Triplets of mutually unbiased bases

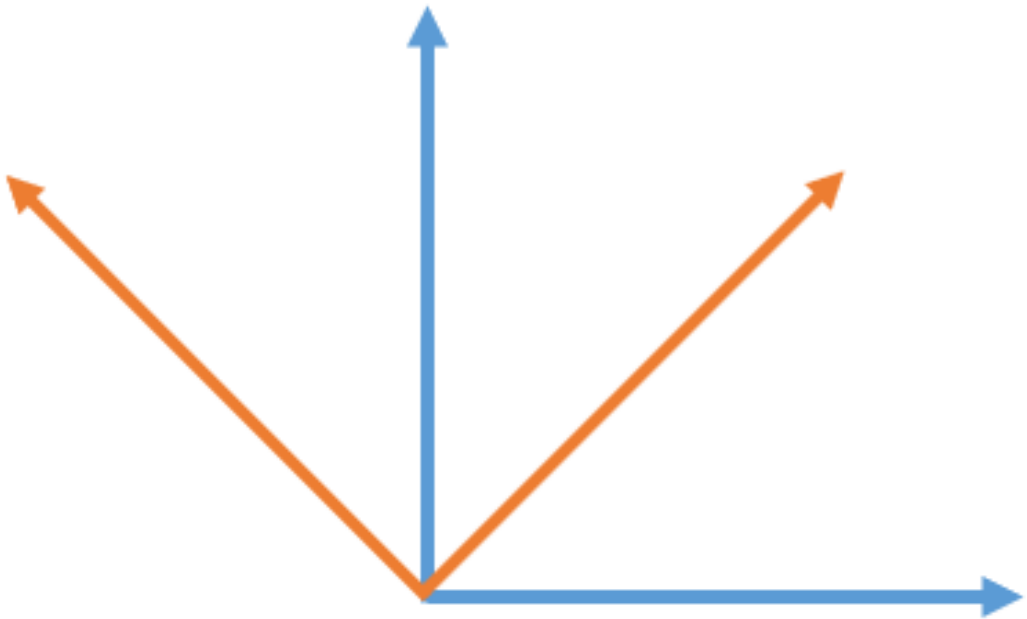
Máté Matolcsi (Rényi Institute)

Joint work with A. Matszangosz, D. Varga, M. Weiner

Hadamard 2025 workshop, Sevilla

Mutually unbiased bases

Two ONBs $X = \{x_1, \ldots, x_d\}$ and $Y = \{y_1, \ldots, y_d\}$ in $\mathbb{C}^d$ are mutually unbiased (MUBs) if $|\langle x_i, y_j \rangle| = \frac{1}{\sqrt{d}}$ for all i, j.



MUBs and Hadamard matrices

Connection to Hadamard matrices:

Real case: $X, Y \subset \mathbb{R}^d$ ONBs are unbiased $\Leftrightarrow$
$\forall\ \langle x_j, y_k \rangle = \pm 1/\sqrt{d} \Leftrightarrow$
$\sqrt{d}XY^* = H$ is a Hadamard matrix.

Customary to assume $Y = I$, $\sqrt{d}X = H$.
So, a pair of MUBs in $\mathbb{R}^d \Leftrightarrow$ Hadamard matrix

Hadamard conjecture: for all $4|d$ we have a pair of MUBs in $\mathbb{R}^d$.

MUBs and complex Hadamard matrices

Complex case: $X, Y \subset \mathbb{C}^d$ ONBs are unbiased $\Leftrightarrow$
$\forall\ |\langle x_j, y_k \rangle| = 1/\sqrt{d} \Leftrightarrow$
$\sqrt{d}XY^* = H$ is a complex Hadamard matrix.

Customary to assume $Y = I$, $\sqrt{d}X = H$.
So, a pair of MUBs in $\mathbb{C}^d \Leftrightarrow$ complex Hadamard matrix

I, F_d (Fourier matrix) is a pair of MUBs for all d

How many real MUBs?

1 MUB in $\mathbb{R}^d$ if $4 \not| d$

2 MUBs: possibly for all $4|d$ (Hadamard conjecture)

3 MUBs: possibly for all $d = 4n^2$, but not more than 3 if n is odd (Holzmann, Kharaghani) – standard terminology: 2 MUHs

4^n MUBs for $d = 4^{2n}$ (Holzmann, Kharaghani)

Some further results...

How many complex MUBs?

In $\mathbb{C}^d$ a pair of MUBs (I, F_d) always exists.

