A Parametric Class of Mutually Unbiased Bases using Resolvable Block Designs

Ajeet Kumar, **Rakesh Kumar**, Subhamoy Maitra

Indian Statistical Institute, Kolkata

Indocrypt-2024

Outline

- Introduction and Motivation
- Definitions and Preliminaries
- Construction of MUBs for $d = s^2$ using RBD
- Introducing Affine Parameters in MUBs and Hadamard Matrices
- Comparisons and Results
- Conclusion and Future work

Mutually Unbiased Bases (MUBs)

Definition: Two orthonormal bases $B_1 = \{a_1, a_2..., a_d\}$ and $B_2 = \{b_1, b_2, ...b_d\}$ in d dimensional Hilbert spaces are mutually unbiased if,

$$|\langle a_i, b_j \rangle| = \frac{1}{\sqrt{d}}; \text{ for every } 1 \leq i, j \leq d.$$

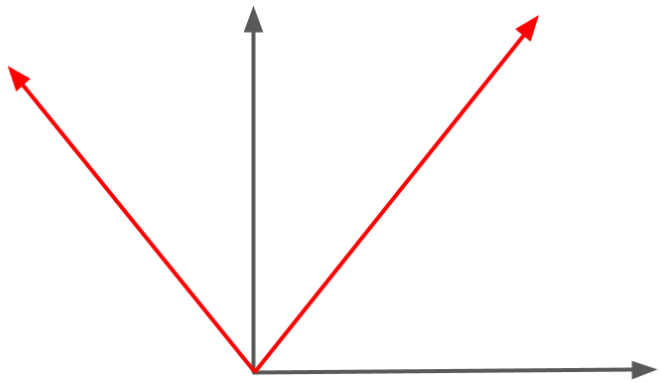
- A set $\{B_1, B_2, \ldots, B_m\}$ of orthonormal bases in C^d is called a set of mutually unbiased bases (a set of MUB) if each pair of bases B_i and B_j are mutually unbiased.

MUBs in dimension 2

$$B_1 = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\},$$

$$B_2 = \frac{1}{\sqrt{2}} \left\{ \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} -1 \\ 1 \end{pmatrix} \right\},$$

$$B_3 = \frac{1}{\sqrt{2}} \left\{ \begin{pmatrix} 1 \\ i \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -i \end{pmatrix} \right\}$$



MUBs in dimension 3

$$B_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

$$B_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix},$$

$$B_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix},$$

$$B_4 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}$$

Most Important Question

Question: Given d, how large can we make n ?

$N(d) := \max\{n :$ there exist n MUBs of $C^d\}$.

What we know

Upper bound: $N(d) \leq d + 1$.

Lower bound: If $d = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ such that $p_1^{k_1} < p_2^{k_2} < ... < p_r^{k_r}$; then

$$N(d) \geq p_1^{k_1} + 1.$$

- $N(p^k) = p^k + 1$ for all primes p.
- If $N(d) = d$ then $N(d) = d + 1$. [Weiner'2013]
- Some special constructions in specific dimensions beat lower bound, e.g. d a perfect square using Latin squares.

  example: We can construct at least 6 MUBs in dimension $d = 26^2$.

What we don't know

Open problem: Determine $N(d)$ exactly for any d, not a prime power, or even just improve on the upper bound :

$$N(d) \leq d - 1 < d + 1$$

Conjecture: $N(6) = 3$ (naive lower bound tight) [Zauner'91]

Philosophical question: What powerful upper bound ideas could we be missing ?

Preliminary concept

Definition:

- **Inner product:**
  Inner product between two d-dimensional complex vectors $|u\rangle = (u_1, \ldots, u_d), |v\rangle = (v_1, \ldots, v_d)$ is $\langle u|v\rangle = u_1 v_1^* + \ldots + u_d v_d^*$, where v_i^* is complex conjugate of v_i. This produces a complex number.
- **Unitary Matrices:**
  A d-dimensional complex-square matrix U is called Unitary if U satisfies $U^\dagger U = UU^\dagger = \mathrm{I}$, where $U^\dagger$ denotes the conjugate-transpose of U and I denotes Identity matrix.
- Two Unitary matrices U_1 and U_2 are called **equivalent,** written $U_1 \equiv U_2$, if their exist diagonal unitary matrices D_1 and D_2 and permutation matrices P_1 and P_2 such that

$$U_1 = D_1 P_1 U_2 P_2 D_2.$$

Definition (Contd...)

