Mutually Unbiased Bases: Existence and Non-Existence

Stefan Weigert

Department of Mathematics, University of York, United Kingdom

EQuaLS3 @ Kuala Lumpur, Malaysia - November 2009

Outline

Mutually Unbiased Bases: Existence and Non-Existence

- Introduction
- Classifying MU bases
- All MU bases for dimensions **two** to **five**
- MU bases in dimension **six**
  - **Analytical** results
  - **Numerical** results
- Conclusions

Outline

- **Introduction**
- Classifying MU bases
- All MU bases for dimensions two to five
- MU bases in dimension six
  - Analytical results
  - Numerical results
- Conclusions

Motivation

- What are MU bases?
- What are MU bases good for?
- What do we know about MU bases?
- What do we **not** know about MU bases?
- What do we know about MU bases in dimension six?

What are MU bases? (1)

a **pair** of MU bases in $\mathbb{C}^d$

- given two orthonormal bases $|\psi_j^{(1)}\rangle$ and $|\psi_k^{(2)}\rangle, j, k = 1 \ldots d$, one requires
$$|\langle\psi_j^{(b)}|\psi_k^{(b')}\rangle| = \chi_{jk}^{bb'} \equiv \begin{cases} \delta_{jk} & \text{if} \quad b = b' \\ 1/\sqrt{d} & \text{if} \quad b \neq b' \end{cases}$$
- given any orthonormal basis $\mathcal{B}_0$ in $\mathbb{C}^d$, one can construct a (symmetric) pair of MU bases, $\mathcal{B}_1, \mathcal{B}_2$ [S60]

What are MU bases? (2)

example: a **triple** of MU bases in $\mathbb{C}^2$:

- let $(m_x = \pm, \ldots)$

$$\mathcal{B}_1 = \{|m_x\rangle\}\,, \quad \mathcal{B}_2 = \{|m_y\rangle\}\,, \quad \mathcal{B}_3 = \{|m_z\rangle\}$$

  be the eigenstates of σ_x, σ_y, σ_z, resp., then

$$|\langle m_x|m_y\rangle|^2 = |\langle m_y|m_z\rangle|^2 = \ldots = \frac{1}{2}$$

- explicitly:

$$B_z = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad B_x = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad B_y = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ i & -i \end{pmatrix}$$

- there are no more...

What are MU bases? (3)

- A **complete set** of MU bases [I81,WF89] in $\mathbb{C}^d$,

$$\mathcal{B}_b = \{|\psi_j^{(b)}\rangle, j = 1 \ldots d\}, b = 1 \ldots d+1$$

consists of $d(d+1)$ pure states such that

$$\left|\langle\psi_j^{(b)}|\psi_{j'}^{(b')}\rangle\right| = \begin{cases} \delta_{jj'} & \text{if } b = b' \\ \frac{1}{\sqrt{d}} & \text{if } b \neq b' \end{cases}$$

- dimension $d = 3$:

$$B_0 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

$$B_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix} \qquad B_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}$$

where $\omega = e^{2\pi i/3}$

What are MU bases good for?

MU bases are used for

- optimal state estimation [WF89,AS08]
- quantum key distribution [BB84,BKB01,CBK02, KMB09,B09]
- generalised Bell inequalities [JLL08]
- quantum challenges: the mean king [AE01,EA01]
- see talks by T. Durt and B.-G. Englert

they **find** and **hide** (quantum) information

What do we know about MU bases?

results **independent** of the dimension d:

- no more than $(d+1)$ MU bases [WF89]
- have **triples** of MU bases for any d [KR03,G04]
- given d MU bases in $\mathbb{C}^d$, $d+1$ MU bases can be found [W09]
- a complete set of MU bases is **equivalent** to an orthogonal decomposition of the Lie algebra $sl_d(\mathbb{C})$ [BST07]

results for **prime power dimensions**, $d = p^k, k \in \mathbb{N}$:

- **complete sets** have been constructed using (cf. [K09])
  - discrete Fourier analysis over Galois fields/rings
  - discrete Wigner functions
  - generalized Pauli matrices
  - mutually orthogonal Latin squares
  - finite geometry methods

results for N **continuous variables**, $d = \infty$ [WW08]

- $N = 1$: **triples** of MU bases
- $N = 2$: **quintuples** of MU bases

What do we **not** know about MU bases?

- for **composite** dimensions $d = 6, 10, 12, \ldots$, the existence of complete MU bases is an **open** problem

- for **composite** dimensions $d = 6, 10, 12, \ldots$, the existence of orthogonal decomposition of the Lie algebra $sl_d(\mathbb{C})$ is an **open** problem

What do we know about MU bases for **composite** d?

results for $d = p_1^{k_1} p_2^{k_2} \ldots p_n^{k_n}$ (with $p_1^{k_1} < p_2^{k_2} < \ldots < p_n^{k_n}$):

- can construct $p_1^{k_1} + 1$ MU bases [KR03]
- for some square dimensions $d = s^2$, there are **more** [WB04]
  - e.g.: if $d = 2^2 \times 13^2$, there are 6 $(= 2^2 + 1 + 1)$ MU bases

prime powers are **sparse** for $d \to \infty$!

