Mutually Unbiased Measurements, Hadamard Matrices, and Superdense Coding

Máté Farkas * Jędrzej Kaniewski † Ashwin Nayak ‡

April 7, 2023

Abstract

Mutually unbiased bases (MUBs) are highly symmetric bases on complex Hilbert spaces, and the corresponding rank-1 projective measurements are ubiquitous in quantum information theory. In this work, we study a recently introduced generalisation of MUBs called *mutually unbiased measurements* (MUMs). These measurements inherit the essential property of complementarity from MUBs, but the Hilbert space dimension is no longer required to match the number of outcomes. This operational complementarity property renders MUMs highly useful for device-independent quantum information processing.

It has been shown that MUMs are strictly more general than MUBs. In this work we provide a complete proof of the characterisation of MUMs that are direct sums of MUBs. We then construct new examples of MUMs that are not direct sums of MUBs. A crucial technical tool for this construction is a correspondence with quaternionic Hadamard matrices, which allows us to map known examples of such matrices to MUMs that are not direct sums of MUBs. Furthermore, we show that—in stark contrast with MUBs—the number of MUMs for a fixed outcome number is unbounded.

Next, we focus on the use of MUMs in quantum communication. We demonstrate how any pair of MUMs with d outcomes defines a d-dimensional superdense coding protocol. Using MUMs that are not direct sums of MUBs, we disprove a recent conjecture due to Nayak and Yuen on the rigidity of superdense coding, for infinitely many dimensions. The superdense coding protocols arising in the refutation reveal how shared entanglement may be used in a manner heretofore unknown.

1 Introduction

A pair of bases for a d-dimensional Hilbert space is said to be *mutually unbiased* if the squared length of the projection of any basis element from the first onto any basis element of the second is exactly $1/d$. Mutually unbiased bases (MUBs) [DEBŻ10] are well-studied objects in quantum information theory, and they are optimal in several tasks, including some in quantum cryptography. Thus, they correspond to a fundamentally important class of measurements.

Mutually unbiased *measurements* (MUMs) were recently introduced by Tavakoli, Farkas, Rosset, Bancal, and Kaniewski [TFR+21] as a generalization of mutually unbiased bases. The optimality of MUBs in information processing tasks can be traced back to their *complementarity relations*.

*ICFO-Institut de Ciencies Fotoniques, The Barcelona Institute of Science and Technology, 08860 Castelldefels, Spain. Email: mate.farkas@icfo.eu .

†Faculty of Physics, University of Warsaw, Pasteura 5, 02-093 Warsaw, Poland. Email: jkaniewski@fuw.edu.pl .

‡Department of Combinatorics and Optimization, and Institute for Quantum Computing, University of Waterloo, 200 University Ave. W., Waterloo, ON, N2L 3G1, Canada. Email: ashwin.nayak@uwaterloo.ca .

MUMs were introduced in the context of Bell inequalities, and it was shown that MUMs have the same complementarity relations as MUBs. Furthermore, MUMs admit the same entropic uncertainty relations and the same measurement incompatibility robustness as MUBs. However, MUMs are defined in a "device-independent" manner, i.e., without reference to the dimension of the Hilbert space on which they act. This makes them particularly useful in the context of device-independent cryptography.

Note that an equivalent definition of MUMs based on complementarity has been introduced earlier in Ref. [TSWR18]. The authors focus on continuous-variable systems and analyse the properties of MUMs in this setting in subsequent works [PWTR18, RW21, SRTW22]. We also note here that an alternative, inequivalent definition of MUMs was introduced in Ref. [KG14]. The authors define MUMs through uniform overlaps of the measurements operators, depending on an "efficiency parameter". Their definition reduces to MUBs when the value of the efficiency parameter is 1, but the authors show that many MUMs can be constructed with lower efficiency parameter. For a detailed account on the difference between the MUM definition in Ref. [KG14] and in Ref. [TFR+21] (which is the one used in the current paper), see Remark 2.3.

Despite all their similarities, it has been shown that MUMs are strictly more general than MUBs: there exist pairs of MUMs that are not "direct sums" of MUBs, and even pairs of MUMs that cannot be mapped to a pair of MUBs by means of a completely positive unital map [TFR+21].

In this work, we expand on the study of MUMs. We first provide an improved and complete proof of the characterization of pairs of MUMs that are direct sums of MUBs (Proposition 2.8), originally proposed in Ref. [TFR+21]. We draw a connection between pairs of MUMs and Hadamard matrices of unitary operators, and further between the latter and quaternionic Hadamard matrices (Theorem 2.12). This enables us to construct novel examples of MUM pairs that are not direct sums of MUBs for new sets of outcome numbers (Section 2.5). Using the same correspondence, we also present an infinite family of such MUMs with four outcomes. Earlier, only two examples of such MUM pairs were known, for four or five outcomes. Finally, we prove that—in stark contrast with MUBs—there exist arbitrarily large collections of pairwise MUMs for every outcome number (Theorem 2.16).

Along with the literature on quaternionic Hadamard matrices, the recipe we provide for the construction of MUM pairs suggests that MUM pairs that are not direct sums of MUBs are more common than one might be led to believe. They are likely not particular to special sets of outcome numbers, and for each outcome number greater than three (and underlying dimension), it is likely that there exist an infinite number of non-equivalent such pairs. For outcome numbers two and three, it has been shown that any pair of MUMs is a direct sum of MUBs [TFR+21].

In the second part of this work, we turn our attention to superdense coding protocols. The original two-party communication protocol due to Bennett and Wiesner [BW92] uses a shared EPR pair and transmits two bits of classical information by sending only *one* qubit. This generalizes to d-dimensional protocols for arbitrary $d \geq 2$ (Definition 3.1). These protocols use a maximally entangled state of local dimension d and transmit an arbitrary message out of d^2 possibilities by sending a d-dimensional quantum state. Superdense coding further generalizes to the transmission of quantum states, and plays an important role in Quantum Shannon Theory (see, e.g., [Wil13, Chapter 6]).

Given one d-dimensional superdense coding protocol, we may construct other equivalent protocols. For example, the two parties may use a maximally entangled state which is obtained by applying arbitrary unitary operators to the two halves of the shared state. We may also "mix" two or more different protocols to construct a seemingly more complicated protocol. Namely, we may use an entangled state of larger dimension to generate a common random string shared by the two parties, and use the shared randomness to select one of several superdense coding protocols

to transmit the classical message. Finally, the sender may apply an arbitrary unitary operator, possibly depending on the classical message, to the part of the entangled state that is retained by her. Nayak and Yuen [NY20] recently showed that any two-dimensional superdense coding protocol may be obtained by performing these transformations on the original Bennett-Wiesner protocol. In other words, they showed that the Bennett-Wiesner protocol is *rigid*. They further conjectured that a similar rigidity property holds for higher dimensional protocols ($d > 2$), up to the choice of the basic protocol (which uses a maximally entangled state of local dimension d); see Conjecture 3.2.

We disprove the rigidity conjecture due to Nayak and Yuen for infinitely many dimensions $d \geq 4$. We do this by first showing that any pair of MUMs with d outcomes defines a d-dimensional superdense coding protocol (Theorem 3.3). We then prove that the rigidity conjecture implies that the MUMs used in the protocol are a direct sum of MUBs (Theorem 3.5). The examples of MUMs that we construct (Sections 2.3 and 2.5) now give us counterexamples for infinite sequences of dimensions d.

The precise power of shared entanglement in quantum communication complexity has been a long-standing open problem (see, e.g., Ref. [Gav08]). Shared entanglement can be used to reduce communication complexity by a factor of two, using superdense coding. It may also be used to generate shared randomness, which in turn can be used to reduce communication complexity of boolean functions on n-bits by an additive $\log n$ term. It is not known whether it leads to a reduction in the communication complexity of computing functions or relations beyond these two phenomena. The superdense coding protocols arising in the counterexamples above show that shared entanglement may be used in a manner heretofore unknown. In particular, it hints at the possibility of new, counter-intuitive ways in which it might aid communication.

Acknowledgements. We are grateful to Henry Yuen for several helpful discussions, and to Curtis Bright for explaining the construction of the perfect sequences in Ref. [BKG20]. This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 754510. M.F. acknowledges funding from the Government of Spain (FIS2020-TRANQI, Severo Ochoa CEX2019-000910-S), Fundació Cellex, Fundació Mir-Puig and Generalitat de Catalunya (CERCA, AGAUR SGR 1381). J.K. acknowledges support from the National Science Centre, Poland under the SONATA project "Fundamental aspects of the quantum set of correlations" (grant no. 2019/35/D/ST2/02014). A.N.'s research is supported in part by a Discovery Grant from NSERC Canada.

2 Mutually unbiased measurements

We define the notion of mutually unbiased measurements and describe several properties of relevance to us in Sections 2.1 and 2.2. We present some explicit examples of MUMs in Section 2.3. We then describe a recipe for constructing MUMs based on generalized Hadamard matrices in Section 2.4. Finally, we describe explicit MUMs based on this construction in Section 2.5.

2.1 Definition and basic properties

For any positive integer n, let $[n]$ denote the set $\{1, 2, \ldots, n\}$. For any integer $d \geq 2$, let $\omega_d := \exp\left(\frac{2\pi \mathrm{i}}{d}\right)$ be a primitive dth root of unity. Consider the standard basis $\{|j\rangle : j \in [d]\}$ and the Fourier basis $\{|\chi_j\rangle : j \in [d]\}$ for $\mathbb{C}^d$, where $|\chi_j\rangle := \frac{1}{\sqrt{d}} \sum_{i=1}^{d} \omega_d^{ij} |i\rangle$. We have $|\langle j|\chi_k\rangle|^2 = \frac{1}{d}$ for

any $j, k \in [d]$, and the bases are said to be *mutually unbiased*. Formally, we define MUBs in terms of the corresponding measurements.

Definition 2.1. *Two d-outcome measurements $\{P_a\}_{a=1}^d$ and $\{Q_b\}_{b=1}^d$ acting on $\mathbb{C}^d$ correspond to* mutually unbiased bases *(MUBs) if the measurement operators are rank-one orthogonal projections, i.e., $P_a = |u_a\rangle\langle u_a|$ and $Q_b = |v_b\rangle\langle v_b|$ for some pure states $|u_a\rangle, |v_b\rangle \in \mathbb{C}^d$, and*

$$|\langle u_a|v_b\rangle|^2 \quad = \quad \frac{1}{d} \qquad \forall a, b \in [d] \ . \tag{2.1}$$

Since $\sum_a P_a = \mathbb{1}$, we see that $\{|u_a\rangle\}$ and $\{|v_b\rangle\}$ are orthonormal bases for $\mathbb{C}^d$.

