UNIVERSITY of York

This is a repository copy of *Mutually Unbiased Product Bases for Multiple Qudits*.

White Rose Research Online URL for this paper:
https://eprints.whiterose.ac.uk/95821/

Version: Accepted Version

Article:

McNulty, Daniel, Pammer, Bogdan and Weigert, Stefan orcid.org/0000-0002-6647-3252 (2016) Mutually Unbiased Product Bases for Multiple Qudits. Journal of Mathematical Physics. 032202. ISSN 1089-7658

https://doi.org/10.1063/1.4943301

Reuse

Items deposited in White Rose Research Online are protected by copyright, with all rights reserved unless indicated otherwise. They may be downloaded and/or printed for private study, or other acts as permitted by national copyright laws. The publisher or other rights holders may allow further reproduction and re-use of the full text version. This is indicated by the licence information on the White Rose Research Online record for the item.

Takedown

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing eprints@whiterose.ac.uk including the URL of the record and the reason for the withdrawal request.

White Rose
university consortium
Universities of Leeds, Sheffield & York

eprints@whiterose.ac.uk
https://eprints.whiterose.ac.uk/

Mutually Unbiased Product Bases for Multiple Qudits

Daniel McNulty[*], Bogdan Pammer[†] and Stefan Weigert[‡]

13 January 2016

[*]*Department of Optics, Palacký University, 17. listopadu 12, 771 46 Olomouc, Czech Republic*
[†]*Faculty of Physics, University of Vienna, Boltzmanngasse 5, 1090 Vienna, Austria*
[‡]*Department of Mathematics, University of York, York YO10 5DD, UK*

Abstract

We investigate the interplay between mutual unbiasedness and product bases for multiple qudits of possibly different dimensions. A product state of such a system is shown to be mutually unbiased to a product basis only if each of its factors is mutually unbiased to all the states which occur in the corresponding factors of the product basis. This result implies both a tight limit on the number of mutually unbiased product bases which the system can support and a complete classification of mutually unbiased product bases for multiple qubits or qutrits. In addition, only maximally entangled states can be mutually unbiased to a maximal set of mutually unbiased product bases.

1 Introduction

Complementarity is considered to be a fundamental concept of quantum mechanics. Loosely speaking, two observables are complementary if measuring one of them prevents an accurate simultaneous measurement of the other. Position and momentum of a quantum particle, or two spin components along different axes, are well-known examples. The properties of complementary observables are crucial in the first protocol of quantum key distribution [1].

Given a system residing in an eigenstate of one observable, the outcomes of measuring a second observable are *equally* likely if the second observable is complementary to the first one. In other words, the eigenbases of a complementary pair of observables are *mutually unbiased*. Explicitly, any two orthonormal bases $\{|a_i\rangle\}$ and $\{|b_j\rangle\}$ of dimension d are mutually unbiased (MU) if and only if

$$\left|\langle a_i|b_j\rangle\right|^2 = \frac{1}{d}, \qquad i,j = 1\ldots d\,. \tag{1}$$

For a qudit with Hilbert space of dimension d, the number of pairwise MU bases is limited by $(d+1)$. The bound is tight [2, 3] if the dimension equals the power of a prime number, $d = p^n$, $n \in \mathbb{N}$. For other dimensions d, it is not known whether the maximum can be reached. A proof is elusive even for the smallest case $d = 6$, although both rigorous results [4–6] and substantial numerical evidence [7,8] support the conjectured maximum of *three* MU bases.

In this paper we report a number of results which follow from the assumption that the MU bases under consideration consist of *product* states only. Product bases do play an important role in the construction of MU bases [9] if the dimension d is not a prime power. For instance, in bipartite dimensions $d = d_1 d_2$, MU bases can be built from the tensor products of sets of MU bases in the subspaces $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$. This construction provides a lower bound on the number of MU bases in any composite dimension, and it has been exceeded only in dimensions d with specific prime decompositions, using mutually orthogonal Latin squares [10].

Product bases also feature in complete sets of MU bases for prime power dimensions $d = p^n$ since one can construct complete sets of $(d + 1)$ MU bases of which $(p + 1)$ are product bases. Experimentally, the distinction is important when implementing quantum information tasks: product measurements on multiple qudits are easier to implement than entangled ones.

One of the main results of this paper is to show that, in a multipartite system, the subsystem with the least number of MU bases severely restricts the possibilities to construct MU product bases. This limitation allows us to find a tight upper bound on the number of MU product bases for multiple qudits, and to classify maximal sets of such bases.

The paper is set out as follows. In the next section we introduce mutually unbiased product bases and prepare the ground by recalling some results relevant in the present context. The third section contains our first main result, a proof of a necessary and sufficient condition for the construction of MU product bases in multipartite systems. In Sec. 4, we derive a tight upper bound on the number of MU product bases in a multipartite system with a subsystem of dimension two or three. Applying this result, we then derive classifications of maximal sets of MU product bases in a number of cases. In Sec. 6 we show that a vector mutually unbiased to a maximal set of MU product bases must be maximally entangled with respect to a specific bipartition of the system. A summary and some concluding remarks are presented in Sec. 7, along with a conjecture on the structure of product bases in multipartite systems.

2 Mutually unbiased product bases

We start by defining product bases for a quantum system composed of n qudits, with dimension $d = d_1 d_2 \dots d_n$. The state space of the r-th qudit is the complex vector space $\mathbb{C}^{d_r}$, with an integer $d_r \geq 2$, $r = 1 \dots n$.

Definition 1. An orthonormal basis $\mathcal{B}$ of the complex vector space $\mathbb{C}^d$ with dimension $d = d_1 d_2 \dots d_n$ is a *product basis* if each basis vector takes the form $|\psi\rangle = |\psi^1\rangle \otimes \dots \otimes |\psi^n\rangle \in \mathbb{C}^d$, with states $|\psi^r\rangle \in \mathbb{C}^{d_r}$, $r = 1 \dots n$.

For a bipartite system with $d = d_1 d_2$, two different types of product bases exist, namely *direct* and *indirect* product bases, a distinction introduced in [11]. Direct product bases consist of $d = d_1 d_2$ states $|v, V\rangle \equiv |v\rangle \otimes |V\rangle$ where $\{|v\rangle, v = 1 \dots d_1\}$ is an orthogonal basis of $\mathbb{C}^{d_1}$ and $\{|V\rangle, V = 1 \dots d_2\}$ is an orthogonal basis of $\mathbb{C}^{d_2}$.

An important link between direct product bases and MU bases has been established in [11].

Lemma 1. *Two* [*direct*] *orthogonal product bases* $\{|u, U\rangle\}$ *and* $\{|v, V\rangle\}$ *in dimension* $d = d_1 d_2$ *are* MU *if and only if* $|u\rangle$ *is* MU *to* $|v\rangle$ *in dimension* d_1 *and* $|V\rangle$ *is* MU *to* $|U\rangle$ *in dimension* d_2.

