The limitations of nice mutually unbiased bases

Andrew Childs
Caltech Institute for Quantum Information

joint work with

Michael Aschbacher
Caltech Department of Mathematics

Paweł Wocjan
Caltech Institute for Quantum Information

quant-ph/0412066

Outline

- Mutually unbiased bases
- Constructing MUBs from unitary error bases
- Main result and proof sketch
- Optimality of the result
- Stronger result for abelian index groups
- Open questions

Mutually unbaised bases

Definition. Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of the Hilbert space $\mathbb{C}^d$ are called *mutually unbiased* iff

$$|\langle\psi'|\psi\rangle|^2 = \frac{1}{d}$$

for all $|\psi\rangle \in \mathcal{B}$ and $|\psi'\rangle \in \mathcal{B}'$.

Mutually unbaised bases

Definition. Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of the Hilbert space $\mathbb{C}^d$ are called *mutually unbiased* iff

$$|\langle\psi'|\psi\rangle|^2 = \frac{1}{d}$$

for all $|\psi\rangle \in \mathcal{B}$ and $|\psi'\rangle \in \mathcal{B}'$.

Example. In $\mathbb{C}^2$, the two bases

$$\mathcal{B} = \{|0\rangle, |1\rangle\}$$

$$\mathcal{B}' = \{\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

are mutually unbiased.

Mutually unbaised bases

Definition. Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of the Hilbert space $\mathbb{C}^d$ are called *mutually unbiased* iff

$$|\langle\psi'|\psi\rangle|^2 = \frac{1}{d}$$

for all $|\psi\rangle \in \mathcal{B}$ and $|\psi'\rangle \in \mathcal{B}'$.

Example. In $\mathbb{C}^2$, the two bases

$$\mathcal{B} = \{|0\rangle, |1\rangle\}$$

$$\mathcal{B}' = \{\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

are mutually unbiased.

We can add a third basis, $\mathcal{B}'' = \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$. Can we add a fourth one?

Mutually unbaised bases

Definition. Two orthonormal bases $\mathcal{B}$ and $\mathcal{B}'$ of the Hilbert space $\mathbb{C}^d$ are called *mutually unbiased* iff

$$|\langle\psi'|\psi\rangle|^2 = \frac{1}{d}$$

for all $|\psi\rangle \in \mathcal{B}$ and $|\psi'\rangle \in \mathcal{B}'$.

Example. In $\mathbb{C}^2$, the two bases

$$\mathcal{B} = \{|0\rangle, |1\rangle\}$$

$$\mathcal{B}' = \{\tfrac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \tfrac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$$

are mutually unbiased.

We can add a third basis, $\mathcal{B}'' = \{\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)\}$.
Can we add a fourth one? **No!**

Why should we care?

Mutually unbiased bases appear in

- Quantum cryptography (e.g., signal states for quantum key distribution)
- Quantum state determination

They are objects of fundamental interest (“quantum designs”).

N_{MUB}

Definition. Let $N_{\mathrm{MUB}}(d)$ denote the maximum number of pairwise mutually unbiased bases of $\mathbb{C}^d$.

Main open question: What is $N_{\mathrm{MUB}}(d)$ for arbitrary d? (For example, even $N_{\mathrm{MUB}}(6)$ is unknown.)

N_{MUB}

Definition. Let $N_{\mathrm{MUB}}(d)$ denote the maximum number of pairwise mutually unbiased bases of $\mathbb{C}^d$.

Main open question: What is $N_{\mathrm{MUB}}(d)$ for arbitrary d? (For example, even $N_{\mathrm{MUB}}(6)$ is unknown.)

What is known?

N_{MUB}

Definition. Let $N_{\mathrm{MUB}}(d)$ denote the maximum number of pairwise mutually unbiased bases of $\mathbb{C}^d$.

Main open question: What is $N_{\mathrm{MUB}}(d)$ for arbitrary d? (For example, even $N_{\mathrm{MUB}}(6)$ is unknown.)

What is known?

- $N_{\mathrm{MUB}}(d) \leq d + 1$ [Delsarte, Goethals, and Seidel 75]

N_{MUB}

Definition. Let $N_{\mathrm{MUB}}(d)$ denote the maximum number of pairwise mutually unbiased bases of $\mathbb{C}^d$.

Main open question: What is $N_{\mathrm{MUB}}(d)$ for arbitrary d? (For example, even $N_{\mathrm{MUB}}(6)$ is unknown.)

What is known?

- $N_{\mathrm{MUB}}(d) \leq d + 1$ [Delsarte, Goethals, and Seidel 75]
- $N_{\mathrm{MUB}}(p) = p + 1$ [Ivanovic 81]

N_{MUB}

Definition. Let $N_{\mathrm{MUB}}(d)$ denote the maximum number of pairwise mutually unbiased bases of $\mathbb{C}^d$.

