

1 UB vectors and continuous families of MUB

Consider a “time-dependent” orthonormed bases (ONB)

$$\mathcal{F}(t) = (\mathbf{f}_1(t), \dots, \mathbf{f}_n(t)). \quad (1)$$

More precisely, assume that $\mathcal{F}(t)$ is an ONB for all $t \in I$ (where for simplicity I is some open interval of \mathbb{R}) and that the map $t \mapsto \mathbf{f}_k(t)$ is smooth for all $k = 1, \dots, n$.

We shall say that $t \mapsto (\mathcal{E}, \mathcal{F}(t))$ is a **continuous family of MUB pair** if $\mathcal{E} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ is a (fixed) ONB such that \mathcal{E} and $\mathcal{F}(t)$ are MUB for all $t \in I$. The question we consider is the following: if we are given a vector \mathbf{b}_0 of unit length which is unbiased (UB) for both \mathcal{E} and $\mathcal{F}(t)$ at $t = 0$, then can we “continue” \mathbf{b}_0 and thus find common UB vectors for \mathcal{E} and $\mathcal{F}(t)$ for some $t \neq 0$?

Ultimately the existence of such continuation can be reduced to the existence of solution of a certain (ordinary) differential equation. Let us see now how. We are looking for a (differentiable) one-parameter family of unit-vectors $t \mapsto \mathbf{b}(t)$ such that $\mathbf{b}(0) = \mathbf{b}_0$ and $\mathbf{b}(t)$ is UB for both \mathcal{E} and $\mathcal{F}(t)$. Clearly, $t \mapsto \mathbf{b}(t)$ is such a family if and only if it is a solution of the system

$$\begin{cases} \frac{d}{dt} |\langle \mathbf{e}_k, \mathbf{b}(t) \rangle|^2 = \frac{d}{dt} |\langle \mathbf{f}_k(t), \mathbf{b}(t) \rangle|^2 = 0 & \text{for all } k = 1, \dots, n, \\ \mathbf{b}(0) = \mathbf{b}_0. \end{cases} \quad (2)$$

The problem with the above system is that it is *implicit*. Instead of having a formula for the derivative of $\mathbf{b}(t)$, we have expressions for the derivative of some *functions* of $\mathbf{b}(t)$. To apply the well-known results regarding the existence and uniqueness of solution of a differential equation, first we need to address the issue of invertibility of these implicit relations.

Actually, it is clear that we cannot completely invert these relations and thus derive the existence of a unique solution. Indeed, if $t \mapsto \mathbf{b}(t)$ is a solution of (2), then so is $t \mapsto e^{ir(t)} \mathbf{b}(t)$ where r is a real smooth function. However, as we shall see, under a certain condition, the “phase” of $\mathbf{b}(t)$ is the *only* ambiguity in the solution.

In order to understand this condition, consider the $n \times n$ complex matrix defined by the formula

$$M_{k,l} := \langle \mathbf{b}_0, \mathbf{e}_k \rangle \langle \mathbf{e}_k, \mathbf{f}_l \rangle \langle \mathbf{f}_l, \mathbf{b}_0 \rangle \quad (3)$$

where for shortness \mathbf{f}_l stands for $\mathbf{f}_l(0)$. Note that $M_{k,l}$ is independent of the phases of $\mathbf{e}_k, \mathbf{f}_l$ and \mathbf{b} (that is, it remains unchanged if we replace these vectors by unit length multiples of them) and that in fact

$$M_{k,l} = \text{Tr}(P_k Q_l R) \quad (4)$$

where P_k, Q_l and R are the orthogonal projections onto the one-dimensional spaces span by the vectors $\mathbf{e}_k, \mathbf{f}_l$ and \mathbf{b}_0 , respectively.

It is quite clear, that M is a Hadamard matrix: indeed, it is equivalent to the Hadamard matrix $(\langle \mathbf{e}_k, \mathbf{f}_l \rangle)_{(k,l=1,\dots,n)}$. In particular, it is unitary and so its rank is maximal. However, the *real* matrix N whose entries are obtained by taking the imaginary part of the entries of M ,

$$N_{k,l} := \text{Im}(M_{k,l}) = \frac{1}{i} \text{Tr}([P_k, Q_l]R) \quad (5)$$

cannot be of maximal rank. Indeed, for all $l = 1, \dots, n$,

$$\sum_k N_{k,l} = \sum_k \frac{1}{i} \text{Tr}([P_k, Q_l]R) = \frac{1}{i} \text{Tr}([\mathbb{1}, Q_l]R) = 0 \quad (6)$$

since $\sum_k P_k = \mathbb{1}$.