Any orthogonal basis consisting of product states only – but not of the form described by a direct product basis – is called an indirect product basis. It may involve more than one orthogonal basis in one subsystem. For example, the set $\mathcal{B} = \{|0,0\rangle, |0,1\rangle, |1,+\rangle, |1,-\rangle\}$ is an indirect product basis in dimension $d = 2 \times 2$ since it contains two different orthogonal bases in the second subsystem, namely $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$, with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$. In general, an indirect product basis of a bipartite system takes the form $\mathcal{B} = \{|\psi_i^1, \psi_i^2\rangle, i = 1 \dots d\}$, with two sets $\{|\psi_i^1\rangle \in \mathbb{C}^{d_1}\}$ and $\{|\psi_i^2\rangle \in \mathbb{C}^{d_2}\}$ of d states each.

It is important to recognize that indirect product bases are not equivalent to direct product bases under local unitary transformations. Therefore, the generalization of Lemma 1 to arbitrary pairs of product bases is not immediate.

Indirect product bases of systems with dimensions four and six were investigated in [13], leading to the following generalization of Lemma 1.

Lemma 2. *A product state* $|\mu^1, \mu^2\rangle \in \mathbb{C}^d, d \equiv d_1 d_2 \leq 6$, *is* MU *to the product basis* $\{|\psi_i^1, \psi_i^2\rangle, i = 1 \dots d\}$, *if and only if* $|\mu^1\rangle$ *is* MU *to* $|\psi_i^1\rangle \in \mathbb{C}^{d_1}$ *and* $|\mu^2\rangle$ *is* MU *to* $|\psi_i^2\rangle \in \mathbb{C}^{d_2}$, *for all* $i = 1 \dots d$.

This result is strong enough to imply a classification of *all* MU product bases in dimensions four and six [13]. It turns out that there is only one way to construct three MU product bases in the space $\mathbb{C}^4$ while two inequivalent MU product triples exist in $\mathbb{C}^6$. For multipartite systems with dimensions $d > 6$, the set of inequivalent product bases is not known. The proof of Lemma 2 relies on exhaustively enumerating all (inequivalent, cf. below) product bases in dimensions four and six. The following section presents an alternative approach which allows us to generalise Lemma 2 to arbitrary multipartite dimensions.

3 Limiting the number of MU product vectors

In this section we generalise Lemma 2 to multipartite systems of dimension $d = d_1 d_2 \dots d_n$, with $d_r \geq 2$, $r = 1 \dots n$. The theorem will be important for the construction of maximal sets of MU product bases.

In a first step, we generalize Lemma 2 to arbitrary *bipartite* systems with dimension $d = d_1 d_2$ [12].

Lemma 3. *A product state $|\mu^1, \mu^2\rangle$ in dimension $d = d_1 d_2$ is* MU *to any product basis $\mathcal{B} = \{|\psi_i^1, \psi_i^2\rangle, i = 1 \dots d\}$ if and only if $|\mu^1\rangle$ is* MU *to all states $|\psi_i^1\rangle \in \mathbb{C}^{d_1}$ and $|\mu^2\rangle$ is mutually unbiased to all states $|\psi_i^2\rangle \in \mathbb{C}^{d_2}$.*

Proof. Assuming the relations $|\langle\psi_i^1|\mu^1\rangle|^2 = 1/d_1$ and $|\langle\psi_i^2|\mu^2\rangle|^2 = 1/d_2$, the state $|\mu^1, \mu^2\rangle$ is indeed found to be MU to the product states of the basis $\mathcal{B}$,

$$\left|\langle\psi_i^1, \psi_i^2|\mu^1, \mu^2\rangle\right|^2 = \left|\langle\psi_i^1|\mu^1\rangle\right|^2 \left|\langle\psi_i^2|\mu^2\rangle\right|^2 = \frac{1}{d_1 d_2}, \qquad i = 1 \dots d. \tag{2}$$

To prove the converse we assume that $|\mu^1, \mu^2\rangle$ is MU to the states of the product basis $\mathcal{B}$, i.e. Eq. (2). Let us now evaluate the traces of two projectors constructed from the states $|\mu^1\rangle$ and $|\mu^2\rangle$, namely

$$\begin{aligned} \operatorname{Tr}\left(|\mu^1\rangle\langle\mu^1| \otimes \mathbb{1}\right) &= \sum_{i=1}^{d} \langle\psi_i^1, \psi_i^2| \left(|\mu^1\rangle\langle\mu^1| \otimes \mathbb{1}\right) |\psi_i^1, \psi_i^2\rangle \\ &= \sum_{i=1}^{d} \left|\langle\psi_i^1|\mu^1\rangle\right|^2 = d_2, \end{aligned} \tag{3}$$

and

$$\operatorname{Tr}\left(\mathbb{1} \otimes |\mu^2\rangle\langle\mu^2|\right) = \sum_{i=1}^{d} \left|\langle\psi_i^2|\mu^2\rangle\right|^2 = d_1. \tag{4}$$

Defining the $2d$ positive numbers

$$x_i = \sqrt{d_1}\left|\langle\psi_i^1|\mu^1\rangle\right|, \qquad y_i = \sqrt{d_2}\left|\langle\psi_i^2|\mu^2\rangle\right|, \qquad i = 1 \dots d,$$

the $(d+2)$ conditions (2)-(4) take the form

$$x_i^2 y_i^2 = 1, \qquad i = 1 \dots d, \tag{5}$$

and

$$\sum_{i=1}^{d} x_i^2 = \sum_{i=1}^{d} y_i^2 = d. \tag{6}$$

These relations imply that

$$\sum_{i=1}^{d} (x_i - y_i)^2 = 0, \tag{7}$$

which can only hold for

$$x_i = y_i, \qquad i = 1 \dots d. \tag{8}$$

Using this result in Eq. (5) we see that indeed

$$\left|\langle\psi_i^1|\mu^1\rangle\right|^2 = \frac{1}{d_1}, \qquad \left|\langle\psi_i^2|\mu^2\rangle\right|^2 = \frac{1}{d_2}, \qquad i = 1 \dots d,$$

must hold. Consequently, any state $|\mu^1, \mu^2\rangle$ MU to the states of a product basis $\mathcal{B}$ must have factors $|\mu^1\rangle$ and $|\mu^2\rangle$ which are MU to all states in the respective subsystems. □

The proof of Lemma 3 would be straightforward if we could transform any basis $\mathcal{B}$ to the canonical (direct) product basis by local unitary operations. However, this approach is not sufficiently general since no such transformations exist for indirect product bases $\mathcal{B}$.