- **Permutation Matrix:**
  A permutation matrix P is a unitary matrix, which has entries from set $\{0, 1\}$, such that every row and column contain exactly one non zero entry.
- **Hadamard Matrices:**
  An d-dimensional unitary matrix $H = (h_{ij}) : 1 \leq i, j \leq d$ is called Hadamard if $|h_{ij}| = \frac{1}{\sqrt{d}}$ for all $i, j \in \{0, 1, \ldots, d\}$.
- Multiplication of arbitrary phase factor to all the elements of the row or column does not change the Hadamard property of the matrix
- Hadamard matrix is equivalent to a Hadamard matrix, having all its entries of first row and first column as 1. Such Hadamard matrix is called a dephased Hadamard matrix.

Preliminary (contd...) RBD

Parallel Class and Resolvable Block Designs(RBD) :

- A parallel class in design (X, A) is a subset of disjoint blocks in A whose union is X.
- For a design (X, A), if A can be partitioned into $r \geq 1$ parallel classes, called resolution, then the design (X, A) is called Resolvable Block Design (RBD).

Example

Consider the combinatorial design (X, A_1) and (X, A_2) with

$X = \{1, 2, 3, 4, 5, 6, 7, 8\}$,
$A_1 = \{(1, 2), (2, 3, 4), (5, 6, 7), (1, 8, 6), (2, 5), (6, 7), (2, 6, 8)\}$ and
$A_2 = \{(1, 2, 3), (2, 4, 6), (3, 5, 8), (6, 8), (1, 7), (4, 5, 7)\}$

Then

- (X, A_2) is a resolvable design since $A_2 = P_1 \cup P_2$ where $P_1 = \{(1, 2, 3), (6, 8), (4, 5, 7)\}$ and $P_2 = \{(1, 7), (2, 4, 6), (3, 5, 8)\}$ form two parallel classes consisting of disjoint sets whose union is set X. We say P_1 and P_2 form resolutions of A_2.
- The design (X, A_1) is not resolvable as such resolutions are not possible in this case.

Preliminary (contd..) Lattin Square

Definition(s):

- A *Latin square of order* s is an $s \times s$ array with entries from a set S of cardinality s such that each element of S appears equally often in every row and every column.
  Example:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \\ 3 & 4 & 1 & 2 \\ 4 & 1 & 2 & 3 \end{array}$$

- Two Latin squares L and L' of order s are said to be *orthogonal* to each other if when one is superimposed on the other the ordered pairs (L_{ij}, L'_{ij}) of corresponding entries consist of all possible s^2 pairs.
- A collection of w Latin squares of order s, any pair of which is orthogonal, is called a set of **mutually orthogonal Latin squares (MOLS)**.

MOLS example

1	4	3	2
2	3	4	1
4	1	2	3
3	2	1	4

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

1,1	4, 2	3, 3	2, 4
2, 2	3, 1	4, 4	1, 3
4, 3	1, 4	2, 1	3, 2
3, 4	2, 3	1, 2	4, 1

Known fact about MOLS

- A Latin square of order s exists for every positive integer s.
- It is known that $N_{MOLS}(s) \leq s-1$ for all s; where $N_{MOLS}(s)$ denote the maximal value w such that w MOLS of order s.
- A construction for complete sets of MOLS of order s is known if s is a prime power.

- In any square dimension $d = s^2$, $w+2$ MUBs can be constructed provided that there are w MOLS of order s. [Wocjan,2002]
- It's known that $N_{MOLS}(26) \geq 4$, so we can construct 6 MUBs in dimension $d = 26^2$.

