Mutually Unbiased Bases in Composite Dimensions

Dan McNulty

Department of Mathematics,
University of York

March 21, 2013

Outline

- **Introduction**
- What we know about MU bases
- Analogous problems
- Results for dimension six
- MU product bases
- Summary and conclusions

What are MU bases?

particle on a line

- position basis $|q\rangle$, $q \in \mathbb{R}$; momentum basis $|p\rangle$, $p \in \mathbb{R}$

$$|\langle q|p\rangle|^2 = \frac{1}{2\pi\hbar}$$

qubit, or spin 1/2

- standard basis $|j_z\rangle$, $j = 0, 1$; x-eignebasis $|k_x\rangle$, $k = 0, 1$

$$|\langle j_z|k_x\rangle|^2 = \frac{1}{2}$$

qudit in $\mathbb{C}^d$

- and two orthonormal bases $|\psi_j\rangle$ and $|\phi_k\rangle$, $j, k = 1, \ldots, d$

$$|\langle \psi_j|\psi_k\rangle|^2 = \frac{1}{d}$$

Complete sets of MU bases

- A **set** of $d+1$ orthogonal bases $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_d\}$ is mutually unbiased if each pair of bases $\mathcal{B}_i$ and $\mathcal{B}_j$ is mutually unbiased
- Dimension $d = 3$

$$I_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

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

where $\omega = e^{2\pi i/3}$ is a third root of unity

Why are MU bases interesting?

Applications

- Optimal state reconstruction [WKW&BDF]
- Quantum cryptography
- Quantum challenges: Mean King problem [LV *et. al*]
- Entanglement detection [CS *et al.*]
- Generalised Bell inequalities [S-WJ *et al.*]

Conceptually

- Complementarity for composite systems

Outline

- Introduction
- **What we know about MU bases**
- Analogous problems
- Results for dimension six
- MU product bases
- Summary and conclusions

MU bases for qudits, $d \in \mathbb{N}$

General results

- There are at most $(d+1)$ MU bases in $\mathbb{C}^d$ [WKW&BDF]
- Triples of MU bases exist for all d
- d MU bases in $\mathbb{C}^d$ gives rise to $(d+1)$ MU bases [MW]
- The entanglement content of a complete set is fixed [MW *et al.*]

Complete MU sets are equivalent to ...

- Maximal sets of d complex MU Hadamard matrices of order d
- Orthogonal decompositions of the Lie algebras $sl_d(\mathbb{C})$ [POB *et al.*]

MU bases in prime power dimensions

$d = p^n$, p a prime, $n \in \mathbb{N}$

Construction of complete sets from:

- Generalised Pauli matrices
- Commuting subsets of a unitary error basis
- Orthogonal Latin squares
- Discrete Fourier analysis over Galois fields
- Discrete Wigner functions

MU bases in composite dimensions

$d = p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, with $p_1^{n_1} < p_2^{n_2} < \ldots < p_k^{n_k}$

Positive

- $(p_1^{n_1} + 1)$ MU bases can be constructed
- $(p_1^{n_1} + 2)$ MU bases exist for specific dimensions (Latin squares imply six $(> 2^2 + 1)$ MU bases for $d = 2^2 \times 13^2$) [PW&TB]
- Entanglement content for complete MU set in $\mathbb{C}^p \otimes \mathbb{C}^q$ $\mathcal{E} = pq(p+q)$ [MW *et al.*]

Negative

- Plausible generalisations of constructions fail

Open questions for MU bases

Open problems

- Do complete sets of $(d+1)$ MU bases exist in $\mathbb{C}^d$?
- Does a complete set of seven MU bases exist in $\mathbb{C}^6$?
- Do four MU bases exist in $\mathbb{C}^6$?
- Does the MU constellation $\{6^3, 1\}$ exist in $\mathbb{C}^6$?

Conjecture

- Only three MU bases exist in $\mathbb{C}^6$ [GZ]
  (compatible with all known results)

Outline

- Introduction
- What we know about MU bases
- **Analogous problems**
- Results for dimension six
- MU product bases
- Summary and conclusions

Orthogonal decompositions of simple Lie algebras

Theorem [POB&VPR]
A set of μ MU bases $\mathcal{B}_1, \ldots, \mathcal{B}_\mu$ of $\mathbb{C}^d$ exists if and only if a set of μ pairwise orthogonal Cartan subalgebras $\mathcal{H}_1, \ldots, \mathcal{H}_\mu$ of $sl_d(\mathbb{C})$, closed under the adjoint operation, exists.

