Equivalence of mutually unbiased bases via orbits: general theory and a $d = 4$ case study

Amit Te'eni[1*] and Eliahu Cohen[1]

[1*]Faculty of Engineering and Institute of Nanotechnology and Advanced Materials, Bar Ilan University, Ramat Gan, 5290002, Israel.

*Corresponding author(s). E-mail(s): amit.teeni@biu.ac.il;

Abstract

In quantum mechanics, mutually unbiased bases (MUBs) represent orthonormal bases that are as "far apart" as possible, and their classification reveals rich underlying geometric structure. Given a complex inner product space, we construct the space of its orthonormal bases as a discrete quotient of the complete flag manifold. We introduce a metric on this space, which corresponds to the "MUBness" distance. This allows us to describe equivalence between sets of mutually unbiased bases in terms of the geometry of this space. The subspace of bases that are unbiased with respect to the standard basis decomposes into orbits under a certain group action, and this decomposition corresponds to the classification of complex Hadamard matrices. More generally, we consider a list of k MUBs, that one wishes to extend. The candidates are points in the subspace comprising all bases which are unbiased with respect to the entire list. This space also decomposes into orbits under a group action, and we prove that points in distinct orbits yield inequivalent MUB lists. Thus, we generalize the relation between complex Hadamard matrices and MUBs. As an application, we identify new symmetries that reduce the parameter space of MUB triples in dimension 4 by a factor of 4.

Keywords: Mutually unbiased bases, Complex Hadamard matrices, Flag manifolds

1 Introduction

Consider the inner product (Hilbert) space $\mathscr{H} = \mathbb{C}^n$, and let $p = \{|\phi_i\rangle\}_{i=1}^n$ and $q = \left\{|\psi_j\rangle\right\}_{j=1}^n$ be two orthonormal bases (ONBs). If the inner products $\langle\phi_i|\psi_j\rangle$ all have the same modulus, then p and q are said to be *mutually unbiased*. In this case the modulus must be $1/\sqrt{n}$, i.e.:

$$\forall i, j, \quad \left|\langle\phi_i|\psi_j\rangle\right|^2 = \frac{1}{n}. \tag{1}$$

The term “mutually unbiased bases” (MUBs) originates in quantum information theory. Suppose $\mathscr{H}$ is the Hilbert space of some quantum system, and consider two consecutive projective measurements of the state: first with respect to the basis p, and then with respect to q. In this scenario, the outcome of the first measurement provides no information regarding the outcome of the second one; the probability distribution for the second measurement is always uniform. In this sense, the two measurements are mutually unbiased. Similarly, a set of orthonormal bases $\{q_k\}_{k=1}^m$ is referred to as a set of MUBs, if any two distinct bases q_k, q_l are mutually unbiased. It can be shown that no such set can contain more than $n+1$ bases [1]. A set of exactly $n+1$ MUBs is called *complete*. Mutually unbiased bases have numerous applications in quantum information theory. A complete set of MUBs yields an optimal scheme for quantum state determination [1–3]. MUBs are also used in quantum key distribution (QKD) [4–10], random access codes [11, 12], quantum tomography [13, 14], entropic uncertainty relations [15–18], and entanglement detection [19–21].

Due to the immense fundamental and practical significance of MUBs, it is important to understand their properties. One puzzle that has attracted the attention of many researchers, pertains to the largest possible set of MUBs. If n is a prime power, then a complete set of MUBs always exists; but in composite dimensions, it is generally unknown whether a complete set exists or not [22–25]. Although the problem is formulated in simple terms of basic linear algebra, it turns out to be a fairly deep one, related to a myriad of fields in physics and mathematics alike [26–33]. A separate (yet related) problem is the classification of MUB sets up to equivalence. Two ordered lists $(p_1,\ldots,p_k)$ and $(q_1,\ldots,q_k)$ of MUBs are *unitarily equivalent* is there exists a unitary U such that U maps p_i to q_i for all $1 \le i \le k$. Inequivalent MUB sets can have distinct formal properties, and may also yield different performance in the aforementioned applications (see Section 3.13 of [25]). Note that equivalence of MUB triples was recently studied theoretically [34] and experimentally [35].

In this paper, we study the classification of MUB sets via group actions on manifolds. Consider $\mathscr{M}_n$, the manifold of unordered "projective" orthonormal bases of $\mathbb{C}^n$ (where "projective" means that we do not distinguish between a basis vector and its scalar multiples). This manifold can be constructed as a quotient of the complete flag manifold with respect to the symmetric group, which acts by permuting basis vectors. $\mathscr{M}_n$ can be endowed with the "MUBness" distance, thus making it into a metric space; and MUBs correspond to maximally-distant points. For a set of points $q_1,\ldots,q_k \in \mathscr{M}_n$, let $\mathscr{N}(q_1,\ldots,q_k) \subseteq \mathscr{M}_n$ denote the subset of points which are unbiased with respect to the k points $q_1,\ldots,q_k$. Using this language, we frame a general heuristic procedure for constructing a list of MUBs. This is done iteratively: we first choose an arbitrary $q_1 \in \mathscr{M}_n$. Then, in the kth iteration we choose an arbitrary point $q_k \in \mathscr{N}(q_1,\ldots,q_{k-1})$. Any set of MUBs can be constructed in this manner, but the choices in each step are highly redundant.

Our main contribution is alleviating this redundancy issue. The unitary group $\mathrm{U}(n)$ acts on $\mathscr{M}_n$, since the latter is a quotient of $\mathrm{U}(n)$. We show that $\mathscr{N}(q_1,\ldots,q_{k-1})$ is closed under the action of the subgroup $\mathrm{U}(n)_{q_1,\ldots,q_{k-1}} \subseteq \mathrm{U}(n)$ that stabilizes $q_1,\ldots,q_{k-1}$. We then prove the following (Theorem 4): two candidates $p,q \in \mathscr{N}(q_1,\ldots,q_{k-1})$ for q_k yield equivalent MUB lists, if and only if they belong to the same $\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$-orbit. For example, consider the submanifold $\mathscr{N}(e)$ comprising bases that are unbiased with respect to the standard basis e. In this case, our partition of $\mathscr{N}(e)$ is essentially equivalent to the standard classification of complex Hadamard matrices. The partition of $\mathscr{N}(q_1,\ldots,q_k)$ is a vast generalization of this classification. We then utilize our results to derive hitherto unknown equivalences between MUB triples in dimension $n = 4$.

This paper is organized as follows. Section 2 outlines our geometric constructions. First we construct $\mathscr{M}_n$, the space of orthonormal bases for $\mathbb{C}^n$, as a discrete quotient of the complete flag manifold. Next, we introduce the MUBness metric (distance) on $\mathscr{M}_n$, and show that the unitary group acts on $\mathscr{M}_n$ via isometries. We then use the MUBness metric to define the subsets $\mathscr{V}(q) \subseteq \mathscr{M}_n$ of q-unbiased bases; $\mathscr{N}(q_1, \ldots, q_k)$ is later defined as the intersection $\bigcap_{i=1}^{k} \mathscr{V}(q_i)$. Section 3 then relates MUB lists to theses geometric structures. We describe a standard procedure for constructing lists of MUBs, using our language. Later we define equivalence of MUB lists, and then we formulate and prove our main result, Theorem 4. For any step in the aforementioned procedure, this theorem characterizes choices that yield equivalent MUB steps, in terms of group orbits in $\mathscr{N}(q_1, \ldots, q_k)$. We then prove that these orbits are discrete. Section 4 demonstrates our results in dimension $n = 4$. This section serves two purposes: to illustrate concretely the abstract framework of the preceding sections; and to derive new results regarding equivalence of MUB triples, thus showcasing the power of our methods. We conclude this paper by summarizing our main insights and proposing directions for future research.

2 The space of orthonormal bases

This section details the geometric constructions that shall be used later. Let us briefly outline the upshot of these constructions. First, there exists a set $\mathscr{M}_n$, whose points correspond to orthonormal bases of $\mathbb{C}^n$; and $\mathscr{M}_n$ is endowed with a transitive $\mathrm{U}(n)$-action. For each $q \in \mathscr{M}_n$, there exists a subset $\mathscr{V}(q) \subseteq \mathscr{M}_n$ comprising all bases which are unbiased with respect to q. $\mathscr{V}(q)$ satisfies two key properties with respect to the $\mathrm{U}(n)$-action:

- For any $U \in \mathrm{U}(n)$, $\mathscr{V}(U \cdot q) = U \cdot \mathscr{V}(q)$;
- $\mathscr{V}(q)$ is closed under the action of the stabilizer subgroup $\mathrm{U}(n)_q$ of q.

Here $\cdot$ denotes the $\mathrm{U}(n)$-action, and $\mathrm{U}(n)_q := \{U \in \mathrm{U}(n) \mid U \cdot q = q\}$. The remainder of this section may be skipped by readers content to accept these results without proof.

2.1 Constructing $\mathscr{M}_n$

Recall that $\mathscr{M}_n$ denotes the set of all orthonormal bases (ONBs) of $\mathbb{C}^n$. Here we construct $\mathscr{M}_n$ as a quotient of the unitary group $\mathrm{U}(n)$. $\mathscr{M}_n$ thus obtains the structure of a smooth manifold.

Before proceeding, we first refine our definitions. Recall that global phases are insignificant in quantum mechanics: the vectors $|\psi\rangle$ and $e^{i\theta}|\psi\rangle$ correspond to the same physical state. If a quantum system is described by the Hilbert space $\mathscr{H}$, then its possible states are the *rays* in $\mathscr{H}$, i.e. the elements of the projective space $\mathbb{P}(\mathscr{H})$. Moreover, from a mathematical perspective, the definition (1) is invariant under multiplication of any basis vector by a phase. Hence, hereon we refer to basis elements "in the projective sense"; i.e., we think of basis elements as rank-one projections (equivalently: points in $\mathbb{CP}^{n-1}$) rather than actual vectors. We say that a set $p = \{P_i\}_{i=1}^n$ of pairwise-orthogonal rank-one projections is *complete* if $\sum_{i=1}^n P_i = I$. Hereon, "orthonormal basis" is taken to mean "complete set of pairwise-orthogonal rank-one projections". Two such complete sets p and $q = \left\{Q_j\right\}_{j=1}^n$ are said to be unbiased if:

$$\forall i, j, \quad \mathrm{Tr}\left(P_i Q_j\right) = \frac{1}{n}. \tag{2}$$

Any unitary matrix $U \in \mathrm{U}(n)$ defines an orthonormal basis by taking its columns as the basis vectors. Thus we obtain a map $\pi : \mathrm{U}(n) \twoheadrightarrow \mathscr{M}_n$. Since any basis can be obtained from some unitary matrix, this map is surjective; however it is not injective. In fact, there are two obstructions to injectivity:

- We do not care about multiplication of basis vectors by phases;
- We do not care about the order of the basis vectors.