MUBs and Complex Hadamard matrices

- Each MU basis in the space C^d consists of d orthogonal unit vectors which is a unitary $d \times d$ matrix.
- k sets of MUBs $\{M_1, M_2, M_3, \ldots, M_k\}$ in C^d can be thought as a k numbers of unitary matrix $d \times d$.
- By doing *unitary* transformation M_1^{-1} applied from left

$$\{M_1, M_2, M_3, \ldots, M_k\} \rightarrow M_1^{-1}\{M_1, M_2, M_3, \ldots, M_k\}$$

$$\equiv \{I, M_1^{-1}M_2, M_1^{-1}M_3, \ldots, M_1^{-1}M_k\},$$

  the new transformed set also becomes the MUBs in C^d.
- $M_i^{-1}M_j$ $(i \neq j)$, is a complex Hadamard matrices having moduli of all their matrix elements equal to $\frac{1}{\sqrt{d}}$.

Contd...

- The existence and classification of MU bases is closely related to the existence of the maximal set of complex Hadamard matrices.
- All (complex) Hadamard matrices are known for dimensions $d \leq 5$ but there is no **complete classification (family)** for $d = 6$.

Construction of Orthonormal Bases Through RBD in Dimension $d = s^2$

- In a design (X, A), choose the elements of X as any set of orthonormal basis vectors of $\mathbb{C}^d$. That is, if $|X| = d$, then $X = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\}$, such that $\langle\psi_i|\psi_j\rangle = \delta_{ij}$. Hence A, which contains blocks made out of the elements from X, would now consist of blocks with the elements from the set of chosen orthonormal basis vectors.
- Let $B = \{b_1, b_2, \ldots, b_s\}$ be one of the parallel class of the design (X, A), where b_i's are disjoint blocks containing elements from X. Since B is a parallel class, this implies $X = b_1 \cup b_2 \cup \ldots \cup b_s$, and $b_i \cap b_j = \phi$ for all $1 \leq i \neq j \leq s$.
- Consider one of the blocks $b_r = \{|\psi_{r_1}\rangle, |\psi_{r_2}\rangle, \ldots, |\psi_{r_{n_r}}\rangle\} \in B$ and let $|b_r| = n_r$. Corresponding to this block, choose any $n_r \times n_r$ unitary matrix whose elements are say u^r_{ij}, $i, j = 1, 2, \ldots, n_r$.

Construction (Continue)

- Next construct n_r many vectors in the following manner, using b_r and u^r_{ij}.

$$|\phi^r_i\rangle = u^r_{i1}\,|\psi_{r_1}\rangle + u^r_{i2}\,|\psi_{r_2}\rangle + \ldots + u^r_{in_r}\,\left|\psi_{r_{n_r}}\right\rangle = \sum_{k=1}^{n_r} u^r_{ik}\,|\psi_{r_k}\rangle : i = 1, 2, \ldots, n_r.$$

- In a similar manner, corresponding to each block $b_j \in B$, construct n_j many vectors where $|b_j| = n_j$, using any $n_j \times n_j$ unitary matrix. Since $\sum_{j=1}^{s} n_j = d$, we will get exactly d many vectors.

Note: If we construct the matrix M_B of size $d \times d$ having column vectors as $|\phi^r_i\rangle$, therefore, $M_B = \left(\left|\phi^1_1\right\rangle, \ldots, \left|\phi^1_{n_1}\right\rangle, \left|\phi^2_1\right\rangle, \ldots, \left|\phi^2_{n_2}\right\rangle, \ldots, |\phi^s_1\rangle, \ldots, \left|\phi^s_{n_s}\right\rangle\right)$. Here, $|\phi^r_i\rangle$'s corresponding to a parallel class B of X form an orthonormal set of basis vectors and hence M_B is a unitary matrix.

Lemma and Theorem in context of above construction

- **Lemma 1:** If X consists of the **computational basis vectors**, then $M_B = P_B \mathrm{H}$, where P_B is a permutation matrix of size $d \times d$ and H is a block diagonal matrix consisting of unitary matrices of size $n_j \times n_j \, (j = 1, 2, \ldots, s)$ as block matrices.
- **Theorem :** Consider an RBD (X, A) such that $|X| = s^2$, then one can construct $MOLS(s) + 2$ many parallel classes, each having s many blocks of size s and any two blocks from different parallel classes will have exactly one point in common.

