

PAPER • OPEN ACCESS

Detecting entanglement can be more effective with inequivalent mutually unbiased bases

To cite this article: B C Hiesmayr *et al* 2021 *New J. Phys.* **23** 093018

View the [article online](#) for updates and enhancements.

You may also like

- [Incompatibility robustness of quantum measurements: a unified framework](#)
Sébastien Designolle, Máté Farkas and Jdrzej Kaniewski
- [Orbits of mutually unbiased bases](#)
Kate Blanchfield
- [Finite-key security analysis for multilevel quantum key distribution](#)
Kamil Brádler, Mohammad Mirhosseini, Robert Fickler et al.



PAPER

Detecting entanglement can be more effective with inequivalent mutually unbiased bases

OPEN ACCESS

RECEIVED
23 June 2021REVISED
19 August 2021ACCEPTED FOR PUBLICATION
25 August 2021PUBLISHED
13 September 2021

Original content from
this work may be used
under the terms of the
[Creative Commons
Attribution 4.0 licence](#).

Any further distribution
of this work must
maintain attribution to
the author(s) and the
title of the work, journal
citation and DOI.

B C Hiesmayr^{1,*} , D McNulty² , S Baek³, S Singha Roy⁴ , J Bae⁵ and
D Chruściński⁶ ¹ University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria² Department of Mathematics, Aberystwyth University, Aberystwyth, Wales, United Kingdom³ Department of Applied Mathematics, Hanyang University (ERICA), 55 Hanyangdaehak-ro, Ansan, Gyeonggi-do, 426-791, Republic of Korea⁴ Instituto de Física Teórica UAM/CSIC, C/ Nicolás Cabrera 13-15, Cantoblanco, 28049 Madrid, Spain⁵ School of Electrical Engineering, Korea Advanced Institute of Science and Technology (KAIST), 291 Daehak-ro Yuseong-gu, Daejeon 34141, Republic of Korea⁶ Institute of Physics, Faculty of Physics, Astronomy, and Informatics, Nicolaus Copernicus University, Grudziadzka 5, 87-100 Torun, Poland

* Author to whom any correspondence should be addressed.

E-mail: Beatrix.Hiesmayr@univie.ac.at**Keywords:** entanglement detection, mutually unbiased bases, unextendible mutually unbiased bases, high dimensional quantum systems

Abstract

Mutually unbiased bases (MUBs) provide a standard tool in the verification of quantum states, especially when harnessing a complete set for optimal quantum state tomography. In this work, we investigate the detection of entanglement via inequivalent sets of MUBs, with a particular focus on unextendible MUBs. These are bases for which an additional unbiased basis cannot be constructed and, consequently, are unsuitable for quantum state verification. Here, we show that unextendible MUBs, as well as other inequivalent sets in higher dimensions, can be more effective in the verification of entanglement. Furthermore, we provide an efficient and systematic method to search for inequivalent MUBs and show that such sets occur regularly within the Heisenberg–Weyl MUBs, as the dimension increases. Our findings are particularly useful for experimentalists since they demonstrate that a clever selection of MUBs allows for entanglement detection with fewer measurements.

1. Introduction

Quantum entanglement is one of the key ingredients responsible for many of the recent advances in quantum technologies, however, the detection of this fundamental property, even with full knowledge of the quantum state, is in general an NP-hard problem [1]. In this contribution we exploit an experimentally feasible protocol to detect entanglement in which the subsequent addition of measurement settings detect a larger class of entangled states. The essential feature of this scheme is for the measurement settings to exhibit complementarity, namely, that the measurements form a set of mutually unbiased bases (MUBs), i.e. the overlap of any pair of vectors from different bases is constant [2]. Physically, this means that exact knowledge of the measurement outcome of one observable implies maximal uncertainty in the other.

Utilising this property, MUBs play an important role in many information processing tasks, such as quantum state tomography [3, 4], quantum key distribution [5], signal processing [6], and quantum error correction [7], to name just a few. Unfortunately, the existence of maximal sets of these highly symmetric bases is a difficult unresolved question: an equivalent formulation of the problem in terms of orthogonal decompositions of the algebra $\mathfrak{sl}_d(\mathbb{C})$ dates back almost forty years [8, 9]. While it is known that maximal sets of $d + 1$ MUBs in \mathbb{C}^d exist when d is a prime or prime-power, e.g. by a construction based on the Heisenberg–Weyl group [10], it is conjectured that fewer MUBs exist in all other dimensions [11, 12]. The classification of subsets of MUBs is an open problem for $d > 5$, and a rich structure of inequivalent MUBs

(up to unitary transformations) exists [13]. Of particular relevance to this work is the property of unextendibility, i.e. sets of MUBs which cannot be completed to a maximal set.

One striking feature of the entanglement witness, first introduced in [14], is that the value of the upper bound (which is violated by entangled states) depends only on the *number* of MUBs and not on the *choice* between inequivalent sets. For example, the experimenter is free to use extendible or unextendible MUBs. The protocol has since been applied to two photons entangled in their orbital angular momentum, and bound entangled (PPT-entangled) states have been verified experimentally for the first time [15, 16]. Further modifications of the witness have also been considered, e.g. with two-designs and orthogonal rotations [17–19], as well as in applications to other scenarios [20, 21].