These obstructions are symmetries of the fibers $\pi^{-1}(q)$; in other words, there are two group actions on $\mathrm{U}(n)$ that preserve the fibers. The first action multiplies each column by some phase $\mathrm{U}(1)$. Clearly, this action is given by right multiplication with an element of the torus subgroup T^n (the diagonal unitaries). Thus, the quotient of $\mathrm{U}(n)$ by the first action is precisely the *complete flag manifold*:

$$\tilde{\mathscr{M}}_n := \mathrm{Flag}\left(1,2,\ldots,n\right) = \mathrm{SL}\left(n;\mathbb{C}\right)/\mathrm{B}^n = \mathrm{SU}\left(n\right)/\left(\mathrm{T}^n \cap \mathrm{SU}\left(n\right)\right) = \mathrm{U}\left(n\right)/\mathrm{T}^n, \qquad (3)$$

where B^n is a Borel subgroup of $\mathrm{SL}\left(n;\mathbb{C}\right)$.

Note we have only resolved the first obstruction, since flag manifolds are sensitive to the ordering of basis vectors. Orthonormal bases correspond to complete flags via:

$$\left\{\mathbf{b}_i\right\}_{i=1}^{n} \longmapsto \left(V_1,\ldots,V_n\right), \text{ where } V_i := \mathrm{span}_{\mathbb{C}}\left\{\mathbf{b}_1,\ldots,\mathbf{b}_i\right\}, \qquad (4)$$

so any reordering of the basis elements $\left\{\mathbf{b}_i\right\}_{i=1}^{n}$ results in a different flag. To eliminate this redundancy we take a second quotient, this time by the action of the symmetric group S_n, that acts by permuting the order of basis vectors. Let us consider S_n as a subgroup of $\mathrm{U}\left(n\right)$, embedded as the permutation matrices; then reordering of basis elements corresponds to right multiplication by a permutation matrix.

Of course, we can also construct our space with a single quotient rather than take two consecutive ones. Define a third subgroup of $\mathrm{U}\left(n\right)$ – the semidirect product $\mathrm{C}_n := \mathrm{S}_n \ltimes \mathrm{T}^n$. This subgroup consists of complex matrices with exactly one nonzero entry in every row and every column, and the nonzero entries all have modulus 1. Notably, we have $\mathrm{C}_n = N\left(\mathrm{T}^n\right)$, i.e. this group is the *normalizer subgroup* of the torus in $\mathrm{U}\left(n\right)$; and the quotient $N\left(\mathrm{T}^n\right)/\mathrm{T}^n \cong \mathrm{S}_n$ is the *Weyl group* of $\mathrm{U}\left(n\right)$ (and also of $\mathrm{SU}\left(n\right)$). C_n is a closed subgroup of $\mathrm{U}\left(n\right)$ (closedness follows because T^n is a torus and S_n is finite), and it has $n!$ connected components. We define $\mathscr{M}_n$ as the quotient of $\mathrm{U}\left(n\right)$ by the right action of C_n:

$$\mathscr{M}_n := \mathrm{U}\left(n\right)/\mathrm{C}_n. \qquad (5)$$

This space differs from $\tilde{\mathscr{M}_n}$ only by the quotient of a discrete group, so they both have the same dimension and share many other important features. Crucially, both are compact connected homogeneous $\mathrm{U}(n)$-spaces. Moreover, $\tilde{\mathscr{M}_n}$ is an $n!$-fold covering space of $\mathscr{M}_n$; the covering map is the natural projection $\tilde{\mathscr{M}_n} \twoheadrightarrow \mathscr{M}_n$ that maps an ordered orthonormal basis to an unordered one. In fact, since the flag manifold $\tilde{\mathscr{M}_n}$ is simply connected it is the universal cover of $\mathscr{M}_n$, hence $\pi_1(\mathscr{M}_n) \cong \mathrm{S}_n$. The space $\mathscr{M}_n$ is the *permutation invariant complete flag manifold*, or the *symmetrized complete flag manifold*, for $\mathbb{C}^n$. It was defined in the same way in [36]. We note that the symmetrized space was less studied in the literature and is often not as convenient to work with as $\tilde{\mathscr{M}_n}$.

Hereon, the points of $\mathscr{M}_n$ are denoted either by small Latin letters (usually p or q, with or without a subscript), or in the form $U\mathrm{C}_n$ (the coset of C_n represented by $U \in \mathrm{U}(n)$).

2.2 MUBness

In Section 3, we use $\mathscr{M}_n$ to define a procedure that yields mutually unbiased bases. To do so, we need to enrich $\mathscr{M}_n$ with additional geometric structure that captures the notion of mutual-unbiasedness, or *MUBness*. Given any two ONBs $p = \{P_i\}_{i=1}^{n}$ and $q = \{Q_j\}_{j=1}^{n}$, their MUBness is defined as [27]:

$$D(p,q) := \sqrt{n - 1 - \sum_i \sum_j \left(\mathrm{Tr}(P_i Q_j) - \frac{1}{n}\right)^2}. \tag{6}$$

Evidently, $0 \leq D(p,q) \leq \sqrt{n-1}$; and $D(p,q) = \sqrt{n-1}$ iff p,q are mutually unbiased. Therefore, $D(p,q)$ indeed captures the extent of "MUBness" between p and q. Here we recast the original derivation of (6) in our own terms; namely, we construct a smooth embedding ϕ of $\mathscr{M}_n$ into a certain Grassmannian manifold. The pullback of the chordal metric (distance function) on the Grassmannian by ϕ then defines the MUBness metric on $\mathscr{M}_n$. In fact, we shall see that ϕ embeds $\mathscr{M}_n$ as a single orbit of a $\mathrm{U}(n)$-action on the Grassmannian. Since $\mathrm{U}(n)$ acts on the Grassmannian by isometries, we get that the $\mathrm{U}(n)$ action on $\mathscr{M}_n$ respects the MUBness metric.

First, recall the definition of $\mathscr{M}_n$ as the coset space $\mathrm{U}(n)/\mathrm{C}_n$, and denote its points as cosets $V\mathrm{C}_n$ for $V \in \mathrm{U}(n)$. Then $\mathrm{U}(n)$ acts on $\mathscr{M}_n$ transitively by left multiplication:

$$\forall U \in \mathrm{U}(n), \quad U \cdot V\mathrm{C}_n := (UV)\,\mathrm{C}_n. \tag{7}$$

Each $V\mathrm{C}_n \in \mathscr{M}_n$ can be represented as the complete set of orthogonal projections $p = \{P_i\}_{i=1}^n$, where $P_i = |v_i\rangle\langle v_i|$ for $|v_i\rangle$ the ith column of V.

Second, we define the Grassmannian and its $\mathrm{U}(n)$ action. Using the physicists' convention, $\mathfrak{su}(n)$ is the Lie algebra of traceless Hermitian matrices. We consider $\mathfrak{su}(n)$ as a real vector space with the Frobenius inner product (which equals the Killing form up to a scalar multiple). Let $\mathrm{Gr}(n-1,\mathfrak{su}(n))$ be the Grassmannian of $(n-1)$-dimensional subspaces of $\mathfrak{su}(n)$. This Grassmannian is naturally endowed with an $\mathrm{SO}(\mathfrak{su}(n))$-action: for $O \in \mathrm{SO}(\mathfrak{su}(n))$ and $W \in \mathrm{Gr}(n-1,\mathfrak{su}(n))$, $O \cdot W$ is the image $O(W)$. Now, $\mathrm{U}(n)$ acts on $\mathfrak{su}(n)$ via $\mathrm{Ad}_U(A) := UAU^\dagger$. This action preserves the Frobenius inner product, i.e. defines an element of $\mathrm{O}(\mathfrak{su}(n))$; and since $\mathrm{U}(n)$ is connected, its image must land in the connected component of the identity, i.e. $\mathrm{SO}(\mathfrak{su}(n))$. Thus, we get a $\mathrm{U}(n)$-action on $\mathrm{Gr}(n-1,\mathfrak{su}(n))$. We define the chordal Grassmannian distance [27] by $d_c(W_1,W_2) := \frac{1}{2}\mathrm{Tr}\left(S_{W_1} - S_{W_2}\right)^2$, where S_W denotes the unique orthogonal projection onto the subspace $W \in \mathrm{Gr}(n-1,\mathfrak{su}(n))$. This metric is $\mathrm{SO}(\mathfrak{su}(n))$-invariant, since:

$$\begin{aligned}\forall O \in \mathrm{SO}(\mathfrak{su}(n)),\ d_c(O\cdot W_1, O\cdot W_2) &= \frac{1}{2}\mathrm{Tr}\left(OS_{W_1}O^T - OS_{W_2}O^T\right)^2 = \\ &= \frac{1}{2}\mathrm{Tr}\left[O\left(S_{W_1} - S_{W_2}\right)O^T\right]^2 = \frac{1}{2}\mathrm{Tr}\left(S_{W_1} - S_{W_2}\right)^2 = d_c(W_1,W_2).\end{aligned}$$

We now arrive at the definition of the map ϕ. Given an ONB $p = \{P_i\}_{i=1}^n \in \mathscr{M}_n$ (recall each P_i is a rank-one projection), we define:

$$\phi(p) := \operatorname{span}_{\mathbb{R}} \left\{ P_i - \frac{\mathbb{1}}{n} \right\}_{i=1}^n . \tag{8}$$

Proposition 1. (8) *defines a smooth embedding* $\phi : \mathscr{M}_n \hookrightarrow \operatorname{Gr}(n-1, \mathfrak{su}(n))$*. Moreover,* ϕ *is equivariant with respect to the* $\mathrm{U}(n)$*-actions on both spaces.*