What do we know about MU bases in dimension six? (1)

analytic results:

- standard prime power construction **cannot** be extended to more than three MU bases [G04]
- **no four** MU bases have been found using a finite list of elements [BBE07]

numerical results:

- **no four** MU bases have been found by numerical searches [BH07]

other results:

- plausible generalisations of number theoretic formulas used for $d = p^r$ **fail** [A05]

conjecture:
There are **only three** MU bases in $\mathbb{C}^6$. [Z99]

What do we know about MU bases in dimension six?(2)

recent **analytic** result:

- all MU bases in dimensions **two** to **five** [BWB09]
- many candidates for MU bases can be excluded [BW09]

recent **numerical** results:

- many small MU constellations seemingly do not exist [BW08]

Outline

- Introduction
- **Classifying MU bases**
- All MU bases for dimensions two to five
- MU bases in dimension six
  - Analytical results
  - Numerical results
- Conclusions

Sets of MU bases in $\mathbb{C}^d$

pairs of MU bases in $\mathbb{C}^2$:

$$\{B_x, B_y\}, \{B_y, B_x\}, \{B_y, B_z\}, \ldots$$

more generally:

- How many **pairs** of MU bases exist in $\mathbb{C}^2$?
- How many **triples** of MU bases exist in $\mathbb{C}^2$?
- How many **pairs** of MU bases exist in $\mathbb{C}^2$?
- $\ldots$
- What types of sets of MU bases exist in $\mathbb{C}^d$?

Equivalent sets of MU bases

many sets of MU bases are **equivalent** to each other:

$$\{B_x, B_y\} \sim \{B_y, B_x\} \sim \{B_y, B_z\} \sim \ldots$$

transformations leaving $|\langle\psi_j^{(b)}|\psi_k^{(b')}\rangle| = \chi_{jk}^{bb'}$ **invariant**:

- an *overall unitary* transformation U
- $(r+1)$ *diagonal unitary* transformations D_ρ
- $(r+1)$ *permutations* of the elements *within* each basis
- *pairwise exchanges* of two bases
- *complex conjugation* of all bases

define a **standard form** of MU bases!

Equivalence transformations of sets of MU bases

two sets of $(r+1)$ MU bases are **equivalent** to each other

$$\{B_0, B_1, \ldots, B_r\} \sim \{B_0', B_1', \ldots, B_r'\}$$

if one is obtained from the other via

- $\{B_0, B_1, \ldots, B_r\} \to \{UB_0, UB_1, \ldots, UB_r\}$
- $\{B_0, B_1, \ldots, B_r\} \to \{B_0 D_0, B_1 D_1, \ldots, B_r D_r\}$
- $\{B_0, B_1, \ldots, B_r\} \to \{B_0 P_0, B_1 P_1, \ldots, B_r P_r\}$
- $\{\ldots, B_\rho, \ldots, B_{\rho'}, \ldots\} \to \{\ldots, B_{\rho'}, \ldots, B_\rho, \ldots\}$
- $\{B_0, B_1, \ldots, B_r\} \sim \{B_0^*, B_1^*, \ldots, B_r^*\}$

define a **standard form** of MU bases!

Standard form of four MU bases

four MU bases for $d = 3$: $\{I, B_1, B_2, B_3\}$ with

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

$$B_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix} \qquad B_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}$$

observation: the matrices B_ρ satisfy

- $B_k^\dagger B_k = I$ (unitarity)
- $|(B_k)_{ij}| = \frac{1}{\sqrt{d}}$, (constant moduli)

they are complex **Hadamard** matrices

Standard form for sets of MU bases (1)

any set of $(r+1)$ MU bases can be written as

$$\{I, H_1, \ldots, H_\rho \ldots, H_r\}$$

where

- first basis is the *standard basis* I
- all matrices H_ρ are complex Hadamard matrices
- first column of H_1 has entries $1/\sqrt{d}$ only
- first row of each Hadamard matrix has entries $1/\sqrt{d}$ only

Standard form for sets of MU bases (2)

example: four MU bases for $d = 3$: $\{I, B_1, B_2, B_3\}$

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \qquad B_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

$$B_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix} \qquad B_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}$$

where

- first basis is the *standard basis* I
- all matrices B_ρ are complex Hadamard matrices
- first column of B_1 has entries $1/\sqrt{3}$ only
- first row of each Hadamard matrix has entries $1/\sqrt{3}$ only
- B_1 has been *dephased*

Pairs of MU bases in $\mathbb{C}^d$

strategy:

- suppose we knew **all** complex Hadamard H matrices in $\mathbb{C}^d$
- then: all pairs $\{I, H\}$ are candidates for inequivalent MU bases
- apply equivalence transformations to obtain standard form
- list remaining inequivalent ones
- done!

need a **list**!

catalog of known complex $(d \times d)$ Hadamard matrices [TZ06]:

- **complete** classification for $d \leq 5$
- **incomplete** classification for $d \geq 6$

MU vectors

task: given $\{I, H\}$ construct additional MU bases

idea: search for all **vectors** $|v\rangle \in \mathbb{C}^d$ which are MU to both I and H in the pair $\{I, H\}$

properties of MU vectors $|v\rangle \in \mathbb{C}^d$:

- $|v_i| = 1/\sqrt{d}$
- $|\langle h(k)|v\rangle| = 1/\sqrt{d}\,, \qquad k = 1, \ldots, d$

requirements on MU vectors $|v\rangle$ to form a *third* MU basis:

- need d independent vectors
- pairwise orthogonality

How to construct sets of MU bases $\mathbb{C}^d$

strategy:

- choose a Hadamard matrix H
- list the constraints on vectors MU to $\{I, H\}$
- determine all solutions
- list all MU vectors $|v_1\rangle, |v_2\rangle, \ldots$
- analyse the vectors to identify additional ON-bases

apply to

- dimensions two to five
- dimension six

Outline

- Introduction
- Classifying MU bases
- **All MU bases for dimensions two to five** [BWB09]
- MU bases in dimension six
  - Analytical results
  - Numerical results
- Conclusions

Dimension $d = 2$

only one dephased complex Hadamard matrix exists in $\mathbb{C}^2$:

$$F_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad \text{(Fourier matrix)}$$

vectors MU to I: $|v\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ e^{i\alpha} \end{pmatrix}, \alpha \in [0, 2\pi)$

vectors MU to $\{I, F_2\}$ satisfy: $\left|1 \pm e^{i\alpha}\right| = \sqrt{2}$

two solutions: $e^{i\alpha} = \pm i \Rightarrow |v_\pm\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ \pm i \end{pmatrix}$

new Hadamard matrix: $H_2 = (v_+ | v_-)$

all sets of MU bases in $\mathbb{C}^2$:

$\{I, F_2\}, \{I, F_2, H_2\}$

Dimension $d = 3$

only one dephased complex Hadamard matrix exists in $\mathbb{C}^3$:

$$F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix} \text{ (Fourier matrix)}$$

vectors MU to I: $|v\rangle = (1, e^{i\alpha}, e^{i\beta})^T/\sqrt{3}, \alpha, \beta \in [0, 2\pi)$
vectors MU to $\{I, F_3\}$ satisfy:

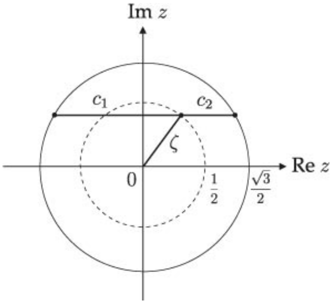
$$\begin{aligned} \sqrt{3} &= |1 + e^{i\alpha} + e^{i\beta}| \\ \sqrt{3} &= |1 + \omega e^{i\alpha} + \omega^2 e^{i\beta}| \\ \sqrt{3} &= |1 + \omega^2 e^{i\alpha} + \omega e^{i\beta}| \end{aligned}$$

graphical solution . . .

Dimension $d = 3$ (cont'd)

... or, with some ζ of modulus $1/2$:

$$\left|\zeta + \cos\frac{\alpha}{2}\right| = \frac{\sqrt{3}}{2} \quad \text{and} \quad \left|\zeta + \cos\left(\frac{\alpha}{2} \pm \frac{2\pi}{3}\right)\right| = \frac{\sqrt{3}}{2}$$



$\Rightarrow$ **six** solutions $(\alpha_j, \beta_j)\,, j = 1 \ldots 6$

Dimension $d = 3$ (cont'd)

$\Rightarrow$ six vectors $|v_1\rangle, \ldots, |v_6\rangle$

two new Hadamard matrices:

$$H_3 = (v_1|v_2|v_3) \text{ and } J_3 = (v_4|v_5|v_6)$$

$$H_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{pmatrix} \quad J_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{pmatrix}$$

note: $\{I, F_3, H_3\} \sim \{I, F_3, J_3\}$

all sets of MU bases in $\mathbb{C}^3$:

$\{I, F_3\}, \{I, F_3, H_3\}, \{I, F_3, H_3, J_3\}$

Triples of MU bases in dimension $d = 4$

one-parameter set ($x \in [0, \pi)$) of Hadamard matrices exists in $\mathbb{C}^4$:

$$F_4(x) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & ie^{ix} & -ie^{ix} \\ 1 & -1 & -ie^{ix} & ie^{ix} \end{pmatrix}, \quad \text{Fourier family}$$

note: Fourier matrix $F_4(0) \equiv F_4$ and $F_4(\pi/2) \equiv F_2 \otimes F_2$

geometric arguments similar to those for $\mathbb{C}^3$:

$$H_4(y,z) = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ -e^{iy} & e^{iy} & e^{iz} & -e^{iz} \\ e^{iy} & -e^{iy} & e^{iz} & -e^{iz} \end{pmatrix}$$

three parameter-family of triples: $\{I, F_4(x), H_4(y,z)\}$

All sets of MU bases in dimension $d = 4$

there is **one quadruple** of MU bases in $\mathbb{C}^4$:

$$\{I, F_4(\pi/2), H_4, J_4\}$$

there is **one quintuple** of MU bases in $\mathbb{C}^4$:

$$\{I, F_4(\pi/2), H_4, J_4, K_4\}$$

all sets of MU bases in $\mathbb{C}^4$:

$$\{I, F_4(x)\}$$
$$\{I, F_4(x), H_4(y, z)\}$$
$$\{I, F_4(\pi/2), H_4, J_4\}$$
$$\{I, F_4(\pi/2), H_4, J_4, K_4\}$$