Example

Let $|X| = 2^2$ such that $X = \{1, 2, 3, 4\}$. The underlying parallel classes can be represented as follows.

$$C_0 : \{1, 2\}, \{3, 4\}, C_1 : \{1, 3\}, \{2, 4\}, C_2 : \{1, 4\}, \{2, 3\}.$$

Consider the two dimensional Hadamard matrix as $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. Therefore the sparse MUBs are denoted by

$$M_0 = P_0 \cdot M_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

$$M_1 = P_1 \cdot M_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

Contd...

$$M_2 = P_2 \cdot M_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix}$$

Using the above matrices, we obtain the following set of two Mutually Unbiased Hadamard matrices:

$$H_1 = M_0^\dagger \cdot M_1 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$H_2 = M_0^\dagger \cdot M_2 = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{pmatrix}.$$

Note: Along with Identity Matrix I_4, we obtain a set of 3 MUBs.

Lemmas in context of introducing affine free parameters

- **Lemma 2 :**
  If D_1 is a diagonal matrix and P_1 is a permutation matrix then $D_1P_1 = P_1D_2$ for some diagonal matrix D_2, having the same diagonal entries as that of D_1.
- **Lemma 3:**
  For a general square matrix M if $MD_1 = D_2M$, where D_1 and D_2 is a diagonal matrix then $D_1 = D_2 = \alpha \mathrm{I}$, where α is some constant.
- **Corollary :**
  For a general block diagonal matrix M_B if $M_BD_1 = D_2M_B$, where D_1 and D_2 is a diagonal matrix then $D_1 = D_2 = D_I$ where D_I is a block diagonal matrix, such that non zero block matrices are of the form $\alpha_r \mathrm{I}_r$. The size of the blocks is equal to the size of the blocks in the matrix M_B and α_r is a constant for each block.

Introducing Affine free parameters in Mutually Unbiased Hadamard Matrices

- If $\mathbb{H}$ is block diagonal matrix where each block is a Hadamard matrix of order s and noting that $D_i(\theta)\mathbb{H}$ is also blocked Hadamard matrix, where $D_i(\theta)$ is a diagonal unitary matrix, with diagonal entries of the form $\exp(\iota\theta_i)$, where θ_i is a independent parameter.
  Then using above we have $\mathbb{M}_i = P_i D_i(\theta)\mathbb{H}$. Therefore,

$$\mathbb{M}_i^\dagger \mathbb{M}_j = \mathbb{H}_0^\dagger D_i^\dagger(\theta) P_i^T P_j D_j(\theta)\mathbb{H}.$$

- From lemma 3, $D_i(\theta)P_i^T P_j D_j(\theta) = \tilde{P}_j \tilde{D}_j(\theta)$, where $\tilde{D}_j(\theta)$ is a unitary diagonal matrix having diagonal entries of the form $\exp(\iota\theta_i)$, for some θ_i where θ_i's are independent parameters and $\tilde{P}_j$ is some permutation matrix.
- Total independent parameters are equal to the dimension of the matrix which is s^2.

Contd..

- The set of Mutually Unbiased Hadamard matrices are

$$\{H_1 = \mathbb{M}_0^\dagger \mathbb{M}_1, H_2 = \mathbb{M}_0^\dagger \mathbb{M}_2, \ldots, H_w = \mathbb{M}_0^\dagger \mathbb{M}_w\},$$

  where

$$H_i = \mathbb{M}_0^\dagger \mathbb{M}_i = \mathbb{H}^\dagger \tilde{P}_j \tilde{D}_j(\theta) \mathbb{H}.$$

- If D is a block diagonal matrix, such that each block matrix is $\alpha_r I_s$, where I_s is the identity matrix of order s then D commutes with block diagonal matrix H, which contain block matrix of size s. Then,

$$\tilde{D}_j(\theta) = \tilde{D}_{j1}(\theta) \tilde{D}_{j2}(\theta),$$

  where, $\tilde{D}_{j2}(\theta)$ is a block diagonal matrix where each block is of form $\exp(\iota\theta_j) I_s$ and $\tilde{D}_{j1}(\theta)$ is block diagonal matrix having diagonal entries of the form $\exp(\iota\theta_j)$.
- From Corollary 1, $\tilde{D}_{j2}(\theta)$ will commute with $\mathbb{H}$. So,

$$H_i = \mathbb{H}^\dagger \tilde{P}_j \tilde{D}_j(\theta) \mathbb{H} = \mathbb{H}^\dagger \tilde{P}_j \tilde{D}_{j1}(\theta) \tilde{D}_{j2}(\theta) \mathbb{H} = \mathbb{H}^\dagger \tilde{P}_j \tilde{D}_{j1}(\theta) \mathbb{H} \tilde{D}_{j2}(\theta).$$

Contd...