Main open question: What is $N_{\mathrm{MUB}}(d)$ for arbitrary d? (For example, even $N_{\mathrm{MUB}}(6)$ is unknown.)

What is known?

- $N_{\mathrm{MUB}}(d) \leq d + 1$ [Delsarte, Goethals, and Seidel 75]
- $N_{\mathrm{MUB}}(p) = p + 1$ [Ivanovic 81]
- $N_{\mathrm{MUB}}(p^e) = p^e + 1$ [Wootters and Fields 89]

N_{MUB}

Definition. Let $N_{\mathrm{MUB}}(d)$ denote the maximum number of pairwise mutually unbiased bases of $\mathbb{C}^d$.

Main open question: What is $N_{\mathrm{MUB}}(d)$ for arbitrary d? (For example, even $N_{\mathrm{MUB}}(6)$ is unknown.)

What is known?

- $N_{\mathrm{MUB}}(d) \leq d+1$ [Delsarte, Goethals, and Seidel 75]
- $N_{\mathrm{MUB}}(p) = p+1$ [Ivanovic 81]
- $N_{\mathrm{MUB}}(p^e) = p^e+1$ [Wootters and Fields 89]
- $N_{\mathrm{MUB}}(d_1 d_2) \geq \min\{N_{\mathrm{MUB}}(d_1), N_{\mathrm{MUB}}(d_2)\}$ [Zauner 99]

N_{MUB}

Definition. Let $N_{\mathrm{MUB}}(d)$ denote the maximum number of pairwise mutually unbiased bases of $\mathbb{C}^d$.

Main open question: What is $N_{\mathrm{MUB}}(d)$ for arbitrary d? (For example, even $N_{\mathrm{MUB}}(6)$ is unknown.)

What is known?

- $N_{\mathrm{MUB}}(d) \leq d + 1$ [Delsarte, Goethals, and Seidel 75]
- $N_{\mathrm{MUB}}(p) = p + 1$ [Ivanovic 81]
- $N_{\mathrm{MUB}}(p^e) = p^e + 1$ [Wootters and Fields 89]
- $N_{\mathrm{MUB}}(d_1 d_2) \geq \min\{N_{\mathrm{MUB}}(d_1), N_{\mathrm{MUB}}(d_2)\}$ [Zauner 99]
- In particular, $N_{\mathrm{MUB}}(d) \geq N_{\mathrm{RPP}}(d) := \min_{p \in \pi(d)} d_p + 1$ where $\pi(d)$ denotes the set of prime factors of d and d_p denotes the largest power of p that divides d. **(reduce to prime power construction)**

Constructions of MUBs for $d = p^e$

Two classes of constructions that obtain $N_{\mathrm{MUB}}(p^e) = p^e + 1$:

- Exponential sums [Klappenecker and Rötteler 03]

- Partitioning a unitary error basis [Bandyopadhyay, Boykin, Roychowdhury, and Vatan 02]

Constructions of MUBs for $d = p^e$

Two classes of constructions that obtain $N_{\mathrm{MUB}}(p^e) = p^e + 1$:

- Exponential sums [Klappenecker and Rötteler 03]

  A natural generalization to arbitrary dimensions cannot do better than the reduce to prime power construction. [Archer 03]

- Partitioning a unitary error basis [Bandyopadhyay, Boykin, Roychowdhury, and Vatan 02]

Constructions of MUBs for $d = p^e$

Two classes of constructions that obtain $N_{\mathrm{MUB}}(p^e) = p^e + 1$:

- Exponential sums [Klappenecker and Rötteler 03]

  A natural generalization to arbitrary dimensions cannot do better than the reduce to prime power construction. [Archer 03]

- Partitioning a unitary error basis [Bandyopadhyay, Boykin, Roychowdhury, and Vatan 02]

  This talk: For unitary error bases with an underlying group structure, this construction cannot do better than the reduce to prime power construction.

Unitary error bases

Definition. A *unitary error basis* is a set of $d \times d$ unitary matrices $\mathcal{E} := \{U_1 = \mathbb{1}, U_2, \ldots, U_{d^2}\}$ that is orthogonal with respect to the trace inner product, i.e.,

$$\mathrm{tr}(U_k^\dagger U_l) = d\,\delta_{k,l}\,, \quad k, l \in \{1, \ldots, d^2\}\,.$$

Unitary error bases

Definition. A *unitary error basis* is a set of $d \times d$ unitary matrices $\mathcal{E} := \{U_1 = \mathbb{1}, U_2, \ldots, U_{d^2}\}$ that is orthogonal with respect to the trace inner product, i.e.,

$$\mathrm{tr}(U_k^\dagger U_l) = d\,\delta_{k,l}\,, \quad k,l \in \{1,\ldots,d^2\}\,.$$