Recently, entanglement witnesses were also shown to have a lower bound [22, 23], which often turns out to be non-trivial, i.e. entanglement is detectable. In this contribution, we compute the lower bounds of the MUB-witness and reveal that, in contrast to the upper bound, the values depend strongly on the *choice* of MUBs, as well as the number of measurements. One consequence of this sensitivity, as we will see, is that unextendible MUBs can be more effective at entanglement detection than extendible ones. Furthermore, this operational distinction between MUBs reveals the existence of inequivalent sets and hence the witness provides a way to classify these sets. We use this criterion to establish inequivalences within the Heisenberg–Weyl MUBs when $d = 5, 7, 9$, as well as for some continuous families and unextendible sets.

This contribution is perhaps the first application of MUBs in which unextendible sets may be the preferred measurement choice over Heisenberg–Weyl subsets. In fact, most applications exhibit no preference for a particular subset of MUBs, and hence the physical differences between inequivalent sets have not been fully realised. Our results complement some recent observations on measurement incompatibility [24] and quantum random access codes (QRAC) [25, 26]. In particular, inequivalent MUBs contain varying degrees of incompatibility when quantified by their noise robustness, meaning that some sets require additional noise to become jointly measurable. Furthermore, measuring different subsets of MUBs in a QRAC protocol reveals ‘anomalies’ in the average success probability, which appear to coincide with our different lower bounds of the witness. Here, by considering entanglement witnesses, we provide a physically significant application which exploits these inequivalences.

2. Inequivalent and unextendible MUBs

Formally, we say a pair of bases in \mathbb{C}^d , labelled $B_k = \{|i_k\rangle\}_{i=0}^{d-1}$ and $B_{k'}$, are mutually unbiased iff

$$|\langle i_k | i'_{k'} \rangle|^2 = \delta_{i,i'} \delta_{k,k'} + (1 - \delta_{k,k'}) \frac{1}{d},$$

for all $i, i' = 0, \dots, d-1$. For prime dimensions the standard Heisenberg–Weyl group provides the essential building blocks for the construction of a complete set of $d+1$ MUBs, while for prime-powers $d = p^n$ the generalised tensor product Heisenberg–Weyl group (as described in the appendix) is used. However, in almost all dimensions, these provide only a small subset of all possible cases. In order to classify MUBs, we need to introduce the notion of equivalence classes. Two sets of m MUBs are equivalent, $\{\mathcal{B}_1, \dots, \mathcal{B}_m\} \sim \{\mathcal{B}'_1, \dots, \mathcal{B}'_m\}$, if one set can be transformed into the other by a unitary or antiunitary transformation, permutations within (or of) bases, and phase factor multiplications. The task of classification is challenging, with success currently limited to $d \leq 5$ [27, 28]. When $d = 2, 3, 5$ the Heisenberg–Weyl MUBs exhaust all possibilities: no inequivalence occurs when $d = 2, 3$ and only two inequivalent triples appear among all possible subsets in $d = 5$. In contrast, $d = 4$ yields a one-parameter family of pairs, and a three-parameter family of triples, inequivalent to all Heisenberg–Weyl subsets [29]. In higher dimensions $d \geq 6$ the situation is complicated and closely related to the (very old [30, 31]) problem of searching for complex Hadamard matrices. A square matrix H is a complex Hadamard matrix if it is unitary and its elements have equal modulus. In some instances, constructions of MUBs produce cases which do not extend to complete sets, and are aptly named *unextendible* MUBs [32, 33]. In dimensions $d = p^n$, the first examples appear when $d = 4$ [28] and $d = 7$ [34], and more generally $d = p^2$ [35, 36].

Finally, we fix some notation. It is often convenient to represent MUBs as sets of unitary matrices, where the columns correspond to orthogonal basis vectors. Due to equivalence transformations, it is possible to express a set of m MUBs for \mathbb{C}^d in Hadamard form,

$$\{\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_m\} \sim \{I, H_1, \dots, H_{m-1}\},$$

where I is the identity matrix and H_i are $(d \times d)$ complex Hadamard matrices with $|h_{ij}| = 1/\sqrt{d}$. Wlog we assume $\mathcal{B}_1 \equiv I$ is the standard basis throughout.