We consider a generalization of MUBs, called MUMs [TFR+21]. The definition of MUMs is "device-independent" in the sense that it does not refer to the dimension of the Hilbert space on which they act.

Definition 2.2. *Two d-outcome measurements $\{P_a\}_{a=1}^d$ and $\{Q_b\}_{b=1}^d$ acting on a Hilbert space $\mathcal{H}$ are called* mutually unbiased measurements *(MUMs) if*

$$P_a \quad = \quad dP_aQ_bP_a \qquad \textit{and} \qquad Q_b \quad = \quad dQ_bP_aQ_b \ , \tag{2.2}$$

for all a and b in $[d]$.

We may verify readily that every pair of MUBs is also a pair of MUMs.

Remark 2.3. We note here that a different notion of MUMs was introduced by Kalev and Gour in Ref. [KG14]. Their definition is different from Definition 2.2 in a few ways: they fix the Hilbert space dimension as well as the number of measurement outcomes (albeit these can be different). They then require the trace of each operator to be 1, and all of the traces of the form $\mathrm{tr}(P_aQ_b)$ to be uniform, dependent only on an "efficiency parameter" (at the same time, the traces $\mathrm{tr}(P_aP_b)$ and $\mathrm{tr}(Q_aQ_b)$ depend only on whether $a = b$, and the efficiency parameter). The measurements of Kalev and Gour are projective only if the efficiency parameter is 1, in which case the measurements are also MUBs. As one can verify that MUMs in Definition 2.2 are always projective, our MUM definition is different from that of Kalev and Gour whenever the measurements do not correspond to MUBs. As such, in the following we will use the term MUM exclusively in the sense of Definition 2.2.

Given d-outcome MUMs, we can construct d'-outcome MUMs for any multiple of d by taking a tensor product with the elements of a suitable MUB.

Lemma 2.4. *Let $\{P_a\}_{a=1}^d$ and $\{Q_b\}_{b=1}^d$ be a pair of d-outcome MUMs on Hilbert space $\mathcal{H}$. Then for any integer $\ell > 1$, there is a pair of d'-outcome MUMs on Hilbert space $\mathcal{H} \otimes \mathbb{C}^\ell$, where $d' := \ell d$.*

Proof. Define orthogonal projection operators

$$\begin{aligned} P'_{a,i} \quad &:= \quad P_a \otimes |i\rangle\langle i| \ , \qquad \text{and} \\ Q'_{b,j} \quad &:= \quad Q_b \otimes |\chi_j\rangle\langle\chi_j| \ , \end{aligned}$$

for $a, b \in [d]$ and $i, j \in [\ell]$, where $(|\chi_j\rangle : j \in [\ell])$ is the Fourier basis for $\mathbb{C}^\ell$. We may verify that $\left\{P'_{a,i}\right\}$ and $\left\{Q'_{b,j}\right\}$ are a pair of d'-outcome MUMs. □

Any pair of (finite dimensional) MUMs can be written as a pair of d orthogonal projections on the tensor product space $\mathbb{C}^n \otimes \mathbb{C}^d$ for some $n \in \mathbb{N}$ that satisfy certain *MUM conditions* [TFR+21] (see also Ref. [NPA12]). I.e., up to a change of basis, the first measurement is simply given by

$$P_a \quad = \quad \mathbb{1} \otimes |a\rangle\langle a| \ , \tag{2.3}$$

where $\{|a\rangle\}_{a=1}^d$ is the computational basis on $\mathbb{C}^d$. In the same basis used to express P_a, the second measurement can be described in full generality by

$$Q_b \quad = \quad \frac{1}{d} \sum_{j,k \in [d]} V_{jk}^b \otimes |j\rangle\langle k| \tag{2.4}$$

for each $b \in [d]$, where V_{jk}^b are linear operators on $\mathbb{C}^n$. The MUM conditions are then given by the following relations in terms of the operators V_{jk}^b [TFR+21, Supplementary materials, Sec. II.B.1]:

$$\begin{aligned} V_{jj}^b &= \mathbb{1} \qquad \forall b, j \\ (V_{jk}^b)^\dagger &= V_{kj}^b \qquad \forall b, j, k \\ V_{jk}^b &= V_{jl}^b V_{lk}^b \qquad \forall b, j, k, l \\ \sum_b V_{jk}^b &= \delta_{jk} d\, \mathbb{1} \qquad \forall j, k \ . \end{aligned} \tag{2.5}$$

The last condition corresponds to the completeness relation $\sum_b Q_b = \mathbb{1}$. Notice that the MUM conditions imply that Q_b are projections, and therefore the completeness relation is sufficient to ensure that $\{Q_b\}$ form a valid measurement. While superfluous, the orthogonality constraint $Q_b Q_{b'} = \delta_{bb'} Q_b$ corresponds to

$$\sum_l V_{jl}^b V_{lk}^{b'} \quad = \quad \delta_{bb'} d V_{jk}^b \ . \tag{2.6}$$

The conditions in Eq. (2.5) make it possible to describe the pair of MUMs in terms of d^2 unitary operators

$$U_j^b \quad := \quad V_{j1}^b \qquad \text{for } b, j \in [d] \ , \tag{2.7}$$

since $V_{jk}^b = U_j^b (U_k^b)^\dagger$ for all b, j, k. The MUM conditions in terms of $\left\{U_j^b\right\}$ are given by

$$\begin{aligned} U_1^b &= \mathbb{1} \qquad \forall b \\ U_j^b (U_j^b)^\dagger &= (U_j^b)^\dagger U_j^b = \mathbb{1} \qquad \forall b, j \\ \sum_b U_j^b (U_k^b)^\dagger &= \delta_{jk} d\, \mathbb{1} \qquad \forall j, k \ . \end{aligned} \tag{2.8}$$

The orthogonality condition in terms of the unitary operators $\left\{U_j^b\right\}$ is given by

$$\sum_j (U_j^b)^\dagger U_j^{b'} \quad = \quad \delta_{bb'} d\, \mathbb{1} \qquad \forall b, b' \in [d] \ . \tag{2.9}$$

Since unitary operators do not commute in general, the order of multiplication of matrices in Eqs. (2.8) and (2.9) is important. If in addition to the MUM conditions in Eq. (2.8), the operators U_j^b satisfy

$$U_j^1 \quad = \quad \mathbb{1} \qquad \forall j \in [d] \ , \tag{2.10}$$

we say that the MUMs are in *canonical form*. We may convert any pair of MUMs into canonical form by a simple transformation.

Lemma 2.5. *Suppose $\{P_a\}$ and $\{Q_b\}$ are a pair of d-outcome MUMs defined by operators (U_j^b) satisfying the MUM conditions in Eq. (2.8). Let $U := \sum_{j=1}^d (U_j^1)^\dagger \otimes |j\rangle\langle j|$. Then $\{UP_aU^\dagger\}$ and $\{UQ_bU^\dagger\}$ are a pair of d-outcome MUMs in canonical form.*

The transformation essentially replaces the operator U_j^b by $\widetilde{U}_j^b := (U_j^1)^\dagger U_j^b$. We leave it to the reader to verify that the operators $(\widetilde{U}_j^b)$ satisfy the MUM conditions, and have $\widetilde{U}_j^1 = \mathbb{1}$ for all $j \in [d]$. A further generalization of this lemma is useful for the characterization of MUMs.

Proposition 2.6. *The conditions*

$$\begin{aligned} (U_j^b)(U_j^b)^\dagger &= (U_j^b)^\dagger U_j^b = \mathbb{1} \qquad \forall b, j \\ \sum_b U_j^b (U_k^b)^\dagger &= \delta_{jk} d\,\mathbb{1} \qquad \forall j, k \\ \sum_j (U_j^b)^\dagger U_j^{b'} &= \delta_{bb'} d\,\mathbb{1} \qquad \forall b, b' \end{aligned} \tag{2.11}$$

are stable under the transformations

$$\begin{aligned} U_j^b &\mapsto U_j^b W^b \\ U_j^b &\mapsto W_j U_j^b \end{aligned} \tag{2.12}$$

where W^b and W_j are arbitrary unitary matrices.

2.2 Direct sum property

MUMs are strictly more general than MUBs. In particular, not all pairs of MUMs can be written as a *direct sum* of MUBs.

Definition 2.7. *We say that two d-outcome measurements, $\{P_a\}_{a=1}^d$ and $\{Q_b\}_{b=1}^d$ on $\mathcal{H}$, are a* direct sum of mutually unbiased bases *if $\mathcal{H} \cong \bigoplus_j \mathbb{C}^d$ and $P_a = \bigoplus_j P_a^j$, $Q_b = \bigoplus_j Q_b^j$, where for every j the pair $\{P_a^j\}_{a=1}^d$ and $\{Q_b^j\}_{b=1}^d$ are mutually unbiased bases acting on the jth direct summand of $\mathcal{H}$.*

When expressed in the canonical form described in Section 2.1, it is straightforward to check if the pair of MUMs $\{P_a\}$ and $\{Q_b\}$ are a direct sum of MUBs due to the equivalence below, stated in Proposition II.6 in the supplementary materials for Ref. [TFR+21]. The proof therein simply claimed the "only if" direction of this characterisation to be "clear" and only gave an argument for the "if" direction. We provide a complete proof, including that for the "only if" direction (i.e, the converse). In fact, the converse crucially relies on the operators (U_j^b) being in canonical form; it provably does not hold otherwise. This subtlety is fully reflected in the proof we provide. (As we show in Section 3, the converse is the direction of relevance to the rigidity of superdense coding protocols.)