Finally, we show that Lemma 3 can be generalized to obtain a stronger result about states MU to multi-partite orthogonal product bases.

Theorem 1. *The product state $|\mu^1, \mu^2, \ldots, \mu^n\rangle$ in dimension $d = d_1 d_2 \ldots d_n$ is* MU *to the orthogonal product basis $\mathcal{B} = \{|\psi_i^1, \psi_i^2, \ldots, \psi_i^n\rangle, i = 1 \ldots d\}$, if and only if, for each $r = 1 \ldots n$, the state $|\mu^r\rangle$ is* MU *to $|\psi_i^r\rangle \in \mathbb{C}^{d_r}$, for all $i = 1 \ldots d$.*

Proof. To derive this result, we consider the basis $\mathcal{B}$ as a bipartite product basis $\{|\psi_i^r, \psi_i^{\bar{r}}\rangle\}$ of the space $\mathbb{C}^d = \mathbb{C}^{d_r} \otimes \mathbb{C}^{d_{\bar{r}}}$, where now $|\psi_i^r\rangle \in \mathbb{C}^{d_r}$, $|\psi_i^{\bar{r}}\rangle \in \mathbb{C}^{d_{\bar{r}}}$, with $d_{\bar{r}} = d/d_r$ and $r = 1 \ldots n$. Similarly, the state $|\mu^1, \mu^2, \ldots, \mu^n\rangle$ is written as $|\mu^r, \mu^{\bar{r}}\rangle$ where $|\mu^r\rangle \in \mathbb{C}^{d_r}$ and $|\mu^{\bar{r}}\rangle \in \mathbb{C}^{d_{\bar{r}}}$. Applying Lemma 3 to each of the n bipartitions, we conclude that $|\mu^r\rangle$ is MU to $|\psi_i^r\rangle \in \mathbb{C}^{d_r}$, for all $r = 1 \ldots n$. □

4 Limiting the number of MU product bases

In this section we present a tight upper bound on the number of MU product bases in multipartite systems with $d = d_1 d_2 \ldots d_n$ whenever at least one subsystem (which we can choose to be the first one) has a dimension smaller than four, i.e. $d_1 = 2$ or $d_1 = 3$.

Theorem 2. *Suppose $d = d_1 d_2 \ldots d_n$, and let $d_1 = 2$ or $d_1 = 3$, and $d_1 \leq d_r, r = 2 \ldots n$. Then there exist at most $(d_1 + 1)$* MU *product bases in $\mathbb{C}^d$.*

Proof. This result follows if we can show that a product basis of the space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ with $d_1 \leq d_r$ contains a subset of d_1 orthogonal states in the subspace $\mathbb{C}^{d_1}$ for $d_1 = 2$ or $d_1 = 3$. To draw this conclusion, we first prove a lemma on the existence of orthogonal bases in the subsystems of a *bipartite* orthonormal product basis.

Lemma 4. *Consider an orthogonal product basis $\mathcal{B} = \{|a_i, b_i\rangle, i = 1 \ldots d\}$ in dimension $d = d_1 d_2$, with $d_1 = 2$ or $d_1 = 3$. Then, for every vector $|a_\kappa, b_\kappa\rangle, \kappa \in \{1 \ldots d\}$, there exists a subset $\mathcal{B}_\kappa$ of $\mathcal{B}$, with elements $\{|a_\kappa, b_\kappa\rangle, |a_\lambda, b_\lambda\rangle, \ldots\}$, such that the vectors $\{|a_\kappa\rangle, |a_\lambda\rangle, \ldots\}$ constitute an orthonormal basis of $\mathbb{C}^{d_1}$.*

It will be useful to call two orthogonal product vectors of $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_2}$ *r-orthogonal*, with $r = 1, 2$, if the two vectors of the r-th subsystem are orthogonal. For example, the state $|1, +\rangle$ of a qubit pair is 1-orthogonal to $|0, 0\rangle$ but not 2-orthogonal, while the state $|1, 1\rangle$ is both 1- and 2-orthogonal to $|0, 0\rangle$. This concept extends naturally to n-partite systems.

To show Lemma 4 we proceed in two steps. To begin, we show that for each vector $|a_\kappa, b_\kappa\rangle$ of a given product basis of $\mathbb{C}^{d_1 d_2}$ we can find $(d_1 - 1)$ vectors which are 1-orthogonal to $|a_\kappa, b_\kappa\rangle$ but not 2-orthogonal. We call this set $\mathcal{A}_\kappa$. For $d_1 = 2$, this result already ensures that the basis vectors of the first system contain an orthonormal basis in the $\mathbb{C}^2$ subsystem.

We then show that for any state $|a_\lambda, b_\lambda\rangle \in \mathcal{A}_\kappa$, there is a set $\mathcal{A}_{\kappa\lambda} \subset \mathcal{B}$ of $(d_1 - 2)$ vectors which are 1-orthogonal but not 2-orthogonal to $|a_\kappa, b_\kappa\rangle$ and $|a_\lambda, b_\lambda\rangle$. Consequently, the set $\mathcal{A}_{\kappa\lambda}$ contains one vector if $d_1 = 3$ which means that we have identified *three* orthogonal vectors in $\mathbb{C}^3$.

Proof. **Step 1**: Choose any vector $|a_\kappa, b_\kappa\rangle$ of the given orthonormal product basis $\mathcal{B}$. Then, each of the remaining $(d-1)$ vectors is either 2-orthogonal to it or not. Let us partition the $(d-1)$ integers $i = 1 \ldots d$, $i \neq \kappa$, accordingly into two sets,

$$\mathcal{I}_\kappa = \{i : \langle b_\kappa | b_i \rangle \neq 0, i \neq \kappa\}\,, \tag{9}$$

$$\mathcal{I}_{\overline{\kappa}} = \{i : \langle b_\kappa | b_i \rangle = 0, \}\,. \tag{10}$$

We denote the associated sets of states by

$$\mathcal{A}_\kappa = \{|a_i, b_i\rangle, i \in \mathcal{I}_\kappa\} \quad \text{and} \quad \mathcal{A}_{\overline{\kappa}} = \{|a_i, b_i\rangle, i \in \mathcal{I}_{\overline{\kappa}}\}\,, \tag{11}$$

respectively. Since the states in $\mathcal{A}_\kappa$ are not 2-orthogonal to $|a_\kappa, b_\kappa\rangle$, they must be 1-orthogonal, i.e. the factors of the first subsystem satisfy the relation $\langle a_\kappa | a_i \rangle = 0$, $i \in \mathcal{I}_\kappa$. Effectively, we have split the product basis of $\mathbb{C}^d$ into three disjoint sets,

$$\mathcal{B} = \{|a_\kappa, b_\kappa\rangle\} \cup \mathcal{A}_\kappa \cup \mathcal{A}_{\overline{\kappa}}\,. \tag{12}$$