Lemma [Bandyopadhyay et al. 02]. For any unitary error basis $\mathcal{E}$, let $\mathcal{E}_1 \cup \cdots \cup \mathcal{E}_n \subset \mathcal{E}$ with $\mathcal{E}_k \cap \mathcal{E}_l = \{\mathbb{1}\}$ for $k \neq l$. Furthermore, for each k, let $\mathcal{E}_k$ consist of d pairwise commuting matrices $U_{k,0} = \mathbb{1}, U_{k,1}, \ldots U_{k,d-1}$. For fixed k, let $\mathcal{B}_k$ consist of the common eigenvectors of the d matries $U_{k,j}$. Then the n bases $\mathcal{B}_k$ are mutually unbiased.

Nice error bases

A particularly nice kind of unitary error basis can be constructed using an underlying group structure.

Definition. Let G be a group of order d^2 with identity element 1 (called the *index group*). We say $\mathcal{N} = \{U_g \in \mathbb{C}^{d\times d} : g \in G\}$ is a *nice error basis* if

- $U_1 = \mathbb{1}$,
- $\operatorname{tr} U_g = d\,\delta_{g,1}$ for all $g \in G$, and
- $U_g U_h = \omega(g,h) U_{gh}$ for all $g, h \in G$, where $\omega(g,h) \in \mathbb{C}$.

(equivalently, $\mathcal{N}$ is a projective unitary representation of G of central type).

A set of mutually unbiased bases constructed by partitioning a subset of a nice error basis is called a set of *nice mutually unbiased bases*.

Main result

Theorem. Let $\mathcal{N}$ be a nice error basis of $\mathbb{C}^{d\times d}$. Then the number $N_{\mathrm{NMUB}}(d)$ of mutually unbiased bases that can be obtained by partitioning a subset of $\mathcal{N}$ is at most

$$N_{\mathrm{RPP}}(d) := \min_{p\in\pi(d)} d_p + 1\,.$$

Idea of the proof:

- Relate commuting subsets of nice error bases to abelian subgroups of the index group.
- Bound the number of abelian subgroups.

Connection to abelian subgroups

Lemma. Let G be the index group of a nice error basis $\mathcal{N} = \{U_{g_1}, \ldots, U_{g_{d^2}}\}$, and let $\mathcal{M} = \{U_{a_1}, \ldots, U_{a_d}\} \subset \mathcal{N}$ be a set of d mutually commuting matrices. Then $A = \{a_1, \ldots, a_d\}$ is an abelian subgroup of G.

Connection to abelian subgroups

Lemma. Let G be the index group of a nice error basis $\mathcal{N} = \{U_{g_1}, \ldots, U_{g_{d^2}}\}$, and let $\mathcal{M} = \{U_{a_1}, \ldots, U_{a_d}\} \subset \mathcal{N}$ be a set of d mutually commuting matrices. Then $A = \{a_1, \ldots, a_d\}$ is an abelian subgroup of G.

Proof. Since the matrices in $\mathcal{M}$ are mutually commuting, they can be simultaneously diagonalized. The trace orthogonality of a unitary error basis implies that the diagonals of $\mathcal{M}$ (written in their common eigenbasis) are pairwise orthogonal as vectors in $\mathbb{C}^d$. Since there can be at most d such vectors, $\mathcal{M}$ is a maximal commuting subset of $\mathcal{N}$. Hence it is closed under multiplication, and therefore corresponds to an abelian subgroup. $\square$

Connection to abelian subgroups

Lemma. Let G be the index group of a nice error basis $\mathcal{N} = \{U_{g_1}, \ldots, U_{g_{d^2}}\}$, and let $\mathcal{M} = \{U_{a_1}, \ldots, U_{a_d}\} \subset \mathcal{N}$ be a set of d mutually commuting matrices. Then $A = \{a_1, \ldots, a_d\}$ is an abelian subgroup of G.

Proof. Since the matrices in $\mathcal{M}$ are mutually commuting, they can be simultaneously diagonalized. The trace orthogonality of a unitary error basis implies that the diagonals of $\mathcal{M}$ (written in their common eigenbasis) are pairwise orthogonal as vectors in $\mathbb{C}^d$. Since there can be at most d such vectors, $\mathcal{M}$ is a maximal commuting subset of $\mathcal{N}$. Hence it is closed under multiplication, and therefore corresponds to an abelian subgroup. $\square$

$\Rightarrow$ A set of nice mutually unbiased bases corresponds to a set $\mathcal{A}$ of trivially intersecting abelian subgroups of the index group, each of order d.

How many abelian subgroups?

Lemma. Let G be a group of order d^2, and let $\mathcal{A}$ be a set of trivially intersecting abelian subgroups, each of order d. Then $|\mathcal{A}| \leq N_{\mathrm{RPP}}(d)$.

