Mutually Unbiased Product Bases

Stefan Weigert

THE UNIVERSITY *of York*

Department of Mathematics, University of York, United Kingdom

Hadamard 2017, Budapest - 11 July 2017

Outline

- **What are MU bases?**
  - concepts and examples
  - Why are MU bases interesting?
- What do we know about MU bases?
- MU product bases
- Summary

What are MU bases?

quantum particle on a line

- position and momentum eigenstates

$$\hat{p}|p\rangle = p|p\rangle\,, \qquad \hat{q}|q\rangle = q|q\rangle\,, \qquad p, q \in \mathbb{R}$$

- ON bases of $L_2(\mathbb{R})$: $\mathcal{B}_p = \{|p\rangle, p \in \mathbb{R}\}$ and $\mathcal{B}_q = \{|q\rangle, q \in \mathbb{R}\}$

prepare position eigenstate $|q\rangle$ and ...

- measure position $\hat{q}$ $\quad\rightarrow\quad$ find q
- measure momentum $\hat{p}$ $\quad\rightarrow\quad$ find any $p \in \mathbb{R}$

flat transition probability density

- $\mathcal{B}_p$ and $\mathcal{B}_q$ are mutually unbiased (MU)

$$\mathcal{B}_p\,\mu\,\mathcal{B}_q \quad\Leftrightarrow\quad |\langle q|p\rangle|^2 = \frac{1}{2\pi\hbar}\,, \qquad p, q \in \mathbb{R}$$

What are MU bases?

quantum spin $s = 1/2$ - or **qubit** with state space $\mathbb{C}^2$

- eigenstates of spin components $\hat{\sigma}_z$ and $\hat{\sigma}_x$

$$\hat{\sigma}_z|j_z\rangle = j_z|j_z\rangle\,, \qquad \hat{\sigma}_x|j_x\rangle = j_x|j_x\rangle\,, \quad j_z, j_x = 0, 1$$

- ON bases of $\mathbb{C}^2$: $\mathcal{B}_z = \{|0_z\rangle, |1_z\rangle\}$ and $\mathcal{B}_x = \{|0_x\rangle, |1_x\rangle\}$

prepare $\hat{\sigma}_z$ **eigenstate** $|0_z\rangle$ **and** ...

- measure z-component $\hat{\sigma}_z \quad \rightarrow \quad$ find 0
- measure x-component $\hat{\sigma}_x \quad \rightarrow \quad$ find any j_x

flat transition probabilities

- $\mathcal{B}_z$ and $\mathcal{B}_x$ are mutually unbiased (MU)

$$\mathcal{B}_z \, \mu \, \mathcal{B}_x \quad \Leftrightarrow \quad |\langle j_z | j_x \rangle|^2 = \frac{1}{2}\,, \qquad j = 0, 1$$

What are MU bases?

complete sets of $(d+1)$ MU bases in $\mathbb{C}^d$...

- ... consist of $(d+1)$ ON bases $\mathcal{B}_b = \{|\psi_j^{(b)}\rangle, j = 1 \dots d\}$

$$\mathcal{B}_b \,\mu\, \mathcal{B}_{b'} \quad \Leftrightarrow \quad |\langle\psi_j^{(b)}|\psi_{j'}^{(b')}\rangle|^2 = \begin{cases} \delta_{jj'} & \text{if } b = b' \\ 1/d & \text{if } b \neq b' \end{cases}$$

example: dimension $d = 3$, with $\omega \equiv e^{2\pi i/3}$ and $1 + \omega + \omega^2 = 0$

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

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

F_3, H, H' are complex Hadamard matrices

Why are MU bases interesting?

conceptually

- concise expression of complementarity
- benchmark states for inequalities
- ubiquitious in quantum information

mathematically

- orthogonal decompositions of Lie algebras $sl_d(\mathbb{C})$
- complete sets of MU bases define 2-designs

physical applications

- quantum cryptography (two MU bases)
- entanglement detection (many MU bases)
- optimal quantum state reconstruction in $\mathbb{C}^d$ (complete sets)

Outline

- What are MU bases?
- **What do we know about MU bases?**
  - arbitrary dimensions
  - prime power dimensions
  - composite dimensions
  - open problems
- MU product bases
- Summary

MU bases for $d > 2$

general results

- upper limit: there are at most $(d+1)$ MU bases in $\mathbb{C}^d$
- minimal number: triples of MU bases exist for all d
- one "free" basis: d MU bases in $\mathbb{C}^d \longrightarrow (d+1)$ MU bases
- entanglement content of a complete set is fixed

complete MU sets are equivalent to . . .

- maximal sets of d complex MU Hadamard matrices of order d
- orthogonal decompositions of the Lie algebras $sl_d(\mathbb{C})$

Should we expect complete MU sets in $\mathbb{C}^d$?

- **No!**
  $d = 7$: 1328 constraints $\gg$ 288 free parameters

MU bases in prime power dimensions $d = p^n$

canonical construction

- Heisenberg-Weyl algebra

$$ZX = \omega XZ\,, \qquad \omega^d = 1$$

- phase and shift operators
$$Z|k\rangle = \omega^k |k\rangle\,, \qquad X|k\rangle = |k+1\rangle\,, \qquad k = 1 \ldots d$$

- $(d+1)$ MU bases are given by the eigenstates of the operators
$$X\,, Z\,, ZX\,, ZX^2\,, \ldots ZX^{d-1}$$

many other constructions

- orthogonal Latin squares
- discrete Wigner functions
- methods from finite geometry

MU bases in composite dimensions

non-prime-power dimensions

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

positive results

- $(p_1^{n_1} + 1)$ MU bases can be constructed
- $(p_1^{n_1} + 2)$ MU exist for specific dimensions
  - **six** MU bases exist for $d = 2^2 \times 13^2$ (not just five)
- entanglement content for complete MU set in $\mathbb{C}^p \otimes \mathbb{C}^q$

$$\mathcal{E} = pq(p+q)$$

negative results

- plausible generalizations of constructions **fail**

What we don't know about MU bases

ever simpler open problems,...

