MUBs

William M. Kantor

Newark

August 2017

MUBs: Mutually unbiased bases

$\mathbb{C}^d$: complex space with hermitian inner product

$$\big((x_i),(y_i)\big) := \sum_i x_i \overline{y}_i$$

- MUBs = Mutually unbiased **orthonormal** bases $\mathcal{B}, \mathcal{B}'$:
  $|(u,v)| =$ constant for $u \in \mathcal{B}, v \in \mathcal{B}'$
  $$\text{and then } |(u,v)| = \frac{1}{\sqrt{d}} \ \ \forall u \in \mathcal{B}, v \in \mathcal{B}'.$$
- Any set of MUBs in $\mathbb{C}^d$ has size $\leq d+1$
  (meaning a set of orthonormal bases that pairwise are MUBs).
- Complete set of MUBs: set of $d+1$ MUBs
  hence involves $(d+1)d = d^2 + d$ vectors.
- Maximal set of MUBs: A set of MUBs that is not a proper subset of another set.
  Complete $\Rightarrow$ maximal but the converse is false.

Sources = History (no time)

Examples from fields

- $d = p^n$, $V = \mathrm{GF}(p^n)$ with dot product w.r.t. fixed $\mathbb{Z}_p$-basis (or trace inner product $Tr(xy)$)
- $p > 2$
- $\zeta \in \mathbb{C}$ primitive pth root of 1
- standard orthonormal basis $\mathcal{B}_\infty := \{e_v \mid v \in V\}$ of $\mathbb{C}^d$

• further bases $(b \in V)$

$\mathcal{B}_b := \{e_{a,b} \mid a \in V\}$ where $e_{a,b} := \frac{1}{\sqrt{d}} \sum_{v \in V} \zeta^{a \cdot v + bv \cdot v} e_v$

Examples from fields

- $d = p^n$, $V = \mathrm{GF}(p^n)$ with dot product w.r.t. fixed $\mathbb{Z}_p$-basis (or trace inner product $Tr(xy)$)
- $p > 2$
- $\zeta \in \mathbb{C}$ primitive pth root of 1
- standard orthonormal basis $\mathcal{B}_\infty := \{e_v \mid v \in V\}$ of $\mathbb{C}^d$

• further bases $(b \in V)$

$\mathcal{B}_b := \{e_{a,b} \mid a \in V\}$ where $e_{a,b} := \frac{1}{\sqrt{d}} \sum_{v \in V} \zeta^{a \cdot v + bv \cdot v} e_v$

• Then $\mathcal{B} := \{\mathcal{B}_\infty\} \cup \{\mathcal{B}_b \mid b \in V\}$ is a complete set of MUBs.

Rediscovered many times - the same examples in different guises.

Examples from fields

- $d = p^n$, $V = \mathrm{GF}(p^n)$ with dot product w.r.t. fixed $\mathbb{Z}_p$-basis (or trace inner product $Tr(xy)$)
- $p > 2$
- $\zeta \in \mathbb{C}$ primitive pth root of 1
- standard orthonormal basis $\mathcal{B}_\infty := \{e_v \mid v \in V\}$ of $\mathbb{C}^d$

• further bases $(b \in V)$

$\mathcal{B}_b := \{e_{a,b} \mid a \in V\}$ where $\quad e_{a,b} := \frac{1}{\sqrt{d}} \sum_{v \in V} \zeta^{a \cdot v + bv \cdot v} e_v$

• Then $\mathcal{B} := \{\mathcal{B}_\infty\} \cup \{\mathcal{B}_b \mid b \in V\}$ is a complete set of MUBs.

Rediscovered many times - the same examples in different guises.

$p = 2$? Mostly omitted today - lack of time.

