langle \tilde{i}| |\tilde{i}\rangle |\tilde{i}\rangle \otimes |\tilde{i}\rangle |\tilde{i}\rangle$ as it yields the same joint probabilities $P_{a,b}(i,i)$ when we use $\{|\tilde{i}\rangle\}$ and $\{|\tilde{i}\rangle\}$.

Hence, to detect entanglement, the mutual predictability $C_{a,b}$ has to be measured in at least two bases, $a, b$ and $a', b'$. Let us consider a pure product state which we write as $|\psi\rangle_{\text{pro}} = |01\rangle \otimes |01\rangle$ in an arbitrary basis $\{|i\rangle\}$. For $\rho_{\text{pro}} = |\psi\rangle_{\text{pro}} |\psi\rangle_{\text{pro}}$, one obtains $C_{1,1} = 1$ if both parties use the basis $\{|i\rangle\}$. However, in a second basis $\{|\tilde{i}\rangle\}$ which is mutually unbiased to $\{|i\rangle\}$, the mutual predictability $C_{2,2}$ is completely lost: Since $\{|i\rangle\}$ and $\{|\tilde{i}\rangle\}$ are mutually unbiased we have that

$$
P_{2,2}(i,i) = \langle i_2|a\rho_{\text{pro}}|i_2\rangle = \langle i_2|a\rho_{\text{pro}}|i_2\rangle = \frac{|\langle i_2|0_1\rangle|^2}{|\langle i_2|0_1\rangle|^2} = \frac{1}{d}, \quad (3)
$$

and consequently $C_{2,2} = \sum_{i=0}^{d-1} P_{2,2}(i,i) = 1/d$.

Inspired by this result, let us consider the quantity $I_2 = I_{1,1} + I_{2,2}$. As shown, with a pure product state we obviously can attain $I_2 = 1 + \frac{1}{d}$ for a pair of MUBs. Similarly, we can...
achieve $I_m = \sum_{k=1}^{m} C_{k,k} \leq 1 + \frac{m-1}{d}$. For a product state using $m$ mutually unbiased bases $B_k$ and corresponding terms $C_{k,k}$, because when the mutual predictability equals 1 in one basis then it is $1/d$ with respect to the other $m-1$ bases. The main result of this paper is that these values are upper bounds for separable states, i.e., for all separable states and any set of $m$ mutually unbiased bases for $A$ and $B$ it holds that

$$I_m = \sum_{k=1}^{m} C_{k,k} \leq 1 + \frac{m-1}{d}. \quad (7)$$

In particular, for a complete set of MUBs we have

$$I_{d+1} = \sum_{k=1}^{d+1} C_{k,k} \leq 2. \quad (8)$$

**Proof.** For an arbitrary pure product state $|a\rangle \otimes |b\rangle \in \mathbb{C}^d \otimes \mathbb{C}^d$ we have

$$I_m = \sum_{k=1}^{m} C_{k,k} = \sum_{k=1}^{m} \sum_{i=0}^{d-1} |\langle i | a \rangle|^2 |\langle i | b \rangle|^2. \quad (9)$$

Here, the inequality of arithmetic and geometric means $(x_1 + x_2 + \cdots + x_n)/n \geq \sqrt[n]{x_1x_2\cdots x_n}$ for positive numbers implies that

$$\sum_{k=1}^{m} C_{k,k} \leq \frac{1}{2} \sum_{k=1}^{m} \sum_{i=0}^{d-1} |\langle i | a \rangle|^4 + |\langle i | b \rangle|^4. \quad (10)$$

Now we can exploit the fact that for any pure state $|a\rangle \in \mathbb{C}^d$ and $m$ mutually unbiased bases it holds that

$$\sum_{k=1}^{m} \sum_{i=0}^{d-1} |\langle i | a \rangle|^4 \leq 1 + \frac{m-1}{d}, \quad (11)$$

which was obtained in Ref. [33] as a generalization of the result established in Ref. [34]. Thus, Eq. (10) together with Eq. (11) prove the validity of (7) for all pure product states. Finally, since $I_m$ is linear in the density matrix $\rho$ it follows that (7) holds for all (mixed) separable states as pure states represent extreme points.