How many abelian subgroups?

Lemma. Let G be a group of order d^2, and let $\mathcal{A}$ be a set of trivially intersecting abelian subgroups, each of order d. Then $|\mathcal{A}| \leq N_{\mathrm{RPP}}(d)$.

Proof (for G nilpotent). A nilpotent group is the product of its Sylow p-subgroups, one for each prime factor of $|G|$. Write $G = G_{p_1} \times \cdots \times G_{p_k}$, where G_p is the Sylow p-subgroup of G, for $p \in \pi(d)$. Again since G is nilpotent, any subgroup $H \leq G$ can be written as $H_{p_1} \times \cdots \times H_{p_k}$ where $H_p := H \cap G_p \leq G_p$. For $A \in \mathcal{A}$, $|A| = d$, so $|A_p| = d_p$. Furthermore, for distinct subgroups $A, B \in \mathcal{A}$, $|A \cap B| = 1$ implies $|A_p \cap B_p| = 1$. By counting non-identity elements of distinct subgroups of G_p, we have $|\mathcal{A}|(d_p - 1) \leq d_p^2 - 1$, which implies $|\mathcal{A}| \leq d_p + 1$. Minimizing over $p \in \pi(d)$ completes the proof. $\square$

How many abelian subgroups?

Lemma. Let G be a group of order d^2, and let $\mathcal{A}$ be a set of trivially intersecting abelian subgroups, each of order d. Then $|\mathcal{A}| \leq N_{\mathrm{RPP}}(d)$.

Proof (for G nilpotent). A nilpotent group is the product of its Sylow p-subgroups, one for each prime factor of $|G|$. Write $G = G_{p_1} \times \cdots \times G_{p_k}$, where G_p is the Sylow p-subgroup of G, for $p \in \pi(d)$. Again since G is nilpotent, any subgroup $H \leq G$ can be written as $H_{p_1} \times \cdots \times H_{p_k}$ where $H_p := H \cap G_p \leq G_p$. For $A \in \mathcal{A}$, $|A| = d$, so $|A_p| = d_p$. Furthermore, for distinct subgroups $A, B \in \mathcal{A}$, $|A \cap B| = 1$ implies $|A_p \cap B_p| = 1$. By counting non-identity elements of distinct subgroups of G_p, we have $|\mathcal{A}|(d_p - 1) \leq d_p^2 - 1$, which implies $|\mathcal{A}| \leq d_p + 1$. Minimizing over $p \in \pi(d)$ completes the proof. $\square$

The proof for the general case is similar but more technical.

Achieving the bound

The bound $N_{\mathrm{NMUB}}(d) \leq N_{\mathrm{RPP}}(d)$ can be achieved, so it is best possible.

- For $d = p$ prime, $G = Z_p \times Z_p$.
- For $d = p^e$, $G = Z_p^{2e}$.
  (Note this is the unique group the achieves $N_{\mathrm{NMUB}}(p^e)$.)
- In general, for $d = p_1^{e_1} \cdots p_k^{e_k}$, $G = Z_{p_1}^{2e_1} \times \cdots \times Z_{p_k}^{2e_k}$.

Stronger result for abelian index groups

Theorem. Let $G = H \times H$ with $H = Z_{d_1} \times \cdots \times Z_{d_k}$, where $d_1, \ldots, d_k$ are prime powers WLOG. Define

$$\mu_p(H) := \max\{d_j : p | d_j\}\,,$$

$$\nu_p(H) := |\{j : d_j = \mu_p(H)\}|\,.$$

Then $|\mathcal{A}| \leq \min_{p \in \pi(d)} p^{\nu_p(H)} + 1$.

Could it be that $N_{\mathrm{MUB}}(d) = N_{\mathrm{RPP}}(d)$?

Could it be that $N_{\mathrm{MUB}}(d) = N_{\mathrm{RPP}}(d)$?

No!

[Wocjan and Beth 04]: $N_{\mathrm{MUB}}(s^2) \geq N_{\mathrm{MOLS}}(s) + 2$ where $N_{\mathrm{MOLS}}(s)$ is the number of mutually orthogonal Latin squares of size s.

1	2	3
3	1	2
2	3	1

1	2	3
2	3	1
3	1	2

$N_{\mathrm{MOLS}}(3) = 2$

Example: For $s = 26$, $N_{\mathrm{MUB}}(26^2) \geq 6$, but $N_{\mathrm{RPP}}(26^2) = 5$.

Open questions

Find constructions of more MUBs than are currently known.

- Partitioning wicked error bases
- Combinatorial constructions (or other constructions unrelated to unitary error bases)

Upper bounds on $N_{\mathrm{MUB}}(d)$.

Computational methods for determining $N_{\mathrm{MUB}}(d)$ for small d, e.g., for $d = 6$.