Proof. By definition of $\mathfrak{su}(n)$, we have $P_i - \frac{\mathbb{1}}{n} \in \mathfrak{su}(n)$ for all i (more generally, the set of all density matrices acting on $\mathbb{C}^n$ is embedded in the affine space $\mathfrak{su}(n) + \frac{\mathbb{1}}{n}$ of unit-trace Hermitian operators). To see that the RHS of (8) has dimension $n-1$, first note that the elements $P_i - \frac{\mathbb{1}}{n}$ sum up to zero, hence are not linearly independent. Moreover, we now show that the subset (say) $\left\{P_i - \frac{\mathbb{1}}{n}\right\}_{i=1}^{n-1}$ *is* linearly independent. If a real linear combination $\sum_{i=1}^{n-1} a_i \left(P_i - \frac{\mathbb{1}}{n}\right)$ vanishes, then

$$\sum_{i=1}^{n-1} a_i P_i = \frac{1}{n} \sum_{i=1}^{n-1} a_i \mathbb{1}.$$

Now, consider the matrix ranks of both sides. Since the P_i are all rank-one projections and the pairwise intersections $\operatorname{im}(P_i) \cap \operatorname{im}(P_j)$ are all trivial (for $i \neq j$), we deduce that $\operatorname{rank}\left(\sum_{i=1}^{n-1} a_i P_i\right) = \#\{1 \leq i \leq n-1 \mid a_i \neq 0\}$. In contrast, the rank of the RHS is zero if $\sum_{i=1}^{n-1} a_i = 0$ and n otherwise. The only way for the two ranks to agree is if $a_i = 0$ for all i, as required. Thus, $\left\{P_i - \frac{\mathbb{1}}{n}\right\}_{i=1}^{n}$ indeed span an $(n-1)$-dimensional subspace of $\mathfrak{su}(n)$; and the definition (8) is independent of the order of the basis elements P_i; thus, ϕ is indeed a well-defined map $\mathscr{M}_n \to \operatorname{Gr}(n-1, \mathfrak{su}(n))$.

Next, we show that ϕ is equivariant. For any $U \in \mathrm{U}(n)$ and $p \in \mathscr{M}_n$, we have:

$$\begin{aligned}\phi(U \cdot p) &= \operatorname{span}_{\mathbb{R}} \left\{ U P_i U^\dagger - \frac{\mathbb{1}}{n} \right\}_{i=1}^n = \operatorname{span}_{\mathbb{R}} \left\{ U \left(P_i - \frac{\mathbb{1}}{n} \right) U^\dagger \right\}_{i=1}^n = \\ &= \operatorname{span}_{\mathbb{R}} \left\{ \operatorname{Ad}_U \left(P_i - \frac{\mathbb{1}}{n} \right) \right\}_{i=1}^n = \operatorname{Ad}_U \left(\operatorname{span}_{\mathbb{R}} \left\{ P_i - \frac{\mathbb{1}}{n} \right\}_{i=1}^n \right) = \operatorname{Ad}_U (\phi(p)),\end{aligned}$$

where $\mathrm{span}_{\mathbb{R}}$ and Ad_U commute since Ad_U is an invertible $\mathbb{R}$-linear transformation.

We can now show that ϕ is smooth, using transitivity of the $\mathrm{U}(n)$-action on $\mathscr{M}_n$ and equivariance of ϕ. First, note ϕ is determined by its value on a single point, say the standard basis $\mathbb{1}\mathrm{C}_n \in \mathscr{M}_n$ (the coset of the identity matrix $\mathbb{1}$). This is true because $\phi(U\mathrm{C}_n) = \phi(U \cdot \mathbb{1}\mathrm{C}_n) = \mathrm{Ad}_U(\phi(\mathbb{1}\mathrm{C}_n))$. Now, the map $\pi : \mathrm{U}(n) \twoheadrightarrow \mathscr{M}_n$ is a surjective smooth submersion, hence by the characteristic property of surjective smooth submersions (Theorem 4.29 in [37]), ϕ is smooth if and only if $\phi \circ \pi : \mathrm{U}(n) \to \mathrm{Gr}(n-1, \mathfrak{su}(n))$ is smooth. For any $U \in \mathrm{U}(n)$ we have $\phi \circ \pi(U) = \phi(U\mathrm{C}_n) = \mathrm{Ad}_U(\phi(\mathbb{1}\mathrm{C}_n))$, which is smooth since the $\mathrm{SO}(\mathfrak{su}(n))$-action on the Grassmannian is smooth.

The equivariant rank theorem implies that ϕ has constant rank. Thus, if ϕ is injective then it is a smooth immersion, hence also a smooth embedding (since its domain $\mathscr{M}_n$ is compact). Let $p, q \in \mathscr{M}_n$, and suppose $\phi(p) = \phi(q)$. By transitivity, there exists $U \in \mathrm{U}(n)$ such that $q = U \cdot p$; hence $\phi(p) = \phi(U \cdot p) = \mathrm{Ad}_U(\phi(p))$, i.e. $U \in \mathrm{Stab}_{\phi(p)}$, the stabilizer of $\phi(p) \in \mathrm{Gr}(n-1, \mathfrak{su}(n))$. Therefore, ϕ is injective if and only if $U \in \mathrm{Stab}_{\phi(p)}$ implies $U \cdot p = p$, i.e. $\mathrm{Stab}_{\phi(p)}$ is a subgroup of the stabilizer of $p \in \mathscr{M}_n$, which is isomorphic to C_n. Equivalently, the stabilizers are isomorphic, since $\mathrm{Stab}_p \subseteq \mathrm{Stab}_{\phi(p)}$ follows directly from equivariance. By transitivity of the $\mathrm{U}(n)$-action on $\mathscr{M}_n$ and equivariance of ϕ, the image $\phi(\mathscr{M}_n)$ comprises a single orbit, hence a homogeneous $\mathrm{U}(n)$-space. Thus, the stabilizer subgroups for all points of $\phi(\mathscr{M}_n)$ are isomorphic; hence, it suffices to show that $\mathrm{Stab}_{\phi(\mathbb{1}\mathrm{C}_n)} \cong \mathrm{C}_n$.

The standard basis $\mathbb{1}\mathrm{C}_n$ is represented by the projections $\{|i\rangle\langle i|\}_{i=1}^n$, which span the subalgebra $\mathfrak{t} \subseteq \mathfrak{su}(n)$ of traceless diagonal Hermitian matrices. A unitary $U \in \mathrm{U}(n)$ belongs to the stabilizer of $\mathfrak{t} \in \mathrm{Gr}(n-1, \mathfrak{su}(n))$ if and only if $U\mathfrak{t}U^\dagger = \mathfrak{t}$. Consider a matrix $A \in \mathfrak{t}$ with distinct diagonal entries. $UAU^\dagger$ is diagonal if and only if the columns of $U^\dagger$ form an orthonormal eigenbasis of A. Since the entries of A are distinct, it has a unique orthonormal eigenbasis – the standard basis – up to phases and reordering. This precisely means that $U^\dagger \in \mathrm{C}_n$, which holds if and only if $U \in \mathrm{C}_n$. This completes the proof. □

This proposition has several corollaries. First, since ϕ is injective, we can use it to pull back d_c and obtain a metric on $\mathscr{M}_n$. As already established in [27], the pullback metric is the MUBness from (6). As mentioned above, these facts imply that $\mathrm{U}(n)$ acts on $\mathscr{M}_n$ by isometries with respect to the MUBness metric – a fact we shall use profusely in the next subsection.

Moreover, the Grassmannian $\mathrm{Gr}(n-1,\mathfrak{su}(n))$ is equipped with a tautological (real) vector bundle of rank $n-1$: the fiber over $V \in \mathrm{Gr}(n-1,\mathfrak{su}(n))$ is the vector space V. The pullback of this bundle defines a vector bundle $\mathscr{B} \to \mathscr{M}_n$, where the fiber over $p = \{P_i\}_{i=1}^n \in \mathscr{M}_n$ is given by $\mathrm{span}_{\mathbb{R}}\left\{P_i - \frac{\mathbb{1}}{n}\right\}_{i=1}^n$. Since the tautological bundle on the Grassmannian is $\mathrm{SO}(\mathfrak{su}(n))$-equivariant, $\mathscr{B}$ is $\mathrm{U}(n)$-equivariant: for a pair (p,A) with $p \in \mathscr{M}_n$ and $A \in \phi(p)$, define $U \cdot (p,A) := \left(U \cdot p, UAU^\dagger\right)$. The data of the equivariant embedding $\phi : \mathscr{M}_n \hookrightarrow \mathrm{Gr}(n-1,\mathfrak{su}(n))$ is the same as that of the equivariant rank-$(n-1)$ vector bundle $\mathscr{B}$. Thus, we get another perspective as to why $\mathscr{M}_n$ embeds in the Grassmannian, hence a new way to look at the geometric origins of MUBness.

As an aside, we note that the space of global sections $\Gamma(\mathscr{B})$ is naturally a representation of $\mathrm{U}(n)$. The embedding ϕ is somewhat analogous to how the flag manifold $\tilde{\mathscr{M}}_n$ (a homogeneous SL_n-space) embeds as a closed $\mathrm{SL}_n(\mathbb{C})$-orbit in $\mathbb{P}V$, where V corresponds to an irreducible representation of $\mathrm{SL}_n(\mathbb{C})$. The pullback of the tautological line bundle on $\mathbb{P}V$ yields an equivariant line bundle, whose space of global sections is a representation of $\mathrm{SL}_n(\mathbb{C})$, equivalent to V. Alternatively, ϕ can be considered analogous to the embedding of $\tilde{\mathscr{M}}_n$ as a coadjoint orbit in $\mathfrak{sl}(n;\mathbb{C})^*$.