Theorem (e.g. Wooters, Fields 1989)

For any dimension d, the number of pairwise mutually unbiased bases is at most $d+1$. If $d = p^\alpha$, full systems of $d+1$ MUBs exist.

If $d = p_1^{\alpha_1} \dots p_n^{\alpha_n}$, then take the minimal prime-power $m = p_i^{\alpha_i}$: at least $m+1$ MUBs exist in dimension d. E.g. if $d = 2 \cdot 10000000001$ then at least 3 MUBs exist...

There is not a single case of a non prime-power d where the maximal number of MUBs is known.

MUBs in dimension 6

SIC-POVMs are conjectured to exist in all dimensions, but the case for MUBs is different.

The MUB-6 problem

What is the maximal number of MUBs in dimension 6?

This is one of the "Five open problems in theory of quantum information" by Pawel Horodecki, Lukasz Rudnicki, Karol Zyczkowski.

Conjecture (Zauner, 1999): The maximal number of MUBs in dimension 6 is 3.

Plenty of numerical evidence supports this conjecture.

Unitary equivalence of MUBs

Let
$X_1 = \{\mathbf{e}_1^{(1)}, \ldots, \mathbf{e}_d^{(1)}\}, \ldots, X_m = \{\mathbf{e}_1^{(m)}, \ldots, \mathbf{e}_d^{(m)}\}$ and
$Y_1 = \{\mathbf{f}_1^{(1)}, \ldots, \mathbf{f}_d^{(1)}\}, \ldots, Y_m = \{\mathbf{f}_1^{(m)}, \ldots, \mathbf{f}_d^{(m)}\}$
be two systems of MUBs.

Let $P_j^{(k)} = |\mathbf{e}_j^{(k)}\rangle\langle\mathbf{e}_j^{(k)}|$ and, similarly, $\tilde{P}_j^{(k)} = |\mathbf{f}_j^{(k)}\rangle\langle\mathbf{f}_j^{(k)}|$.

We say that the two system of MUBs $(X_1, \ldots, X_m)$, $(Y_1, \ldots, Y_m)$ are directly unitary equivalent if there exists a unitary operator U on $\mathbb{C}^d$ such that $UP_j^{(k)}U^* = \tilde{P}_j^{(k)}$ for all $1 \leq k \leq m, 1 \leq j \leq d$.

They are permutationally unitary equivalent if the bases and the vectors are allowed to be permuted.

Pairs of MUBs and complex Hadamard matrices

If the bases X, Y are MUB, then $h_{i,j} = \sqrt{d}\langle x_i, y_j\rangle$ forms a complex Hadamard matrix (i.e. complex orthogonal matrix with unimodular entries).

Two complex Hadamard matrices H_1 and H_2 are called equivalent, $H_1 = D_1 P_1 H_2 P_2 D_2$ with some unitary diagonal matrices D_1, D_2 enphasing, and permutation matrices P_1, P_2.

Easy to show: a pair of MUBs X_1, X_2 is permutationally unitary equivalent to Y_1, Y_2 iff $H_{X_1,X_2} \cong H_{Y_1,Y_2}$ or $H^*_{Y_1,Y_2}$.

Complex Hadamards of order 6

If $X_0, \dots X_d$ are MUBs then introducing coordinates wrt X_0 we get matrices $I, \frac{1}{\sqrt{d}}H_1, \dots, \frac{1}{\sqrt{d}}H_d$ where each H_i is a complex Hadamard matrix, and each $\frac{1}{\sqrt{d}}H_i^* H_j$ is also complex Hadamard for each $i \neq j$ (transition matrices).

For $d = 2, 3, 4, 5$ we have a simple analytic classification of complex Hadamard matrices of order d. Therefore, it is easy to check which pair $I, \frac{1}{\sqrt{d}}H_1$ can be extended to a full system of $d + 1$ MUBs.

Same strategy for $d = 6$?

State of the art: Ferenc Szöllősi constructed a 4-parameter family of complex Hadamards of order 6, and there is an additional single isolated matrix outside this family. This is conjectured to be a complete classification.

Families of complex Hadamard matrices

Some submanifolds of the 4-parameter family are given by "nice" formulas:
The Fourier family: $\omega = e^{2i\pi/3}$

$$F(x,y) = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega^2 & \omega & x & \omega^2 x & \omega x \\ 1 & \omega & \omega^2 & y & \omega y & \omega^2 y \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \omega^2 & \omega & -x & -\omega^2 x & -\omega x \\ 1 & \omega & \omega^2 & -y & -\omega y & -\omega^2 y \end{bmatrix} \tag{1}$$

Theorem (Jaming, M., Móra, Szöllősi, Weiner, 2009)

Any pair $I, \frac{1}{\sqrt{d}}F(x,y)$ cannot be extended to four (!) MUBs.