3. Entanglement detection via MUBs

In reference [14] an experimentally friendly protocol was introduced that can verify the entanglement of a bipartite state ρ on $\mathbb{C}^d \otimes \mathbb{C}^d$, by subsequently measuring a set of MUBs. Both parties, which may be locally separated, and usually called Alice and Bob, each possess the (same) set of m MUBs in \mathbb{C}^d . Applying identical projections from each basis, they calculate

$$M_m(\rho) := \sum_{k=1}^m \sum_{i=0}^{d-1} P(i, i | \mathcal{B}_k, \mathcal{B}_k), \quad (1)$$

where $P(i, i | \mathcal{B}_k, \mathcal{B}_k) = \text{tr}(|i_k\rangle\langle i_k| \otimes |i_k\rangle\langle i_k| \rho)$ denotes the joint probability of Alice and Bob each obtaining outcome i of the basis measurement \mathcal{B}_k , given the state ρ . The authors of reference [14] showed that the correlation function M_m is bounded above for all separable states by U_m (see equation (3)). This is easily seen when we assume that the source produces the separable state $|i_l i_l\rangle$, with $|i_l\rangle \in \mathcal{B}_l$. Here, the joint probability $P(i, i | \mathcal{B}_l, \mathcal{B}_l)$ is obviously maximal, i.e. 1, and for any other basis choice $k \neq l$, the joint probabilities result in $\sum_i P(i, i | \mathcal{B}_k, \mathcal{B}_k) = \frac{1}{d}$ due to the unbiasedness condition. The bound follows by exploiting the arithmetic mean and the convexity of separable states. Recently, it was shown in [22] that the very definition of an entanglement witness also yields a non-trivial second bound, which for the MUB-witness results in a lower bound. Thus, the quantity M_m has two bounds,

$$L_m \stackrel{\forall \text{ separable states}}{\leq} M_m(\rho) \stackrel{\forall \text{ separable states}}{\leq} U_m \quad (2)$$

and any violation of the above inequality detects entanglement of the state ρ . The upper bound has the simple form

$$U_m = 1 + \frac{m-1}{d}, \quad (3)$$

and is independent of the *choice* of MUBs, which implies that only the unbiasedness property is exploited [14]. One should also note that although the upper bound is independent of the *ordering* of the MUBs, the results depend on the initial correlation of the considered quantum state ρ . This in turn can be compensated by Alice or Bob applying local unitaries to the state. Further note that observing entanglement in any *pure* quantum state via the above inequality only requires measurements in (any) two MUBs. For a complete set, the bounds are $L_{d+1} = 1$ and $U_{d+1} = 2$, which follow from the two-design property of MUBs [17], and the witness is most effective at detecting entangled states.

4. Detection with inequivalent MUBs

In striking contrast with the upper bound of the function $M_m(\rho)$, the lower bound L_m depends not only on the dimension d and the number of MUBs, m , but also on the choice of MUBs. In other words, the bound is highly sensitive to the particular set of MUBs chosen, and therefore inequivalent sets often yield different values of L_m . In the following, we analyse this dependence to understand its effect on entanglement detection. We restrict our analysis to dimensions $d < 10$ to ensure that the numerical optimisations of the bounds are reliable, where we exploit the composite parameterization of unitaries introduced by [37]. For higher dimensions alternative methods may be successful such as e.g. semidefinite programming [38]. Let us first formulate three main observations in the form of theorems, which we will further discuss in the next section:

Theorem A. *If sets of m MUBs have different lower bounds $L_m = \min_{\rho_{\text{SEP}}} M_m(\rho_{\text{SEP}})$, they are inequivalent.*

Theorem B. *Unextendible MUBs can result in a stricter lower bound L_m and may therefore detect a larger set of entangled states.*

Theorem C. *Unextendible sets of MUBs may detect a larger set of entangled states via both the upper and lower bounds, U_m and L_m .*

5. Discussions

Unextendible MUBs in $d = 4$: the first inequivalent sets of MUBs appear in dimension four, and provide a simple example of theorem A. There exists a one-parameter family of inequivalent pairs $\{I, F(x)\}$ and a three-parameter family of triples $\{I, F(x), H(y, z)\}$ where $H_1 = F(x)$ is the Fourier family and $H_2 = H(y, z)$

Table 1. Lower (L_m) and upper (U_m) bounds of the MUB-witness are summarized for m MUBs and $d = 2, 3, 4$. For $d = 4$, the unextendible sets lead to a stricter bound.

m	$d = 2$	$d = 3$	$d = 4$		$d = 2$	$d = 3$	$d = 4$
	L_m	L_m	$L_m^{\text{ext.}}$	$L_m^{\text{unext.}}$	U_m	U_m	U_m
2	$\frac{1}{2}$	0.211	0	0	$\frac{3}{2}$	$\frac{4}{3}$	$\frac{5}{4}$
3	1	$\frac{1}{2}$	$\frac{1}{4}$	$(\frac{1}{4}, \frac{1}{2}]$	2	$\frac{5}{3}$	$\frac{6}{4}$
4		1	$\frac{1}{2}$	--		2	$\frac{7}{4}$
5			1	--			2