Proposition 2.8. *Suppose $\{P_a\}$ and $\{Q_b\}$ are a pair of d-outcome MUMs in canonical form defined by operators $(U_j^b : b, j \in [d])$ satisfying the MUM conditions in Eq. (2.8) and the canonical form condition in Eq. (2.10). Then $\{P_a\}$ and $\{Q_b\}$ are a direct sum of MUBs if and only if*

$$[U_j^b, U_{j'}^{b'}] = 0 \qquad \forall b, b', j, j' \ . \tag{2.13}$$

Proof. Suppose the MUMs $\{P_a\}$ and $\{Q_b\}$ are defined by the operators $(U_j^b : b, j \in [d])$ in canonical form. I.e., we fix a choice of basis in which the operators P_a are expressed as

$$P_a \quad = \quad \mathbb{1} \otimes |a\rangle\langle a| \ ,$$

where the second Hilbert space factor is isomorphic to $\mathbb{C}^d$ and $\{|a\rangle\}$ is an orthonormal basis for it. Furthermore, the Q_b operators are expressed as

$$Q_b \quad = \quad \frac{1}{d} \sum_{j,k \in [d]} U_j^b (U_k^b)^\dagger \otimes |j\rangle\langle k| \ ,$$

where the operators U_j^b satisfy the conditions in Eq. (2.8) and Eq. (2.10). Suppose, without loss of generality, that the Hilbert space on which the MUMs are defined is isomorphic to $\mathcal{H} := \mathbb{C}^{d'} \otimes \mathbb{C}^d$ in the basis used for the canonical form, for some positive integer d'.

We start with the "if" direction of the characterization. Suppose the operators U_j^b all commute with each other. Then there is an orthonormal basis $\{|e_t\rangle : t \in [d']\}$ for $\mathbb{C}^{d'}$ in which the operators U_j^b are simultaneously diagonal. I.e.,

$$U_j^b \quad = \quad \sum_{t=1}^{d'} \lambda_{jt}^b \, |e_t\rangle\langle e_t| \ ,$$

for some unit complex numbers λ_{jt}^b, for all $b, j \in [d]$. Consider the direct sum decomposition

$$\mathcal{H} \quad = \quad \bigoplus_{t=1}^{d'} |e_t\rangle\langle e_t| \otimes \mathbb{C}^d \ ,$$

and the orthogonal projection operators $R_t := |e_t\rangle\langle e_t| \otimes \mathbb{1}$ into the t-th direct summand, for $t \in [d']$. Define $P_a^t := R_t P_a R_t = |e_t\rangle\langle e_t| \otimes |a\rangle\langle a|$, and

$$Q_b^t \quad := \quad R_t Q_b R_t \quad = \quad |e_t\rangle\langle e_t| \otimes \frac{1}{d} \sum_{jk} \lambda_{jt}^b \overline{\lambda_{kt}^b} \, |j\rangle\langle k| \ .$$

We have $P_a = \bigoplus_{t \in [d']} P_a^t$ and $Q_b = \bigoplus_{t \in [d']} Q_b^t$. Moreover, P_a^t, Q_b^t are rank 1 projection operators and $\mathrm{Tr}(P_a^t Q_b^t) = 1/d$, for all t, a, b. So the pair of MUMs $\{P_a\}$ and $\{Q_b\}$ are a direct sum of MUBs.

To prove the "only if" direction, suppose that $\{P_a\}$ and $\{Q_b\}$ are a direct sum of MUBs. Then $\mathcal{H}$ is a direct sum of d' subspaces $\mathcal{H}_t$ ($t \in [d']$), and each subspace $\mathcal{H}_t$ has dimension d. Let S_t be the orthogonal projection operator onto $\mathcal{H}_t$.

By the direct sum property, we have

$$\begin{aligned} P_a \quad &= \quad \sum_t S_t P_a S_t \ , \qquad \text{and} \\ Q_b \quad &= \quad \sum_t S_t Q_b S_t \ , \end{aligned}$$

for all a, b. So $S_t P_a = S_t P_a S_t = P_a S_t$ and similarly, the operators S_t and Q_b also commute. In particular, S_t and P_a are simultaneously diagonalisable. Since the eigenvectors of P_a are all of the form $|v\rangle|a\rangle$ for some $|v\rangle \in \mathbb{C}^{d'}$, we may express S_t as $S_t = \sum_a S_{ta} \otimes |a\rangle\langle a|$, for some orthogonal projection operators S_{ta}.

Since the MUMs are in canonical form, we have $U_j^1 = \mathbb{1}$ for all j. So $Q_1 = \mathbb{1} \otimes (1/d) \sum_{j,k} |j\rangle\langle k|$. From the commutation of S_t and Q_1 we have

$$\frac{1}{d} \sum_{j,k} S_{tj} \otimes |j\rangle\langle k| \quad = \quad S_t Q_1 \quad = \quad Q_1 S_t \quad = \quad \frac{1}{d} \sum_{j,k} S_{tk} \otimes |j\rangle\langle k| \ .$$

So $S_{tj} = S_{tk}$ for all j, k. Let $S'_t := S_{t1}$. Then $S_t = S'_t \otimes \mathbb{1}$, and $\sum_t S'_t = \mathbb{1}$.

Since $\{S_t P_a S_t : a \in [d]\}$ and $\{S_t Q_b S_t : b \in [d]\}$ are MUBs for every t, these projection operators are all rank 1. As $S_t P_a S_t = S'_t \otimes |a\rangle\langle a|$, we infer that $\{S'_t\}$ are also rank 1 and we have $S'_t = |f_t\rangle\langle f_t|$ for some orthonormal basis $\{|f_t\rangle\}$ for $\mathbb{C}^{d'}$. Since $Q_b = \sum_t S_t Q_b S_t$, we have

$$\frac{1}{d} \sum_{j,k \in [d]} U_j^b (U_k^b)^\dagger \otimes |j\rangle\langle k| \quad = \quad \frac{1}{d} \sum_{j,k \in [d]} \sum_{t \in [d']} \langle f_t | U_j^b (U_k^b)^\dagger | f_t \rangle \ |f_t\rangle\langle f_t| \otimes |j\rangle\langle k| \ .$$

Thus

$$U_j^b (U_k^b)^\dagger \quad = \quad \sum_{t \in [d']} \langle f_t | U_j^b (U_k^b)^\dagger | f_t \rangle \ |f_t\rangle\langle f_t|$$

for every $b, j, k \in [d]$. Taking $k = 1$, and noting that $U_1^b = \mathbb{1}$ for all b, we see that all the operators U_j^b are diagonal in the basis $\{|f_t\rangle\}$. Thus, they all commute. □

We present examples of MUMs in the next section which violate the commutation relations in Eq. (2.13), and therefore cannot be expressed as a direct sum of MUBs.

2.3 Examples of MUMs

In this section, we provide explicit MUM constructions for $d = 4, 5, 6$ that are not direct sums of MUBs. The examples for $d = 4, 5$ were first reported in Ref. [TFR+21, Sec. II.C.2, Supplementary materials], essentially in terms of the operators V_{jk}^b. The example for $d = 6$ is new.

We provide these constructions in terms of the unitary operators U_j^b satisfying the MUM conditions in Eq. (2.8) as well as Eq. (2.10), so that the MUMs are in canonical form. We leave it to the reader to verify that the conditions are satisfied. In all the constructions, the Hilbert space is $\mathbb{C}^2 \otimes \mathbb{C}^d$, and we use the single-qubit Pauli matrices $\mathbb{1}$, X, Y and Z:

$$\mathbb{1} := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \ , \qquad X := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \ , \qquad Y := \begin{pmatrix} 0 & -\mathrm{i} \\ \mathrm{i} & 0 \end{pmatrix} \ , \text{ and } \qquad Z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} .$$

We provide the unitary operators U_j^b in one block matrix H_d, whose (b, j)-block corresponds to U_j^b, i.e., $H_d := \sum_{b,j \in [d]} |b\rangle\langle j| \otimes U_j^b$, where $(|b\rangle : b \in [d])$ is the standard basis of $\mathbb{C}^d$. The MUMs for $d = 4$ are given by

$$H_4 \quad := \quad \begin{pmatrix} \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & \frac{2\mathrm{i}}{3}(Z - Y) - \frac{1}{3}\mathbb{1} & \frac{2\mathrm{i}}{3}(X - Z) - \frac{1}{3}\mathbb{1} & \frac{2\mathrm{i}}{3}(Y - X) - \frac{1}{3}\mathbb{1} \\ \mathbb{1} & \mathrm{i}Y & -\mathbb{1} & -\mathrm{i}Y \\ \mathbb{1} & -\frac{2}{3}\mathbb{1} - \frac{\mathrm{i}}{3}(2Z + Y) & \frac{1}{3}\mathbb{1} + \frac{2\mathrm{i}}{3}(Z - X) & -\frac{2}{3}\mathbb{1} + \frac{\mathrm{i}}{3}(2X + Y) \end{pmatrix} \ . \tag{2.14}$$

The MUMs for $d = 5$ are given by

$$H_5 \quad := \quad \begin{pmatrix} \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & -\mathbb{1} & -\mathrm{i}cY - \mathrm{i}sX & -\mathrm{i}cY + \mathrm{i}sX & -\mathrm{i}Y \\ \mathbb{1} & -\mathrm{i}cY - \mathrm{i}sX & -\mathbb{1} & -\mathrm{i}Y & -\mathrm{i}cY + \mathrm{i}sX \\ \mathbb{1} & -\mathrm{i}cY + \mathrm{i}sX & -\mathrm{i}Y & -\mathbb{1} & -\mathrm{i}cY - \mathrm{i}sX \\ \mathbb{1} & -\mathrm{i}Y & -\mathrm{i}cY + \mathrm{i}sX & -\mathrm{i}cY - \mathrm{i}sX & -\mathbb{1} \end{pmatrix} \ , \tag{2.15}$$

where $s := \sin(\frac{2\pi}{3})$ and $c := \cos(\frac{2\pi}{3})$. The new example of MUMs, for $d = 6$, is given by

$$H_6 \quad := \quad \begin{pmatrix} \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} & \mathbb{1} \\ \mathbb{1} & -\mathbb{1} & -\mathrm{i}Z & \mathrm{i}Z & \mathrm{i}Y & -\mathrm{i}Y \\ \mathbb{1} & -\mathrm{i}X & -\mathbb{1} & \mathrm{i}Y & -\mathrm{i}Y & \mathrm{i}X \\ \mathbb{1} & \mathrm{i}X & \mathrm{i}Y & -\mathbb{1} & -\mathrm{i}Y & -\mathrm{i}X \\ \mathbb{1} & \mathrm{i}Y & -\mathrm{i}Y & -\mathrm{i}Y & -\mathbb{1} & \mathrm{i}Y \\ \mathbb{1} & -\mathrm{i}Y & \mathrm{i}Z & -\mathrm{i}Z & \mathrm{i}Y & -\mathbb{1} \end{pmatrix} . \tag{2.16}$$

By Proposition 2.8, checking that these MUMs are not direct sums of MUBs reduces to checking that not all operators U_j^b commute. We may check this readily.