Theorem 1.1. *If $\text{rk}(N) = n - 1$ then there exists an $\epsilon > 0$ such that system (2) has a solution \mathbf{b} in the interval $(-\epsilon, \epsilon)$ and if $\tilde{\mathbf{b}}$ is another solution in $(-\epsilon, \epsilon)$ then $\tilde{\mathbf{b}}(t)$ is a (possibly t -dependent) multiple of $\mathbf{b}(t)$ for all $t \in (-\epsilon, \epsilon)$.*

Proof. N □

A common UB vector \mathbf{b} for the MUB pair $(\mathcal{E}, \mathcal{F})$ for which there exists an $\epsilon > 0$ such that if $\tilde{\mathbf{b}}$ is not a multiple of \mathbf{b} and is also a common UB vector for $(\mathcal{E}, \mathcal{F})$ then

$$\|\mathbf{b} - \tilde{\mathbf{b}}\| > \epsilon \quad (7)$$

will be called an **isolated UB vector**.

Theorem 1.2. *If $\text{rk}(N) = n - 1$ where N is the matrix defined by equations (3) and (5), then \mathbf{b} is an isolated common UB vector.*

Proof. Well.. □

Corollary 1.3. *Let $t \mapsto (\mathcal{E}, \mathcal{F}(t))$ be a continuous family of MUB pair such that at $t = 0$ for all common (normalized) UB vector \mathbf{b} the matrix N defined by (3) and (5) has rank equal to $n-1$. Then there exists a (finite) nonnegative integer k and an $\epsilon > 0$ such that up to multiples, $(\mathcal{E}, \mathcal{F}(t))$ has exactly k common normalized UB vectors for every $t \in (-\epsilon, \epsilon)$.*

Proof. Well.. □

2 The symmetry group of a MUB

When dealing with MUB pairs, we are not really interested in *bases*. If $\mathcal{E} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ and $\mathcal{F} = (\mathbf{f}_1, \dots, \mathbf{f}_n)$ are two ONB forming a MUB pair, then by “changing the phases” of the bases vectors (that is, multiplying them by complex numbers with unit absolute value) and changing the orders of the vectors in the individual bases they still remain two ONB forming a MUB pair. Of course we do not want to distinguish between the original and the thus obtained MUB pair, but formally we are dealing with different bases.

For the explained reason, from the abstract point of view, instead of an ONB $\mathcal{E} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$, it is better to consider the maximal abelian star algebra associated to \mathcal{E}

$$\mathcal{A}_{\mathcal{E}} := \text{Span}\{P_{\mathbf{e}_k} | k = 1, \dots, n\} \quad (8)$$

where $P_{\mathbf{e}_k}$ is the orthogonal projection onto $\mathbb{C}\mathbf{e}_k$, ($k = 1, \dots, n$). Indeed, $\mathcal{A}_{\mathcal{E}}$ is invariant under reordering and changing phases of the vectors in \mathcal{E} . Moreover, as is well known (and in any case: an exercise to show), $\mathcal{E} = (\mathbf{e}_1, \dots, \mathbf{e}_n)$ and $\mathcal{F} = (\mathbf{f}_1, \dots, \mathbf{f}_n)$ are two ONB forming a MUB pair if and only if $\mathcal{A}_{\mathcal{E}}$ and $\mathcal{A}_{\mathcal{F}}$ are *quasi-orthogonal*¹ with respect to the usual Hilbert-Schmidt scalar product.

We shall therefore define the **symmetries** of a MUB pair $(\mathcal{E}, \mathcal{F})$ in the following ways. We shall call an α automorphism² of the star-algebra of linear operators preserving

- the subspace $\mathcal{A}_{\mathcal{E}} + \mathcal{A}_{\mathcal{F}}$: a **generalized symmetry** of $(\mathcal{E}, \mathcal{F})$
- the subspace $\mathcal{A}_{\mathcal{E}} + \mathcal{A}_{\mathcal{F}}$: a **generalized unitary symmetry** of $(\mathcal{E}, \mathcal{F})$ if further α is unitarily implementable,

¹Two maximal abelian star algebras \mathcal{A}, \mathcal{B} — as subspaces in $M_n(\mathbb{C})$ — cannot be orthogonal, since $\mathbb{1}$ is included in both. The “best” we can have is that $\mathbb{1}^\perp \cap \mathcal{A}$ is orthogonal to $\mathbb{1}^\perp \cap \mathcal{B}$. This is what is called quasi-orthogonality.

²Recall that such an α is always of the form $\alpha(X) = UXU^*$ where U is either a unitary or an anti-unitary operator.