Families of complex Hadamard matrices

Another two-parameter family $X(\alpha)$ found by F. Szöllősi given in a block-circulant form (where the entries depend on a complex parameter $\alpha = u + iv$):

$$X(\alpha) = \begin{bmatrix} a & b & c & d & e & f \\ c & a & b & f & d & e \\ b & c & a & e & f & d \\ \overline{d} & \overline{f} & \overline{e} & -\overline{a} & -\overline{c} & -\overline{b} \\ \overline{e} & \overline{d} & \overline{f} & -\overline{b} & -\overline{a} & -\overline{c} \\ \overline{f} & \overline{e} & \overline{d} & -\overline{c} & -\overline{b} & -\overline{a} \end{bmatrix}$$

Theorem (Szöllősi, 2010)

Any pair $I, \frac{1}{\sqrt{d}}X(\alpha)$ can be extended to a triplet of MUBs I, X, H. In any such triplet H is in the Fourier (or transposed) family, so the triplet cannot be extended to a quadruplet.

MUB-triplets for $d = 6$

MUB pairs correspond to complex Hadmard matrices and as we saw, they are hard to classify analytically (4-dim family).

Instead, let us try to classify all MUB-triplets. They are possibly easier to describe.

We have searched for MUB-triplets numerically, and the evidence suggests that they form a 2-parameter family, plus an isolated point:
$(I, X(\alpha), F(x_\alpha, y_\alpha))$ and (I, F, F_0)
up to permutational unitary equivalence.

Associated projectors

For a MUB-triplet X, Y, Z consider the 1-dimensional orthogonal projectors $P_i = |x_i\rangle\langle x_i|$. Similarly for Y, Z, let $Q_j = |y_j\rangle\langle y_j|$, and $R_k = |z_k\rangle\langle z_k|$.

The operators $\sqrt{d}P_iQ_j$ $(1 \leq i, j \leq d)$ form an orthonormal basis of the space of $d \times d$ matrices wrt to the H-S inner product. Indeed, $Tr((P_iQ_j)^*P_kQ_m) = Tr(Q_jP_iP_kQ_m) = 0$ if $(i, j) \neq (k, m)$, and $Tr((P_iQ_j)^*P_kQ_m) = |\langle x_i, y_j\rangle|^2 = \frac{1}{d}$ if $(i, j) = (k, m)$.

From MUB-triplets to Hadamard cubes

Given a MUB-triplet X, Y, Z we associate a $d \times d \times d$ cube $\tilde{C}$

$\tilde{c}_{i,j,k} = Tr(P_i Q_j R_k) = Tr(|x_i\rangle\langle x_i|y_j\rangle\langle y_j|z_k\rangle\langle z_k|) = \langle x_i|y_j\rangle\langle y_j|z_k\rangle\langle z_k|x_i\rangle$.

What are the properties of the Hadamard cube $C = d^{3/2}\tilde{C}$?

(1) All entries of the cube C have modulus 1, and all 2-dim slices are complex Hadamard matrices.

(2) Parallel slices are "phase-equivalent" to each other (i.e. one is obtained from the other by multiplying the rows and columns by appropriate phases).

(3) All 1-dim lines sum up to $\sqrt{d}$

(2') Haagerup condition:

$C_{j',k,l} C_{j,k',l} C_{j,k,l'} C_{j',k',l'} = C_{j,k,l} C_{j',k',l} C_{j,k',l'} C_{j',k,l'}$

A uniqueness result

Uniquness theorem

Assume that MUB-triplets P_i, Q_j, R_k and $\tilde{P}_i, \tilde{Q}_j, \tilde{R}_k$ generate the same cube C. Then the two MUB-triplets are directly unitary equivalent, i.e. there is a unitary U such that $\tilde{P}_i = U^* P_i U, \tilde{Q}_j = U^* Q_j U, \tilde{R}_k = U^* R_K U$.

Proof: Define a mapping $T : \mathbb{C}^{d\times d} \to \mathbb{C}^{d\times d}$ by $P_i Q_j \to \tilde{P}_i \tilde{Q}_j$, and extend linearly. We claim that this is $*$-star algebra isomorphism. It preserves products because a product $P_a Q_b P_m Q_s$ can be expanded in the basis $P_i Q_j$ with the help of the cube entries in C, so that the same expansion is valid for the tilde operators.