Lemma 2.4 implies that there are d-outcome MUMs which are not direct sums of MUBs whenever d is a multiple of $4, 5, 6$.

2.4 MUMs from Hadamard matrices

Here we describe a recipe for constructing MUMs from generalized Hadamard matrices, via representations of suitable associative algebras, in particular of the algebra of quaternions.

In general, MUMs correspond to a collection of unitary matrices satisfying Eq. (2.8). If we remove the first condition, namely that $U_1^b = \mathbb{1}$ for all b, and add the orthogonality condition in Eq. (2.9), we obtain the conditions in Eq. (2.11). These conditions describe a collection of unitary matrices strongly resembling the orthogonality properties of Hadamard matrices. We call a block matrix with such unitary operators a *Hadamard matrix of unitary operators*.

Definition 2.9. *A* Hadamard matrix of unitary operators *of size d with block size k is a $(dk) \times (dk)$ block matrix $\sum_{b,j=1}^{d} |b\rangle\langle j| \otimes U_j^b$ whose blocks U_j^b, for $b, j \in [d]$, are operators on a k-dimensional Hilbert space satisfying the relations* (2.11).

We recover complex Hadamard matrices by setting the block size k to 1 (and real Hadamard matrices by only allowing $U_j^b = \pm 1$). The examples presented in Eqs. (2.14), (2.15) and (2.16) are all Hadamard matrices of unitary operators with block size $k = 2$. Note that a similar definition has been considered by Banica [Ban18], with the additional constraints

$$\begin{aligned} \sum_b (U_j^b)^\dagger U_k^b &= \delta_{jk} d\, \mathbb{1} \qquad \forall j, k \\ \sum_j U_j^b (U_j^{b'})^\dagger &= \delta_{bb'} d\, \mathbb{1} \qquad \forall b, b' \ . \end{aligned}$$

These conditions impose orthogonality-type conditions for block-rows (and block-columns) of unitary matrices with respect to both possible orders of multiplication of the matrices.

We draw on a correspondence between quaternions and the single-qubit Pauli operators to give a general construction of Hadamard matrices of unitary operators with block size $k = 2$. Recall that the real algebra of quaternions may be represented as

$$\mathbb{H} \quad := \quad \{\alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k} \mid \alpha, \beta, \gamma, \delta \in \mathbb{R}\} \ ,$$

where $\mathbf{i}, \mathbf{j}, \mathbf{k}$ are the *basic quaternions*, and satisfy the relations

$$\mathbf{i}^2 = \mathbf{j}^2 = -1, \quad \mathbf{ij} = \mathbf{k}, \quad \mathbf{ji} = -\mathbf{k} \ .$$

(Note the distinction between the quaternion $\mathbf{i}$ and the complex imaginary unit i.) The algebra is endowed with a conjugation operation which satisfies $\alpha^* = \alpha$ for $\alpha \in \mathbb{R}$, $\mathbf{i}^* = -\mathbf{i}$, $\mathbf{j}^* = -\mathbf{j}$ (and hence, $\mathbf{k}^* = -\mathbf{k}$). Conjugation also distributes over addition, and satisfies $(\boldsymbol{q}_1 \boldsymbol{q}_2)^* = \boldsymbol{q}_2^* \boldsymbol{q}_1^*$. The norm $\|\boldsymbol{q}\|$ of a quaternion $\boldsymbol{q}$ is given by

$$\|\boldsymbol{q}\| \quad := \quad \sqrt{\boldsymbol{q}\boldsymbol{q}^*} \quad = \quad \sqrt{\boldsymbol{q}^*\boldsymbol{q}} \ ,$$

and when $\boldsymbol{q} \neq 0$, its multiplicative inverse $\boldsymbol{q}^{-1}$ is given by $\boldsymbol{q}^{-1} := \boldsymbol{q}^* / \|\boldsymbol{q}\|$. The set of quaternions with norm 1 are called *unit quaternions*. The unit quaternions form a (non-commutative) group under the multiplication operation.

For a $d \times d$ matrix M over $\mathbb{H}$, define $M^\dagger$ as its conjugate-transpose, i.e., the matrix given by $(M^\dagger)_{ij} := M^*_{ji}$ for all $i, j \in [d]$.

Definition 2.10. *A $d \times d$ matrix quaternionic matrix M is called a* quaternionic Hadamard matrix *if all its entries are unit quaternions, i.e., $\|M_{ij}\| = 1$ for all $i, j \in [d]$, and $MM^\dagger = d\,\mathbb{1}$.*

We say that a quaternionic Hadamard matrix M is dephased *if the elements in its first row and the first column are all* 1*, i.e., $M_{1j} = M_{i1} = 1$ for all $i, j \in [d]$.*

The condition $MM^\dagger = d\,\mathbb{1}$ is equivalent to $\sum_{j=1}^{d} M_{bj} M^*_{b'j} = \delta_{bb'} d\,\mathbb{1}$ for all $b, b' \in [d]$. Note that the order of multiplication of matrices in this definition is important, since multiplication in $\mathbb{H}$ is not commutative.

Consider the linear map $f : \mathbb{H} \to \mathcal{L}(\mathbb{C}^2)$, from quaternions to linear operators on $\mathbb{C}^2$, defined on the quaternion basis elements as

$$f(1) := \mathbb{1}, \quad f(\mathbf{i}) := \mathrm{i}X, \quad f(\mathbf{j}) := -\mathrm{i}Y, \quad f(\mathbf{k}) := \mathrm{i}Z \ .$$

We may verify that f is a group isomorphism between the quaternion group

$$\mathsf{Q}_8 \quad := \quad \{\pm 1, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$$

of $\mathbb{H}$ and the subgroup $\mathsf{P} := \{\pm\mathbb{1}, \pm\mathrm{i}X, \pm\mathrm{i}Y, \pm\mathrm{i}Z\}$ of the Pauli group. This isomorphism extends to a group isomorphism between the multiplicative group of unit quaternions and the subgroup of unitary operators in the real algebra generated by the subgroup P. In particular, the function f commutes with conjugation, i.e., $f(\boldsymbol{q}^*) = (f(\boldsymbol{q}))^\dagger$ for all unit $\boldsymbol{q} \in \mathbb{H}$. This further extends to an algebra isomorphism between $\mathbb{H}$ and the real algebra generated by P. (The latter algebra is a strict subset of the space of 2×2 complex matrices. For example, the Pauli operator X does not belong to this algebra.) Therefore, through the isomorphism f, every quaternionic Hadamard matrix can be mapped to a Hadamard matrix of unitary operators with block size 2.

Lemma 2.11. *For any $d \times d$ quaternionic Hadamard matrix M, the $(2d) \times (2d)$ block matrix H defined as*

$$H \quad := \quad \sum_{b,j=1}^{d} |b\rangle\langle j| \otimes f(M^*_{bj}) \ ,$$

is a Hadamard matrix of unitary operators of size d with block size 2.

Proof. Since M_{bj} is a unit quaternion for every $b, j \in [d]$, $f(M^*_{bj})$ is a unitary operator. Further, for $b, b' \in [d]$, we have

$$\sum_{j=1}^{d} f(M^*_{bj})^\dagger f(M^*_{b'j}) \quad = \quad \sum_{j} f(M_{bj})\, f(M^*_{b'j}) \quad = \quad f\left(\sum_{j} M_{bj} M^*_{b'j}\right) \quad = \quad \delta_{bb'} d\,\mathbb{1} \ , \qquad (2.17)$$

as f is a unital algebra isomorphism. This is the third property in Eq. (2.11). Consider the matrix K defined as

$$K \quad := \quad \frac{1}{\sqrt{d}} \sum_{b,j=1}^{d} |j\rangle\langle b| \otimes f(M_{bj}^*) \ .$$

The property in Eq. (2.17) is equivalent to $K^\dagger K = \mathbb{1}$, i.e., K is unitary. So $KK^\dagger = \mathbb{1}$, which is equivalent to the second property in Eq. (2.11). □

Furthermore, the canonical form of a pair of MUMs corresponds to a *dephased* quaternionic Hadamard matrix. According to Proposition 2.6, this dephasing can be done by multiplying every row of the Hadamard matrix by the conjugate of its first element from the right, and every column by the conjugate of its first element from the left; the resulting matrix is also a Hadamard matrix. Due to the isomorphism f and Proposition 2.8, the corresponding MUMs are a direct sum of MUBs if and only if all elements in the dephased quaternionic Hadamard matrix commute pairwise. Thus, we get the following correspondence.

Theorem 2.12. *Any $d \times d$* dephased *quaternionic Hadamard matrix M with at least one pair of non-commuting elements defines a pair of d-outcome MUMs that are not a direct sum of MUBs.*

2.5 Further examples of MUMs

Using constructions of quaternionic Hadamard matrices in the literature, we exhibit infinitely many new MUMs. Following Theorem 2.12, we focus on Hadamard matrices which have non-commuting elements after dephasing.