All sets of MU bases in dimension $d = 5$

only one dephased complex Hadamard matrix exists in $\mathbb{C}^5$:

$$F_5 = \frac{1}{\sqrt{5}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{pmatrix}, \quad \omega = e^{2\pi i/5}$$

computer-assisted (cf. later) **exact** result:

all sets of MU bases in $\mathbb{C}^5$:

$$\{I, F_5\}$$
$$\{I, F_5, H_5\}, \{I, F_5, J_5\}$$
$$\{I, F_5, H_5, J_5\}$$
$$\{I, F_5, H_5, J_5, K_5\}$$
$$\{I, F_5, H_5, J_5, K_5, L_5\}$$

All MU bases for dimensions two to five

	$\mathbb{C}^2$	$\mathbb{C}^3$	$\mathbb{C}^4$	$\mathbb{C}^5$	$\mathbb{C}^6$
pairs	1	1	∞^1	1	$\geq \infty^2$
triples	1	1	∞^3	2	$\geq \infty^1$
quadruples	-	1	1	1	?
quintuples	-	-	1	1	?
sextuples	-	-	-	1	?

main results:

- a three-parameter family of triples in $\mathbb{C}^4$
- two inequivalent triples in $\mathbb{C}^5$
- prime power construction of complete sets is unique for $d \leq 5$

Outline

- Introduction
- Classifying MU bases
- All MU bases for dimensions two to five
- MU bases in dimension six
  - **Analytic** results [BW09]
  - Numerical results
- Conclusions

Overview

- MU bases and complex Hadamard matrices
- known Hadamard matrices in dimension six
- MU vectors as solutions of multivariate polynomial equations
- Buchberger's algorithm and Gröbner bases
- Result: only **triples** of MU bases in $\mathbb{C}^6$ (so far)

MU bases and complex Hadamard matrices

$(d+1)$ MU bases in $\mathbb{C}^d$ are characterized by

d **complex** $(d \times d)$ **Hadamard matrices** $H, H', H'' \ldots$, satisfying

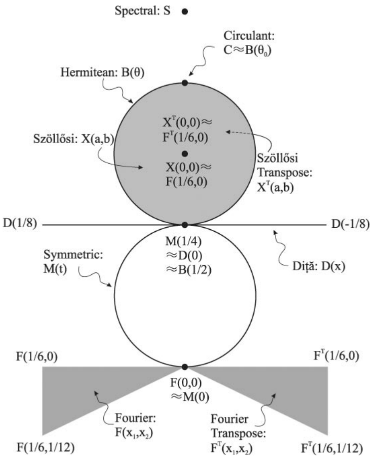
- $|H_{ij}| = 1/\sqrt{d}\,, \qquad i,j = 1,\ldots,d$
- $H^\dagger H' = H''$

example ($\omega = e^{2\pi i/3}$):

$$I\,, \quad H_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}\,, \quad H_2 = \ldots\,, \quad H_3 = \ldots$$

- given $\{I, F_6\}$, **no** further MU vectors have been found [G04]
- generalize F_6 to any complex Hadamard matrix H
- complete classification for $d \leq 5$ only!

Complex Hadamard matrices of dimension six



- landscape of **known** Hadamard matrices for $d = 6$
- recent two-parameter family: $K(x, y)$ [Ka09]

Constructing MU vectors in $\mathbb{C}^d$

given: identity I and some Hadamard matrix H
find all $|v\rangle \in \mathbb{C}^d$ MU w.r.t. to the columns $|h(k)\rangle$ of H and of I

- $|v_k| = 1/\sqrt{d}$
- $|\langle h(k)|v\rangle|^2 = 1/d\,, \quad k = 1, \ldots, d$

algorithm

- choose a Hadamard matrix H
- list the constraints
- construct solutions **using Buchberger's algorithm**! [G04]
- list all MU vectors
- analyse the vectors

Buchberger's algorithm: solving polynomial equations

Buchberger's algorithm [B65]:
Gaussian elimination for non-linear polynomial equations!

$$x^2 - y = 0 \ \& \ x - y = 0 \quad \Leftrightarrow \quad x^2 - x = 0 \ \& \ x - y = 0$$

with solutions $(x, y) = (0, 0)$ or $(1, 1)$

search for **simple** description of the algebraic variety:

- **have** polynomials $P \equiv \{p_n(\mathbf{x}), n = 1, \ldots, N\}$
- **want** solutions of $P = 0$
- use **Buchberger's algorithm** to find **Gröbner basis** for P: $G = \{g_m(\mathbf{x}), m = 1, \ldots, M\}$
- **solve** 'triangular' set of equations $G = 0$

Example: four MU bases in $\mathbb{C}^3$

- choose $H \equiv F_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$, where $\omega = e^{2\pi i/3}$
- **constraints** $P = 0$, using $v = (1, x_1 + iy_1, x_2 + iy_2)^T/\sqrt{3}$:

$$\begin{aligned} 1 - x_1^2 - y_1^2 &= 0 \\ 1 - x_2^2 - y_2^2 &= 0 \\ x_1 + x_2 + x_1 x_2 + y_1 y_2 &= 0 \\ x_1 + x_2 - \sqrt{3} y_1 + \sqrt{3} y_2 + x_1 x_2 - \sqrt{3} x_1 y_2 + \sqrt{3} y_1 x_2 + y_1 y_2 &= 0 \end{aligned}$$