- Since all the θ_j's are free parameters, we can absorb s many of them in $\tilde{D}_{j2}(\theta)$. Further, multiplying the Unitary Diagonal Matrix from left to an MUB matrix does not affect the equivalence of the MUBs, as it corresponds to multiplying an MUB vector with some arbitrary phase. Thus

$$H_i \equiv \mathbb{H}^\dagger \tilde{P}_j \tilde{D}_{j1}(\theta)\mathbb{H},$$

where the number of independent parameters become

$$s^2 - s = s(s-1).$$

Theorem 2 (Main Result)

- For dimension $d = s^2$ let $w = MOLS(s) + 1$, there exists a set of MUBs $\{\mathrm{I}, H_1, H_2, \ldots, H_w\}$ consisting of the identity matrix and the MUHMs, such that each Hadamard matrix H_i have at least $s(s-1)$ many independent affine parameters, that cannot be absorbed by a global unitary operation.

Affine parametric MUBs for d=4

The matrices $\mathbb{M}_0^\dagger\mathbb{M}_1$ and $\mathbb{M}_0^\dagger\mathbb{M}_2$ can be made affine parametric MUBs, each having $2(2-1)=2$ free parameters, by pulling out parameters only from the columns and not from the rows.

$$\mathbb{M}_0^\dagger\mathbb{M}_1 = \frac{1}{2}\begin{pmatrix} e^{i\theta_1} & e^{i\theta_1} & e^{i\theta_2} & e^{i\theta_2} \\ e^{i\theta_1} & e^{i\theta_1} & -e^{i\theta_2} & -e^{i\theta_2} \\ e^{i\theta_3} & -e^{i\theta_3} & e^{i\theta_4} & -e^{i\theta_4} \\ e^{i\theta_3} & -e^{i\theta_3} & -e^{i\theta_4} & e^{i\theta_4} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ e^{i\alpha} & -e^{i\alpha} & e^{i\beta} & -e^{i\beta} \\ e^{i\alpha} & -e^{i\alpha} & -e^{i\beta} & e^{i\beta} \end{pmatrix},$$

$$\mathbb{M}_0^\dagger\mathbb{M}_2 = \frac{1}{2}\begin{pmatrix} e^{i\phi_1} & e^{i\phi_1} & e^{i\phi_2} & e^{i\phi_2} \\ e^{i\phi_1} & e^{i\phi_1} & -e^{i\phi_2} & -e^{i\phi_2} \\ e^{i\phi_4} & -e^{i\phi_4} & e^{i\phi_3} & -e^{i\phi_3} \\ -e^{i\phi_4} & e^{i\phi_4} & e^{i\phi_3} & -e^{i\phi_3} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ e^{i\gamma} & -e^{i\gamma} & e^{i\delta} & -e^{i\delta} \\ -e^{i\gamma} & e^{i\gamma} & e^{i\delta} & -e^{i\delta} \end{pmatrix}.$$

Note: The matrices $\{\mathrm{I}_d, \mathbb{M}_0^\dagger\mathbb{M}_1(\alpha,\beta), \mathbb{M}_0^\dagger\mathbb{M}_2(\gamma,\delta)\}$ form a class of affine parametric MUBs for dimension 4.

Comparison to Goyenche et.al

- In Goyenche's construction: Introduction of parameters depends upon the existence of real MUBs in dimension $d = s^2$.
  Any set of m real MUBs existing in dimension $d > 2$ can admit the introduction of $\frac{(m-1)d}{2} = \frac{(m-1)s^2}{2}$ free parameters
- In our construction, we obtain a class of $MOLS(s) + 2$ many affine parametric MUBs for dimension $d = s^2$, which is independent of the existence of m real MUBs and each having $s(s-1)$ many free parameters other than the identity matrix.

Conclusion and Future Work

Main contribution:

- Novel construction of parametric MUBs
- More free parameters than previous methods

Thank You.