The quantities $I_m$ together with the corresponding bounds for separable states can serve as criteria for entanglement detection in mixed states. However, what about the detection strength? Let us consider the $d$-dimensional isotropic states $\rho_1 = \alpha |\phi^+_d\rangle\langle \phi^+_d| + \frac{1-\alpha}{d^2} \mathbb{1}$ with $|\phi^+_d\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle$. These are known to be entangled for $\alpha > 1/(d+1)$ and separable for $\alpha \leq 1/(d+1)$ [35]. For an arbitrary basis choice $x \leftrightarrow [\langle i | x \rangle]$ in system $A$ and $x^* \leftrightarrow [\langle i^* | x^* \rangle]$ in $B$ the mutual predictability is always $C_{x,x^*} = \alpha + (1-\alpha)/d$ since $\rho_1$ is $U \otimes U^*$ invariant [36]. Thus, using mutually unbiased bases $\{B_k\}$ for $A$ and $\{B_k\}$ for $B$ we attain $I_m = m(\alpha + (1-\alpha)/d)$ which violates (7) for $\alpha > 1/m$. Consequently, entanglement allows for values $I_m > 1 + \frac{m-1}{d}$ which can be considered as an exact quantification of the statement that quantum correlations are more resistant against changes of the basis than ordinary correlations in separable states. As we also see the noise robustness of the criteria (7) increases with the number of MUBs (see Fig. 1). If there exists a complete set of $m = d+1$ MUBs the criterion (8) is necessary and sufficient for the separability of $\rho_1$ as $\alpha = 1/(d+1)$ is the exact bound of separability.

**Fig. 1.** Schematic illustration of the parameter regions detected by the criterion (7) for the $d$-dimensional isotropic states $\rho_1 = \alpha |\phi^+_d\rangle\langle \phi^+_d| + \frac{1-\alpha}{d^2} \mathbb{1}$ in dependence on the number of mutually unbiased bases $m$. The detection strength improves with increasing $m$ until for $m = d+1$ all entangled states are detected.

The significance of these results is manifold: First, the criterion (7) is surprisingly powerful. Each isotropic state is locally unitarily equivalent to any other maximally entangled state mixed with white noise [37]. By incorporating the corresponding local basis transformation that brings such a state into the isotropic form, we can detect all entanglement when $d$ is of prime-power dimension. Remarkably, only two MUBs are needed for detecting entanglement up to a threshold of 50% noise. In comparison, Bell inequalities are often used as indicators of entanglement as they are simple to realize in experiments [2,4,5]. However, using two measurement settings for each party they merely reach a maximal noise threshold between 29.289% and 32.656% depending on the dimension $d$ [38,39]. Notably, two MUBs suffice to verify all entangled pure states in arbitrary dimension, as is proven in Appendix A. Moreover, regarding experimental verification of entanglement, we are now in the position that we can customize the number of MUBs depending on what is experimentally feasible.

Second, we emphasize that with the presented concept we establish a direct link between the separability boundary and the maximum number of MUBs (illustrated in Fig. 1). Notice that if there were $m > d+1$ MUBs for a Hilbert space $H = \mathbb{C}^d$, then we would have $I_m > 1 + \frac{m-1}{d}$ for separable states, namely, for isotropic states $\rho_1$ with $1/m < \alpha \leq 1/(d+1)$. This, however, is not compatible with the statement of Eq. (7), and thus we have shown by contradiction that there cannot exist more than $d+1$ MUBs.

Last, it should be noted that our criteria are adaptable for arbitrary mixed states, i.e., for verifying entanglement in density matrices beyond the white noise scenario. In general, if one applies our criteria to an arbitrary unclassified state $\rho$ one can improve the detection by maximizing the outcome of $I_m$ over local unitaries (by seeking the optimal transformation $\rho \rightarrow U_A \otimes U_B \rho U_A^\dagger \otimes U_B^\dagger$) and permuting the order of the basis vectors in the mutually unbiased bases. Appropriate tools for this optimization can be found in Refs. [40,41]. An analysis of a broader class of states which is related to a geometric structure of the Hilbert-Schmidt space is given in Appendix B.