- both subspaces $\mathcal{A}_\mathcal{E}, \mathcal{A}_\mathcal{F}$ (separately): a **symmetry** of $(\mathcal{E}, \mathcal{F})$,
- both subspaces $\mathcal{A}_\mathcal{E}, \mathcal{A}_\mathcal{F}$ (separately): a **unitary symmetry** of $(\mathcal{E}, \mathcal{F})$, if further α is unitarily implementable.

Accordingly, we shall talk about the **generalized symmetry**, **generalized unitary symmetry**, **symmetry**, and **unitary symmetry group** of $(\mathcal{E}, \mathcal{F})$. Note all of these groups are subgroups of the first listed one and that last one is a subgroup of all the previous ones.

There is a natural homomorphism from the group of symmetries of $(\mathcal{E}, \mathcal{F})$ to $S_n \times S_n$. Indeed, a symmetry takes a minimal projection of $\mathcal{A}_\mathcal{E}$ and $\mathcal{A}_\mathcal{F}$ into a minimal projection of $\mathcal{A}_\mathcal{E}$ and $\mathcal{A}_\mathcal{F}$, respectively. Thus if α is a symmetry, then there exist two permutations $\sigma, \mu \in S_n$ such that

$$\alpha(P_{\mathbf{e}_k}) = P_{\mathbf{e}_{\sigma(k)}} \quad \text{and} \quad \alpha(P_{\mathbf{f}_k}) = P_{\mathbf{f}_{\mu(k)}} \quad (9)$$

for all $k = 1, \dots, n$. Moreover, it is quite evident, that the pair (σ, μ) , as a function of α , defines a homomorphism.

Theorem 2.1. *The above defined natural homomorphism to $S_n \times S_n$, when restricted to the group of unitary symmetries, is injective. In particular the group of unitary symmetries can have at most $(n!)^2$ and that of symmetries at most $2(n!)^2$ elements.*

Proof. For the injectivity all we need to show is that if U is a unitary operator such that $UP_{\mathbf{e}_k}U^* = P_{\mathbf{e}_k}$ and $UP_{\mathbf{f}_k}U^* = P_{\mathbf{f}_k}$ for all $k = 1, \dots, n$ then U is a multiple of $\mathbb{1}$. However, the assumed invariance means that both the vectors of \mathcal{E} and the vectors of \mathcal{F} are eigenvectors for U . Thus U is commuting with all elements of both abelian algebras, namely $\mathcal{A}_\mathcal{E}$ and $\mathcal{A}_\mathcal{F}$. As these are maximal abelian, this implies that $U \in \mathcal{A}_\mathcal{E} \cap \mathcal{A}_\mathcal{F}$. However, by the quasi-orthogonality this intersection contains multiples of the identity, only.

The injectivity of the map in question shows that the number of elements in the group of unitary symmetries must be less or equal to the number of elements of $S_n \times S_n$; that is, less or equal than $(n!)^2$. The estimate regarding the number of symmetries follows since the product of two anti-unitary operators is a unitary operator and hence the unitary symmetry group either coincides with the full symmetry group or it is an index 2 subgroup. \square

Let us discuss now the role of symmetries in the task of finding common UB vectors. Suppose $(\mathcal{E}, \mathcal{F})$ is a MUB pair. We would like to find vectors

of unit length that are unbiased for both \mathcal{E} and for \mathcal{F} . Suppose further that \mathbf{b} is such a vector. Can we somehow use \mathbf{b} to produce more such vectors? Of course we can change the phase of \mathbf{b} , but that we do not regard as a “new” common UB vector. However, it is quite evident, that if the unitary or anti-unitary U implements a symmetry of $(\mathcal{E}, \mathcal{F})$ at least in the generalized sense, then $U\mathbf{b}$ is also a common UB vector for $(\mathcal{E}, \mathcal{F})$.

To illustrate what was so far said, consider the pair $(\mathcal{E}, \mathcal{F})$ formed by the standard and the Fourier bases in \mathbb{C}^n . Let U, V be the linear operators defined by the formula

$$U\mathbf{e}_k = e^{i\frac{2\pi}{n}}\mathbf{e}_k, \quad \text{and} \quad V\mathbf{e}_k = \mathbf{e}_{k+1} \quad (10)$$

where the index “ $k + 1$ ” is meant by modulo n . Then U, V are unitary, $U^n = V^n = \mathbb{1}$ and $UV = e^{i\frac{2\pi}{n}}VU$. However, by the definition of the Fourier bases, a simple check shows that

$$V\mathbf{f}_k = e^{i\frac{2\pi}{n}}\mathbf{f}_k, \quad \text{and} \quad U\mathbf{f}_k = \mathbf{f}_{k+1} \quad (11)$$

for all $k = 1, \dots, n$ (where again, the index “ $k + 1$ ” is meant by modulo n). Thus U and V only “changes the phases” / reorders the vectors of not only \mathcal{E} but also of \mathcal{F} and hence they both implement unitary symmetries of $(\mathcal{E}, \mathcal{F})$. So in particular, if \mathbf{b} is a common UB vector for both the standard and the Fourier bases, then so is $U^k V^l \mathbf{b}$ for all $k, l = 1, \dots, n$.