To show that $\mathcal{A}_\kappa$ is not empty, we evaluate the trace of the product $M \otimes |b_\kappa\rangle\langle b_\kappa|$ in two ways, where M is an arbitrary operator acting on $\mathbb{C}^{d_1}$. We have, of course,

$$\text{tr}\,(M \otimes |b_\kappa\rangle\langle b_\kappa|) = \text{tr}_1 M\,, \tag{13}$$

and, using the orthonormal product basis $\mathcal{B}$, we also find

$$\text{tr}\,(M \otimes |b_\kappa\rangle\langle b_\kappa|) = \sum_{i=1}^{d} M_i\,|\langle b_i | b_\kappa \rangle|^2 = M_\kappa + \sum_{i \in \mathcal{I}_\kappa} M_i |\langle b_i | b_\kappa \rangle|^2\,, \tag{14}$$

where $M_i \equiv \langle a_i | M | a_i \rangle$. The expressions on the right-hand side of the last two equations must coincide for any operator M. This is only possible if the vector $|a_\kappa\rangle$ combined with the states $\{|a_i\rangle, i \in \mathcal{I}_\kappa\}$, i.e. those present in the product states of $\mathcal{A}_\kappa$, span the space $\mathbb{C}^{d_1}$. If they do not, define $M = |\chi\rangle\langle\chi|$, where $|\chi\rangle$ is any state in the complement of their span. This choice leads to a contradiction since the right-hand side of (14) evaluates to zero while that of (13) can be non-zero. Thus, the set $\mathcal{A}_\kappa$ must contain at least $(d_1 - 1)$ elements. For $d_1 = 2$, this result proves Lemma 4.

Step 2: If we now pick an arbitrary element $|a_\lambda, b_\lambda\rangle$ from $\mathcal{A}_\kappa$ and apply a reasoning parallel to Step 1, the product basis can be further divided into the following disjoint subsets

$$\mathcal{B} = \{|a_\kappa, b_\kappa\rangle, |a_\lambda, b_\lambda\rangle\} \cup \mathcal{A}_{\kappa\lambda} \cup \mathcal{A}_{\overline{\kappa\lambda}}\,, \tag{15}$$

where the sets of integers

$$\mathcal{I}_{\kappa\lambda} = \{i : \langle b_\kappa | b_i \rangle \langle b_\lambda | b_i \rangle \neq 0, i \neq \kappa, i \neq \lambda\} \subset \mathcal{I}_\kappa, \tag{16}$$

$$\mathcal{I}_{\overline{\kappa\lambda}} = \{i : \langle b_\kappa | b_i \rangle \langle b_\lambda | b_i \rangle = 0\} \tag{17}$$

give rise to the sets of states $\mathcal{A}_{\kappa\lambda} = \{|a_i, b_i\rangle, i \in \mathcal{I}_{\kappa\lambda}\}$ and $\mathcal{A}_{\overline{\kappa\lambda}} = \{|a_i, b_i\rangle, i \in \mathcal{I}_{\overline{\kappa\lambda}}\}$, respectively. We want to show that the vectors of $\mathcal{A}_{\kappa\lambda}$ in conjunction with $|a_\lambda\rangle$ and $|a_\kappa\rangle$ form an orthonormal basis of the first subsystem. To do so, we express the trace over an arbitrary operator M on $\mathbb{C}^{d_1}$ as

$$\mathrm{tr}_1 M = \frac{1}{\langle b_\kappa | b_\lambda \rangle} \mathrm{tr}(M \otimes |b_\lambda\rangle\langle b_\kappa|) \, ; \tag{18}$$

the number $\langle b_\kappa | b_\lambda \rangle$ is different from zero since these vectors are not 2-orthogonal by construction. Using the product basis $\mathcal{B}$ of $\mathbb{C}^d$ to evaluate the right-hand side of Eq. (18), we find

$$\frac{1}{\langle b_\kappa | b_\lambda \rangle} \sum_{i=1}^{d} M_i \langle b_i | b_\lambda \rangle \langle b_\kappa | b_i \rangle = M_\kappa + M_\lambda + \frac{1}{\langle b_\kappa | b_\lambda \rangle} \sum_{i \in \mathcal{I}_{\kappa\lambda}} M_i \langle b_i | b_\lambda \rangle \langle b_\kappa | b_i \rangle \, , \tag{19}$$

since the terms in the sum with labels from the set $\mathcal{I}_{\overline{\kappa\lambda}}$ do not contribute. The relation

$$\mathrm{tr}_1 M = M_\kappa + M_\lambda + \sum_{i \in \mathcal{I}_{\kappa\lambda}} M_i \frac{\langle b_i | b_\lambda \rangle \langle b_\kappa | b_i \rangle}{\langle b_\kappa | b_\lambda \rangle} \tag{20}$$

must hold for all choices of M. In analogy to Step 1, the vectors $\{|a_i\rangle, i \in \mathcal{I}_{\kappa\lambda}\}$ must, when supplemented with $|a_\kappa\rangle$ and $|a_\lambda\rangle$, span the space $\mathbb{C}^{d_1}$ in order to avoid a contradiction. Hence, $\mathcal{A}_{\kappa\lambda}$ has at least $(d_1 - 2)$ elements. If $d_1 = 3$, we have shown the existence of three orthogonal vectors in $\mathbb{C}^{d_1}$ which completes the proof of Lemma 4. □

A product basis of $\mathbb{C}^{d_1 \dots d_n}$ is also a product basis of $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_{\bar{1}}}$, with $d_{\bar{1}} = d/d_1$. Thus, Lemma 4 implies that each MU product basis of $\mathbb{C}^d$ contains a subset of d_1 orthogonal states in the subspace $\mathbb{C}^{d_1}$ when $d_1 = 2$ or $d_1 = 3$. On the basis of Theorem 1 we finally conclude that at most $(d_1 + 1)$ MU product bases exist in $\mathbb{C}^{d_1 \dots d_n}$ so that Theorem 2 holds. □

The bound we obtain in Theorem 2 suggests that a more general result holds.

Conjecture 1. *Suppose $d = d_1 d_2 \dots d_n$. Then there exist at most $(d_m + 1)$* MU *product bases in $\mathbb{C}^d$, where d_m is the dimension of the subsystem with the* least *number of* MU *bases.*

One way to prove the conjecture is to check whether the collection of d vectors figuring in the m-th subsystem of a product basis of $\mathbb{C}^d$ contain an orthonormal basis of the space $\mathbb{C}^{d_m}$. Assuming this is true, Theorem 1 limits the number of MU product bases of $\mathbb{C}^d$ since only $(d_m + 1)$ MU bases exist in $\mathbb{C}^{d_m}$. The subsystem with the smallest number of MU bases, i.e. $\mathbb{C}^{d_m}$, therefore restricts the number of MU product bases which can exist in the system of dimension d — which is the content of Conjecture 1. Our proof of Theorem 2 implements exactly this strategy but we are not able to include higher dimensions.