Symmetric matrices

Goal: Generalize the preceding examples

- $d = p^n$, $V = \mathbb{Z}_p^n$, with dot product
- $p > 2$, $\zeta \in \mathbb{C}$ primitive pth root of 1
- standard orthonormal basis $\mathcal{B}_\infty := \{e_v \mid v \in V\}$ of $\mathbb{C}^d$
- $\mathcal{K}$: a set of d symmetric $n \times n$ matrices M over $\mathbb{Z}_p$
- $\mathcal{B}_M^{\mathcal{K}} := \{e_{a,M} \mid a \in V\}, M \in \mathcal{K}$, where

$$e_{a,M} := \frac{1}{\sqrt{d}} \sum_{v \in V} \zeta^{a \cdot v + vM \cdot v/2} e_v$$

Symmetric matrices

Goal: Generalize the preceding examples

- $d = p^n$, $V = \mathbb{Z}_p^n$, with dot product
- $p > 2$, $\zeta \in \mathbb{C}$ primitive pth root of 1
- standard orthonormal basis $\mathcal{B}_\infty := \{e_v \mid v \in V\}$ of $\mathbb{C}^d$
- $\mathcal{K}$: a set of d symmetric $n \times n$ matrices M over $\mathbb{Z}_p$
- $\mathcal{B}_M^{\mathcal{K}} := \{e_{a,M} \mid a \in V\}, M \in \mathcal{K}$, where

$$e_{a,M} := \frac{1}{\sqrt{d}} \sum_{v \in V} \zeta^{a \cdot v + vM \cdot v/2} e_v$$

Theorem (CCKS = Calderbank-Cameron-K-Seidel):

$$\mathcal{B}^{\mathcal{K}} := \{\mathcal{B}_\infty\} \cup \left\{\mathcal{B}_M^{\mathcal{K}} \mid M \in \mathcal{K}\right\}$$ is a complete set of MUBs

$\iff$ the difference of any two members of $\mathcal{K}$ is nonsingular.

- Rediscovered by Bandyopadhyay-Boykin-Roychowdhury-Vatan.
- Previous examples? $V = GF(p^n)$ and $\mathcal{K}$ is all $x \mapsto xm$, $m \in V$.

Digression: Equivalence of sets of MUBs

Means: equivalence of the set of 1-spaces they determine under a unitary transformation of $\mathbb{C}^d$

☞ *e.g.* $Aut(\mathcal{B})$ *can contain many diagonal matrices.*

Affine planes

Affine planes are related to the **preceding** construction:

- Again start with $V = \mathbb{Z}_p^n$ and
- $\mathcal{K}$: a set of $d = p^n$
  $n \times n$ matrices $/\mathbb{Z}_p$ s.t. the difference of any 2 is nonsingular
  (NO assumption that they are symmetric matrices).
- Affine "translation plane" $\mathfrak{A}(\mathcal{K})$ of order d:
  points: vectors in $V \oplus V$
  lines: $x = c$ and $y = xM + b$ for $M \in \mathcal{K}$, $b \in V$

Affine planes

Affine planes are related to the **preceding** construction:

- Again start with $V = \mathbb{Z}_p^n$ and
- $\mathcal{K}$: a set of $d = p^n$
  $n \times n$ matrices $/\mathbb{Z}_p$ s.t. the difference of any 2 is nonsingular
  (NO assumption that they are symmetric matrices).
- Affine "translation plane" $\mathfrak{A}(\mathcal{K})$ of order d:
  points: vectors in $V \oplus V$
  lines: $x = c$ and $y = xM + b$ for $M \in \mathcal{K}$, $b \in V$

$\therefore$ Just-constructed-complete-set-$\mathcal{B}^{\mathcal{K}}$-of-MUBs $\leftrightarrow$ certain plane $\mathfrak{A}(\mathcal{K})$.

"Symplectic translation plane" $\mathfrak{A}(\mathcal{K})$ when $\mathcal{K}$ is symmetric matrices.