Chterental and Đoković [CĐ08] present two infinite families of 4×4 quaternionic Hadamard matrices. The first is a *special family* paramatrized by two unit quaternions $\boldsymbol{a}, \boldsymbol{b}$, where

$$\begin{aligned} \boldsymbol{a} \quad &\in \quad \{\alpha_1 + \alpha_2 \mathbf{i} : \alpha_1, \alpha_2 \in \mathbb{R}\} \ , \qquad \text{and} \\ \boldsymbol{b} \quad &\in \quad \{\beta_1 + \beta_2 \mathbf{j} : \beta_1, \beta_2 \in \mathbb{R}\} \ . \end{aligned}$$

The Hadamard matrix corresponding to $\boldsymbol{a}, \boldsymbol{b}$ is

$$M_{\boldsymbol{a},\boldsymbol{b}} \quad := \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & \boldsymbol{b} & -\boldsymbol{b} \\ 1 & \boldsymbol{a} & \boldsymbol{x} & \boldsymbol{z} \\ 1 & -\boldsymbol{a} & \boldsymbol{y} & \boldsymbol{w} \end{pmatrix} \ ,$$

where

$$\begin{aligned} \boldsymbol{x} \quad &:= \quad -\frac{1}{2}(1 + \boldsymbol{a} + \boldsymbol{b} - \boldsymbol{a}\boldsymbol{b}) \qquad & \boldsymbol{z} \quad &:= \quad -\frac{1}{2}(1 + \boldsymbol{a} - \boldsymbol{b} + \boldsymbol{a}\boldsymbol{b}) \\ \boldsymbol{y} \quad &:= \quad -\frac{1}{2}(1 - \boldsymbol{a} + \boldsymbol{b} + \boldsymbol{a}\boldsymbol{b}) \qquad & \boldsymbol{w} \quad &:= \quad -\frac{1}{2}(1 - \boldsymbol{a} - \boldsymbol{b} - \boldsymbol{a}\boldsymbol{b}) \ . \end{aligned}$$

Whenever $\boldsymbol{a}$ and $\boldsymbol{b}$ are both not real, they do not commute. The corresponding Hadamard matrix of unitary operators gives us 4-outcome MUMs which are not direct sums of MUBs. The second *generic* family of 4×4 quaternionic Hadamard matrices in Ref. [CĐ08] similarly gives us MUMs of this type. (Chterental and Đoković follow a different convention in the definition of a quaternionic Hadamard matrix M, viz., they require that $M^\dagger M = d\,\mathbb{1}$. We take the conjugate-transpose of their constructions to get Hadamard matrices as defined in this article.)

Barrera Acevedo and Dietrich [BAD18, Lemma 5] point out a one-to-one correspondence between $d \times d$ circulant quaternionic Hadamard matrices and *perfect sequences* of unit quaternions of length d.

Definition 2.13. *A* perfect sequence *of quaternions of length d is a sequence $Q := (\boldsymbol{q}_0, \boldsymbol{q}_1, \ldots, \boldsymbol{q}_{d-1})$ of quaternions such that its periodic t-autocorrelation values*

$$\mathrm{AC}_Q(t) \quad := \quad \sum_{l=0}^{d-1} \boldsymbol{q}_l \boldsymbol{q}^*_{(l+t \mod d)} \tag{2.18}$$

satisfy $\mathrm{AC}_Q(t) = 0$ *for all* $t \neq 0 \mod d$.

A $d \times d$ circulant quaternionic Hadamard matrix M can be constructed from a perfect sequence $(\boldsymbol{q}_l)$ of unit quaternions of length d by taking the first row of the matrix to be the sequence, and the rest of the rows to be successive cyclic shifts of the first row. That is, we define $M_{ij} := \boldsymbol{q}_{(i+j-2 \mod d)}$ for $i, j \in [d]$.

Perfect sequences have been found for small prime lengths $5, 7, 9, 11, 13, 17, 19$, and 23 by Kuznetsov [Kuz10, Example 7.3]. It turns out that all of these sequences correspond to MUMs that are not direct sums of MUBs. We first demonstrate this on the smallest example of length 5.

Example 2.14. The perfect sequence of quaternions $(1, \mathbf{j}, \mathbf{j}, 1, \boldsymbol{q})$ with

$$\boldsymbol{q} \quad := \quad \frac{-1 + \mathbf{i} - \mathbf{j} - \mathbf{k}}{2}$$

corresponds to a pair of 5-outcome MUMs that are not a direct sum of MUBs. To see this, note that $\boldsymbol{q}$ is a unit quaternion, and consider the corresponding circulant Hadamard matrix

$$\begin{pmatrix} 1 & \mathbf{j} & \mathbf{j} & 1 & \boldsymbol{q} \\ \boldsymbol{q} & 1 & \mathbf{j} & \mathbf{j} & 1 \\ 1 & \boldsymbol{q} & 1 & \mathbf{j} & \mathbf{j} \\ \mathbf{j} & 1 & \boldsymbol{q} & 1 & \mathbf{j} \\ \mathbf{j} & \mathbf{j} & 1 & \boldsymbol{q} & 1 \end{pmatrix}. \tag{2.19}$$

We dephase the first row, that is, multiply every column by the conjugate of its first element from the left to get

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ \boldsymbol{q} & -\mathbf{j} & 1 & \mathbf{j} & \boldsymbol{q}^* \\ 1 & -\mathbf{j}\boldsymbol{q} & -\mathbf{j} & \mathbf{j} & \boldsymbol{q}^*\mathbf{j} \\ \mathbf{j} & -\mathbf{j} & -\mathbf{j}\boldsymbol{q} & 1 & \boldsymbol{q}^*\mathbf{j} \\ \mathbf{j} & 1 & -\mathbf{j} & \boldsymbol{q} & \boldsymbol{q}^* \end{pmatrix}.$$

Lastly, we dephase the first column by multiplying every row by the conjugate of the first element of that row from the right to get

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & -\mathbf{j}\boldsymbol{q}^* & \boldsymbol{q}^* & \mathbf{j}\boldsymbol{q}^* & \boldsymbol{q}^*\boldsymbol{q}^* \\ 1 & -\mathbf{j}\boldsymbol{q} & -\mathbf{j} & \mathbf{j} & \boldsymbol{q}^*\mathbf{j} \\ 1 & -1 & \mathbf{j}\boldsymbol{q}\mathbf{j} & -\mathbf{j} & \boldsymbol{q}^* \\ 1 & -\mathbf{j} & -1 & -\boldsymbol{q}\mathbf{j} & -\boldsymbol{q}^*\mathbf{j} \end{pmatrix}.$$

These two transformations preserve the Hadamard property, according to Proposition 2.6. The result is a quaternionic Hadamard matrix with non-commuting elements. For example, the last two elements of the second row, $\mathbf{j}\boldsymbol{q}^*$ and $\boldsymbol{q}^*\boldsymbol{q}^*$, do not commute. To see this, note that $\mathbf{j}\boldsymbol{q}^*$ and $\boldsymbol{q}^*\boldsymbol{q}^*$ commute iff $\mathbf{j}$ and $\boldsymbol{q}^*\boldsymbol{q}^*$ commute. The property follows by noting that the square of a quaternion of the form $(1/2)(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})$ is also of the same form.

By Lemma 2.11, we obtain a Hadamard matrix of unitary operators that are in canonical form. By the properties of f, some of these unitary operators do not non-commute. Hence, we get a pair of 5-outcome MUMs that are not a direct sum of MUBs.

A similar argument shows that all the examples in Ref. [Kuz10, Example 7.3] give rise to MUMs that are not direct sums of MUBs. In particular, all of the examples are perfect sequences of the form $(1, \mathbf{j}, \ldots, \mathbf{j}, 1, \boldsymbol{q})$ where

$$\boldsymbol{q} \quad \in \quad \left\{ \frac{\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}}{2} \right\} \ .$$

The elements in the sequence that we have left unspecified all belong to the quaternion group Q_8. Quaternions $\boldsymbol{q}$ as above all have unit norm. The corresponding circulant matrix and its dephasing gives us

$$\begin{pmatrix} 1 & \mathbf{j} & \ldots & \mathbf{j} & 1 & \boldsymbol{q} \\ \boldsymbol{q} & 1 & \mathbf{j} & \ldots & \mathbf{j} & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \to \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 1 \\ \boldsymbol{q} & -\mathbf{j} & \ldots & \ldots & \mathbf{j} & \boldsymbol{q}^* \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} \to \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 1 \\ 1 & -\mathbf{j}\boldsymbol{q}^* & \ldots & \ldots & \mathbf{j}\boldsymbol{q}^* & \boldsymbol{q}^*\boldsymbol{q}^* \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \end{pmatrix} . \tag{2.20}$$

We have $\boldsymbol{q}^* \in \{(\pm 1 \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k})/2\}$, and thus $\mathbf{j}\boldsymbol{q}^*$ and $\boldsymbol{q}^*\boldsymbol{q}^*$ do not commute, by the same reasoning as in Example 2.14. Therefore, the dephased quaternionic Hadamard matrix in Eq. (2.20) defines a pair of MUMs that are not a direct sum of MUBs. From the examples in Ref. [Kuz10], Theorem 2.12, and Lemma 2.4 we thus get MUMs that are not direct sums of MUBs whenever the outcome number d is a multiple of $5, 7, 9, 11, 13, 17, 19$, or 23.

Bright, Kotsireas, and Ganesh [BKG20] construct perfect quaternion sequences of length 2^t for all $t \geq 0$. Example 13 in their article explicitly lists the sequences given by their construction for $t \in [0, 7]$. The sequences for $t = 5, 6, 7$ all yield dephased Hadamard matrices with non-commuting elements in the second row. All the elements in these sequences belong to Q_8. All three sequences have occurrences of each of the three basic quaternions $\mathbf{i}, \mathbf{j}, \mathbf{k}$ immediately followed by ± 1, have -1 as the first element, and $\mathbf{i}$ or 1 as the last element. Thus, the second row of the corresponding dephased Hadamard matrices have occurrences of each of $\mathbf{i}, \mathbf{j}, \mathbf{k}$. We include the perfect sequence for $t = 5$ below as an illustration:

$$(-1, \mathbf{i}, 1, 1, \mathbf{j}, -\mathbf{j}, -1, -\mathbf{k}, -1, \mathbf{k}, -1, \mathbf{j}, \mathbf{j}, -1, 1, -\mathbf{i}, -1, -\mathbf{i}, 1, -1, \mathbf{j}, \mathbf{j}, -1, \mathbf{k}, -1, -\mathbf{k}, -1, -\mathbf{j}, \mathbf{j}, 1, 1, \mathbf{i}) \ .$$

Their construction yields the following perfect sequence for $t = 4$, which also gives us a dephased Hadamard matrix with non-commuting elements:

$$(-1, 1, \mathbf{i}, -\mathbf{j}, 1, \mathbf{j}, \mathbf{i}, -1, -1, -1, \mathbf{i}, \mathbf{j}, 1, -\mathbf{j}, \mathbf{i}, 1) \ .$$

The construction of perfect sequences of length 2^t described in Theorem 7 of Ref. [BKG20] is recursive, and implies the following relationship between the sequence Q_t of length 2^t and the sequence Q_{t+2} of length 2^{t+2}, for all $t \geq 2$. The projection of Q_{t+2} to the even indices in $[0, 2^{t+2} - 1]$ equals (Q_t, Q_t). I.e., if we delete the entries of Q_{t+2} given by the odd indices, we get Q_t concatenated with itself. This implies that deleting every second row and column from the upper-left submatrix of the dephased Hadamard matrix M_{t+2} obtained from Q_{t+2} gives us the dephased Hadamard matrix M_t obtained from Q_t. I.e., $(M_t)_{ij} = (M_{t+2})_{2i-1,2j-1}$ for $i, j \in [2^t]$. The perfect sequence of length 2^t starting from the sequence for $t = 4$ or $t = 5$ listed above thus yields a $2^t \times 2^t$ dephased quaternionic Hadamard matrix with non-commuting elements for any $t \geq 4$. These matrices all give us MUMs that are not direct sums of MUBs. The resulting MUMs are different from the ones obtained from H_4 in Section 2.3. This provides further evidence for the prevalence

of perfect sequences, quaternionic Hadamard matrices, and MUMs that are not direct sums of MUBs.