2.3 Subsets of q-unbiased bases

Let $p,q \in \mathscr{M}_n$ be any two ONBs; recall that $D^2(p,q) = n-1$ iff p and q are unbiased. Therefore:

$$\mathscr{V}(q) := \left\{p \in \mathscr{M}_n \mid D^2(p,q) = n-1\right\} \tag{9}$$

defines $\mathscr{V}(q) \subseteq \mathscr{M}_n$ as the subset of all bases that are q-unbiased (i.e. unbiased with respect to q). For example, consider the standard basis $e := \mathbb{1}\mathrm{C}_n$ (the coset of the identity matrix $\mathbb{1}$). We have

$$\mathscr{V}(e) = \left\{ H\mathrm{C}_n \mid H \in \mathrm{U}(n) \text{ and } \forall i,j,\ \left|H_{ij}\right| = 1/\sqrt{n} \right\}. \tag{10}$$

Matrices H that satisfy these conditions (unitary matrices where all entries have modulus $1/\sqrt{n}$) are called *complex Hadamard matrices*. Two Hadamard matrices H_1, H_2 represent the same point in $\mathscr{V}(e)$ iff $H_1^\dagger H_2 \in \mathrm{C}_n$. Note that $\mathscr{V}(q)$ is a closed subset of $\mathscr{M}_n$ (for every q), but generally it may not be a submanifold (i.e. it may be singular). Moreover, any two $\mathscr{V}(q)$ are homeomorphic. Indeed, let $U \in \mathrm{U}(n)$ be a unitary that maps q to q' via the left action: $q' = U \cdot q$ (transitivity of the action means that such a unitary always exists). Then we have:

$$\begin{aligned}\mathscr{V}(U \cdot q) &= \left\{ p \in \mathscr{M}_n \mid D^2(p, U \cdot q) = n-1 \right\} = \\ &= \left\{ p \in \mathscr{M}_n \mid D^2\left(U^\dagger \cdot p, q\right) = n-1 \right\} = \left\{ p \in \mathscr{M}_n \mid U^\dagger \cdot p \in \mathscr{V}(q) \right\} = \\ &= U \cdot \mathscr{V}(q),\end{aligned} \tag{11}$$

using the fact that $\mathrm{U}(n)$ acts via isometries. Let $\mathrm{U}(n)_q := \{U \in \mathrm{U}(n) \mid U \cdot q = q\}$ denote the isotropy (stabilizer) subgroup. By the definition of a quotient space, if $q = V\mathrm{C}_n$ then $\mathrm{U}(n)_q = V\mathrm{C}_n V^\dagger$. Now, let $U \in \mathrm{U}(n)_q$; from (11) we see that U defines an *automorphism* $U : \mathscr{V}(q) \to \mathscr{V}(q)$. Thus, for $q = V\mathrm{C}_n$ we have that $\mathscr{V}(V\mathrm{C}_n)$ is closed under the action of the isotropy group $V\mathrm{C}_n V^\dagger$. For example, the set $\mathscr{V}(e)$ of complex Hadamard matrices is closed under left multiplication by a C_n matrix.

3 Mutually unbiased bases in the space of orthonormal bases

In this section, we consider lists (finite ordered sets) of MUBs. Every MUB list may be constructed via a generic iterative procedure. Let us describe this procedure informally. We start with an empty list, and each iteration adds one additional basis. The additional basis is chosen out of the set X, which is guaranteed to comprise all viable choices for the next basis.

We initialize X as $\mathscr{M}_n$; in the ith iteration, we choose some $q \in X$; and then we replace X by its subset of q-unbiased bases. We stop under one of two conditions: either we reached the desired number of MUBs; or X is empty. The latter means we constructed an *unextendible* MUB list, i.e., there is no basis which is mutually unbiased with respect to every element of the list.

Using the definitions from the previous section, we can see that the q-unbiased points in X are given by $X \cap \mathscr{V}(q)$. Therefore, after k iterations, the set X is given by:

$$\mathscr{N}(q_1, \dots, q_k) := \bigcap_{j=1}^{k} \mathscr{V}(q_j). \tag{12}$$

The elements of $\mathscr{N}(q_1, \dots, q_k)$ comprise the ONBs which are unbiased with respect to q_i for all $i = 1, 2, \dots, k$. However, explicit descriptions of the subsets $\mathscr{N}(q_1, \dots, q_k)$ may be difficult to obtain; the lack of such explicit descriptions means that our procedure is conceptual rather than computational.

We now describe our procedure formally:

```
Require: $n \geq 1, m \in \{1, \dots, n+1\}$
Ensure: $\forall i \neq j$, $q_i, q_j \in \mathscr{M}_n$ are mutually unbiased, and $\{q_i\}_{i=1}^{k-1}$ is unextendible or has length $m$
k ⇐ 1
while $\mathscr{N}(q_1, \dots, q_{k-1}) \neq \emptyset$ and $k \leq m$ do
    choose $q_k \in \mathscr{N}(q_1, \dots, q_{k-1})$
    $k \Leftarrow k + 1$
end while
```

For $k = 1$, $\mathscr{N}(\varepsilon)$ is interpreted as $\mathscr{M}_n$, where ε denotes the “empty list” of 0 points.

We now define a notion of equivalence between lists of MUBs.

Definition 2. *Let* $(p_1,\ldots,p_k)$ *and* $(q_1,\ldots,q_k)$ *be two lists of k MUBs in dimension n. These two MUB lists are said to be* equivalent *if there exists a unitary* $U\in\mathrm{U}(n)$ *such that* $U\cdot p_i=q_i$ *for all i.*

The remainder of this section deals with the following question: when does the above procedure produce equivalent MUB lists? As we shall see, the subset $\mathcal{N}(q_1,\ldots,q_{k-1})$ is closed under the action of a certain $\mathrm{U}(n)$-subgroup: the *simultaneous stabilizer* of $q_1,\ldots,q_{k-1}$. And two choices for q_k in the k-th step of the procedure yield equivalent MUB lists, if and only if they lie in the same orbit of the simultaneous stabilizer. This is the content of Theorem 4. Next, we study properties of these orbits, and show they are finite and discrete for any $k>2$.

Note we refer to $\mathcal{N}(q_1,\ldots,q_k)$ as mere subsets; in fact, their partition into orbits (of the simultaneous stabilizer) corresponds to a *stratification*. However, we do not use this fact.

3.1 Resolving redundancies

In the beginning of the current section we outlined a procedure that can yield any MUB list. Let us take a closer look at this procedure, and review what is already known about equivalent MUB lists.

We start by noting that existing analytic constructions of MUBs have utilized procedures similar to ours. Brierley and Weigert [31] construct all MUB sets in dimensions 2 to 5. Given a list of $k-1$ MUBs, they compute all vectors which are unbiased to all elements of the current bases, and then find all the ways to put them together into ONBs. To simplify the enumeration of all MUB sets, they define a *standard form* for MUB lists, and claim that any MUB list is equivalent to a standard-form one. The following Lemma describes the standard form using this paper's terminology.

Lemma 3 ([31])**.** *Any list of k MUBs is equivalent to a list of the form* $(\mathbb{1}\mathrm{C}_n,H_2\mathrm{C}_n\ldots,H_k\mathrm{C}_n)$ *that obeys the following conditions:*

(i) The first basis is $e=\mathbb{1}\mathrm{C}_n$*, the standard basis;*

(ii) The matrices $H_2\ldots,H_k$ *are complex Hadamard matrices;*

(iii) The entries in the first column of H_2 all equal $1/\sqrt{n}$;

(iv) The first row of each of the Hadamard matrices $H_2 \ldots, H_k$ has only the entries $1/\sqrt{n}$.

Proof. Let $(q_1, \ldots, q_k)$ be a MUB list. Since $\mathscr{M}_n$ is a homogeneous space, there always exists a unitary U such that $U \cdot q_1 = e$. Thus, as a first step we choose such U and note that $(q_1, \ldots, q_k)$ is equivalent to $(U \cdot q_1, \ldots, U \cdot q_k)$. Now, $U \cdot q_1 = e$; and since it is a MUB list, we must have $U \cdot q_i \in \mathscr{N}(e)$ for all $i > 1$. As we had mentioned previously, $\mathscr{N}(e) = \mathscr{V}(e)$ comprises all bases $H\mathrm{C}_n$ where H is a $n \times n$ complex Hadamard matrix. Thus, any MUB list is equivalent to one of the form $(\mathbb{1}\mathrm{C}_n, H_2\mathrm{C}_n \ldots, H_k\mathrm{C}_n)$, where H_i are complex Hadamard matrices. This fact ensures that conditions (i) and (ii) can always be satisfied.

Next, recall that all entries of a Hadamard matrix have the form $e^{i\theta}/\sqrt{n}$; so we can "dephase" the first row of each H_i by replacing $H_i \to H_i D$, where $D \in \mathrm{C}_n$ is a suitable diagonal matrix. But how can we satisfy the third condition? Similar to how rows can be dephased via right-multiplication by a C_n element, a column can be dephased via *left*-multiplication by a C_n element. Explicitly: let $(\mathbb{1}\mathrm{C}_n, H_2\mathrm{C}_n, \ldots, H_k\mathrm{C}_n)$ be a list that obeys conditions (i), (ii) and (iv), and let the $\left(1, e^{i\theta_2}, \ldots, e^{i\theta_n}\right)^T / \sqrt{n}$ be the first column of H_2. Define D to be the diagonal matrix with entries $e^{-i\theta_j}$; clearly DH_2 satisfies condition (iii). Of course, we do not have the freedom to replace H_2 by DH_2; but we do have the freedom to act on *the entire list* with D on the left. Crucially, the first element remains unchanged, since $D \cdot \mathbb{1}\mathrm{C}_n = D\mathrm{C}_n = \mathbb{1}\mathrm{C}_n$ (because $D \in \mathrm{C}_n$); and one easily verifies that each DH_i is a complex Hadamard matrix with the same first row as H_i. Thus, the new list $(\mathbb{1}\mathrm{C}_n, DH_2\mathrm{C}_n, \ldots, DH_k\mathrm{C}_n)$ satisfies conditions (i) to (iv), as required. □

As is evident from the proof, there is a deep reason why conditions (i) and (iii) can be satisfied simultaneously. We can replace $(q_1, \ldots, q_k) \to (U \cdot q_1, \ldots, U \cdot q_k)$, so we choose U that fixes the first basis to be the standard one. However, this condition does not fix U completely; rather, we can multiply it by an element of C_n, which is the stabilizer group of e. Indeed, if $U \cdot q_1 = \mathbb{1}\mathrm{C}_n$ and $P \in \mathrm{C}_n$, then $PU \cdot q_1 = P \cdot \mathbb{1}\mathrm{C}_n = P\mathrm{C}_n = \mathbb{1}\mathrm{C}_n$.