**IV. ENTAILMENT DETECTION: CONTINUOUS VARIABLE STATES**

The concepts introduced in the previous section are not limited to discrete systems but can easily be applied to continuous-variable states. As the noise robustness of the
criterion (7) increases with the number of MUBs, it is to be expected that we can find quite strong entanglement detection criteria for CV systems since in this case there exist infinitely many MUBs [7]. From a theoretical point of view it would certainly be interesting to study the generalization of our concept for a continuum of MUBs. However, in the current paper we take the viewpoint of a pragmatic experimentalist who has access to only a limited number of complementary observables. Let us study the simplest case where one has access to only two mutually unbiased bases corresponding to position (x) and momentum (p) measurements of single particles. Consider the two-mode squeezed-state wave function [42]

\[ \psi_s(x_1, x_2) = \sqrt{\frac{2}{\pi}} \exp[-e^{-2r}(x_1 + x_2)^2/2 - e^{+2r}(x_1 - x_2)^2/2]. \]  

\[ \psi_s(p_1, p_2) = \sqrt{\frac{2}{\pi}} \exp[-e^{-2r}(p_1 - p_2)^2/2 - e^{+2r}(p_1 + p_2)^2/2]. \]

depending on the squeezing parameter \( r \), whose entanglement we would like to verify in an experiment by measuring joint probabilities. We use the mutual predictabilities \( C_{x,x} = P_{x,x}(1,1) + P_{x,x}(2,2) \) of correlated positions,

\[ P_{x,x}(1,1) = \int_{-\infty}^{0} \int_{-\infty}^{0} |\psi_s(x_1, x_2)|^2 dx_1 dx_2, \]

\[ P_{x,x}(2,2) = \int_{0}^{\infty} \int_{0}^{\infty} |\psi_s(x_1, x_2)|^2 dx_1 dx_2, \]

and \( C_{p,p} = P_{p,p}(1,2) + P_{p,p}(2,1) \) of anticorrelated momenta,\(^1\)

\[ P_{p,p}(1,2) = \int_{-\infty}^{0} \int_{-\infty}^{0} |\psi_s(p_1, p_2)|^2 dp_1 dp_2, \]

\[ P_{p,p}(2,1) = \int_{0}^{\infty} \int_{0}^{\infty} |\psi_s(p_1, p_2)|^2 dp_1 dp_2. \]

Even though the correlations are measured quite precisely by dividing the space state into only two regions for each particle and observable (which can be regarded as a detector with very low resolution that produces only two access to each particle and observable (which can be regarded as a labeling of the measurement outcomes. Further MUBs and use a finer partitioning of the Hilbert space if experimentally possible, we are always allowed to add many MUBs [7]. From a theoretical point of view it would be expected that we can find quite strong entanglement detection in a squeezed state: Via the detector with very low resolution that produces only two observable (which can be regarded as a labeling of the measurement outcomes.

Let us discuss our approach by the example of an n-partite n-dimensional singlet state [49,50], known as the Aharonov state [51,52],

\[ |S_n\rangle = \frac{1}{\sqrt{n!}} \sum_{j,...,l=0}^{n-1} \varepsilon_{j,...,l} |j,...,l\rangle, \]

\[ |S_3\rangle = \frac{1}{\sqrt{6}} (|012\rangle + |120\rangle + |201\rangle - |021\rangle - |102\rangle - |210\rangle). \]

The Aharonov state has two central properties. First, from a correlation point of view, it is completely anticorrelated. This

\[ ^1 \text{Note that correlations and anticorrelations are the same up to the labeling of the measurement outcomes.} \]
implies that if one performs measurements on \( n - 1 \) parties and is aware of all outcomes then one can predict with certainty the outcome of the remaining party. Furthermore, this state is \( U^{\otimes n} \) invariant, implying that these anticorrelations always hold when all of the \( n \) parties choose the same local basis \([49,50]\).

With respect to the mentioned symmetries of the state, it is reasonable to introduce an \( n \)-particle anticorrelation function

\[
A_{a_1,\ldots,a_n} = \sum_{j_1,\ldots,j_n=0}^{n-1} |e_{j_1,\ldots,j_n}| P_{a_1,\ldots,a_n}(j_1,\ldots,j_n) \tag{20}
\]

\[
A_{a_1,\ldots,a_n} = \sum_{j_1,\ldots,j_n=0}^{n-1} |e_{j_1,\ldots,j_n}| \langle j_a,\ldots,j_z | \rho | j_a,\ldots,j_z \rangle, \tag{21}
\]

which is \( A_{a_1,\ldots,a_n} = 1 \) if and only if all local measurement outcomes of the observables \( \{a,\ldots,z\} \) are always unequal. Specifically, \( A_{a_1,\ldots,a_n} = 1 \) for the Aharonov state when \( a = \cdots = z \), i.e., when the same basis is chosen for all subsystems (as explained above). We build the linear combination

\[
J_m = \sum_{a=1}^{m} A_{a_1,\ldots,a} \tag{22}
\]

using \( m \) mutually unbiased bases. This quantity \( J_m \) is bounded by

\[
J_m \leq 1 + \frac{m - 1}{n} \tag{23}
\]

for biseparable states.