- find Gröbner basis using Buchberger's algorithm
- list all MU vectors
- analyse the vectors

Example: four MU bases in $\mathbb{C}^3$ (2)

- choose $H \equiv F_3$
- constraints $P = 0$
- **find Gröbner basis** G via Buchberger's algorithm, put $G = 0$:

$$\begin{aligned} 3y_2 - 4y_2^3 &= 0 \\ 1 - x_2 - 2y_2^2 &= 0 \\ 1 + 2x_1 + 4y_1y_2 - 4y_2^2 &= 0 \\ 3 - 4y_1^2 + 4y_1y_2 - 4y_2^2 &= 0 \end{aligned}$$

  with solutions:

$$\begin{aligned} \mathbf{s}_a &= \tfrac{1}{2}(-1,-1,\sqrt{3},\sqrt{3})\,, & \mathbf{s}_b &= \tfrac{1}{2}(-1,2,-\sqrt{3},0)\,, \\ \mathbf{s}_c &= \tfrac{1}{2}(2,-1,0,-\sqrt{3})\,, & \mathbf{s}_d &= \tfrac{1}{2}(-1,-1,-\sqrt{3},-\sqrt{3})\,, \\ \mathbf{s}_e &= \tfrac{1}{2}(2,-1,0,\sqrt{3})\,, & \mathbf{s}_f &= \tfrac{1}{2}(-1,2,\sqrt{3},0) \end{aligned}$$

- list all MU vectors
- analyse the vectors

Example: four MU bases in $\mathbb{C}^3$ (3)

- choose $H \equiv F_3$
- constraints $P = 0$
- solve $G = 0$ to find $\mathbf{s}_a, \ldots, \mathbf{s}_f$
- **list MU vectors**:

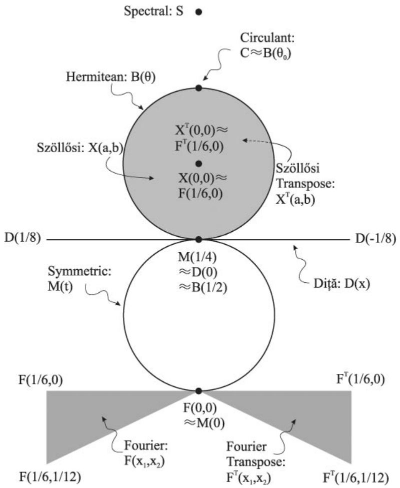
$$v_a = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega \end{pmatrix}, \; v_b = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ 1 \end{pmatrix}, \; v_c = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega^2 \end{pmatrix},$$
$$v_d = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega^2 \end{pmatrix}, \; v_e = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ \omega \end{pmatrix}, \; v_f = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ 1 \end{pmatrix}$$

- **analyse the vectors**: $H_3 \sim [v_a, v_b, v_c]$ and $H_2 \sim [v_d, v_e, v_f]$
- **done**

Results: Special Hadamard matrices

H	N_v	N_t
F_6	48	16
$D(0)$	120	10
C	38	0
S	90	0

- N_v: number of vectors MU to $\{I, H\}$
- N_t: number of triples of MU bases

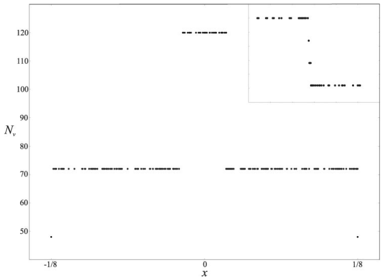


Results: Affine Hadamard matrices

H	$\mathbf{x}$	$\#(\mathbf{x})$	N_v	N_t
$D(x)$	grid Γ_D	36	$72/120$	4
	random	500	$72/120$	4
$F(\mathbf{x})$	grid Γ_F	168	48	$8/70$
	random	2,000	48	8
$F^T(\mathbf{x})$	grid Γ_F	168	48	$8/70$
	random	2,000	48	8

- $\#(\mathbf{x})$: points chosen
- N_v: vectors MU to $\{I, H\}$
- N_t: triples of MU bases

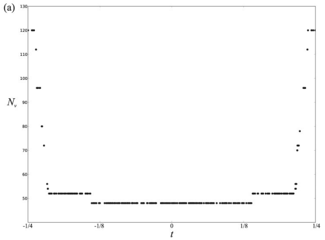
Diţă



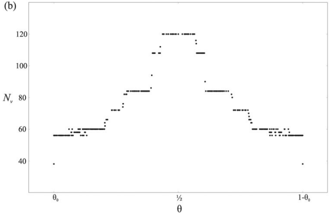
Results: Non-affine Hadamard matrices (approximate!)

H	$\mathbf{x}$	$\#(\mathbf{x})$	N_v	N_t
$M(t)$	grid Γ_M	70	48-120	0
	random	300	48-120	0
$B(\theta)$	grid Γ_B	34	56-120	0
	random	300	56-120	0

symmetric



Hermitean

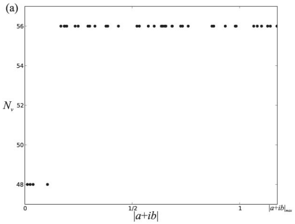


- $N_v(t)$ for the pair $\{I, M(t)\}$
- $N_v(\theta)$ for the pair $\{I, B(\theta)\}$

Results: Szöllősi family (approximate!)