We can put this insight in more general terms. First, consider $k=1$, i.e. lists (q_1) comprising a single basis (it is a MUB list, vacuously). By homogeneity of $\mathscr{M}_n$, all such lists are equivalent; so without loss of generality, we may assume $q_1 = \mathbb{1}\mathrm{C}_n$. Now, suppose we have two lists of length $k=2$, and we wish to decide whether they are equivalent or not. We can bring the lists to the form $(\mathbb{1}\mathrm{C}_n, p)$, $(\mathbb{1}\mathrm{C}_n, q)$, where $p,q \in \mathscr{V}(e)$. The two lists are equivalent iff there exists a unitary U that obeys $U \cdot p = q$ *and* $U \cdot \mathbb{1}\mathrm{C}_n = \mathbb{1}\mathrm{C}_n$. The latter condition means that $U \in \mathrm{C}_n$. As we have seen in Section 2.3, $\mathscr{V}(e)$ is closed under the action of C_n. However, it is not always a homogeneous space. Hence, there may not exist a unitary $U \in \mathrm{C}_n$ that maps p to q. By definition, such a unitary exists iff p,q lie in the same orbit of the C_n action. Recall that two complex Hadamard matrices H_1, H_2 are said to be equivalent if there exist permutation matrices P_1, P_2 and diagonal unitary matrices D_1, D_2 such that:

$$H_1 = D_1 P_1 H_2 P_2 D_2. \tag{13}$$

Since the torus is normal in C_n, there exists some $\tilde{D}_1 \in \mathrm{T}^n$ s.t. $P_1 \tilde{D}_1 = D_1 P_1$. Hence we can replace the above condition by:

$$H_1 = P_1 \tilde{D}_1 H_2 P_2 D_2, \tag{14}$$

where it is transparent that H_1, H_2 are equivalent iff the points $H_1\mathrm{C}_n, H_2\mathrm{C}_n \in \mathscr{V}(e)$ lie in the same C_n-orbit. Therefore, the classification of complex Hadamard matrices is equivalent to the classification of MUB pairs.

We now state and prove a generalization of this idea. First, recall from Section 2.3 that the stabilizer of $q_i = U_i\mathrm{C}_n$ is $\mathrm{U}(n)_{q_i} = U_i \mathrm{C}_n U_i^\dagger$. We define the *simultaneous stabilizer* of $q_1, \ldots, q_k \in \mathscr{M}_n$ as the intersection $\mathrm{U}(n)_{q_1,\ldots,q_k} := \bigcap_{i=1}^k \mathrm{U}(n)_{q_i}$. As a subgroup of $\mathrm{U}(n)$, the simultaneous stabilizer acts on $\mathscr{M}_n$ (the restriction of the $\mathrm{U}(n)$-action (7)). The following theorem characterizes equivalent MUB lists via orbits of this action.

Theorem 4. *If $(q_1, \ldots, q_{k-1})$ is a MUB list, then $\mathscr{N}(q_1, \ldots, q_{k-1})$ is closed under the action of the simultaneous stabilizer $\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$. Moreover, for any $p, r \in \mathscr{N}(q_1, \ldots, q_{k-1})$, the* *two MUB lists* $(q_1,\ldots,q_{k-1},p)$ *and* $(q_1,\ldots,q_{k-1},r)$ *are equivalent iff* p *and* r *belong to the same* $\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$*-orbit in* $\mathscr{N}(q_1,\ldots,q_{k-1})$.

Proof. First, recall from Section 2.3 that $\mathscr{V}(q_i)$ is closed under the action of $\mathrm{U}(n)_{q_i}$. This implies the intersection $\mathscr{N}(q_1,\ldots,q_{k-1}) = \bigcap_{i=1}^{k-1}\mathscr{V}(q_i)$ is preserved by each stabilizer $\mathrm{U}(n)_{q_i}$, hence by $\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$. Thus, indeed there is a well-defined $\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$-action on $\mathscr{N}(q_1,\ldots,q_{k-1})$.

By definition, the two lists $(q_1,\ldots,q_{k-1},p)$ and $(q_1,\ldots,q_{k-1},r)$ are equivalent iff there exists a unitary U that satisfies both conditions:

- $U\cdot q_i = q_i$ for all $1\le i\le k-1$;
- $U\cdot p = r$.

U obeys the first condition iff it stabilizes all q_i, which occurs iff $U\in\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$. By the definition of orbit, there exists an element $U\in\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$ that maps p to r iff these two points belong to the same $\mathrm{U}(n)_{q_1,\ldots,q_{k-1}}$-orbit. This completes the proof. □

In the context of our procedure, the above theorem completely characterizes the inequivalent choices for the kth basis.

Remark. Our theorem characterizes ordered MUB lists. However, when considering *MUB sets*, the order of MUBs should be irrelevant. Therefore, two inequivalent MUB lists may correspond to equivalent MUB sets; this can occur, for example, if one is obtained from the other by reordering.

3.2 The orbit structure of $\mathscr{N}(q_1,\ldots,q_k)$

As pointed out earlier, the subsets $\mathscr{N}(q_1,\ldots,q_k)$ may fail to be submanifolds of $\mathscr{M}_n$. This fact poses difficulties in analyzing our procedure; otherwise, we could have hoped to compute the dimension of every $\mathscr{N}(q_1,\ldots,q_k)$, and use this data to find the maximal number of steps (hence the maximal MUB set). But if $\mathscr{N}(q_1,\ldots,q_k)$ is not a differentiable manifold (i.e. it is singular), then its dimension is not even well-defined. In this subsection, we study the decomposition of $\mathscr{N}(q_1,\ldots,q_k)$ into $\mathrm{U}(n)_{q_1,\ldots,q_k}$-orbits, where $\mathrm{U}(n)_{q_1,\ldots,q_k}$ is the simultaneous stabilizer defined in Section 3.1. We show that this decomposition corresponds to a *stratification* of $\mathscr{N}(q_1,\ldots,q_k)$. We start with the familiar case of $k=1$, corresponding to the classification of complex Hadamard matrices. Then we mention the general case. As our theorem suggests, an explicit description of the stratification in the general case can be used to simplify the construction of MUB lists.

We start with the simplest case: $k=1$ and $q_1=e$ is the standard basis; so $\mathscr{N}(q_1)=\mathscr{V}(e)$. For some values of n (e.g. $2,3,5$), *all* complex Hadamard matrices are equivalent; that is, the C_n action on $\mathscr{V}(e)$ is transitive, thus making it a homogeneous C_n-space. More generally, $\mathscr{V}(e)$ decomposes as a disjoint union of double cosets:

$$\mathscr{V}(e)=\bigsqcup_{i\in\mathscr{I}}\left(\mathrm{C}_nH_i\mathrm{C}_n\right)/\mathrm{C}_n, \tag{15}$$

where the quotient should be understood as referring only to the right C_n factor. Another way of writing this down is:

$$\mathscr{V}(e)=\bigsqcup_{i\in\mathscr{I}}\mathrm{C}_n\cdot q_i, \tag{16}$$

where each element in the disjoint union is the orbit (under the left C_n action) of the point $q_i:=H_i\mathrm{C}_n\in\mathscr{V}(e)$. Each H_i is a representative of a double coset, or equivalently – a representative of an equivalence class of complex Hadamard matrices. Hence, finding the partition (16) is the same as classifying the $n\times n$ complex Hadamard matrices up to equivalence. The set $\mathscr{I}$ can be quite general: for $n\in\{2,3,5\}$ it is a single point; but generally, it may be a union of isolated points and families parameterized by multiple real coordinates. This classification problem is unsolved for $n\geq 6$ [38, 39]. Note that it would be good to have a canonical choice for the representative H_i of an arbitrary double coset. We can always choose H_i to be *dephased*, i.e. with all entries in the first row and first column equal 1. However, we still have the freedom to reorder the $n-1$ last rows and columns. Hence, there is more than one dephased representative in each double coset – but there is only a finite number of those.

Recall that $\mathscr{M}_n$ is a homogeneous space, so there is nothing special about the standard basis $e = \mathbb{1}\mathrm{C}_n$. For any $q = U\mathrm{C}_n \in \mathscr{M}_n$ we have an equivalent decomposition:

$$\mathscr{V}(q) = U \cdot \mathscr{V}(e) = \bigsqcup_{i\in\mathscr{I}} \left(U\mathrm{C}_n U^\dagger\right) \cdot (U \cdot q_i), \tag{17}$$

where $U \cdot q_i = UH_i\mathrm{C}_n$. Note that the orbits now correspond to the left action of $U\mathrm{C}_n U^\dagger$ (the stabilizer of q). Recall a unitary matrix V represents a $U\mathrm{C}_n$-unbiased basis iff $H = U^\dagger V$ is a complex Hadamard matrix; thus, UH indeed represents a point in $\mathscr{V}(q)$ (where H is an arbitrary Hadamard matrix).

$\mathscr{V}(q)$ is a stratified space, with the stratification given by (17). Each component of (17) is an orbit of the compact Lie group $\left(U\mathrm{C}_n U^\dagger\right)$, acting smoothly on the smooth manifold $\mathscr{M}_n$. This ensures that every component is an embedded closed submanifold. By the same arguments, the $\mathrm{U}(n)_{q_1,\ldots,q_k}$-orbits define a stratification of $\mathscr{N}(q_1,\ldots,q_k)$.

We now show that for $k > 1$, the $\mathrm{U}(n)_{q_1,\ldots,q_k}$-orbits are all discrete. We start with the following proposition:

Proposition 5. *For any complex Hadamard matrix H, the connected component of $\mathrm{C}_n \cap H\mathrm{C}_n H^\dagger$ that contains the identity is $Z(\mathrm{U}(n)) \cong \mathrm{U}(1)$, i.e. the center of $\mathrm{U}(n)$, comprising precisely the scalar unitary matrices.*

Proof. As we have already noted, C_n has $n!$ connected components, and the connected component of the identity is the torus T^n. Similarly, the connected component of the identity of $H\mathrm{C}_n H^\dagger$ is the conjugated torus $H\mathrm{T}^n H^\dagger$. Thus, the connected component of the identity in the intersection $\mathrm{C}_n \cap H\mathrm{C}_n H^\dagger$ is $\mathrm{T}^n \cap H\mathrm{T}^n H^\dagger$, which we now show to equal $Z(\mathrm{U}(n))$.