5 Maximal sets of MU product bases

All sets of MU product bases are known for bipartite systems with dimensions $d = 2 \times 2$ and $d = 2 \times 3$ [13]. For $d = 6$ they contain several continuous families of MU product pairs and two triples. Theorem 2 allows us to draw conclusions about the structure of MU product bases of more general bipartite and multipartite systems with dimensions $d = d_1 \dots d_n$, as long as $d_1 = 2$ or $d_1 = 3$. In particular, we will enumerate *maximal* sets of $(d_1 + 1)$ MU product bases if $d = 2^n$ and $d = 3^n$, identifying a unique triple and quadruple of MU product bases, respectively. *Inequivalent* triples and quadruples, respectively, are found to exist already for $d = 2p$ and $d = 3p$, with prime numbers $p \geq 5$.

MU product bases are *equivalent* if they can be mapped onto each other without affecting both the product structure of the states and the modulus of their inner products. As explained in [13], the allowed equivalence transformations consist of local unitary maps acting on all bases simultaneously, the multiplication of any state by an arbitrary phase factor, the permutation of states within a basis, and the local complex conjugation of all bases; in addition, the bases may be written down in an arbitrary order.

To begin, we recall the unique complete sets of MU bases of the spaces $\mathbb{C}^2$ and $\mathbb{C}^3$, expressing each basis as a square matrix, with columns given by the components of (unnormalised) basis vectors relative to the standard basis. In dimension $d = 2$, one triple of MU product bases exists,

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}; \tag{21}$$

any other triple associated with the space $\mathbb{C}^2$ is equivalent to this one. Clearly, the bases are determined by the eigenstates of the Pauli operators σ_z, σ_x and σ_y, respectively, $\{|j_z\rangle\}$, $\{|j_x\rangle\}$ and $\{|j_y\rangle\}$, with $j = 0, 1$.

For $d = 3$, the set of four MU bases

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix}, \tag{22}$$

where $\omega = e^{2\pi i/3}$, is also unique up to equivalence. Here the column vectors emerge as the eigenstates $\{|J_z\rangle\}$, $\{|J_x\rangle\}$, $\{|J_y\rangle\}$ and $\{|J_w\rangle\}$, $J = 0, 1, 2$, of generalised Pauli operators Z, X, XZ, and XZ^2 in $\mathbb{C}^3$. The operators give rise to the discrete Heisenberg-Weyl group in $\mathbb{C}^3$, via the relation $ZX = \omega XZ$, where X and Z are the Heisenberg-Weyl shift and phase operators, respectively.

Dimension $d = 2^n$

Here we consider product bases of dimension $d = d_1 \dots d_n$, where $d_r = 2$, for each $r = 1 \dots n$.

Corollary 1. *In the space* $\mathbb{C}^d$ *with dimension* $d = 2^n$*, a unique triple of* MU *product bases exists,*

$$\mathcal{B}_0 = \{|j_z^1\rangle \otimes \ldots \otimes |j_z^n\rangle\}, \tag{23}$$
$$\mathcal{B}_1 = \{|j_x^1\rangle \otimes \ldots \otimes |j_x^n\rangle\}, \tag{24}$$
$$\mathcal{B}_2 = \{|j_y^1\rangle \otimes \ldots \otimes |j_y^n\rangle\}, \tag{25}$$

up to local equivalence transformations; here $\{|j_b^r\rangle, j = 0, 1\}$*,* $b = z, x, y$*, are, for each* $r = 1 \ldots n$*, the eigenstates of the three Pauli operators in* $\mathbb{C}^2$*.*

Proof. First we show that any triple of MU product bases in dimension $d = 2^n$ consists of direct product bases. According to Lemma 4, every product basis of dimension $d = 2q$ contains a pair of orthogonal states in the $\mathbb{C}^2$ subspace. Hence, Theorem 1 implies that each product basis of an MU triple in dimension $d = 2q$ contains a unique pair of orthogonal states in $\mathbb{C}^2$. Applying this argument to all bipartitions $\mathbb{C}^2 \otimes \mathbb{C}^{2^{n-1}}$ of $\mathbb{C}^{2^n}$, we conclude that only one pair of orthogonal states occurs in each subsystem $\mathbb{C}^2$. Hence, all three MU bases are direct product bases.

By performing local unitary transformations, we turn the first basis into the standard basis, displayed in Eq. (23). The remaining two bases $\mathcal{B}_1$ and $\mathcal{B}_2$ contain either eigenstates of σ_x or σ_y in each of their subsystems. Whenever the states $|j_y\rangle$ appear in a subsystem of the second basis we apply the unitary transformation $|0_z\rangle\langle 0_z| + \omega |1_z\rangle\langle 1_z|$, where $\omega = i$, to it. This operation, a rotation by $\pi/2$ about the z-axis exchanges the operators σ_x and σ_y, hence their eigenstates, and it leaves the states $|j_z\rangle$ unchanged, up to phase factors. These properties of the transformation can be directly verified by inspecting Eq. (21). Hence, the second and third bases can always be mapped to $\mathcal{B}_1$ and $\mathcal{B}_2$, respectively, which completes the proof of Corollary 1. □

Dimension $d = 3^n$

We now prove an analogous result for product bases of dimension $d = d_1 \ldots d_n$, where $d_r = 3$, for each $r = 1 \ldots n$.

Corollary 2. *In the space* $\mathbb{C}^d$ *with dimension* $d = 3^n$*, a unique quadruple of* MU *product bases exists,*

$$\mathcal{B}_0 = \{|J_z^1\rangle \otimes \ldots \otimes |J_z^n\rangle\}, \tag{26}$$
$$\mathcal{B}_1 = \{|J_x^1\rangle \otimes \ldots \otimes |J_x^n\rangle\}, \tag{27}$$
$$\mathcal{B}_2 = \{|J_y^1\rangle \otimes \ldots \otimes |J_y^n\rangle\}, \tag{28}$$
$$\mathcal{B}_3 = \{|J_w^1\rangle \otimes \ldots \otimes |J_w^n\rangle\}, \tag{29}$$

up to local equivalence transformations; here $\{|J_b^r\rangle, J = 0, 1, 2\}$*,* $b = z, x, y, w$*, are, for each* $r = 1 \ldots n$*, the eigenstates of* Z*,* X*,* XZ *and* XZ^2*, respectively, where* X *and* Z *are the Heisenberg-Weyl shift and phase operators in* $\mathbb{C}^3$*.*