**Proof.** Suppose we have a pure state \( |\Psi_{a_1,\ldots,a_n}\rangle \) which is biseparable with respect to any bipartition \( \{X|Y\} \). In general, such a state can reach \( A_{a_1,\ldots,a_n} = 1 \) for a certain choice of observables \( a_1,\ldots,a_n \). However, if we replace the local bases \( \{a_1,\ldots,a_n\} \) by corresponding mutually unbiased bases \( \{a',\ldots,a'_n\} \) then the predictability is lost, similarly to the bipartite qudit case (Sec. III). We thus obtain \( A_{a_1,\ldots,a_n} \leq 1/n! \) for all \( 1 \leq n \leq \min\{d_X,d_Y\} \) where \( d_X \) and \( d_Y \) are the dimensions of \( X \) and \( Y \). Since \( d = n \) is the minimum dimension over all bipartitions of the \( n \)-partite \( n \)-dimensional system it is guaranteed that \( A_{a_1,\ldots,a_n} \leq 1/n! \leq 1/n \) holds for all biseparable states. Consequently, with \( m \) MUBs we arrive at (23), and since \( J_m \) is linear in the density matrix \( \rho \) it follows that any violation directly implies the existence of genuine multiparticle entanglement in a (mixed) state.

Let us discuss the detection strength of the criterion (23) by the example of the Aharonov state in the presence of white noise, \( \rho_{aw} = |\langle S_a|S_a\rangle + 1\rho_{aw}| \). For the pure Aharonov state \( |\langle S_a|S_a\rangle \) we have \( A_{a_1,\ldots,a_n} = 1 \) for all \( a, \) and for white noise \( \rho_{aw} \) we have \( A_{a_1,\ldots,a_n} = 1/n! \). Thus, in total we obtain \( J_m = J_m(\alpha + (1 - \alpha)n!/n^m) \) which for

\[
\alpha > \frac{n!(m + n - 1) - mnm!}{mn(n^m - n!)} \tag{24}
\]

leads to a violation of \( J_m \leq 1 + \frac{m - 1}{n} \). Figure 2 illustrates the noise robustness of the criterion (23) \((\alpha = 0.8)\) in dependence on the number of used mutually unbiased bases \( m \). As can be seen therein, while the concept used is rather simple, the derived criterion is remarkably powerful in detecting genuine multipartite entanglement in the vicinity of the Aharonov state. For protocols where this particular state is used as a resource (e.g. \([49,53,54]\)) this could be exploited to test whether the state was correctly distributed between all parties. Note that there currently exists no comparable test for verifying genuinely multipartite entanglement in \( \rho_{aw} \) and that the actual noise threshold is unknown. Note furthermore that it is to be presumed that our concept can easily be adopted to other multipartite states by taking into account their symmetries and correlations. In many cases this should lead to criteria with a valuable experimental-effort-to-detection-strength ratio.

**VI. SUMMARY AND OUTLOOK**

In conclusion we have established a connection between mutually unbiased bases and entanglement detection. We showed that MUBs allow for an intuitive way of constructing entanglement criteria for arbitrarily high-dimensional systems. These criteria are beneficial for experiments since they require only a few local measurements. By means of the isotropic and Bell-diagonal states (Appendix B), we demonstrated that our approach can yield necessary and sufficient criteria for separability if a complete set of MUBs is available for the local subsystems. In addition, we found that the number of MUBs can be related to the separability problem and provided an alternative proof that for a \( d \)-dimensional system there cannot exist more than \( d + 1 \) MUBs.