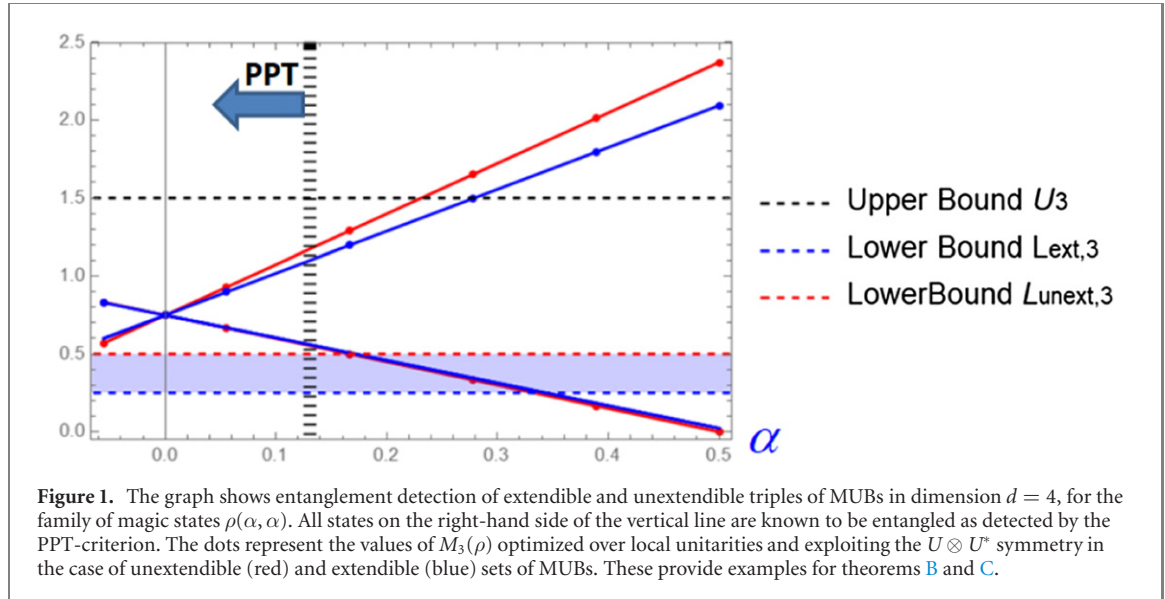


Figure 1. The graph shows entanglement detection of extendible and unextendible triples of MUBs in dimension $d = 4$, for the family of magic states $\rho(\alpha, \alpha)$. All states on the right-hand side of the vertical line are known to be entangled as detected by the PPT-criterion. The dots represent the values of $M_3(\rho)$ optimized over local unitarities and exploiting the $U \otimes U^*$ symmetry in the case of unextendible (red) and extendible (blue) sets of MUBs. These provide examples for theorems B and C.

is a family of Hadamard matrices defined in the appendix with $x, y, z \in [0, \pi]$. These cover all pairs and triples in $d = 4$ [28] and coincide with the Heisenberg–Weyl case when $x = y = z = \frac{\pi}{2}$ (for which it extends to a complete set). The triple is unextendible for all other parameter choices. As summarized in table 1 the upper bound is calculated by equation (3), but the lower bound L_3 depends strongly on the choice of triple. For the (extendible) Heisenberg–Weyl triple, we find $L_3^{\text{ext}} = 1/4$, whereas $L_3^{\text{unext}} \in (1/4, 1/2]$ for all unextendible sets. The strongest possible bound $L_3^{\text{unext}} = 1/2$ is reached when $x = \pi/2$ and $y = z = 0$, and is achieved for any pure separable state $\rho = |a, b\rangle\langle a, b|$ with $\langle a|b\rangle = 0$. In contrast, the Heisenberg–Weyl triple saturates the lower bound only for particular separable states, e.g. $\frac{1}{\sqrt{2}}(|0\rangle - |2\rangle) \otimes \frac{1}{\sqrt{2}}(|1\rangle + |3\rangle)$. We note that $L_2 = 0$ for all inequivalent pairs.

Unextendible MUBs are more efficient: let us now study whether unextendible MUBs are more efficient at detecting entanglement (theorems B and C), which is suggested by the stricter lower bounds. However, this need not be the case since the witness itself is also altered and may act differently on any given state.

Let us consider a state from the magic simplex [39–41], e.g. $\rho_{\alpha, \beta} = (1 - \alpha - \beta)\mathbb{1}/d^2 + \alpha P_{0,0} + \beta P_{0,1}$ (it applies for any two Bell states), where the entanglement properties are also fully known. Here $P_{0,0} = \frac{1}{d} \sum_{s,t=0}^{d-1} |ss\rangle\langle tt|$ denotes a Bell state and any other Bell state $P_{k,l}$ can be obtained by locally applying in one subsystem a unitary Weyl operator $W_{(k,l)} = \sum_{j=0}^{d-1} \omega_d^{jk} |j\rangle\langle j+l|$ with $\omega_d = e^{\frac{2\pi i}{d}}$. The results for $d = 4$ and $\alpha = \beta$ are summarized in figure 1 and show the unextendible sets are more efficient in detecting entanglement, as described in theorems B and C.