There are a number of other constructions of quaternionic Hadamard matrices in the literature; see, e.g., Ref. [BAD19]. It is likely that there be many more families of such MUMs.

2.6 The number of MUMs

Given the close connection of MUMs to MUBs, it is natural to ask what the maximal number of d-outcome measurements is such that they are pairwise mutually unbiased (i.e., pairwise MUMs). Note that for MUBs, this is a long-standing open problem for composite dimensions [Zau99, Zau11]. The only known generic upper bound for MUBs is $d+1$ in dimension d, which is known to be saturated in prime power dimensions [WF89]. In composite dimensions, however, the best known generic lower bound is p^r+1, where p^r is the smallest prime power factor in the prime decomposition of the dimension. There is no composite dimension in which the exact number of MUBs is known.

We prove that the situation is drastically different for MUMs: in fact, there exist an unbounded number of MUMs for every outcome number d. We show this via a construction using Hilbert spaces of unbounded dimension. We first make use of a result from Ref. [KŠT+19, Proposition B.1]. Recall that ω_d is a primitive dth root of unity, and let $Z_d := \sum_{j=1}^{d} \omega_d^j |j\rangle\langle j|$ and $X_d := \sum_{j=1}^{d} |j+1\rangle\langle j|$ be the generalized Pauli Z and X operators, respectively, in dimension d. (In this definition, we "round" $d+1$ down to 1.)

Proposition 2.15 (Proposition B.1 [KŠT+19])**.** *Let A_1 and A_2 be unitary operators acting on a finite-dimensional Hilbert space $\mathcal{H}$, satisfying $A_1^d = A_2^d = \mathbb{1}$ for some integer $d \geq 2$. Suppose that A_1 and A_2 satisfy the commutation relation*

$$A_1 A_2 \quad = \quad \omega_d A_2 A_1 \ . \tag{2.21}$$

Then, $\dim \mathcal{H} = d \cdot d'$ *for some integer $d' \geq 1$ and there exists a unitary operator $U : \mathcal{H} \to \mathbb{C}^d \otimes \mathbb{C}^{d'}$ such that*

$$U A_1 U^\dagger = Z_d \otimes \mathbb{1}_{d'} \qquad \text{and} \qquad U A_2 U^\dagger = X_d \otimes \mathbb{1}_{d'} \ .$$

Now we are in the position to state the result on the number of MUMs.

Theorem 2.16. *For any $d, n \in \mathbb{N}$ such that $d, n \geq 2$ there exist n MUMs with outcome number d.*

Proof. We start with the canonical construction of a pair of MUBs in dimension d, via the eigenbases of Z_d and X_d. That is, we write these operators in their spectral decomposition,

$$Z_d = \sum_{a=1}^{d} \omega_d^a \, P_a, \qquad X_d = \sum_{b=1}^{d} \overline{\omega}_d^b \, Q_b \ ,$$

where $P_a := |a\rangle\langle a|$ and $Q_b := |\chi_b\rangle\langle\chi_b|$, and $(|\chi_b\rangle)$ is the Fourier basis for $\mathbb{C}^d$. Since $\{P_a\}$ and $\{Q_b\}$ are MUBs, they are also MUMs. From Definition 2.2, if $\{P_a\}$ and $\{Q_b\}$ are MUMs then so are $\{P_a \otimes \mathbb{1}\}$ and $\{Q_b \otimes \mathbb{1}\}$, as are $\{UP_aU^\dagger\}$ and $\{UQ_bU^\dagger\}$ for an arbitrary unitary operator U. It follows from these observations and Proposition 2.15 that two unitary operators A_1 and A_2 define a pair of d-outcome MUMs through their spectral decomposition if they satisfy $A_1^d = A_2^d = \mathbb{1}$ and the commutation relation in Eq. (2.21). Hence, in order to define n MUMs with d outcomes, it is sufficient to find n unitary operators $\{A_j : j \in [n]\}$ such that $A_j^d = \mathbb{1}$ for all j and $A_j A_k = \omega_d A_k A_j$ for all $j < k$.

For such a construction, consider the unitary operators $\{A_j\}$ defined on $(\mathbb{C}^d)^{\otimes n}$ as

$$A_j \quad := \quad \left(\bigotimes_{k=1}^{j-1} X_d\right) \otimes Z_d \otimes \left(\bigotimes_{l=j+1}^{n} \mathbb{1}_d\right) \quad ,$$

that is,

$$\begin{aligned} A_1 &= Z_d \otimes \mathbb{1}_d \otimes \mathbb{1}_d \otimes \mathbb{1}_d \otimes \cdots \otimes \mathbb{1}_d \\ A_2 &= X_d \otimes Z_d \otimes \mathbb{1}_d \otimes \mathbb{1}_d \otimes \cdots \otimes \mathbb{1}_d \\ A_3 &= X_d \otimes X_d \otimes Z_d \otimes \mathbb{1}_d \otimes \cdots \otimes \mathbb{1}_d \\ &\vdots \\ A_n &= X_d \otimes X_d \otimes X_d \otimes X_d \otimes \cdots \otimes Z_d \ . \end{aligned}$$

It is straightforward to verify that these operators satisfy $A_j^d = \mathbb{1}$ for all j and $A_j A_k = \omega_d A_k A_j$ for all $j < k$. Hence, they define n MUMs with outcome number d. □

3 Superdense coding and MUMs

In this section, we describe some connections between MUMs and superdense coding protocols. We present the rigidity conjecture due to Nayak and Yuen in Section 3.1. We show how the encoding operators in optimal protocols can be constructed from any pair of MUMs in Section 3.2. Then we prove the connection between rigidity of superdense coding and the expressibility of MUMs as a direct sum of MUBs in Section 3.3. This yields the counterexamples to the conjecture claimed in Section 1.

3.1 The rigidity conjecture

In a d-dimensional superdense coding protocol, two parties, Alice and Bob, share a quantum state τ on a bipartite Hilbert space $\mathcal{H}_A \otimes \mathcal{H}_B$. We assume without loss of generality that $\mathcal{H}_A$ factors as $\mathcal{H}_{A'} \otimes \mathcal{H}_{A''}$, where $\mathcal{H}_{A''}$ is isomorphic to $\mathbb{C}^d$. Given an input $i \in [d^2]$, Alice applies a unitary operator W_i (called an *encoding operator*) to her share of τ (with support in the space $\mathcal{H}_A$), and sends the qubits in A'' to Bob. Bob then performs a measurement on the Hilbert space $\mathcal{H}_{A''} \otimes \mathcal{H}_B$ to determine what the input i is. (Since Bob does not know the input i, the measurement is independent of i.) We may define the protocol formally as follows.

Definition 3.1 (Superdense coding protocol)**.** *Let d be a positive integer. Let $\mathcal{H}_A := \mathcal{H}_{A'} \otimes \mathcal{H}_{A''}$ and $\mathcal{H}_B$ be finite dimensional Hilbert spaces where $\mathcal{H}_{A''}$ is isomorphic to $\mathbb{C}^d$. Let τ denote a quantum state on $\mathcal{H}_A \otimes \mathcal{H}_B$ and let $(W_i : i \in [d^2])$ denote a sequence of d^2 unitary operators acting on $\mathcal{H}_A$. We say that $(\tau, (W_i))$ is a* d-dimensional superdense coding protocol *if there exists a measurement $(M_i : i \in [d^2])$ acting on $\mathcal{H}_{A''} \otimes \mathcal{H}_B$ such that $\mathrm{Tr}(M_i \rho_i) = 1$ for all $i \in [d^2]$, where ρ_i denotes the reduced state on registers $A''B$, i.e., $\rho_i := \mathrm{Tr}_{A'}[(W_i \otimes \mathbb{1})\tau(W_i \otimes \mathbb{1})^\dagger]$. The operators (W_i) are then called the* encoding operators.

A canonical protocol for d-dimensional superdense coding is as follows. Alice and Bob share the d-dimensional maximally entangled state $|\phi_d\rangle := \frac{1}{\sqrt{d}} \sum_{e=1}^{d} |e\rangle|e\rangle$. Given message $i \in [d^2]$, Alice applies a unitary operator E_i to her share of $|\phi_d\rangle$, and sends it over to receiver. The family of unitary operators $\{E_i\}$ can be any orthogonal unitary basis for the space of $d \times d$ complex matrices.

(The orthogonality property means that $\mathrm{Tr}(E_i^\dagger E_j) = 0$ if and only if $i \neq j$.) An example of such a basis is the set of Heisenberg-Weyl operators (also called the generalized Pauli operators). The d^2 possible states with which the receiver, Bob, ends up are then mutually orthogonal, and may be distinguished perfectly via a suitable measurement.

Werner [Wer01] described, without proof, how non-equivalent orthogonal unitary bases may be constructed. Nayak and Yuen [NY20] presented explicit constructions of such bases for dimensions three and higher, and proved their non-equivalence. In light of this, and the rigidity of the Bennett-Wiesner protocol that they established, they conjectured the rigidity of superdense coding for all dimensions, up to the choice of an orthogonal unitary basis. In more detail, they defined a notion of *local equivalence*, and conjectured that every d-dimensional superdense coding protocol is locally equivalent to one in which the sender measures a part of the shared entangled state to generate a shared random string r, and then runs a protocol using an orthogonal unitary basis depending on r.