Besides optimal detection through complete sets of MUBs, we showed that even using only two local complementary measurement settings it is possible to verify entanglement with a quite adequate robustness to noise. For experiments where the set of measurable observables is limited this may be of valuable help. For instance, for systems in high-energy physics investigated at accelerator facilities only a restricted observable space is available due to the laborious effort and technical limitations. However, e.g., for neutral entangled \( K \) mesons \([55]\) one could realize two MUBs during the time evolution of the system, allowing for a direct test of entanglement via the introduced criteria. Two MUBs are also sufficient for detecting all entangled pure states of any two-qudit system (Appendix A) and allow for powerful
entanglement detection in continuous variables. Even the presence of genuine multipartite entanglement can be tested very effectively through correlations in MUBs, which we demonstrated by the example of the Aharonov state.

For prime-power dimensions, MUBs enable a complete state tomography. Consequently, local information and correlations with respect to MUBs should provide necessary and sufficient information to detect all entanglement in systems which are composed of subsystems with prime-power dimensionality. For such systems, it should be possible to develop a general framework of entanglement detection based on complementary observables. For qubit systems, such a framework should be equivalent to the concept of correlation tensors (see, e.g., Refs. [56–58]), as the decomposition of density matrices in terms of Pauli matrices is intrinsically linked to MUBs. However, a generalization of correlation tensors to higher-dimensional systems has so far been addressed only by means of the generators of the special unitary group [58–60]. Here, a theory in terms of MUBs should allow for an alternative method to investigate multilevel quantum correlations which is expected to be experimentally advantageous.

The presented scheme might also yield further results on systems with non-prime-power dimensions: Just as we have shown that an upper bound on the number of MUBs can be deduced from the separability problem via the isotropic states, it might also be possible to determine the actual number of MUBs using a certain state and/or system. Finally, as numerous quantum features such as discord [61], steering [62], and nonlocality (see Ref. [63] and references therein) give rise to particular correlations, it is conceivable that they can also be brought into relation with mutually unbiased bases, or even be directly formulated in terms of them.

ACKNOWLEDGMENTS

We would like to thank Andreas Winter, Renato Renner, Colin Wilkott, Shengjun Wu, and Sergey Filippov for their valuable comments. C.S. and M.H. acknowledge financial support from the Austrian FWF (Project No. 21947N16) and the ERC. S.B. would like to thank the Heilbronn Institute for Mathematical Research for financial support. This project was cofinanced by the SoMoPro program. B.C.H. acknowledges funding from the European Community within the Seventh Framework Program under Grant Agreement No. 229603 and the COST action MP1006.

APPENDIX A: SUFFICIENCY OF TWO MUBS FOR PURE STATES

We show that two MUBs are sufficient to verify all entangled pure states of any bipartite qudit system $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B = C^d \otimes C^d$. Assume our objective is to prepare a particular pure state $|\psi\rangle = \sum_{m,n=0}^{d-1} c_{m,n} |m\rangle \otimes |n\rangle$. In order to achieve that the mutual predictability is maximal, i.e.,

$$ C_{1,1} = \sum_{i=0}^{d-1} \langle i_1 | \otimes \langle i_1 | \langle i_1 | \otimes |i_1\rangle = 1, \quad (A1) $$

we use the measurement bases $\{|i_1\rangle\}$ on $A$ and $B$ for which our target state takes on the Schmidt form $|\psi\rangle = \sum_{i=0}^{d-1} \lambda_i |i_1\rangle \otimes |i_1\rangle$ with $0 \leq r \leq d - 1$, $\lambda_i \geq 0$, and $\sum_{i=0}^{d-1} \lambda_i^2 = 1$. For a second measurement of the mutual predictability $C_{2,2'}$, we choose the (mutually unbiased) basis $\{|i_2\rangle, \ldots, |d - 1\rangle\}$ with $|i_2\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^k |k_1\rangle$ and $\omega = \exp(2 \pi i / d)$, determined by the discrete Fourier transform. For the composite basis vectors we have

$$ |i_2\rangle \otimes |i_2\rangle^* = \frac{1}{d} \sum_{k,l=0}^{d-1} \omega^{(k-l)/d} |k_1\rangle \otimes |l_1\rangle. \quad (A2) $$