A second example is provided by Werner states ρ_W , which are invariant under any local unitary $U \otimes U$ [42]. The lower bound of (2) detects all entangled Werner states for a complete set of MUBs, and becomes less effective as the number of measurements is reduced. Due to $U \otimes U$ invariance, the quantity $M_m(\rho_W)$ is independent of the choice of MUBs, therefore the value of the bound plays a fundamental role in its effectiveness. For three MUBs, the unextendible triple with the strictest lower bound $L_3^{\text{unext}} = 1/2$ detects the largest set of entangled states.

Inequivalent subsets: we now analyse the lower bound L_m for all subsets of Heisenberg–Weyl MUBs when $d = 5, \dots, 9$, to search for inequivalent sets.

Table 2. Lower (L_m) and upper (U_m) bounds of the function M_m for the Heisenberg–Weyl MUBs in $d = 5$.

m	\mathcal{O}	L	U
$d = 5$			
2	$\mathcal{B}_1\mathcal{B}_2$	0.0297	$\frac{6}{5}$
3	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3$ [10 times]	0.2764	$\frac{7}{5}$
3	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_4$ [10 times]	0.1273	$\frac{7}{5}$
4	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4$	0.3350	$\frac{8}{5}$
5	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5$	$\frac{1}{2}$	$\frac{9}{5}$
6	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5\mathcal{B}_6$	1	2

Table 3. Lower (L_m) and upper (U_m) bounds of the function M_m for the Heisenberg–Weyl MUBs and unextendible MUBs in $d = 7$.

m	\mathcal{O}	L	U
$d = 7$			
2	$\mathcal{B}_1\mathcal{B}_2$	0.0034	$\frac{8}{7}$
3	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3$	0.0698	$\frac{9}{7}$
3	$\mathcal{B}_1\mathcal{B}_2\mathcal{A}_7$	0.0557	$\frac{9}{7}$
4	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4$ [42 times]	0.1514	$\frac{10}{7}$
4	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_5$ [28 times]	0.20101	$\frac{10}{7}$
5	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5$	0.2750	$\frac{11}{7}$
6	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5\mathcal{B}_6$	0.3896	$\frac{12}{7}$
7	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5\mathcal{B}_6\mathcal{B}_7$	0.5	$\frac{13}{7}$
8	$\mathcal{B}_1\mathcal{B}_2\mathcal{B}_3\mathcal{B}_4\mathcal{B}_5\mathcal{B}_6\mathcal{B}_7\mathcal{B}_8$	1	2

Dimension $d = 5$: here, a full classification is already known [27, 28], and our search recovers all equivalence classes. All subsets of equal cardinality are equivalent except for triples, which can be grouped into one of two classes: $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\} \approx \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_4\}$. Computing the lower bound L_3 over all $\binom{6}{3} = 20$ triples, we find two different bounds, as summarized in table 2. No other inequivalent sets appear from the 2^6 permutations, in agreement with previous results.

Dimension $d = 7$: searching over all subsets, we find only two inequivalent quadruplets

$$\mathcal{Q}_1 := \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_4\} \approx \{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_5\} := \mathcal{Q}_2.$$

These appear by observing $L_{\mathcal{Q}_1} = 0.1514$ and $L_{\mathcal{Q}_2} = 0.20101$. There are $\binom{8}{4} = 70$ combinations of size four, with 42 sets achieving the first bound and 28 the second (higher bound). To explain this distribution, note that no inequivalent triples exist, i.e. any triple is equivalent to $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3\}$. Hence, there are only five possible extensions to a quadruplet, namely $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{B}_3, \mathcal{B}_k\}$, $k = 4, \dots, 8$. If $k = 4, 6, 8/5, 7$ the quadruplets are equivalent to $\mathcal{Q}_1/\mathcal{Q}_2$, therefore the distribution is split as above rather than evenly. We note that two inequivalent quadruplets were also found by analysing the incompatibility content of these subsets [24] and their success in a QRAC protocol [26]. This case is also interesting due to the existence of an unextendible triple, $\{\mathcal{B}_1, \mathcal{B}_2, \mathcal{A}_7\}$, defined in the appendix. For this set, the lower bound $L_3 = 0.0557$ is smaller than the Heisenberg–Weyl bound (0.0698). Again, we have examples of the above theorems. The results are summarized in table 3.

Dimension $d = 8$: we find a very distinct picture within the Heisenberg–Weyl set, with no inequivalent sets found, in contrast with odd prime and prime-power dimensions. In particular, the bounds are given by $L_{m=2,\dots,4} = 0$, $L_5 = \frac{1}{8}$, $L_6 = \frac{2}{8}$, $L_7 = \frac{3}{8}$, $L_8 = \frac{1}{2}$, $L_9 = 1$.