More precisely, given an arbitrary protocol $(\tau, (W_i))$ for superdense coding, Nayak and Yuen conjectured that there exist local isometries V, W such that if Alice applies V and Bob applies W to their respective shares of τ, then a maximally entangled state $|\phi_d\rangle$ is extracted, in tensor product with an auxiliary state ρ. Alice then performs a projective measurement $\{P_r\}$ on her part of the auxiliary state ρ to obtain some outcome r. Based on r, Alice applies the ith operator from a unitary orthogonal basis $\{E_{r,i}\}$ to her half of the maximally entangled state. Finally, after sending her half of the state $(E_{r,i} \otimes \mathbb{1})|\phi_d\rangle$, the sender applies some unitary operator C_i on the remaining qubits in her possession. (This final operation does not affect Bob's reduced state or measurement in any way.) Bob measures his part of ρ with the same projective measurement $\{P_r\}$ as Alice. Using the outcome r, he measures the remaining qubits appropriately to recover the classical message i.

Formally, the rigidity conjecture may be stated as follows. In this statement, for any three operators C, D, E, the notation $C =_E D$ denotes that $CEC^\dagger = DED^\dagger$.

Conjecture 3.2 (Nayak and Yuen [NY20])**.** Let $(\tau, (W_i))$ be a d-dimensional superdense coding protocol. Then there exist

1. Unitary operators V acting on $\mathcal{H}_{A'} \otimes \mathcal{H}_{A''}$ and $(C_i)_{i \in [d^2]}$ acting on $\mathcal{H}_{A'}$,
2. An isometry W mapping $\mathcal{H}_B$ to a Hilbert space $\mathcal{H}_{B'} \otimes \mathcal{H}_{B''}$ where $\mathcal{H}_{B''}$ is isomorphic to $\mathbb{C}^d$,
3. A density matrix ρ on $\mathcal{H}_{A'} \otimes \mathcal{H}_{B'}$,
4. A set of pairwise orthogonal projectors $\{P_r\}$ on $\mathcal{H}_{A'}$ that sum to the identity, and
5. For every r, an orthogonal unitary basis $\{E_{r,i}\}_{i \in [d^2]}$ for the space of $d \times d$ complex matrices,

such that, letting $\tau' := (V \otimes W)\tau(V \otimes W)^\dagger$, we have

$$\tau' \quad = \quad \rho^{A'B'} \otimes |\phi_d\rangle\langle\phi_d|^{A''B''}$$

and for $i \in [d^2]$,

$$(C_i^\dagger \otimes \mathbb{1}) W_i V^\dagger \quad =_{\tau'} \quad \sum_r P_r \otimes E_{r,i} \,.$$

In other words, any d-dimensional superdense coding protocol is locally equivalent to a canonical protocol, in which the ancillary part of the shared state τ in register A' serves as a source of randomness, and for each "randomness string" r, the encoding operators are given by an orthogonal unitary basis $\{E_{r,i}\}$.

3.2 Encoding operators from MUMs

Consider any pair of d-outcome MUMs, $\{P_a\}_{a=1}^d$ and $\{Q_b\}_{b=1}^d$ in the form given by Eqs. (2.3) and (2.4). By the characterization of MUMs described in Section 2.1, the space on which the MUMs act is isomorphic to $\mathbb{C}^n \otimes \mathbb{C}^d$ for some positive integer n. Define the maximally entangled state on $(\mathbb{C}^n \otimes \mathbb{C}^d)^{\otimes 2}$, corresponding to registers A and B, as

$$|\phi^+\rangle \quad := \quad \frac{1}{\sqrt{nd}} \sum_{p=1}^{nd} |p\rangle^A |p\rangle^B \ .$$

Define unitary operators

$$R \quad := \quad \sum_{a=1}^{d} \omega^a P_a \qquad \text{and} \qquad S \quad := \quad \sum_{b=1}^{d} \omega^b Q_b \ , \tag{3.1}$$

where $\omega := \mathrm{e}^{\frac{2\pi \mathrm{i}}{d}}$ is a primitive d-th root of unity. Consider the set $\{W_{st}\}_{s,t=1}^d$, where $W_{st} := R^s S^t$. We claim that these give us a superdense coding protocol.

Theorem 3.3. *The pair $(\phi^+, (W_{st}))$ is a d-dimensional superdense coding protocol.*

Proof. We design a superdense coding protocol using the operators W_{st} as follows. Registers A and B consist of subregisters $A'A''$ and $B'B''$, respectively. The subregisters A', B' are both n-dimensional, and A'', B'' are both d-dimensional. In the superdense coding protocol, Alice and Bob hold registers A and B, respectively, jointly prepared in state $|\phi^+\rangle$. On input $st \in [d] \times [d]$, Alice applies the unitary operator W_{st} on her half of the maximally entangled state (in register A), and sends the d-dimensional marginal state in subregister A'' to Bob.

Recall the property that for every linear operator O on $\mathbb{C}^{nd}$, we have $O \otimes \mathbb{1}_{nd} |\phi^+\rangle = \mathbb{1}_{nd} \otimes O^{\mathrm{T}} |\phi^+\rangle$, where the transposition is in the standard basis. Using this, we see that Bob ends up with the state ρ_{st} in registers $A''B$, where

$$\begin{aligned} \rho_{st} \quad &= \quad \mathrm{Tr}_{A'} \left[(W_{st} \otimes \mathbb{1}_{nd}) |\phi^+\rangle\langle\phi^+| (W_{st}^\dagger \otimes \mathbb{1}_{nd}) \right] \\ &= \quad \mathrm{Tr}_{A'} \left[(\mathbb{1}_{nd} \otimes W_{st}^{\mathrm{T}}) |\phi^+\rangle\langle\phi^+| (\mathbb{1}_{nd} \otimes (W_{st}^\dagger)^{\mathrm{T}}) \right] \\ &= \quad \frac{1}{n} \sum_{x=1}^{n} |\psi_{st}^x\rangle\langle\psi_{st}^x| \ , \end{aligned}$$

and the states $|\psi_{st}^x\rangle$ are defined as

$$|\psi_{st}^x\rangle \quad := \quad \frac{1}{\sqrt{d}} \sum_{l=1}^{d} |l\rangle \otimes W_{st}^{\mathrm{T}} |xl\rangle \ .$$

Now

$$\langle \psi_{st}^x | \psi_{s't'}^{x'} \rangle \quad = \quad \frac{1}{d} \langle x | \left[\mathrm{Tr}_{B''} \left(\overline{W_{st}} W_{s't'}^{\mathrm{T}} \right) \right] |x'\rangle \ , \tag{3.2}$$

where $\overline{O}$ denotes the entry-wise complex conjugation of the operator O in the standard basis. Since $\{P_a\}$ and $\{Q_b\}$ are a pair of projective measurements, the unitary operators W_{st} can be written as

$$W_{st} \quad = \quad \sum_{a,b=1}^{d} \omega^{sa+tb} P_a Q_b \ . \tag{3.3}$$

Since $Q_b^{\mathrm{T}} = \overline{Q_b}$, and $\{Q_b^{\mathrm{T}}\}$ is also a projective measurement, we have

$$\begin{aligned}\mathrm{Tr}_{B''}\left(\overline{W_{st}}W_{s't'}^{\mathrm{T}}\right) &= \mathrm{Tr}_{B''}\left(\sum_{a,b=1}^{d}\omega^{-sa-tb}P_a\overline{Q_b}\sum_{a',b'=1}^{d}\omega^{s'a'+t'b'}Q_{b'}^{\mathrm{T}}P_{a'}\right)\\ &= \sum_{a,b=1}^{d}\omega^{(s'-s)a+(t'-t)b}\,\mathrm{Tr}_{B''}\left(P_aQ_b^{\mathrm{T}}P_a\right)\ .\end{aligned}$$

Moreover $P_a^{\mathrm{T}} = P_a$, and by definition of MUMs, we have $P_a = P_a^{\mathrm{T}} = dP_aQ_b^{\mathrm{T}}P_a$. Hence

$$\begin{aligned}\mathrm{Tr}_{B''}\left(\overline{W_{st}}W_{s't'}^{\mathrm{T}}\right) &= \frac{1}{d}\sum_{a,b=1}^{d}\omega^{(s'-s)a+(t'-t)b}\,\mathrm{Tr}_{B''}\left(P_a\right)\\ &= \delta_{ss'}\delta_{tt'}d\,\mathbb{1}\ ,\end{aligned}$$

and by Eq. (3.2), $\langle\psi_{st}^{x}|\psi_{s't'}^{x'}\rangle = \delta_{xx'}\delta_{ss'}\delta_{tt'}$. This implies that

$$\mathrm{Tr}(\rho_{st}\rho_{s't'}) = \delta_{ss'}\delta_{tt'}\ ,$$

i.e., the states ρ_{st} are mutually orthogonal. So there is a measurement that perfectly distinguishes these states, and $(\phi^+, (W_{st}))$ is a d-dimensional superdense coding protocol. □

3.3 Rigidity and the direct-sum property

It turns out that Conjecture 3.2 implies that any superdense coding protocol derived from MUMs are direct sums of MUBs. We start by showing that the conjecture imposes a direct sum, i.e., block-diagonal structure on the encoding operators R, S defined in Section 3.2.

Proposition 3.4. *Suppose the MUMs $\{P_a\}$ and $\{Q_b\}$ are in canonical form. If Conjecture 3.2 is true, then there is a basis $(|v_j\rangle : j \in [n])$ for $\mathbb{C}^n$ and unitary operators $(S_j : j \in [n])$ on $\mathbb{C}^d$ such that $S = \sum_{j=1}^{n}|v_j\rangle\langle v_j| \otimes S_j$.*

Proof. Let $T_0 := R$ and $T_1 := S$. Note that $R = \mathbb{1} \otimes Z_d$, where Z_d is the generalized Pauli Z operator on $\mathbb{C}^d$ (also called the "clock" operator). Since the MUMs are in canonical form, we have $Q_1 = \mathbb{1} \otimes |u\rangle\langle u|$, where $|u\rangle := \frac{1}{\sqrt{d}}\sum_{j=1}^{d}|j\rangle$.