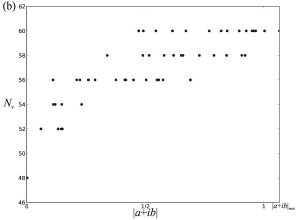
H	$\mathbf{x}$	$\#(\mathbf{x})$	N_v	N_t
$X(a,b)$	Λ	50	$48/56$	0
	Λ'	50	48-60	0
	random	300	48-120	0

along the line Λ



- N_v for the pair $\{I, X(a,b)\}$

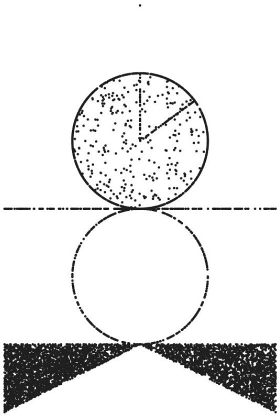
along the line Λ'



- N_v for the pair $\{I, X(a,b)\}$

Summary

29,000hrs later, on a single 2.2 GHz processor:



At most **three** MU bases in $\mathbb{C}^6$ for 5,980 cases!

- Fourier families allow for MU triples only [JMM09]

Outline

- Introduction
- Classifying MU bases
- All MU bases for dimensions two to five
- MU bases in dimension six
  - Analytic results
  - **Numerical** results [BW08]
- Conclusions

Overview

- MU constellations
- Numerical results
- Summary

MU constellations

search **numerically** for complete sets of MU bases in $\mathbb{C}^6$

problem: search for seven complex (6×6) matrices
$\rightarrow 7 \times 2 \times 6^2 = 504$ real parameters!

idea: consider **subsets** of complete MU bases

define MU **constellations**:

$$\{x\}_d \equiv \{x_0, x_1, \ldots, x_d\}_d$$

i.e. $d+1$ sets of x_b pure states that define the MU conditions

MU constellations define a **lattice**:

- **all** smaller MU constellations must exist for a complete set
- any **missing** subset implies non-existence of a complete set

Examples of MU constellations

MU **constellations**:

$$\{x\}_d \equiv \{x_0, x_1, \ldots, x_d\}_d\,, \quad x \in (\mathbb{Z} \bmod (d-1))^{d+1}$$

note: need to specify only $(d-1)$ vectors in each basis

Examples:

- $\{2,2,2,2\}_3$ is a complete set in $\mathbb{C}^3$
- Butterley and Hall studied $\{5,5,5,5\}_6$ [BH07]
- We can always find $\{d-1, d-1, d-1\}_d$ [KR03]
- Grassl considered $\{5,5,5,1\}_6$ containing $\{I, F_6\}$ [G04]

MU constellations as global minima

consider constellations of the form $\{5, x, y, z\}_6$

define a continuous function

$$F(\vec{\alpha}) = \sum_{\text{all indices}} \left(|\langle \psi_j^b(\vec{\alpha}) | \psi_{j'}^{b'}(\vec{\alpha}) \rangle| - \chi_{jj'}^{bb'} \right)^2$$

where

$$\chi_{jj'}^{bb'} = \begin{cases} \delta_{jj'} & \text{if } b = b' \\ \frac{1}{\sqrt{d}} & \text{if } b \neq b' \end{cases}$$

then, a constellation **is** MU if

$$F(\vec{\alpha}) = 0$$

Minimising $F(\vec{\alpha})$

- use form with fewest possible parameters
- search for minima starting at random points
- use method by Levenberg-Marquardt
- take $F(\vec{\alpha}) < 10^{-7}$ as numerical cut-off for a zero

this is a **hard problem**: can get stuck in **local** minima!

Testing the program

success rates for searches of constellations $\{d-1, d-1, d-1\}_d$:

d	2	3	4	5	6	7	8
%	100.0	81.9	96.6	49.3	67.9	24.0	48.5

success rates for searches of MU constellations $\{4, x, y, z\}_5$:

$d=5$	parameters p_5				success rate			
x, y	z				z			
	1	2	3	4	1	2	3	4
1,1	8	-	-	-	100.0	-	-	-
2,1	12	-	-	-	100.0	-	-	-
2,2	16	20	-	-	100.0	96.4	-	-
3,1	16	-	-	-	100.0	-	-	-
3,2	20	24	-	-	92.0	35.7	-	-
3,3	24	28	32	-	68.3	38.0	29.0	-
4,1	20	-	-	-	99.0	-	-	-
4,2	24	28	-	-	56.2	37.0	-	-
4,3	28	32	36	-	55.8	31.8	21.8	-
4,4	32	36	40	44	37.4	20.1	14.9	9.7

1,000 initial points randomly chosen in $\mathcal{C}_5(4, x, y, z)$

success rates for searches of MU constellations $\{6, x, y, z\}_7$:

$d = 7$	parameters p_7						success rate					
x, y	z						z					
	1	2	3	4	5	6	1	2	3	4	5	6
1,1	12	-	-	-	-	-	100.0	-	-	-	-	-
2,1	18	-	-	-	-	-	100.0	-	-	-	-	-
2,2	24	30	-	-	-	-	100.0	100.0	-	-	-	-
3,1	24	-	-	-	-	-	100.0	-	-	-	-	-
3,2	30	36	-	-	-	-	100.0	100.0	-	-	-	-
3,3	36	42	48	-	-	-	100.0	100.0	99.3	-	-	-
4,1	30	-	-	-	-	-	100.0	-	-	-	-	-
4,2	36	42	-	-	-	-	100.0	100.0	-	-	-	-
4,3	42	48	54	-	-	-	99.9	95.6	0.0	-	-	-
4,4	48	54	60	66	-	-	52.3	0.0	0.0	0.0	-	-
5,1	36	-	-	-	-	-	100.0	-	-	-	-	-
5,2	42	48	-	-	-	-	100.0	37.9	-	-	-	-
5,3	48	54	60	-	-	-	2.6	0.0	0.1	-	-	-
5,4	54	60	66	72	-	-	0.0	0.0	0.0	0.1	-	-
5,5	60	66	72	78	84	-	0.2	0.2	0.2	0.1	0.2	-
6,1	42	-	-	-	-	-	57.5	-	-	-	-	-
6,2	48	54	-	-	-	-	1.1	0.0	-	-	-	-
6,3	54	60	66	-	-	-	0.0	0.1	0.0	-	-	-
6,4	60	66	72	78	-	-	0.2	0.0	0.1	0.3	-	-
6,5	66	72	78	84	90	-	0.3	0.4	0.1	0.1	0.1	-
6,6	72	78	84	90	96	102	0.5	0.2	0.2	0.0	0.4	0.3

1,000 initial points randomly chosen in $\mathcal{C}_7(6, x, y, z)$

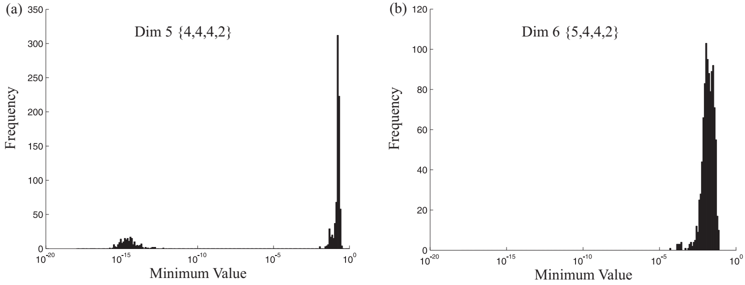
Application to Dimension 6

success rates for searches of MU constellations $\{5, x, y, z\}_6$:

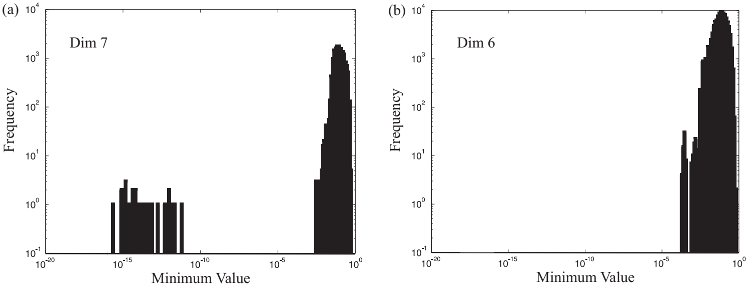
$d = 6$	parameters p_6					success rate				
x, y	z					z				
	1	2	3	4	5	1	2	3	4	5
1,1	10	-	-	-	-	100.00	-	-	-	-
2,1	15	-	-	-	-	100.00	-	-	-	-
2,2	20	25	-	-	-	100.00	100.00	-	-	-
3,1	20	-	-	-	-	100.00	-	-	-	-
3,2	25	30	-	-	-	99.95	100.00	-	-	-
3,3	30	35	40	-	-	99.42	39.03	0.00	-	-
4,1	25	-	-	-	-	100.00	-	-	-	-
4,2	30	35	-	-	-	92.92	44.84	-	-	-
4,3	35	40	45	-	-	12.97	0.00	0.00	-	-
4,4	40	45	50	55	-	0.74	0.00	0.00	0.00	-
5,1	30	-	-	-	-	95.40	-	-	-	-
5,2	35	40	-	-	-	76.71	10.96	-	-	-
5,3	40	45	50	-	-	1.47	0.00	0.00	-	-
5,4	45	50	55	60	-	0.00	0.00	0.00	0.00	-
5,5	50	55	60	65	70	0.00	0.00	0.00	0.00	0.00

10,000 initial points randomly chosen in $\mathcal{C}_6(5, x, y, z)$

Histograms of search results



Log-log histograms of search results



Summary

seemingly, not all MU constellations $\{5, x, y, z\}_6$ exist:

- only 18 MU constellations identified
- 17 unobserved MU constellations
- **largest existing** constellation is $\{5, 5, 3, 1\}_6$ with 16 states
- **smallest missing** sets: $\{5, 3, 3, 3\}_6$ and $\{5, 4, 3, 2\}_6$

strongest numerical evidence for non-existence of $\{5^7\}_6$ so far!

observation:
$\{5^7\}_6$ has **145** free parameters and there are **495** constraints!