Dimension $d = 9$: within the Heisenberg–Weyl set we find no inequivalences for $m = 2, 3$ with $L_2 = L_3 = 0$, but three inequivalent sets for $m = 4$ ($L_4 = 0, 0.077, \frac{1}{6}$) with occurrence 15 : 180 : 15, three inequivalent sets for $m = 5$ ($L_5 = 0.140, 0.191, 0.198$) with occurrence 90 : 72 : 90, three inequivalent sets for $m = 6$ ($L_6 = \frac{2}{11}, 0.259, \frac{1}{3}$) with occurrence 15 : 180 : 15, two inequivalent sets for $m = 7$ ($L_7 = \frac{1}{3}, 0.331$) with occurrence 60 : 60 and no inequivalent sets for $m = 8, 9, 10$ ($L_8 = 0.418, L_9 = \frac{1}{2}, L_{10} = 1$). We note that these results depend heavily on numerical optimizations. The inequivalences are in full agreement with those found in [24, 26], except when $d = 9, m = 3$, where we detect no inequivalent triples ($L_3 = 0$) unlike

the two cases found in [24] and the anomaly in [26]. Furthermore, we observe that $L_m < L_{m+1}$ does not always hold, which is of particular importance for experimental realisations.

Dimension $d = 6$: this is the first dimension where a maximal set has not been found, and it is conjectured four MUBs do not exist [43]. The Heisenberg–Weyl construction yields only three bases, although many inequivalent pairs and triples exist [44, 45]. There is only one known unextendible pair, $\{\mathcal{B}_1, S_6\}$, where S_6 is the Tao matrix [46, 47] defined in the appendix. The lower bound for any pair (extendible and unextendible) results in $L_2 = 0$. The lower bound for the unextendible Heisenberg–Weyl triple is $L_3 = 0.1056$.

6. Summary and outlook

We have studied the role that inequivalent MUBs play in the detection of entanglement, as well as providing a method to systematically distinguish inequivalent sets. The dual bounds of the witness exhibit contrasting behaviours, as the choice of MUBs plays a fundamental role in the effectiveness of the lower bound. This is a crucial observation for experimentalists who want to maximise their success in detecting entanglement. Little is known about the physical significance of inequivalent MUBs, and our witness is perhaps the first application where unextendible MUBs are the preferred choice. This leads to questions of whether other applications exist which prioritise one set over another (as is the case for QRACs [26]), or if inequivalent MUBs have other properties responsible for their varying degrees of usefulness. One such possibility is their incompatibility content, which also distinguishes between equivalence classes of MUBs [24]. Exploring connections between incompatibility, inequivalent MUBs, and entanglement detection, such as the role incompatibility plays in the effectiveness of entanglement witnesses, may reveal new insights into these topics. Finally, we point out that our findings provide an alternative method to study the structure of the convex set of separable states and subsequently, the rich structure of entanglement.

Acknowledgments

BH acknowledges gratefully the Austrian Science Fund (FWF-P26783). DM has received funding from the European Union’s Horizon 2020 research and innovation programme under the Marie Skłodowska–Curie Grant Agreement No. 663830. JB is supported by the National Research Foundation of Korea (NRF-2021R1A2C2006309, NRF-2020K2A9A2A15000061) and Institute of Information & communications Technology Planning & Evaluation (IITP) grant (Grant No. 2019-0-00831, the ITRC Program/IITP-2021-2018-0-01402). DC was supported by the National Science Centre Project 2018/30/A/ST2/00837. The computational results presented have been achieved in part using the Vienna Scientific Cluster (VSC). We thank M Grassl for helpful comments and suggestions.

Data availability statement

The data that support the findings of this study are available upon reasonable request from the authors.

Appendix A. Heisenberg–Weyl MUBs

The unitary Heisenberg–Weyl shift and phase operators, acting on \mathbb{C}^d , are defined by

$$X = \sum_{j=0}^{d-1} |j+1\rangle\langle j|, \quad Z = \sum_{j=0}^{d-1} \omega_d^j |j\rangle\langle j|, \quad (\text{A.1})$$

respectively, where $\omega_d = \exp(2\pi i/d)$. For prime dimensions, $d = p$, the eigenstates of $Z, X, XZ, XZ^2, \dots, XZ^{d-1}$ form a complete set of $d + 1$ MUBs, and can be written in the concise form

$$|jk\rangle = \frac{1}{\sqrt{p}} \sum_{\ell=0}^{p-1} \omega_p^{(k\ell^2 + j\ell)} |\ell\rangle, \quad (\text{A.2})$$

where $k, j \in \mathbb{F}_p$, such that k labels each basis, j the elements within each basis, and $|\ell\rangle$ the elements of the canonical basis. Together with the standard basis, the bases form a set of $p + 1$ MUBs. We can also represent this in matrix form, with $B_1 = I, B_2 = F_d$, and

$$\mathcal{B}_{i+2} = D_d^i F_d, \quad (\text{A.3})$$

for $i = 1, \dots, d-1$, where F_d is the $(d \times d)$ Fourier matrix with elements

$$f_{jk} = \frac{1}{\sqrt{d}} \exp(2\pi i(j-1)(k-1)/d), \tag{A.4}$$

and D_d a diagonal matrix. For $d = 5, 7$, the complete sets are generated using

$$D_5 = \text{diag}(1, \omega_5, \omega_5^4, \omega_5^4, \omega_5) \tag{A.5}$$

and

$$D_7 = \text{diag}(1, \omega_7, \omega_7^4, \omega_7^2, \omega_7^2, \omega_7^4, \omega_7). \tag{A.6}$$