Any $*$-star algebra isomorphism is given by a unitary equivalence.

Reconstruction of MUBs from a cube

Reconstruction theorem

Assume that cube C has properties (1), (2) and (3). Then there exists a (unique) MUB-triplet P_i, Q_j, R_k such that the associated cube is exactly C.

The proof relies on the fact that the projectors P_i, Q_j can be identified by a single facet (slice) of the cube, and then the projectors R_k can be expanded in the basis $P_i Q_j$ with the help of the cube entries.

A roadmap to classify MUB-triplets in $d = 6$

A MUB-triplet defines a Hadamard-cube C. In all numerical triplets, the slices of the cube belong to the families $F(x, y)$ and/or $X(\alpha)$.

We can think of C as 216 variables $C_{i,jk}$ satisfying all constraints given by properties (1), (2), (3) above. These properties can be listed as algebraic identities.

We were hoping to find other non-trivial identities $P(c_{i,j,k}) = 0$ which imply that the facets of the cube must belong to the Fourier family $F(a, b)$ or the Szöllősi family $X(u, v)$.

Partial success

And we did find such identities...

(without proof as yet)

Fourier analysis on $\mathbb{T}^d$

Let $v = (v_1, \ldots, v_d) \in \mathbb{T}^d$ and $\gamma = (\gamma_1, \ldots, \gamma_d) \in \mathbb{Z}^d$.

Fourier analysis on $\mathbb{T}^d$ is just fancy language for considering monomials

$$v^\gamma = v_1^{\gamma_1} v_2^{\gamma_2} \ldots v_d^{\gamma_d}$$

If $h_1, \ldots, h_d$ are the rows of a complex Hadamard matrix H, define $g_H(\gamma) = \sum_{j=1}^d h_j^\gamma$, and $G_H(\gamma) = |g_H(\gamma)|^2$.

E.g. $g_H(1, 1, 1, -1, -, 1 - 1) = \sum_{j=1}^6 z_1^{(j)} z_2^{(j)} z_3^{(j)} \overline{z_4^{(j)} z_5^{(j)} z_6^{(j)}}$

If $h_1, \ldots, h_d$ are the rows of a complex Hadamard matrix H, define $g_H(\gamma) = \sum_{j=1}^{d} h_j^{\gamma}$, and $G_H(\gamma) = |g_H(\gamma)|^2$.

Conjecture 1

For any permutation π, and any complex Hadamard H of order 6 (with the exception of the isolated matrix S_6), we have $G_H(\pi(1, 1, 1, -1, -, 1 - 1)) = 0$.

Conjecture 2

For any permutation π, and any slice of the cube C we have $G_H(\pi(3, 3, 3, -3, -3, -3))G_{H^*}(\pi(3, 3, 3, -3, -3, -3)) = 0$.

Exploiting the conjectures

The point of the conjectures is the following

Theorem (M., Matszangosz, Varga, Weiner 2025)

A complex Hadamard matrix H satisfies $G_H(1,1,1,-1,-,1-1)=0$ and $G_H(3,3,3,-3,-3,-3)G_{H^*}(3,3,3,-3,-3,-3)=0$ if and only if a dephased form of H contains three distinct rows or columns containing an entry -1.

Theorem (Szöllősi, Matszangosz 2024)

If a dephased form of H contains three distinct rows or columns containing an entry -1, then H belongs to the family $F(x,y)$, $F^T(x,y)$ or $X(\alpha)$.

A small caveat

Assuming the validity of the conjectures, the theorems above imply that in any MUB-triplet (X, Y, Z) the transition matrices XY^*, YZ^* and ZX^* all belong to $F(x, y)$, $F^T(x, y)$ or $X(\alpha)$.

If any transition matrix is in $F(x, y)$ or $F^T(x, y)$, the triplet cannot be extended to a quadruplet.

However, we cannot exclude the case that all transition matrices are in $X(\alpha)$. There was a result in the literature claiming exactly that, but alas... its proof is wrong.

Hopeless?

Before you say that the conjectured identities are hopeless to prove:

Theorem

Let $H_1, \ldots, H_6$ be six parallel slices of the cube in $d = 6$, and let $\gamma \in \mathbb{Z}^d$ be such that $\sum_{j=1}^{6} \gamma_j = \pm 1$. Then $\sum_{k=1}^{6} G_{H_j}(\gamma) = 36$.

This is a consequence of the cube properties (1), (2), (3).

Thank you