Conjecture

- The simple Lie algebra $sl_d(\mathbb{C})$ admits an orthogonal decomposition only if d is a prime power

Implication for MU bases

- Existence of orthogonal decomposition iff a complete set of MU bases exist

Complex Hadamard matrices

Definition

- A square matrix H of order d is a Hadamard matrix if it is unitary and all its elements have equal modulus

Open problem

- In dimension **six** a complete classification of Hadamard matrices is unknown
- Thus, a complete classification of pairs of MU bases remains unknown

Affine planes

Definition

An affine plane of order d is collection of d^2 points and $d(d+1)$ lines which satisfy the following

- Any two points lie on just one line
- Given any line ℓ and any point p not lying on ℓ, there exists exactly one line through p that is parallel (disjoint) to ℓ
- There exists three noncollinear points

Results on affine planes

- Affine planes of order $d = p^n$ exist for p prime, $n \in \mathbb{N}$
- No affine plane of order six exists.

Conjecture

- The non-existence of an affine plane of order d implies there exist less than $d+1$ MU bases [MS et al.]

Outline

- Introduction
- What we know about MU bases
- Analogous problems
- **Results for dimension six**
- MU product bases
- Summary and conclusions

Computer-aided results in dimension six

Numerical evidence

- No evidence for the existence of **four** MU bases [PB&WH],[SB&SW]

Exact numerics

(discretize phase space and use rigorous estimates)

- Pair $\{I, F_6(a,b)\}$: not part of a quadruple of MU bases – numerical calculation with rigorous error bounds [PJ et al.]

Computer-algebraic efforts

- Pair $\{I, F_6\}$: not part of a quadruple of MU bases [MG]
- Pair $\{I, S_6\}$: not part of a triple of MU bases [SB&SW]

Analytic results in dimension six

Existence results specific to $d = 6$

- There exists a three parameter family of complex Hadamard matrices of order six [BRK]
- Continuous families of MU triples exist

Limitations specific to $d = 6$

- Various construction methods yield at most three MU bases, e.g. monomial bases, nice error bases and Latin squares (affine planes) [POB et al.] [MA et al.]
- If a complete set contains three MU product bases, the remaining four bases contain entangled states only [MW et al.]
- No pair of real Hadamard matrices can be part of a complete set of MU bases [MM et al.]

Outline

- Introduction
- What we know about MU bases
- Analogous problems
- Results for dimension six
- MU product bases
- Summary and conclusions

All MU product bases of $\mathbb{C}^6$

Distinguish between two types of product bases

- *direct* product bases, e.g.

$$B_2 \otimes B_3 \equiv \{|j_z, J_z\rangle\}, \quad j_z = 0, 1 \quad J_z = 0, 1, 2$$

- *indirect* product bases, e.g.

$$\{|0_z, J_z\rangle, |1_z, J_x\rangle\}, \quad J_z, J_x = 0, 1, 2$$

Classify all sets of MU product bases for $d = 6$

- All pairs: four families $\mathcal{P}_0$,$\mathcal{P}_1$,$\mathcal{P}_2$ and $\mathcal{P}_3$
- All triples:

$$\mathcal{T}_0 = \{|j_z, J_z\rangle; |j_x, J_x\rangle; |j_y, J_y\rangle\}$$
$$\mathcal{T}_1 = \{|j_z, J_z\rangle; |j_x, J_x\rangle; |0_y, J_y\rangle, |1_y, J_w\rangle\}$$

The limited role of MU product bases

Complete list of triples $\mathcal{T}_0$ and $\mathcal{T}_1$ $\Longrightarrow$

- **Analytic results**
  No complete set contains three product bases $\{6^3\}_6^{\otimes}$
  (no state is MU to either $\mathcal{T}_0$ or $\mathcal{T}_1$)
  No complete set contains the product constellation $\{6^2, 4\}_6^{\otimes}$

Complete list of pairs $\mathcal{P}_0$,$\mathcal{P}_1$,$\mathcal{P}_2$ and $\mathcal{P}_3$ $\Longrightarrow$

- **Analytic result ∪ computer-aided results**
  A complete set contains at most one product basis
  (all MU pairs contain $\{I, F_6(a,b)\}$ or $\{I, S_6\}$ which do not extend to complete MU sets)

Outline

- Introduction
- What we know about MU bases
- Analogous problems
- Results for dimension six
- MU product bases
- **Summary and conclusions**

Summary and conclusions

Current status in dimension six

- Strong evidence for non-existence of complete MU sets
- $\{6^3, 1\}$ has never been observed
- Some MU pairs and triples are unextendible
- A complete MU set contains at most one product basis

Lessons?

- Existence of a complete MU set is surprising
- Sensitivity of quantum theory to factors of d

Thank you