For $d = p^n$, the operators $X^{k_1} Z^{\ell_1} \otimes \dots \otimes X^{k_n} Z^{\ell_n}$, where $k_j, \ell_j \in \mathbb{F}_p$, each acting on the Hilbert space $\mathbb{C}^p \otimes \dots \otimes \mathbb{C}^p$, generate the complete set. Partitioning the operators into commuting classes and finding their common eigenvectors yield the $d + 1$ bases. If p is odd, the basis elements can be written in the succinct form

$$|jk\rangle = \frac{1}{\sqrt{d}} \sum_{\ell \in \mathbb{F}_d} \omega_p^{\text{tr}(k\ell^2 + j\ell)} |\ell\rangle, \tag{A.7}$$

where \mathbb{F}_d is the Galois field, and the trace of $\alpha \in \mathbb{F}_d$ is defined as $\text{tr}(\alpha) = \alpha + \alpha^p + \dots + \alpha^{p^{n-1}}$. Hence, the bases $\mathcal{B}_k, k \in \mathbb{F}_d$, together with the standard basis, form the complete set. If p is even, i.e. $d = 2^n$, the construction is based on Galois rings [9], with basis elements given by

$$|jk\rangle = \frac{1}{\sqrt{2^n}} \sum_{\ell \in \mathcal{T}_n} i^{\text{tr}(k+2j)\ell} |\ell\rangle, \tag{A.8}$$

where k and j are elements of the Teichmüller set \mathcal{T}_n . In this case, the trace map $\text{tr} : \text{GR}(4, n) \rightarrow \mathbb{Z}/4\mathbb{Z}$ is defined as $\text{tr}(x) = \sum_{t=0}^{n-1} \sigma^t(x)$ where σ is the automorphism $\sigma(k + 2j) = k^2 + 2j^2$.

Appendix B. Unextendible MUBs

Here, we provide the explicit forms of the unextendible MUBs discussed in the paper. In dimension $d = 4$, the three-parameter family of mutually unbiased triples $\{I, F(x), H(y, z)\}$ [29], is given by the one-parameter Fourier family

$$F(x) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & ie^{ix} & -ie^{ix} \\ 1 & -1 & -ie^{ix} & ie^{ix} \end{pmatrix},$$

and the two-parameter family of Hadamard matrices

$$H(y, z) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -e^{iy} & e^{iy} & e^{iz} & -e^{iz} \\ e^{iy} & -e^{iy} & e^{iz} & -e^{iz} \end{pmatrix},$$

with $x, y, z \in [0, \pi]$. These triples are unextendible unless $x = y = z = \pi/2$, where they coincide with the Heisenberg–Weyl case.

The only unextendible pair in $d = 6$ is given by $\{I, S_6\}$, where S_6 is the Tao matrix [47]:

$$S_6 = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & \omega_3 & \omega_3 & \omega_3^2 & \omega_3^2 \\ 1 & \omega_3 & 1 & \omega_3^2 & \omega_3^2 & \omega_3 \\ 1 & \omega_3 & \omega_3^2 & 1 & \omega_3 & \omega_3^2 \\ 1 & \omega_3^2 & \omega_3^2 & \omega_3 & 1 & \omega_3 \\ 1 & \omega_3^2 & \omega_3 & \omega_3^2 & \omega_3 & 1 \end{pmatrix}. \tag{B.1}$$

The set $\{I, F_7, A_7\}$ found in [34] for $d = 7$, is an unextendible triple of MUBs, with F_7 the Fourier matrix and setting $\alpha = (\sqrt{-7} - 3)/4$,

$$A_7 = \frac{1}{\sqrt{7}} \begin{pmatrix} \alpha & \alpha & \alpha & 1 & \alpha & 1 & 1 \\ 1 & \alpha & \alpha & \alpha & 1 & \alpha & 1 \\ 1 & 1 & \alpha & \alpha & \alpha & 1 & \alpha \\ \alpha & 1 & 1 & \alpha & \alpha & \alpha & 1 \\ 1 & \alpha & 1 & 1 & \alpha & \alpha & \alpha \\ \alpha & 1 & \alpha & 1 & 1 & \alpha & \alpha \\ \alpha & \alpha & 1 & \alpha & 1 & 1 & \alpha \end{pmatrix}. \quad (\text{B.2})$$