Counting parameters

free parameters of the constellation $\{(d-1)^{d+1}\}_d$:

$$p_d = (d-1)(d^2-d-1)$$

number of **constraints** on the vectors in $\{(d-1)^{d+1}\}_d$:

$$c_d = \frac{1}{2}d(d-1)(d^2-3)$$

thus

$$c_d > p_d\,, \quad d > 2$$

e.g. in dimension 7:

$$c_7 = 1328 > 288 = p_7$$

Outline

- Introduction
- Classifying MU bases
- All MU bases for dimensions two to five
- MU bases in dimension six
  - Analytic results
  - Numerical results
- **Conclusions**

Conclusions

main observations in dimension $d = 6$:

- **no** evidence for seven MU bases
- evidence for **non**-existence of seven MU bases

moral:

- surprise: **existence** of some complete sets of MU bases!
- **plausibility** of non-existence from parameter counting!

implications for physics:

- optimal state estimation only in prime powers dimensions?!
- properties of quantum systems vary with dimension:
  kinematics of two qubits different from qubit-qutrit system?
- **has number** theory yet another say on quantum theory?

References

[A05] C. Archer, J. Math. Phys. **46** 022106 (2005)

[AE01] Y. Aharonov and B.-G. Englert, Z. Naturforsch. **56**a, 16 (2001)

[AS08] R.B. Adamson and A.M. Steinberg: *Improving Quantum State Estimation with Mutually Unbiased Bases*, arXiv:0808.0944

[B09] S. Brierley: *Quantum Key Distribution Highly Sensitive to Eavesdropping* arXIV:0910.2578

[B65] B. Buchberger, *An Algorithm for Finding the Basis Elements of the Residue Class Ring of a Zero Dimensional Polynomial Ideal.* Ph.D. Dissertation, University of Innsbruck (1965) (English translation by M. Abramson in J. Symb. Comp. **41**, 471 (2006))

[BBE07] I. Bengtsson, W. Bruzda, Å. Ericsson, J-Å. Larsson, W. Tadej and K.Życzkowski, Mubs and Hadamards of order six, J. Math. Phys. **48**, 052106 (2007)

[BBR02] S. Bandyopadhyay, P.O. Boykin, V. Roychowdhury, and F. Vatan Algorithmica **34**, 512 (2002)

[BH07] P. Butterley and W. Hall, Phys. Lett. A **369**, 5 (2007)

[BKB01] M. Bourennane, A. Karlsson and G. Björk, Phys. Rev. A **64**, 012306 (2001)

[BST07] P.O. Boykin, M. Sitharam, P.H Tiep and P. Wocjan, Quantum Inf. Comp. **7**, 371 (2007)

[BW08] S. Brierley and S. Weigert, Phys. Rev. A **78**, 042312 (2008)

[BW09] S. Brierley and S. Weigert: Phys. Rev. A **79**, 052316 (2009)

[BWB09] S. Brierley, S. Weigert and I. Bengtsson, *All mutually unbiased bases in dimensions two to five*, arXiv:0907.4097

[CBK02] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin: Phys. Rev. Lett. **88**, 127902 (2002)

[EA01] B.-G. Englert, Y. Aharonov, Phys. Lett. A **284**, 1 (2001)

[G04] M. Grassl, *On SIC-POVMs and MUBs in Dimension 6*, in: *Proc. ERATO Conference on Quantum Information Science (EQUIS 2004)*, J. Gruska (ed.)

[I81] I. D. Ivanović, J. Phys. A **14**, 3241 (1981)

[JLL08] S-W Ji, J. Lee, J Lim,K Nagata,H-W Lee, Phys. Rev. A **78**, 052103 (2008)

[JMM09] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi and M. Weiner, J. Phys. A: Math. Theor. **42** 245305 (2009)

[Ka09] B.R. Karlsson, J. Math. Phys. **50**, 082104 (2009)

[K09] M. Kibler, *An angular momentum approach to quadratic Fourier transform, Hadamard matrices, Gauss sums, mutually unbiased bases, unitary group and Pauli group*, arXiv:0907.2838

References

[KMB09] M. Khan, M. Murphy and A. Beige, New J. Phys. **11**, 063043 (2009)

[KR03] A. Klappenecker, M. Rötteler, *Constructions of Mutually Unbiased Bases*, quant-ph/0309120

[S60] J. Schwinger, Proc. Nat. Acad. Sci. U.S.A., **46**, 560, (1960)

[TZ06] W. Tadej and K. Życzkowski, Open Systems and Infor. Dyn. **13** 133-177 (2006) (cf. `http://chaos.if.uj.edu.pl/~karol/hadamard/`

[W09] M. Weiner: *A gap for the maximum number of mutually unbiased bases*, arXiv:0902.0635

[WB04] P. Wocjan and T. Beth, *New Construction of Mutually Unbiased Bases in Square Dimensions*, arXiv:quant-ph/0407081

[WF89] W. K. Wootters and B. D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989)

[WW08] S. Weigert and M. Wilkinson, Phys. Rev. A **78**, 020303(R) (2008)

[Z99] G. Zauner, *Quantendesigns. Grundzüge einer nichtkommutativen Designtheorie.* PhD thesis, University of Wien, 1999.