This leads to

$$ C_{2,2'} = \sum_{i=0}^{d-1} \langle i_2 | \otimes \langle i_2 | |\psi\rangle \langle i_2 | \otimes |i_2\rangle^* = \sum_{i=0}^{d-1} \frac{|\langle \psi | i_2\rangle \otimes |i_2\rangle^*|^2}{d} = \sum_{i=0}^{d-1} \left[ \sum_{n=0}^{d-1} \lambda_n |n_1\rangle \otimes |n_1\rangle \right] \left[ \frac{1}{d} \sum_{k,l=0}^{d-1} \omega^{(k-l)/d} |k_1, l_1\rangle \right]^2. \quad (A3) $$

We see that the only relevant vectors are those with $k = l$, in which case we have $\omega^{(k-l)/d} = 1$, and get

$$ C_{2,2'} = \sum_{i=0}^{d-1} \frac{1}{d} \sum_{n=0}^{r} \lambda_n^2. \quad (A4) $$

Here the squared absolute value $|\sum_{n=0}^{d-1} \lambda_n|^2$ can be rewritten as

$$ C_{2,2'} = \frac{1}{d} \sum_{n=0}^{d-1} \lambda_n^2 + \sum_{m \neq n} \lambda_m \lambda_n \quad (A5) $$

Thus, altogether we obtain

$$ I_2 = C_{1,1} + C_{2,2'} = 1 + \frac{1}{d} \left( \sum_{m \neq n} \lambda_m \lambda_n \right). \quad (A6) $$

For any separable state $|\psi\rangle$ the Schmidt rank is 1, and consequently $\sum_{m \neq n} \lambda_m \lambda_n = 0$ since there is only one Schmidt coefficient $\lambda_m$, which equals 1, whereas, we have $\sum_{\forall m \neq n} \lambda_m \lambda_n > 0$ for any entangled state because they have Schmidt rank greater than or equal to 2, i.e., there are at least two nonzero Schmidt coefficients $\lambda_m > 0$. Consequently, two MUBs are sufficient to detect all entangled pure states, as all of them achieve $I_2 > 1 + \frac{1}{d}$. $$

$^2$Note that $I_2 > 1 + 1/d$ unambiguously implies the presence of entanglement regardless of which pairs of MUBs we use. However, just as for any entanglement verification scheme that does not require a full state tomography, we have to adjust our setup according to the expected state to achieve optimal detection.
APPENDIX B: ENTANGLEMENT DETECTION AND GEOMETRY

In Ref. [37], a special simplex of locally maximized mixed two-qudit states, also known as Bell-diagonal states, was introduced. This set of states is given by

$$W = \left\{ \sum_{k,l=0}^{d-1} c_{k,l} P_{k,l} \mid c_{k,l} \geq 0, \sum_{k,l=0}^{d-1} c_{k,l} = 1 \right\},$$  \hspace{1cm} (B1)$$

where $P_{k,l} = |\Omega_{k,l}\rangle\langle \Omega_{k,l}|$ are the projectors of $d^2$ mutually orthogonal Bell states, generated by applying the unitary Weyl operators

$$W_{k,l} = \sum_{s=0}^{d-1} \omega^{sk}|s\rangle\langle s + l| \mod d |$$  \hspace{1cm} (B2)$$

with $\omega = \exp(2\pi i/d)$ and $k,l \in \{0, \ldots, d-1\}$ on the maximally entangled state $|\Omega_{0,0}\rangle = \frac{1}{\sqrt{d}} \sum_{i=0}^{d-1} |i\rangle \otimes |i\rangle$, i.e.,

$$|\Omega_{k,l}\rangle = (W_{k,l} \otimes 1)|\Omega_{0,0}\rangle.$$  \hspace{1cm} (B3)$$

The isotropic states from Sec. III are also contained in this set. Here, for a complete set of MUBs, the quantity $I_{d+1}$ from Eq. (8) reads

$$I_{d+1} = 1 + hd,$$  \hspace{1cm} (B4)$$

where $h = \max\{c_{k,l}\}$ is the largest coefficient. Consequently, the region with $I_{d+1} \leq 2$ corresponds to the so-called enclosure polytope [37], whose facets are defined by the $d^2$ hyperplanes corresponding to optimal entanglement witnesses for all $\rho = \frac{1}{d^2}1 + \alpha P_{k,l}$. It was shown that all states outside this polytope are entangled [37]. Hence, the quantity $I_{d+1}$ based on the maximum number of MUBs reflects the geometric structure of the enclosure polytope, which itself shares the symmetries of the simplex $W$. 