ORCID iDs

B C Hiesmayr  <https://orcid.org/0000-0001-9062-6039>

D McNulty  <https://orcid.org/0000-0002-3276-0587>

S Singha Roy  <https://orcid.org/0000-0002-6603-7661>

J Bae  <https://orcid.org/0000-0002-2345-1619>

D Chruściński  <https://orcid.org/0000-0002-6582-6730>

References

- [1] Gurvits L 2004 *J. Comput. Syst. Sci.* **69** 448
- [2] Schwinger J 1960 *Proc. Natl Acad. Sci.* **46** 570
- [3] Wootters W K and Fields B D 1989 *Ann. Phys., NY* **191** 363
- [4] Ivanović I D 1981 *J. Phys. A* **14** 3241
- [5] Bennett C H and Brassard G 1984 *Proc. IEEE Int. Conf. Computers, Systems and Signal Processing* vol 175
- [6] Sarwate D 1979 *IEEE Trans. Inform. Theory* **25** 720
- [7] Calderbank A R, Rains E M, Shor P W and Sloane N J A 1997 *Phys. Rev. Lett.* **78** 405
- [8] Kostrikin A I, Kostrikin I A and Ufnarovskii V A 1981 *Trudy Matemat. Inst. VA Steklova* **158** 105
- [9] Klappenecker A and Rötteler M 2004 *Lect. Notes Comput. Sci.* **2948** 262
- [10] Bandyopadhyay S, Boykin P O, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512
- [11] Boykin P O, Sitharam M, Tiep P H and Wocjan P 2007 *Quantum Inf. Comput.* **7** 371
- [12] Durt T, Englert B-G, Bengtsson I and Życzkowski K 2010 *Int. J. Quantum Inf.* **08** 535
- [13] Kantor W M 2012 *J. Math. Phys.* **53** 032204
- [14] Spengler C, Huber M, Brierley S, Adaktylos T and Hiesmayr B C 2012 *Phys. Rev. A* **86** 022311
- [15] Hiesmayr B C and Löffler W 2013 *New J. Phys.* **15** 083036
- [16] Hiesmayr B C and Löffler W 2014 *Phys. Scr.* **T160** 014017
- [17] Bae J, Hiesmayr B C and McNulty D 2019 *New J. Phys.* **21** 013012
- [18] Chruściński D, Sarbicki G and Wudarski F 2018 *Phys. Rev. A* **97** 032318
- [19] Bruzda W, Goyeneche D and Życzkowski K 2017 *Phys. Rev. A* **96** 022105
- [20] Singh A, Gautam A, Arvind A and Dorai K 2019 *Phys. Lett. A* **383** 1549
- [21] Tasca D S, Rudnicki L, Aspden R S, Padgett M J, Souto Ribeiro P H and Walborn S P 2018 *Phys. Rev. A* **97** 042312
- [22] Bae J, Chruściński D and Hiesmayr B C 2020 *NPJ Quantum Inf.* **6** 15
- [23] Kalev A and Bae J 2013 *Phys. Rev. A* **87** 062314
- [24] Designolle S, Skrzypczyk P, Fröwis F and Brunner N 2019 *Phys. Rev. Lett.* **122** 050402
- [25] Tavakoli A, Hameedi A, Marques B and Bourennane M 2015 *Phys. Rev. Lett.* **114** 170502
- [26] Aguilar E A, Borkala J J, Mironowicz P and Pawowski M 2018 *Phys. Rev. Lett.* **121** 050501
- [27] Haagerup U 1997 *Operator Algebras and Quantum Field Theory* (Cambridge: International Press)
- [28] Brierley S, Weigert S and Bengtsson I 2010 *Quantum Inf. Comput.* **10** 803
- [29] Kraus K 1987 *Phys. Rev. D* **35** 3070
- [30] Hadamard J 1893 *Sci. Am.* **68** 240
- [31] Tadej W and Życzkowski K 2006 *Open Syst. Inf. Dyn.* **13** 133
- [32] Mandayam P, Bandyopadhyay S, Grassl M and Wootters W K 2014 *Quant. Inf. Comput.* **14** 0823
- [33] Thas K 2016 *Entropy* **18** 395
- [34] Grassl M, McNulty D, Mišta L and Paterek T 2017 *Phys. Rev. A* **95** 012118
- [35] Szántó A 2016 *Linear Algebr. Appl.* **496** 392
- [36] Jedwab J and Yen L 2016 arXiv:1604.04797
- [37] Spengler C, Huber M and Hiesmayr B C 2012 *J. Math. Phys.* **53** 013501
- [38] Doherty A C, Parrilo P A and Spedalieri F M 2004 *Phys. Rev. A* **69** 022308
- [39] Baumgartner B, Hiesmayr B C and Narnhofer H 2006 *Phys. Rev. A* **74** 032327
- [40] Baumgartner B, Hiesmayr B C and Narnhofer H 2007 *J. Phys. A: Math. Theor.* **40** 7919
- [41] Baumgartner B, Hiesmayr B C and Narnhofer H 2008 *Phys. Lett. A* **372** 2190
- [42] Werner R F 1989 *Phys. Rev. A* **40** 4277
- [43] Zauner G 2011 *Int. J. Quantum Inf.* **09** 445
- [44] Karlsson B R 2011 *Linear Algebr. Appl.* **434** 247
- [45] Jaming P, Matolcsi M, Móra P, Szöllösi F and Weiner M 2009 *J. Phys. A: Math. Theor.* **42** 245305
- [46] Brierley S and Weigert S 2009 *Phys. Rev. A* **79** 052316
- [47] Tao T 2004 *Math. Res. Lett.* **11** 251