As is well known in case of the Fourier bases, of these UB vectors one can always put together an ONB and thus obtain a MUB triplet. This is because if \mathbf{b} is a common (normalized) UB vector for $(\mathcal{E}, \mathcal{F})$ then the vectors

$$\mathbf{b}, V\mathbf{b}, V^2\mathbf{b}, \dots, V^{n-1}\mathbf{b} \quad (12)$$

form an ONB. The same thing holds if one replaces V by U .

However we would not like to limit ourselves to the case of Fourier bases. So the natural question for us: what can be generalized of the last mentioned property? Having a common UB vector, can we still produce a pairwise orthogonal collection of UB vectors?

In the simple Fourier case, by looking at the action of U and V on the bases vectors of \mathcal{E} and \mathcal{F} , we see that under the natural injection into $S_n \times S_n$, the symmetries implemented by U and V go into (id, σ) and (σ, id) , respectively, where $\sigma \in S_n$ is a cyclic permutation of n . We shall now show how the well-known fact concerning the orthogonality of the mentioned sets

of UB vectors can be deduced just from this piece of information, and how the whole thing can be turned into a general statement (rather than a particular one regarding the Fourier case).

Theorem 2.2. *Let $(\mathcal{E}, \mathcal{F})$ be a MUB pair, \mathbf{b} a common normalized UB vector and $\alpha_0 = id, \alpha_1, \dots, \alpha_k$ be unitary symmetries implemented by the unitaries $U_0 = \mathbb{1}, U_1, \dots, U_k$, respectively. Suppose that for all $j \neq l$ the image of $\alpha_j^{-1} \circ \alpha_l$ under the natural injection into $S_n \times S_n$ is of the form (σ, id) or (id, σ) where $\sigma \in S_n$ is a permutation with no fixed points. Then*

$$U_0 \mathbf{b} = \mathbf{b}, U_1 \mathbf{b}, \dots, U_k \mathbf{b}$$

are all common normalized UB vectors for $(\mathcal{E}, \mathcal{F})$ and are pairwise orthogonal to each other.

Proof. Suppose that the image of $\alpha_j^{-1} \circ \alpha_l$ under the natural injection into $S_n \times S_n$ is of the form (σ, id) . Then each vector of \mathcal{F} must be an eigenvector for $U_j^* U_l$: there exist some $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ such that $U_l^* U_j \mathbf{f}_k = \lambda_k \mathbf{f}_k$. Thus

$$\begin{aligned} \langle U_j \mathbf{b}, U_l \mathbf{b} \rangle &= \langle U_l^* U_j \mathbf{b}, \mathbf{b} \rangle = \sum_k \langle U_l^* U_j \mathbf{b}, \mathbf{f}_k \rangle \langle \mathbf{f}_k, \mathbf{b} \rangle \\ &= \sum_k \langle \mathbf{b}, U_j^* U_l \mathbf{f}_k \rangle \langle \mathbf{f}_k, \mathbf{b} \rangle = \sum_k \lambda_k |\langle \mathbf{b}, \mathbf{f}_k \rangle|^2 = \frac{1}{n} \text{Tr}(U_j^* U_l) \end{aligned} \quad (13)$$

since $|\langle \mathbf{b}, \mathbf{f}_k \rangle|^2 = 1/n$ for all $k = 1, \dots, n$ (as \mathbf{b} is a normalized UB vector for \mathcal{F}) and the sum of eigenvalues gives the trace. However,

$$\text{Tr}(U_j^* U_l) = \sum_k \langle \mathbf{e}_k, U_j^* U_l \mathbf{e}_k \rangle = \sum_k \langle \mathbf{e}_k, \mathbf{e}_{\sigma(k)} \rangle = 0 \quad (14)$$

as \mathbf{e}_k is always orthogonal to $\mathbf{e}_{\sigma(k)}$ (since σ has no fixed points). \square

3 Application to the case of $\mathcal{F}(a, b)$

We shall now apply the general statements so far made to our case of interest, namely to the MUB pair $(\mathcal{E}, \mathcal{F}(a, b))$.