Note that $A \in \mathrm{T}^n \cap H\mathrm{T}^n H^\dagger$ iff both A and $H^\dagger A H$ are diagonal unitary matrices. For all $1 \le i \le n$ and any diagonal A, we have:

$$\left[H^\dagger A H\right]_{ii} = \sum_{j=1}^{n} \left[H^\dagger\right]_{ij} [AH]_{ji} = \sum_{j=1}^{n} h_{ji}^* a_{jj} h_{ji} = \sum_{j=1}^{n} \left|h_{ji}\right|^2 a_{jj} = \sum_{j=1}^{n} \frac{1}{n} a_{jj} =$$

$$= \frac{1}{n} \mathrm{Tr}\left(A\right), \tag{18}$$

where we have used the fact the H is a complex Hadamard matrix, hence $\left|h_{ji}\right|^2 = \frac{1}{n}$ for all i, j. Thus, the diagonal entries of $H^\dagger AH$ are all equal, implying that A and $H^\dagger AH$ are both diagonal iff $H^\dagger AH$ is a scalar matrix, which of course implies that $H^\dagger AH = A$. □

Note the proof has the following corollary:

$$\mathrm{Core}_{\mathrm{U}(n)}\left(\mathrm{T}^n\right) := \bigcap_{V \in \mathrm{U}(n)} V\mathrm{T}^n V^\dagger = Z\left(\mathrm{U}\left(n\right)\right), \tag{19}$$

where $\mathrm{Core}_{\mathrm{U}(n)}\left(\mathrm{T}^n\right)$ is the largest subgroup of T^n which is normal in $\mathrm{U}\left(n\right)$. The intersection $\bigcap_{V\in\mathrm{U}(n)} V\mathrm{T}^n V^\dagger$ over *all* unitaries V equals the intersection $\mathrm{T}^n \cap H\mathrm{T}^n H^\dagger$, for any Hadamard matrix H. Intuitively, this indicates that Hadamard matrices are the strongest obstructions for T^n being normal (in $\mathrm{U}\left(n\right)$). We also note that the normalizer of T^n is C_n, the monomial matrices. In contrast, Hadamard matrices are the least monomial unitaries, in the sense that all entries have the same absolute value.

Now, consider a MUB pair $\left(e, q\right) = \left(\mathbb{1}\mathrm{C}_n, H\mathrm{C}_n\right)$ where H is a Hadamard matrix (by Lemma 3, any MUB pair is equivalent to one of this form). We would like to show that the $\mathrm{U}\left(n\right)_{e,q}$-orbits in $\mathscr{N}\left(e,q\right)$ are discrete. Any such orbit is diffeomorphic to the quotient $\mathrm{U}\left(n\right)_{e,q} / \mathrm{U}\left(n\right)_{e,q,p}$ for $p \in \mathscr{N}\left(e,q\right)$. Recalling $\mathrm{U}\left(n\right)_{e,q} = \mathrm{C}_n \cap H\mathrm{C}_n H^\dagger$, the above proposition implies that $\mathrm{U}\left(n\right)_{e,q} / Z\left(\mathrm{U}\left(n\right)\right)$ is a finite group ($\mathrm{U}\left(n\right)_{e,q}$ has finitely many connected components since the same holds for C_n and $H\mathrm{C}_n H^\dagger$). By the discussion above, the center is contained in *every* stabilizer, hence $\mathrm{U}\left(n\right)_{e,q,p} \supseteq Z\left(\mathrm{U}\left(n\right)\right)$. Therefore, the orbit $\mathrm{U}\left(n\right)_{e,q} / \mathrm{U}\left(n\right)_{e,q,p}$ is contained in the aforementioned finite group. The same reasoning holds for the $\mathrm{U}\left(n\right)_{q_1,\ldots,q_k}$-orbits of $\mathscr{N}\left(q_1, \ldots, q_k\right)$, for any $k > 1$.

Remark. Since the center $Z\left(\mathrm{U}\left(n\right)\right)$ is the intersection of all stabilizers $\mathrm{U}\left(n\right)_p$, the $\mathrm{U}\left(n\right)$-action on $\mathscr{M}_n$ induces a faithful $\mathrm{PU}\left(n\right)$-action on $\mathscr{M}_n$, where $\mathrm{PU}\left(n\right) := \mathrm{U}\left(n\right) / Z\left(\mathrm{U}\left(n\right)\right)$.

4 Application: new equivalences of MUB triples in dimension $n = 4$

In this section, we apply our results in dimension $n = 4$. For a fixed MUB pair (e, f_0), we decompose $\mathscr{N}(e, f_0)$ into $\mathrm{U}(n)_{e,f_0}$-orbits and discover new equivalences between MUB triples. We begin by rephrasing known results via our geometric perspective, and then provide a detailed explanation of a general method for computing $\mathrm{U}(n)_{e,f_0}$ and its orbits.

In dimension 4, the classification of complex Hadamard matrices is known [31]. Every 4×4 Hadamard matrix is equivalent to one of the following form:

$$F_4(x) = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & ie^{ix} & -ie^{ix} \\ 1 & -1 & -ie^{ix} & ie^{ix} \end{pmatrix}, \quad x \in [0, \pi]. \tag{20}$$

Let us recast this fact in our terms: the set of 4×4 complex Hadamard matrices is $\bigsqcup_{x \in [0,\pi]} \mathrm{C}_4 F_4(x) \mathrm{C}_4$, where $\mathrm{C}_4 F_4(x) \mathrm{C}_4$ is the double coset of $F_4(x)$ under the two C_4-actions (left and right multiplication). Equivalently, the subset $\mathscr{V}(e) \subseteq \mathscr{M}_4$ has the following decomposition into orbits of the left C_4-action:

$$\mathscr{V}(e) \cong \bigsqcup_{x \in [0,\pi]} \mathrm{C}_4 \cdot f_x, \quad f_x := F_4(x) \mathrm{C}_4, \tag{21}$$

so in this case the index set $\mathscr{I}$ from (16) is the interval $[0, \pi]$, and the representative H_x is denoted $F_4(x)$.

Now, consider the MUB pair (e,f_0), where $f_0 = F_4(0)\mathrm{C}_4$. From [31], the only dephased unitary matrices which are mutually-unbiased to both $\mathbb{1}$ and $F_4(0)$ are of the form:

$$H_4(y,z) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -e^{iy} & e^{iy} & e^{iz} & -e^{iz} \\ e^{iy} & -e^{iy} & e^{iz} & -e^{iz} \end{pmatrix}, \quad y,z \in [0,\pi). \tag{22}$$

For each y,z we obtain a distinct coset $h_{y,z} := H_4\mathrm{C}_4(y,z)$, hence $\mathscr{N}(e,f_0) = \{h_{y,z} \mid y,z \in [0,\pi)\}$. We would like to know which (if any) of the MUB triples $(e,f_0,h_{y,z})$ are equivalent. By Theorem 4, $h_{y,z}$ and $h_{y',z'}$ yield equivalent MUB triples iff they lie in the same orbit of the group $\tilde{G} := \mathrm{C}_4 \cap F_4(0)\mathrm{C}_4F_4(0)^\dagger$. By Proposition 5 we know that $G := \tilde{G}/Z(\mathrm{U}(n))$ is a finite group, and by the above remark, it suffices to characterize $\mathscr{N}(e,f_0)$ up to G-orbits. We compute G explicitly via the following procedure. For $\rho \in \mathrm{S}_4$, let C_4^ρ denote the corresponding connected component of C_4, i.e.,

$$\mathrm{C}_4^\rho := \left\{U \in \mathrm{U}(4) \mid U_{ij} = 0 \quad \forall i,j \text{ s.t. } j \neq \rho(i)\right\}. \tag{23}$$

If $U \in \tilde{G}$, there exist $\rho,\sigma \in \mathrm{S}_4$ such that $U \in \mathrm{C}_4^\rho$ and $F_4(0)^\dagger UF_4(0) \in \mathrm{C}_4^\sigma$. Let $u_i := U_{i,\rho(i)}$ denote the nonzero entries of U. Since $F_4(0)^\dagger UF_4(0) \in \mathrm{C}_4^\sigma$, we obtain from (23) the following homogeneous linear equations for u_i:

$$\begin{aligned} & \left[F_4(0)^\dagger UF_4(0)\right]_{kl} = 0 && \forall k,l \text{ s.t. } l \neq \sigma(k) \\ \Leftrightarrow \quad & \sum_{m=1}^{4}\left[F_4(0)^\dagger\right]_{j,\rho^{-1}(m)}\left[F_4(0)\right]_{m,l} u_{\rho^{-1}(m)} = 0 && \forall k,l \text{ s.t. } l \neq \sigma(k). \end{aligned} \tag{24}$$

It is straightforward to go over all pairs $\rho,\sigma \in \mathrm{S}_4$ and seek all nontrivial solutions to this system of equations. The solution space turns out either trivial or one-dimensional; and in one-dimensional cases the u_i always have equal modulus, and by normalizing we obtain a unique element of G. It turns out that only 8 out of the 24 permutations participate in nontrivial intersections; out of those 8 permutations, each one intersects 4 (including itself); thus, $|G| = 32$. Moreover, G is given by a semidirect product $G \cong B \ltimes \mathbb{Z}_4$, where $B \subseteq \mathrm{S}_4$ is given by:

$$B := \{\mathrm{id}, (12), (34), (12)(34), (13)(24), (1324), (1423), (14)(23)\}, \tag{25}$$

and is generated by (12), (34) and $(13)(24)$. $\mathbb{Z}_4$ is realized by diagonal matrices $D_a \in \mathrm{T}^4$. The diagonal entries of each D_a are given by another row of $F_4(0)$:

$$D_0 = \mathbb{1}, \quad D_1 = \mathrm{diag}\begin{pmatrix} 1 \\ -1 \\ i \\ -i \end{pmatrix}, \quad D_2 = \mathrm{diag}\begin{pmatrix} 1 \\ 1 \\ -1 \\ -1 \end{pmatrix}, \quad D_3 = \mathrm{diag}\begin{pmatrix} 1 \\ -1 \\ -i \\ i \end{pmatrix}. \tag{26}$$

One easily verifies that $D_a D_b = D_{a+b \bmod 4}$. Letting R_π denote the permutation matrix corresponding to $\pi \in B$, we can provide a complete description of G: all products $R_\pi D_a$, up to a scalar matrix $e^{i\theta}\mathbb{1} \in \mathrm{Z}(\mathrm{U}(n))$. Equivalently, the matrices $R_\pi D_a$ form a *projective representation* of G; for example, $D_1 R_{(13)(24)} D_1 = i R_{(13)(24)}$ (we shall use this fact later).