Proof. As in the previous case, we first use Lemma 4 and Theorem 1 to conclude that all four MU product bases must be *direct* product bases, constructed from various tensor products of the complete set of four MU bases in dimension three. Any one of these product bases can always be transformed to the standard basis $\mathcal{B}_0$ by a suitable product of local unitary operations. Then, the remaining three product bases consist of tensor products of various combinations of the bases $\{|J_b^r\rangle, J = 0,1,2\}$, $b = w, x, y$. Pick any of these three bases and apply the operator $|0_z\rangle\langle 0_z| + \omega^k|1_z\rangle\langle 1_z| + \omega^k|2_z\rangle\langle 2_z|$, where $\omega = e^{2\pi i/3}$ and $k \in \{0,1,2\}$, in the following way: choose $k = 0$ (or $k = 1$ or $k = 2$) for the factors which contain the x-basis (or the y- basis or the w-basis, respectively). This operation maps the product bases of the second basis to the tensor product Fourier basis $\mathcal{B}_1$ which can be seen directly upon inspecting the expressions given in (22). The states of the basis $\mathcal{B}_0$ only pick up irrelevant phase factors during this process.

Finally, the last two bases must be products of either $\{|J_y\rangle\}$ and $\{|J_w\rangle\}$. Picking one of them, each factor $\{|J_w\rangle\}$ can be turned into $\{|J_y\rangle\}$ by a local complex conjugation which swaps $\{|J_y\rangle\}$ and $\{|J_w\rangle\}$ and leaves invariant the bases $\{|J_z\rangle\}$ and $\{|J_y\rangle\}$ (see (22)). Therefore, the last two bases have indeed been mapped to the product bases $\mathcal{B}_2$ and $\mathcal{B}_3$ listed in Corollary 2. □

Dimension $d = 2 \times 5$

In dimension five, there exists a single complete set of six MU bases. We shall denote these bases by $\mathcal{G}_i$, $i = 0 \dots 5$, and refer to [14] for their explicit form.

Theorem 2 implies that at most three MU product bases exist in dimension $d = 2 \times 5$. In addition, Theorem 1 has implications for their structure.

Corollary 3. *In the space* $\mathbb{C}^d$ *with dimension* $d = 2 \times 5$*, any triple of* MU *product bases must be of the form*

$$\mathcal{B}_0 = \{|0_z\rangle \otimes \mathcal{G}(0_z)\,,\ |1_z\rangle \otimes \mathcal{G}(1_z)\}, \tag{30}$$

$$\mathcal{B}_1 = \{|0_x\rangle \otimes \mathcal{G}(0_x)\,,\ |1_x\rangle \otimes \mathcal{G}(1_x)\}, \tag{31}$$

$$\mathcal{B}_2 = \{|0_y\rangle \otimes \mathcal{G}(0_y)\,,\ |1_y\rangle \otimes \mathcal{G}(1_y)\}, \tag{32}$$

up to local equivalence transformations; here $\{|j_b\rangle, j = 0,1\}$, $b = z, x, y$, *are the eigenstates of the three Pauli operators in* $\mathbb{C}^2$*, and* $\mathcal{G}(j_b)$ *are bases of* $\mathbb{C}^5$ *for each* j_b*, such that* $\mathcal{G}(j_b) \in \mathcal{G}_i$.

Proof. As we have already seen, every product basis of dimension $d = 2q$ contains a pair of orthogonal states in the $\mathbb{C}^2$ subspace. For a set of three MU product bases, each basis contains one unique pair, given by the eigenstates of σ_x, σ_y and σ_z. To satisfy orthogonality, each state in $\mathbb{C}^2$ is paired with an orthogonal basis in $\mathbb{C}^5$. These six bases in $\mathbb{C}^5$, according to Theorem 1, are grouped into three mutually unbiased sets, $\{\mathcal{G}(0_z), \mathcal{G}(1_z)\}$, $\{\mathcal{G}(0_x), \mathcal{G}(1_x)\}$ and $\{\mathcal{G}(0_y), \mathcal{G}(1_y)\}$. The bases within each set are taken from the complete set of six MU bases $\mathcal{G}_i$, $i = 0 \dots 5$. This follows from the fact that all inequivalent triples, quadruples, quintuples and sextuples of MU bases in $\mathbb{C}^5$ are given by subsets of the complete set [14]. □

The above result implies that several *inequivalent* triples of MU product bases exist. For example, the six bases in $\mathbb{C}^5$ may be chosen such that $\mathcal{G}(0_z) = \mathcal{G}(1_z)$, $\mathcal{G}(0_x) = \mathcal{G}(1_x)$ and $\mathcal{G}(0_y) = \mathcal{G}(1_y)$, in which case $\mathcal{B}_0$, $\mathcal{B}_1$, and $\mathcal{B}_2$ form direct product bases. Alternatively, if none of the six bases coincide, three *indirect* MU product bases emerge.

Dimension $d = 2^k d_2 \dots d_n, k \in \mathbb{N}$

Suppose we consider product bases of dimension $d = 2^k d_2 \dots d_n, k \in \mathbb{N}$, in the space $(\mathbb{C}^2)^{\otimes k} \otimes \mathbb{C}^{d_2} \otimes \dots \otimes \mathbb{C}^{d_n}$. We can generalise the previous corollary as follows.

Corollary 4. *In the space $\mathbb{C}^d$ with dimension $d = 2^k d_2 d_3 \dots d_n$, any triple of* MU *product bases must be of the form*

$$\mathcal{B}_0 = \{|j_z\rangle \otimes \mathcal{G}(j_z)\}, \tag{33}$$
$$\mathcal{B}_1 = \{|j_x\rangle \otimes \mathcal{G}(j_x)\}, \tag{34}$$
$$\mathcal{B}_2 = \{|j_y\rangle \otimes \mathcal{G}(j_y)\}, \tag{35}$$

up to local equivalence transformations; here $\{|j_b\rangle, j = 0 \dots (2^k - 1)\}$, $b = z, x, y$, are the eigenstates of $\sigma_z^{\otimes k}$, $\sigma_x^{\otimes k}$ and $\sigma_y^{\otimes k}$, respectively, and $\mathcal{G}(j_b)$ are bases of $\mathbb{C}^{d_2} \otimes \dots \otimes \mathbb{C}^{d_n}$ for each j_b, such that the three sets $\{\mathcal{G}(j_b), j = 0 \dots (2^k - 1)\}$ are mutually unbiased.

Note that the three sets $\{\mathcal{G}(j_b), j = 0 \dots (2^k - 1)\}$, $b = z, x, y$, are mutually unbiased if the bases within each set are mutually unbiased to the bases of the other two sets. The bases within each set need not be mutually unbiased.