- Do complete sets of $(d+1)$ MU bases exist for all $\mathbb{C}^d$?
- 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 $\{6^3, 1\}_6$ exist in $\mathbb{C}^6$?
- List all pairs of MU bases $\{I, H\}$!
  (requires a list of all complex Hadamard matrices of order six)

conjecture (Zauner 1999)

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

Outline

- Introduction
- What do we know about MU bases?
- **MU product bases** (with D McNulty & B Pammer)
  - ... in bipartite systems with $d = 6$
  - ... in bipartite systems with $d = pq$
  - ... in some multipartite systems with $d = d_1 d_2 \ldots d_n$
- Summary

MU product bases

types of orthogonal product bases

- direct product bases:
  - example in $\mathbb{C}^6$: $\{|j_z, J_z\rangle\}, \quad j_z = 0, 1, \quad J_z = 0, 1, 2$
  - general form: $\mathcal{B}_2 \otimes \mathcal{B}_3$

- indirect product bases:
  - example in $\mathbb{C}^6$: $\{|0_z, J_z\rangle, |1_z, J_x\rangle\}, \quad J_z, J_x = 0, 1, 2$
  - general form: $\mathcal{B} = \{|\psi_j^1, \psi_j^2\rangle \in \mathbb{C}^{d_1 d_2}, j = 1 \ldots d_1 d_2\}$

Lemma (WPZ)

Two [direct] orthogonal product bases $\{|u, U\rangle\}$ and $\{|v, V\rangle\}$in dimension $d = d_1 d_2$ are MU iff the states $|u\rangle$ are MU to all $|v\rangle$ and the states $|U\rangle$ are MU to all $|V\rangle$.

The limited role of MU product bases for $d \leq 6$

Lemma (MW)
The product state $|\mu^1, \mu^2\rangle \in \mathbb{C}^d, d = d_1 d_2 \leq 6$, is MU to the (direct or indirect) orthogonal product basis $\{|\psi_j^1, \psi_j^2\rangle \in \mathbb{C}^d, j = 1 \dots d\}$, iff $|\mu^1\rangle$ is MU to $|\psi_j^1\rangle \in \mathbb{C}^{d_1}$ and $|\mu^2\rangle$ is MU to $|\psi_j^2\rangle \in \mathbb{C}^{d_2}$, for all $j = 1 \dots d$.

$\Longrightarrow$ **classification of all sets of orthogonal MU product bases for** $d = 6$

- all pairs: (complicated, long list)
- all triples:

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

$\Longrightarrow$ **e.g.:**
No complete set contains three product bases $\{6^3\}_6^{\otimes}$.
(no state is MU to either $\mathcal{T}_0$ or $\mathcal{T}_1$)

MU product bases for $d = d_1 d_2 \dots d_n$

Lemma (MPW)
The product state $|\mu^1, \mu^2, \dots, \mu^n\rangle \in \mathbb{C}^d, d = d_1 d_2 \dots d_n$, is MU to any orthogonal product basis $\{|\psi_j^1, \psi_j^2, \dots, \psi^{n_j}\rangle \in \mathbb{C}^d, j = 1 \dots d\}$, iff for each $r = 1 \dots n$, the state $|\mu^r\rangle$ is MU to $|\psi_j^r\rangle \in \mathbb{C}^{d_r}$, for all $j = 1 \dots d$.

Theorem (MPW)
Suppose that $d = d_1 d_2 \dots d_n$ and let $d_1 = 2$ or $d_1 = 3$, and $d_1 \leq d_r, r = 2 \dots n$. Then there exist at most $(d_1 + 1)$ MU product bases.

Conjecture (MPW)
Suppose that $d = d_1 d_2 \dots d_n$. Then there exist at most $(d_m + 1)$ MU product bases where d_m is the dimension of the subsystem with the least number of MU bases.

Maximal MU product bases for $d = d_1 d_2 \dots d_n$

Corollaries

- $d = 2^k$: there is a unique triple of MU product bases
- $d = 3^k$: there is a unique quadruple of MU product bases
- $d = 2 \times 5$: three inequivalent triples of MU product bases exist

- $d = 2^k d_2 \dots d_n$: list of all triples of MU product bases
- $d = 3^k d_2 \dots d_n$: list of all quadruples of MU product bases

MU vectors

- strong limitations on vectors MU to maximal MU product bases exist

Summary

MU bases in composite dimensions

- $\{6^3, 1\}_6$ has never been observed
- some MU pairs/triples are unextendible
- a complete MU set contains at most one product basis
- number of MU product bases is strongly limited

any lessons?

- *existence* of complete MU sets is surprising
- sensitivity of quantum theory to factors of d

What is nature really telling us?

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

[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)

[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)

[JMMSW09] 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)

[Ka10] B.R. Karlsson,

References

[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

[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

[MW12a] D. McNulty and S. Weigert

[MW12b] D. McNulty and S. Weigert

[MW12c] D. McNulty and S. Weigert

[MRW12] M. Matolcsi,

[RLE11]

[SHBAH12]

[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

[WD10] S. Weigert and T. Durt

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

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