Now we can compute all the left actions $R_\pi D_a \cdot h_{y,z}$, and test whether any two distinct $h_{y,z}$ are in the same G-orbit. Starting with $\mathbb{Z}_4$, we find:

$$D_1 H_4(y,z) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -ie^{iy} & ie^{iy} & ie^{iz} & -ie^{iz} \\ -ie^{iy} & ie^{iy} & -ie^{iz} & ie^{iz} \end{pmatrix}. \tag{27}$$

This matrix is not in the form of the canonical representative (22), but we can bring it to this form using the *right* C_n-action; and since the first row is already dephased, we need only consider column permutations. To get the second row in the correct form we must swap the first two columns with the second two, but how do we know which way to do it? Note that $[H_4(y,z)]_{32}$ is either 1, or has strictly positive imaginary part. If $0 \leq z < \frac{\pi}{2}$, then $ie^{iz} = e^{i\left(z+\frac{\pi}{2}\right)}$ obeys this condition; otherwise, $-ie^{iz} = e^{i\left(z-\frac{\pi}{2}\right)}$ obeys this condition. An analogous statement holds for $\pm ie^{iy}$, based on the range of y. Denote:

$$y' := \begin{cases} z+\frac{\pi}{2}; & 0 \leq z < \frac{\pi}{2} \\ z-\frac{\pi}{2}; & \frac{\pi}{2} < z < \pi \end{cases}, \quad z' := \begin{cases} y+\frac{\pi}{2}; & 0 \leq y < \frac{\pi}{2} \\ y-\frac{\pi}{2}; & \frac{\pi}{2} < y < \pi \end{cases}. \tag{28}$$

By choosing a column permutation suitable to the ranges of y,z, we obtain a matrix $H_4(y',z')$. Thus, we have found $D_1 \cdot h_{y,z} = h_{z+\frac{\pi}{2} \bmod \pi,\, y+\frac{\pi}{2} \bmod \pi}$. Moving forward, we find:

$$D_2 H_4(y,z) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ e^{iy} & -e^{iy} & -e^{iz} & e^{iz} \\ -e^{iy} & e^{iy} & -e^{iz} & e^{iz} \end{pmatrix} \xrightarrow{c_1 \leftrightarrow c_2, c_3 \leftrightarrow c_4} H_4(y,z), \tag{29}$$

by which we mean that after swapping the first column with second and the third column with the fourth, we obtain the matrix $H_4(y,z)$ again. Thus, D_2 stabilizes $H_4(y,z)$ for all y,z; hence $D_2 \in \mathrm{U}(n)_{e,f_0,h_{y,z}}$. Since $D_3 = D_1 D_2$, we already know that the action of D_3 would be the same as that of D_1.

Now we can proceed to examine the action of B on $\mathcal{N}(e, f_0)$. We have:

$$R_{(12)}H_4(y,z) = \frac{1}{2}\begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & 1 & 1 & 1 \\ -e^{iy} & e^{iy} & e^{iz} & -e^{iz} \\ e^{iy} & -e^{iy} & e^{iz} & -e^{iz} \end{pmatrix} \xrightarrow{\text{dephasing}} \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -e^{iy} & e^{iy} & -e^{iz} & e^{iz} \\ e^{iy} & -e^{iy} & -e^{iz} & e^{iz} \end{pmatrix}, \tag{30}$$

where the dephasing step multiplies the two rightmost columns by -1. By swapping the third and fourth columns of the matrix we obtained above, we get $H_4(y,z)$; hence, $R_{(12)}$ is in the stabilizer. We can similarly verify that $R_{(34)}$ belongs to the stabilizer as well. Finally, we should examine the action of $R_{(13)(24)}$; for the sake of convenience, we first consider $R_{(13)(24)}D_1$:

$$R_{(13)(24)}D_1H_4(y,z) \xrightarrow{\text{dephasing}} \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ ie^{-iy} & -ie^{-iy} & -ie^{-iz} & ie^{-iz} \\ -ie^{-iy} & ie^{-iy} & -ie^{-iz} & ie^{-iz} \end{pmatrix}. \tag{31}$$

Recall we want the entry in the third row and first column to be either -1 or have negative imaginary part, and note that $ie^{-iy} = e^{i\left(\frac{\pi}{2}-y\right)} = -e^{i\left(\frac{3\pi}{2}-y\right)}$. Thus, if $\frac{\pi}{2} < y < \pi$ this condition is satisfied, and we can define $y' = \frac{3\pi}{2} - y$; otherwise we should swap the first two columns and define $y' = \frac{\pi}{2} - y$. Applying the same logic for z, we find that $R_{(13)(24)}D_1 \cdot h_{y,z} = h_{\left(\frac{3\pi}{2}-y\right)\bmod\pi,\ \left(\frac{3\pi}{2}-z\right)\bmod\pi}$.

To summarize, we computed the $\mathrm{U}(n)_{e,f_0}$-action on $h_{y,z} \in \mathcal{N}(e, f_0)$, which is equivalent to the G-action (by the remark at the end of Section 3.2). For each y,z, we found that the stabilizer $G_{h_{y,z}}$ of $h_{y,z}$ is generated by D_2, $R_{(12)}$ and $R_{(34)}$. These are commuting elements of order two, hence $G_{h_{y,z}} \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. The orbit of $h_{y,z}$ under G is diffeomorphic to $G/G_{h_{y,z}}$;

thus, it has four elements:

$$
\begin{aligned}
\mathbb{1} \cdot h_{y,z} &= h_{y,z}, \\
D_1 \cdot h_{y,z} &= h_{\left(z+\frac{\pi}{2}\right) \operatorname{mod} \pi,\ \left(y+\frac{\pi}{2}\right) \operatorname{mod} \pi}, \\
R_{(13)(24)} D_1 \cdot h_{y,z} &= h_{\left(\frac{3\pi}{2}-y\right) \operatorname{mod} \pi,\ \left(\frac{3\pi}{2}-z\right) \operatorname{mod} \pi}, \\
R_{(13)(24)} \cdot h_{y,z} &= h_{(\pi-z) \operatorname{mod} \pi,\ (\pi-y) \operatorname{mod} \pi}.
\end{aligned}
\tag{32}
$$

To compute $R_{(13)(24)} \cdot h_{y,z}$ we used the fact $D_1 R_{(13)(24)} D_1 = i R_{(13)(24)}$, which implies that $R_{(13)(24)} \cdot h_{y,z} = D_1 \cdot \left(R_{(13)(24)} D_1 \cdot h_{y,z}\right)$.

Thus, we have established the following:

Proposition 6. *The MUB triples $(e, f_0, h_{y,z})$ and $\left(e, f_0, h_{y',z'}\right)$ are equivalent (in the sense of Definition 2) if and only if one of the following holds:*

- $y' = y$ *and* $z' = z$;
- $y' = \left(z + \frac{\pi}{2}\right) \operatorname{mod} \pi$ *and* $z' = \left(y + \frac{\pi}{2}\right) \operatorname{mod} \pi$;
- $y' = \left(\frac{3\pi}{2} - y\right) \operatorname{mod} \pi$ *and* $z' = \left(\frac{3\pi}{2} - z\right) \operatorname{mod} \pi$;
- $y' = (\pi - z) \operatorname{mod} \pi$ *and* $z' = (\pi - y) \operatorname{mod} \pi$.

Proof. The proposition follows from Theorem 4, combined with our computation of the $\mathrm{U}(n)_{e,f_0}$-orbit of $h_{y,z}$. □

These equivalences were hitherto unknown (to our knowledge), and reduce the parameter space by a factor of 4.

Note that the method we used in this section can be executed for any value of n. Moreover, we can classify MUB quadruples, quintuples etc. In fact, in the process of classifying MUB triples we already computed the simultaneous stabilizer $U_{e,f_0,h_{y,z}}$ of a triple, which shall be required to classify quadruples. This is a general feature: when finding the $\mathscr{U}(n)_{q_1,\ldots,q_{k-1}}$-orbit of a point $p \in \mathscr{N}(q_1, \ldots, q_{k-1})$, we compute the stabilizer $\mathscr{U}(n)_{q_1,\ldots,q_{k-1},p}$.

5 Conclusion

In this paper, we considered the task of constructing an ordered list of mutually unbiased bases. We introduced a geometric formulation of this task. To do so, we defined a manifold endowed with a metric and an isometric action of the unitary group. The points of the manifold correspond to orthonormal bases, and the geometric structure captures the notions of mutual-unbiasedness and equivalence. We outlined a procedure for constructing MUB lists, where on the kth step one chooses a new basis, unbiased to all previously-chosen bases. We proved a theorem that characterizes in geometric terms choices that yield equivalent MUB lists.

Our results shed new light on the connection between mutually unbiased bases and complex Hadamard matrices. Our theorem explains the significance of classifying Hadamard matrices to the study of MUBs, and demonstrates that this classification is a special case of a more general decomposition. Moreover, we can reformulate the existence problem of mutually unbiased bases in geometric terms: a set of m MUBs exists in dimension n, iff there exist points $q_1,\ldots,q_m \in \mathscr{M}_n$ such that $\forall i,\ q_i \in \mathscr{N}(q_1,\ldots,q_{i-1})$. Our geometric perspective clarifies existing classifications of mutually unbiased bases, and also generates new ones. It may help to (i) shrink parameter spaces dramatically, (ii) make full numerical MUB searches feasible, and (iii) unify scattered Hadamard families.

There are several promising directions in which our results could be extended. Recall that we have only considered (ordered) MUB lists; however, for many applications of MUBs, two MUB lists with the same elements appearing in a different order would be considered equivalent. Thus, future work may seek to generalize our results and characterize (unordered) MUB sets up to equivalence.

Our results may also open up the possibility of applying additional mathematical tools to the existence problem of MUBs. Indeed, the spaces we have defined are endowed with a rich geometric structure, of which we only utilized very little. Smooth manifolds with compact Lie group actions have a rich theory, which may allow for a systematic study of the stratification of

$\mathscr{N}(q_1,\ldots,q_{i-1})$. In particular, the geometric formulation may assist with the classification of Hadamard matrices in dimension $n=6$, where it is still open. We also note that $\mathscr{M}_n$ is closely related to the complete flag manifold $\tilde{\mathscr{M}}_n$, which has important applications in representation theory. By the Borel-Weil theorem, each irreducible representation of $\mathrm{U}(n)$ is given as the space of global sections of a certain holomorphic line bundle on $\tilde{\mathscr{M}}_n$. In contrast, our $\mathscr{M}_n$ is naturally equipped with a *real* vector bundle of rank $n-1$. The cohomology groups (actually real vector spaces) of this vector bundle furnish representations of $\mathrm{U}(n)$. There may be an unexplored connection between these representations, and those realized on the line bundles on $\mathrm{U}(n)$. Moreover, $\tilde{\mathscr{M}}_n$ is a Kähler manifold, while $\mathscr{M}_n$ inherits a Riemannian metric via its embedding in the real Grassmannian $\mathrm{Gr}(n-1,\mathfrak{su}(n))$. Curiously, the chordal distance on $\mathscr{M}_n$ (also inherited from the Grassmannian) seems to be more directly pertinent to the problem of MUBs, compared to the richer geometric structures of the vector bundle and Riemannian metric. Future work may wish to seek connections between all of these structures and MUBs. Finally, note the decomposition (15) of $\mathscr{V}(q)$ into double cosets holds a striking resemblance to the *Bruhat decomposition* of $\mathscr{M}_n$. These facts may hint towards the possibility of applying further representation-theoretic tools to study the geometric problems presented in this paper.