Dimension $d = 3^k d_2 \dots d_n, k \in \mathbb{N}$

By considering product bases of the space $(\mathbb{C}^3)^{\otimes k} \otimes \mathbb{C}^{d_2} \otimes \dots \otimes \mathbb{C}^{d_n}$ we find that any set of four MU bases has the following structure.

Corollary 5. *In the space $\mathbb{C}^d$ with dimension $d = 3^k d_2 d_3 \dots d_n$, any quadruple of* MU *product bases must be of the form*

$$\mathcal{B}_0 = \{|J_z\rangle \otimes \mathcal{G}(J_z)\}, \tag{36}$$
$$\mathcal{B}_1 = \{|J_x\rangle \otimes \mathcal{G}(J_x)\}, \tag{37}$$
$$\mathcal{B}_2 = \{|J_y\rangle \otimes \mathcal{G}(J_y)\}, \tag{38}$$
$$\mathcal{B}_3 = \{|J_w\rangle \otimes \mathcal{G}(J_w)\}, \tag{39}$$

up to local equivalence transformations; here $\{|J_b\rangle, J = 0 \dots (3^k - 1)\}$, $b = z, x, y, w$, are the eigenstates of $Z^{\otimes k}$, $X^{\otimes k}$, $XZ^{\otimes k}$ and $XZ^{2^{\otimes k}}$, respectively, where X and Z are the Heisenberg-Weyl shift and phase operators in $\mathbb{C}^3$, and $\mathcal{G}(J_b)$ are bases of $\mathbb{C}^{d_2} \otimes \dots \otimes \mathbb{C}^{d_n}$ for each J_b, such that the four sets $\{\mathcal{G}(J_b), J = 0 \dots (3^k - 1)\}$ are mutually unbiased.

We omit proofs of Corollaries 4 and 5 since they closely follow the proof of Corollary 3.

6 Vectors mutually unbiased to MU product bases

In a bipartite system with dimension $d = pq$, complete sets of MU bases come with a fixed amount of entanglement [11] which implies an upper bound on the number of MU *product* bases in a complete set: the space $\mathbb{C}^{pq}$ can accommodate at most $(p+1)$ MU product bases for any pair of prime numbers satisfying $p \leq q$. In addition, all of the remaining states must be maximally entangled. If, for example, a hypothetical complete set in dimension $d = 2 \times 3$ contained *three* MU product bases, the other four bases would be maximally entangled.

Furthermore, it has been shown for $d = 6$ that any vector MU to a set of three MU product bases is maximally entangled [15]. We will now generalize this property: a vector $|\mu\rangle \in \mathbb{C}^d$ of an n-partite qudit system with $d = d_1 d_2 \ldots d_n$ is mutually unbiased to a set of $(d_1 + 1)$ MU product bases only if $|\mu\rangle$ is maximally entangled.

Lemma 5. *Let $d = d_1 \ldots d_n$ with $d_r = p_r^{k_r}$, p_r prime and $k_r \in \mathbb{N}$, $r = 1 \ldots n$, such that $d_1 \leq \ldots \leq d_n$. A vector $|\mu\rangle$, mutually unbiased to a set of (d_1+1)* MU *product bases (where the product bases of $\mathbb{C}^d$ contain at least one orthogonal set of d_1 vectors in the subsystem $\mathbb{C}^{d_1}$), is maximally entangled across $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_{\bar{1}}}$, with $d_{\bar{1}} = d/d_1$.*

Proof. Let us consider the n-partite system as a bipartite system with state space $\mathbb{C}^{d_1} \otimes \mathbb{C}^{d_{\bar{1}}}$, where $d_{\bar{1}} = d/d_1$. Following from Theorem 1 we write the set of $(d_1 + 1)$ MU product bases as $\mathcal{B}_b = \{|v_b, \overline{v}(v_b)\rangle, v = 1 \ldots d_1, \overline{v} = 1 \ldots d_{\bar{1}}\}$, with $b = 0 \ldots d_1$, such that $\{|v_b\rangle\}$ is an orthonormal basis of $\mathbb{C}^{d_1}$ for each b and $\{|\overline{v}(v_b)\rangle\}$ is an orthonormal basis of $\mathbb{C}^{d_{\bar{1}}}$ for each v and b.

The unit vector $|\mu\rangle$ is MU to the product bases if the $d(d_1+1)$ equations

$$|\langle v_b, \overline{v}(v_b)|\mu\rangle|^2 = \frac{1}{d} \tag{40}$$

are satisfied. Summing over the values of $\overline{v}$, we find

$$\sum_{\overline{v}=1}^{d_{\bar{1}}} |\langle v_b, \overline{v}(v_b)|\mu\rangle|^2 = \langle v_b|(\mathrm{tr}_{\bar{1}}|\mu\rangle\langle\mu|)|v_b\rangle = \langle v_b|\rho_1|v_b\rangle = \frac{1}{d_1}, \tag{41}$$

where $\rho_1 = \mathrm{tr}_{\bar{1}}|\mu\rangle\langle\mu|$ is the reduced density matrix of the first subsystem, given by the partial trace of $|\mu\rangle\langle\mu|$ over the second subsystem.

We now show that Eqs. (41) can only hold if the state ρ_1 is maximally mixed. To see this, we rewrite ρ_1 in terms of a complete set of MU bases [2], i.e.

$$\rho_1 = \sum_{b=0}^{d_1} \sum_{v=1}^{d_1} p_b^v |v_b\rangle\langle v_b| - \mathbb{1}, \tag{42}$$

where $p_b^v \equiv \langle v_b|\rho_1|v_b\rangle = 1/d_1$ for all v and b, according to Eq. (41). Using $\sum_{v=1}^{d_1} p_b^v |v_b\rangle\langle v_b| = \mathbb{1}/d_1$ for each basis, we find that Eq. (42) reduces to

$$\rho_1 = \frac{1}{d_1}\mathbb{1}, \tag{43}$$

which means that the state ρ_1 is maximally mixed, completing the proof of Lemma 5. □

For the special case of $d = p^n$, a stronger restriction on the set of mutually unbiased vectors can be found.

Lemma 6. *Let $d = d_1 \dots d_n = p^n$ with $d_r = p$, $r = 1 \dots n$, and a prime number p. A vector $|\mu\rangle$, mutually unbiased to a set of $(p+1)$ MU product bases (where the product bases of $\mathbb{C}^d$ contain at least one orthogonal set of d_r vectors in each subsystem $\mathbb{C}^{d_r}$), is maximally entangled across all bipartitions $\mathbb{C}^p \otimes \mathbb{C}^{p^{n-1}}$.*

Proof. To show that $|\mu\rangle$ is maximally entangled, we apply Lemma 5 to each of the n possible bipartition $\mathbb{C}^p \otimes \mathbb{C}^{p^{n-1}}$. Hence, the state $|\mu\rangle$ maximally entangled across all such bipartitions. □

It is interesting to compare the content of Lemma 5 with results known for the cases $d = 2d_2$ and $d = 3d_2$. To do so we adapt Lemma 5 accordingly.