Suppose Conjecture 3.2 holds. Then there are unitary operators V, W on $\mathbb{C}^n \otimes \mathbb{C}^d$, unitary operators C_0, C_1 on $\mathbb{C}^n$, an integer $m \in [n]$, orthogonal projection operators $(\Pi_r : r \in [m])$, and for each $r \in [m]$ and orthogonal unitary basis $(E_{ri} : i \in [d^2])$ for the vector space of linear operators on $\mathbb{C}^d$ such that for each $i \in \{0, 1\}$,

$$((C_i \otimes \mathbb{1})T_iV^\dagger) \otimes \mathbb{1})(V \otimes W)|\phi^+\rangle = \left(\sum_{r=1}^{m}\Pi_r \otimes E_{ri} \otimes \mathbb{1}\right)(V \otimes W)|\phi^+\rangle\ .$$

Since $(V \otimes W)|\phi^+\rangle = (\mathbb{1} \otimes WV^{\mathrm{T}})|\phi^+\rangle$, we get

$$((C_i \otimes \mathbb{1})T_iV^\dagger) \otimes \mathbb{1})|\phi^+\rangle = \left(\sum_{r=1}^{m}\Pi_r \otimes E_{ri} \otimes \mathbb{1}\right)|\phi^+\rangle\ .$$

Since a unitary operator on $\mathbb{C}^n \otimes \mathbb{C}^d$ is completely determined by its action on the maximally entangled state $|\phi^+\rangle$, this is equivalent to

$$(C_i \otimes \mathbb{1})T_i V^\dagger \quad = \quad \sum_{r=1}^{m} \Pi_r \otimes E_{ri} \ .$$

Multiplying the adjoint of the operators for $i = 0$ to those for $i = 1$ on the right, we get

$$(C_1 \otimes \mathbb{1})T_1 V^\dagger V T_0^\dagger (C_0^\dagger \otimes \mathbb{1}) \quad = \quad \sum_{r=1}^{m} \Pi_r \otimes E_{r1} E_{r0}^\dagger \ .$$

Using $T_0 = R = \mathbb{1} \otimes Z_d$ and $T_1 = S$, this is equivalent to

$$S \quad = \quad \sum_{r=1}^{m} (C_1^\dagger \Pi_r C_0) \otimes (E_{r1} E_{r0}^\dagger Z_d) \ .$$

By definition of S and the orthgonality of $\{Q_b\}$, we have $Q_1 S Q_1 = \omega Q_1$. So

$$\sum_{r=1}^{m} (C_1^\dagger \Pi_r C_0) \langle u|(E_{r1} E_{r0}^\dagger Z_d)|u\rangle \otimes |u\rangle\langle u| \quad = \quad \omega\, \mathbb{1} \otimes |u\rangle\langle u| \ .$$

Define $\alpha_r := \langle u|(E_{r1} E_{r0}^\dagger Z_d)|u\rangle$. The above equation implies that

$$C_1^\dagger \left(\sum_{r=1}^{m} \alpha_r \Pi_r \right) C_0 \quad = \quad \omega\, \mathbb{1} \ ,$$

$$\text{i.e.,} \qquad \sum_{r=1}^{m} \alpha_r \Pi_r \quad = \quad \omega C_1 C_0^\dagger \ .$$

In particular, the operator on the LHS above is unitary, and $|\alpha_r| = 1$ for all r. Thus, $C_1^\dagger = \omega C_0^\dagger \sum_r \bar{\alpha_r} \Pi_r$, and

$$S \quad = \quad \sum_{r} (C_0^\dagger \Pi_r C_0) \otimes \left(\omega \bar{\alpha_r} E_{r1} E_{r0}^\dagger Z_d \right) \ .$$

The proposition follows. □

Finally, we show that the block-diagonal structure of the encoding operators carries over to the MUMs.

Theorem 3.5. *Suppose the MUMs $\{P_a\}$ and $\{Q_b\}$ are in canonical form. If Conjecture 3.2 is true, then the MUMs $\{P_a\}$ and $\{Q_b\}$ are a direct sum of MUBs.*

Proof. By Proposition 3.4, $S = \sum_{k=1}^{n} |v_k\rangle\langle v_k| \otimes S_k$ for some orthonormal basis $(|v_k\rangle)$ for $\mathbb{C}^n$, and unitary operators (S_k) on $\mathbb{C}^d$. Since $S^d = \mathbb{1}$, we have $S_k^d = \mathbb{1}$ for all k. So all the eigenvalues of S_k are dth roots of unity.

We may write $P_a = \sum_k |v_k\rangle\langle v_k| \otimes |a\rangle\langle a|$. The operator Q_b inherits the same structure, as we may extract it from the encoding operator S as follows:

$$\begin{aligned} Q_b \quad &= \quad \frac{1}{d} \sum_{j=1}^{d} \omega^{-bj} S^j \\ &= \quad \sum_{k=1}^{n} |v_k\rangle\langle v_k| \otimes \frac{1}{d} \sum_{j=1}^{d} \omega^{-bj} S_k^j \ . \end{aligned}$$

The operator $Q_{bj} := \frac{1}{d}\sum_{j=1}^{d} \omega^{-bj} S_k^j$ is the orthogonal projection onto the ω^b eigenspace of S_k. So Q_b is also a direct sum of orthogonal projection operators. The MUM property implies that for each j, $\{|a\rangle\langle a| : a \in [d]\}$ and $\{Q_{bj} : b \in [d]\}$ are MUBs. The lemma follows. □

In Sections 2.3 and 2.5 we presented MUMs that are not direct sums of MUBs. It follows from Theorem 3.5 that Conjecture 3.2 is false for an infinite number of dimensions $d \geq 4$.

References

[BAD18] Santiago Barrera Acevedo and Heiko Dietrich. Perfect sequences over the quaternions and $(4n, 2, 4n, 2n)$-relative difference sets in $C_n \times Q_8$. *Cryptography and Communications*, 10(2):357–368, 2018.

[BAD19] Santiago Barrera Acevedo and Heiko Dietrich. New infinite families of Williamson Hadamard matrices. *Australasian Journal of Combinatorics*, 73(1):207–219, January 2019.

[Ban18] Teodor Banica. Complex Hadamard matrices with noncommutative entries. *Annals of Functional Analysis*, 9(3):354–368, 2018.

[BKG20] Curtis Bright, Ilias Kotsireas, and Vijay Ganesh. New infinite families of perfect quaternion sequences and Williamson sequences. *IEEE Transactions on Information Theory*, 66(12):7739–7751, December 2020.

[BW92] Charles H. Bennett and Stephen J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physical review letters*, 69(20):2881, 1992.

[CĐ08] Oleg Chterental and Dragomir Ž. Đoković. On orthostochastic, unistochastic and qustochastic matrices. *Linear Algebra and its Applications*, 428(4):1178–1201, 2008.

[DEBŻ10] Thomas Durt, Berthold-Georg Englert, Ingemar Bengtsson, and Karol Życzkowski. On mutually unbiased bases. *International Journal of Quantum Information*, 08(04):535–640, 2010.

[Gav08] Dmitry Gavinsky. On the role of shared entanglement. *Quantum Information and Computation*, 8(1&2):82–95, 2008.

[KG14] Amir Kalev and Gilad Gour. Mutually unbiased measurements in finite dimensions. *New Journal of Physics*, 16(5):053038, 2014.

[KŠT+19] Jędrzej Kaniewski, Ivan Šupić, Jordi Tura, Flavio Baccari, Alexia Salavrakos, and Remigiusz Augusiak. Maximal nonlocality from maximal entanglement and mutually unbiased bases, and self-testing of two-qutrit quantum systems. *Quantum*, 3:198, 2019.

[Kuz10] Oleg Kuznetsov. *Perfect Sequences over the Real Quaternions*. PhD thesis, School of Mathematical Sciences, Monash University, Australia, 2010.

[NPA12] Miguel Navascués, Stefano Pironio, and Antonio Acín. SDP relaxations for noncommutative polynomial optimization. In Miguel F. Anjos and Jean B. Lasserre, editors, *Handbook on Semidefinite, Conic and Polynomial Optimization*, chapter 21, pages 601–634. Springer US, Boston, MA, 2012.

[NY20] Ashwin Nayak and Henry Yuen. Rigidity of superdense coding. Technical Report arXiv:2012.01672v1 [quant-ph], arXiv Pre-print server, `https://arxiv.org/abs/2012.01672`, December 2020.

[PWTR18] E. C. Paul, S. P. Walborn, D. S. Tasca, and Łukasz Rudnicki. Mutually unbiased coarse-grained measurements of two or more phase-space variables. *Physical Review A*, 97:052103, 2018.

[RW21] Łukasz Rudnicki and Stephen P. Walborn. Entropic uncertainty relations for mutually unbiased periodic coarse-grained observables resembling their discrete counterparts. *Physical Review A*, 104:042210, 2021.

[SRTW22] Thais L. Silva, Łukasz Rudnicki, Daniel S. Tasca, and Stephen P. Walborn. Discretized continuous quantum-mechanical observables that are neither continuous nor discrete. *Physical Review Research*, 4:013060, 2022.

[TFR+21] Armin Tavakoli, Máté Farkas, Denis Rosset, Jean-Daniel Bancal, and Jędrzej Kaniewski. Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments. *Science Advances*, 7(7), 2021.

[TSWR18] Daniel S. Tasca, Piero Sánchez, Stephen P. Walborn, and Łukasz Rudnicki. Mutual unbiasedness in coarse-grained continuous variables. *Physical Review Letters*, 120:040403, 2018.

[Wer01] Reinhard F. Werner. All teleportation and dense coding schemes. *Journal of Physics A: Mathematical and General*, 34(35):7081–7094, August 2001.

[WF89] William K. Wootters and Brian D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191(2):363–381, 1989.

[Wil13] Mark M. Wilde. *Quantum Information Theory*. Cambridge University Press, Cambridge, UK, 2013.

[Zau99] Gerhard Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, Austria, 1999.

[Zau11] Gerhard Zauner. Quantum designs: Foundations of a non-commutative Design Theory. *International Journal of Quantum Information*, 09(01):445–507, 2011. English translation of [Zau99].