Acknowledgements. We are grateful to Leonid Polterovich, Boris Kunyavskii, Joseph Bernstein and Mikhail Katz for helpful discussions.

Declarations

Funding. This work was partially supported by the European Union's Horizon Europe research and innovation programme under grant agreement No. 101178170 and by the Israel Science Foundation under grant agreement No. 2208/24.

Competing interests. The authors have no relevant financial or non-financial interests to disclose.

Ethics approval. Not applicable.

Consent for publication. Not applicable.

Data availability. No datasets were generated or analysed during the current study.

Materials availability. Not applicable.

Code availability. The code used in this study is publicly available at https://github.com/smitke6/Equivalent-MUB-lists.

Author contributions. Both authors contributed to conceiving the project. The proofs and computations were performed by Amit Te'eni. The manuscript was written by Amit Te'eni with comments and edits provided by Eliahu Cohen.

References

[1] Wootters, W.K., Fields, B.D.: Optimal state-determination by mutually unbiased measurements. Ann. Phys. **191**(2), 363–381 (1989) https://doi.org/10.1016/0003-4916(89)90322-9

[2] Ivonovic, I.D.: Geometrical description of quantal state determination. J. Phys. A: Math. Gen. **14**(12), 3241 (1981) https://doi.org/10.1088/0305-4470/14/12/019

[3] Adamson, R.B.A., Steinberg, A.M.: Improving quantum state estimation with mutually unbiased bases. Phys. Rev. Lett. **105**, 030406 (2010) https://doi.org/10.1103/PhysRevLett.105.030406

[4] Ekert, A.K.: Quantum cryptography based on bell's theorem. Phys. Rev. Lett. **67**, 661–663 (1991) https://doi.org/10.1103/PhysRevLett.67.661

[5] Bruß, D.: Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett. **81**, 3018–3021 (1998) https://doi.org/10.1103/PhysRevLett.81.3018

[6] Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Security of quantum key distribution using d-level systems. Phys. Rev. Lett. **88**, 127902 (2002) https://doi.org/10.1103/PhysRevLett.88.127902

[7] Scarani, V., Acín, A., Ribordy, G., Gisin, N.: Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations. Phys. Rev. Lett. **92**, 057901 (2004) https://doi.org/10.1103/PhysRevLett.92.057901

[8] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. **81**, 1301–1350 (2009) https://doi.org/10.1103/RevModPhys.81.1301

[9] Pirandola, S., Andersen, U.L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., *et al.*: Advances in quantum cryptography. Adv. Opt. Photon. **12**(4), 1012–1236 (2020) https://doi.org/10.1364/AOP.361502

[10] Ashkenazy, A., Idan, Y., Korn, D., Fixler, D., Dayan, B., Cohen, E.: Photon number splitting attack–proposal and analysis of an experimental scheme. Adv. Quantum Technol. **7**(7), 2300437 (2024) https://doi.org/10.1002/qute.202300437

[11] Casaccino, A., Galvão, E.F., Severini, S.: Extrema of discrete Wigner functions and applications. Phys. Rev. A **78**, 022310 (2008) https://doi.org/10.1103/PhysRevA.78.022310

[12] Tavakoli, A., Hameedi, A., Marques, B., Bourennane, M.: Quantum random access codes using single d-level systems. Phys. Rev. Lett. **114**, 170502 (2015) https://doi.org/10.1103/PhysRevLett.114.170502

[13] Huszár, F., Houlsby, N.M.T.: Adaptive bayesian quantum tomography. Phys. Rev. A **85**, 052120 (2012) https://doi.org/10.1103/PhysRevA.85.052120

[14] Lima, G., Neves, L., Guzmán, R., Gómez, E.S., Nogueira, W.A.T., Delgado, A., Vargas, A., Saavedra, C.: Experimental quantum tomography of photonic qudits via mutually unbiased basis. Opt. Express **19**(4), 3542–3552 (2011) https://doi.org/10.1364/OE.19.003542

[15] Liu, S., Mu, L.-Z., Fan, H.: Entropic uncertainty relations for multiple measurements. Phys. Rev. A **91**, 042133 (2015) https://doi.org/10.1103/PhysRevA.91.042133

[16] Xie, B.-F., Ming, F., Wang, D., Ye, L., Chen, J.-L.: Optimized entropic uncertainty relations for multiple measurements. Phys. Rev. A **104**, 062204 (2021) https://doi.org/10.1103/PhysRevA.104.062204

[17] Rastegin, A.E.: Uncertainty relations for mubs and sic-povms in terms of generalized entropies. Eur. Phys. J. D **67**(12), 269 (2013) https://doi.org/10.1140/epjd/e2013-40453-2

[18] Wu, S., Yu, S., Mølmer, K.: Entropic uncertainty relation for mutually unbiased bases. Phys. Rev. A **79**, 022104 (2009) https://doi.org/10.1103/PhysRevA.79.022104

[19] Spengler, C., Huber, M., Brierley, S., Adaktylos, T., Hiesmayr, B.C.: Entanglement detection via mutually unbiased bases. Phys. Rev. A **86**, 022311 (2012) https://doi.org/10.1103/PhysRevA.86.022311

[20] Tavakoli, A., Farkas, M., Rosset, D., Bancal, J.-D., Kaniewski, J.: Mutually unbiased bases and symmetric informationally complete measurements in bell experiments. Sci. Adv. **7**(7), 3847 (2021) https://doi.org/10.1126/sciadv.abc3847

[21] Hiesmayr, B., McNulty, D., Baek, S., Roy, S.S., Bae, J., Chruściński, D.: Detecting entanglement can be more effective with inequivalent mutually unbiased bases. New J. Phys. **23**(9), 093018 (2021) https://doi.org/10.1088/1367-2630/ac20ea

[22] Brierley, S., Weigert, S.: Constructing mutually unbiased bases in dimension six. Phys. Rev. A **79**(5), 052316 (2009) https://doi.org/10.1103/PhysRevA.79.052316

[23] Weiner, M.: A gap for the maximum number of mutually unbiased bases. Proc. Am. Math. Soc. **141**(6), 1963–1969 (2013) https://doi.org/10.1090/S0002-9939-2013-11487-5

[24] Horodecki, P., Rudnicki, Ł., Życzkowski, K.: Five open problems in quantum information theory. PRX Quantum **3**, 010101 (2022) https://doi.org/10.1103/PRXQuantum.3.010101

[25] McNulty, D., Weigert, S.: Mutually unbiased bases in composite dimensions – a review. arXiv:2410.23997 (2024) https://doi.org/10.48550/arXiv.2410.23997

[26] Planat, M., Rosu, H.C., Perrine, S.: A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements. Found. Phys. **36**(11), 1662–1680 (2006) https://doi.org/10.1007/s10701-006-9079-3

[27] Bengtsson, I.: Three ways to look at mutually unbiased bases. AIP Conf. Proc. **889**(1), 40–51 (2007) https://doi.org/10.1063/1.2713445

[28] Bengtsson, I., Bruzda, W., Ericsson, Å., Larsson, J.-Å., Tadej, W., Życzkowski, K.: Mutually unbiased bases and hadamard matrices of order six. J. Math. Phys. **48**(5), 052106 (2007) https://doi.org/10.1063/1.2716990

[29] Boykin, P.O., Sitharam, M., Tiep, P.H., Wocjan, P.: Mutually unbiased bases and orthogonal decompositions of lie algebras. Quantum Info. Comput. **7**(4), 371–382 (2007) https://doi.org/10.5555/2011725.2011731

[30] Brierley, S.: Mutually unbiased bases in low dimensions. PhD thesis, University of York (2009). https://etheses.whiterose.ac.uk/id/eprint/587/1/BrierleyThesis09.pdf

[31] Brierley, S., Weigert, S., Bengtsson, I.: All mutually unbiased bases in dimensions two to five. arXiv:0907.4097 (2009) https://doi.org/10.48550/arXiv.0907.4097

[32] Godsil, C., Roy, A.: Equiangular lines, mutually unbiased bases, and spin models. Eur. J. Comb. **30**(1), 246–262 (2009) https://doi.org/10.1016/j.ejc.2008.01.002

[33] Durt, T., Englert, B.-G., Bengtsson, I., Życzkowski, K.: On mutually unbiased bases. Int. J. Quantum Inf. **08**(04), 535–640 (2010) https://doi.org/10.1142/S0219749910006502

[34] Matolcsi, M., Matszangosz, Á.K., Varga, D., Weiner, M.: Triplets of mutually unbiased bases. arXiv:2503.14752 (2025) https://doi.org/10.48550/arXiv.2503.14752

[35] Yan, W.-Z., Li, Y., Hou, Z., Zhu, H., Xiang, G.-Y., Li, C.-F., Guo, G.-C.: Experimental demonstration of inequivalent mutually unbiased bases. Phys. Rev. Lett. **132**, 080202 (2024) https://doi.org/10.1103/PhysRevLett.132.080202

[36] Tirkkonen, O., Boyd, C., Vehkalahti, R.: Grassmannian codes from multiple families of mutually unbiased bases. In: 2017 IEEE International Symposium on Information Theory (ISIT), pp. 789–793 (2017). https://doi.org/10.1109/ISIT.2017.8006636

[37] Lee, J.M.: Introduction to Smooth Manifolds. Springer, New York, NY (2012). https://doi.org/10.1007/978-1-4419-9982-5

[38] Dita, P.: Some results on the parametrization of complex hadamard matrices. J. Phys. A: Math. Gen. **37**(20), 5355 (2004) https://doi.org/10.1088/0305-4470/37/20/008

[39] Tadej, W., Życzkowski, K.: A concise guide to complex hadamard matrices. Open Syst. Inf. Dyn. **13**(2), 133–177 (2006) https://doi.org/10.1007/s11080-006-8220-2