Corollary 6. *Suppose that $d = d_1 d_2$ with $d_1 = 2$ or $d_1 = 3$, d_2 prime, and $d_2 \geq d_1$. Any vector $|\mu\rangle$, mutually unbiased to a set of $(d_1 + 1)$ MU product bases of dimension d, is maximally entangled.*

This statement is stronger that the one given in [11] which states that given a hypothetical complete set of $(d+1)$ MU bases in dimension $d = d_1 d_2$ containing $(d_1 + 1)$ MU product bases, the remaining vectors must be maximally entangled. Corollary 6 is valid without assuming the existence of a complete set.

For dimension $d = 6$, Corollary 6 implies that no vector is mutually unbiased to a set of three MU product bases [15]. We expect similar results to hold for larger product dimensions such as $d = 2 \times 5$, but we have not been able to generalize the proof for $d = 6$.

Finally, let us make explicit Lemma 6 for the case of n qubits or qutrits, i.e. $d = p^n$, with $p = 2$ or $p = 3$.

Corollary 7. *Any vector $|\mu\rangle$, mutually unbiased to a set of $(p+1)$ MU product bases in dimension $d = p^n$, with $p = 2$ or $p = 3$, is maximally entangled with respect to every partition $\mathbb{C}^p \otimes \mathbb{C}^{p^{n-1}}$.*

7 Conclusions

In this paper we investigated the relationship between product bases and mutually unbiased bases for multipartite systems. Our first main result is Theorem 1 which states that, for *any* dimension $d = d_1 \dots d_n$, a product vector $|\mu\rangle$ is mutually unbiased to a product basis if and only if the r-th factor of $|\mu\rangle$ is mutually unbiased to the r-th factor of each vector present in the basis. This result considerably generalises what had been known before, for bipartite systems with dimension four or six only [13].

We also derived a tight upper bound on the number of MU product bases in any composite dimension if at least one subsystem has dimension two or three (Theorem 2). We expect a similar bound to hold in general, i.e. for *all* composite dimensions as stated in Conjecture 1. One way to prove the conjecture would be to show that a product basis of dimension $d = d_1 d_2 \ldots d_n$ contains an orthonormal set of d_r states in the subspace $\mathbb{C}^{d_r}$, for all $r = 1 \ldots n$ — which we consider highly plausible.

Theorem 1 and Lemma 4 allow us to classify all maximal sets of MU product bases in dimensions $d = 2^n$ and $d = 3^n$. Somewhat surprisingly, only one triple of MU product bases exists in dimension $d = 2^n$ according to Corollary 1, and only one quadruple exists for $d = 3^n$ (Corollary 2). Furthermore, we have shown that *inequivalent* triples of MU product bases exist if $d = 2 \times 5$, complementing a result of [13] which finds two such triples if $d = 2 \times 3$.

Finally, we analysed the entanglement structure of vectors mutually unbiased to product bases. We find that vectors mutually unbiased to maximal sets of MU product bases must be maximally entangled (Lemmas 5 and 6). If one of the subsystems has dimension two or three, this result generalises to *all* maximal sets of MU product bases (Corollaries 6 and 7). This fact is in line with the bipartite case $d = 2 \times 3$ for which any vector mutually unbiased to a set of three MU product bases had been shown to be maximally entangled [6].

We conclude by noting that all the evidence available to us points to a natural and beautiful structure of orthogonal product bases in multipartite quantum systems. For simplicity, we restrict ourselves to the bipartite case.

Conjecture 2. *The set $\mathcal{B} = \{|a_i, b_i\rangle, i = 1 \ldots d\}$ is an orthonormal product basis of the space $\mathbb{C}^d$, with $d = d_1 d_2$, if and only if the d vectors $\{|a_i\rangle \in \mathbb{C}^{d_1}, i = 1 \ldots d\}$ and the d vectors $\{|b_i\rangle \in \mathbb{C}^{d_2}, i = 1 \ldots d\}$ can be grouped into d_2 orthonormal bases $\mathcal{B}_{i_2}(d_1), i_2 = 1 \ldots d_2$, and d_1 orthonormal bases $\mathcal{B}_{i_1}(d_2), i_1 = 1 \ldots d_1$, respectively.*

Future progress towards a solution of the existence problem of MU bases in non-prime power dimensions might take a twisted route involving mutually unbiased product bases.

Acknowledgments

D. M. acknowledges the support of the Operational Program Education for Competitiveness Project No. CZ.1.07/2.3.00/30.0041 co-financed by the European Social Fund and the Czech Ministry of Education. B. P. would like to thank Anton Zeilinger for helpful discussions.

References

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* **175**, 8 (1984).

[2] I. D. Ivanović, *J. Phys. A* **14**, 3241 (1981).

[3] W. K. Wootters and B. D. Fields, *Ann. Phys. (N.Y.)* **191**, 363 (1989).

[4] M. Grassl, in *Proc. ERATO Conf. on Quantum Information Science 2004 (EQIS 2004)*; also: e-print arXiv:quant-ph/0406175 (2004).

[5] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi and M. Weiner, *J. Phys. A: Math. Theor.* **42**, 245305 (2009).

[6] D. McNulty and S. Weigert, *J. Phys. A: Math. Theor.* **45**, 102001 (2012).

[7] P. Butterley and W. Hall, *Phys. Lett. A* **369**, 5 (2007).

[8] S. Brierley and S. Weigert, *Phys. Rev. A* **78**, 042312 (2008).

[9] A. Klappenecker and M. Rötteler, in *Finite Fields and Applications*, vol. 2948 of *Lecture Notes in Computer Science*, pp. 137-144, Springer, Berlin, (2004).

[10] P. Wocjan and T. Beth, *Quantum Inf. Comput.* **5**, 93-101 (2005).

[11] M. Wieśniak, T. Paterek and A. Zeilinger, *New J. Phys.* **13**, 053047 (2011).

[12] B. Pammer, *Mutually Unbiased Quantum Bases: Existence, Entanglement, Information*, Wien (unpublished, 2015).

[13] D. McNulty and S. Weigert, *J. Phys. A: Math. Theor.* **45**, 135307 (2012).

[14] S. Brierley, S. Weigert and I. Bengtsson, *Quantum. Inf. Comput.* **10**, 803 (2010).

[15] D. McNulty and S. Weigert, *Int. J. Quant. Inf.* **10**, 1250056 (2012).