Affine planes

Affine planes are related to the **preceding** construction:

- Again start with $V = \mathbb{Z}_p^n$ and
- $\mathcal{K}$: a set of $d = p^n$
  $n \times n$ matrices $/\mathbb{Z}_p$ s.t. the difference of any 2 is nonsingular
  (NO assumption that they are symmetric matrices).
- Affine "translation plane" $\mathfrak{A}(\mathcal{K})$ of order d:
  points: vectors in $V \oplus V$
  lines: $x = c$ and $y = xM + b$ for $M \in \mathcal{K}$, $b \in V$

$\therefore$ Just-constructed-complete-set-$\mathcal{B}^{\mathcal{K}}$-of-MUBs $\leftrightarrow$ certain plane $\mathfrak{A}(\mathcal{K})$.

"Symplectic translation plane" $\mathfrak{A}(\mathcal{K})$ when $\mathcal{K}$ is symmetric matrices.

Theorem (CCKS): If $\mathcal{K}$ and $\mathcal{K}'$ consist of symmetric matrices then
$\mathcal{B}^{\mathcal{K}}$ and $\mathcal{B}^{\mathcal{K}'}$ are equivalent
$\iff$ $\mathfrak{A}(\mathcal{K})$ and $\mathfrak{A}(\mathcal{K}')$ are isomorphic planes.

There is an analogue for $p = 2$.

Basic questions:

1. Are there complete sets of MUBs in $\mathbb{C}^d$ for d not a prime power?

   Open

   Answer NO was conjectured by some mathematical physicists BECAUSE there "is" apparent relationship between ANY complete set of MUBs and a projective plane, AND assuming prime power conjecture for projective planes.

Recall: Complete set of MUBs: set of $d + 1$ MUBs
hence involves $(d + 1)d = d^2 + d$ vectors,
which is the number of lines of an affine plane of order d.

Basic questions continued:

2. For d a prime power, are there inequivalent complete sets of MUBs in $\mathbb{C}^d$?

   Yes if $d > 8$ is not prime. Open otherwise.

3. For d a prime power, are there **a lot** of inequivalent complete sets of MUBs?

Basic questions continued:

2. For d a prime power, are there inequivalent complete sets of MUBs in $\mathbb{C}^d$?

   Yes if $d > 8$ is not prime. Open otherwise.

3. For d a prime power, are there **a lot** of inequivalent complete sets of MUBs?

Known: ($d = p^n$ is a prime power)

- For d even: the number of pairwise inequivalent complete sets of MUBs in $\mathbb{C}^d$ is not bounded above by any polynomial in d.
- For d odd: the number of known pairwise inequivalent complete sets of MUBs in $\mathbb{C}^d$ is $< d$. However, for odd d the number of pairwise inequivalent complete sets of MUBs is not bounded.

Basic questions continued:

4. Are there complete sets of MUBs not equivalent to any of those just described?
Yes: using Coulter-Matthews planar functions 1997 where $d = 3^n$ (via Godsil-Roy).

Conjecture: Yes, lots.

5. Are there "large" maximal sets of MUBs in $\mathbb{C}^d$ (perhaps not complete sets) in $\mathbb{C}^d$ with d not a prime power?

Discussed soon.

6. Are there exponentially many pairwise inequivalent complete sets of MUBs in $\mathbb{C}^d$ for an infinite set of dimensions d?

Conjecture: Yes. Why not?

Basic questions continued:

4. Are there complete sets of MUBs not equivalent to any of those just described?
Yes: using Coulter-Matthews planar functions 1997 where $d = 3^n$ (via Godsil-Roy).

Conjecture: Yes, lots.

5. Are there "large" maximal sets of MUBs in $\mathbb{C}^d$ (perhaps not complete sets) in $\mathbb{C}^d$ with d not a prime power?

Discussed soon.

6. Are there exponentially many pairwise inequivalent complete sets of MUBs in $\mathbb{C}^d$ for an infinite set of dimensions d?

Conjecture: Yes. Why not?

Basic questions continued:

4. Are there complete sets of MUBs not equivalent to any of those just described?
Yes: using Coulter-Matthews planar functions 1997 where $d = 3^n$ (via Godsil-Roy).
    Conjecture: Yes, lots.

5. Are there "large" maximal sets of MUBs in $\mathbb{C}^d$ (perhaps not complete sets) in $\mathbb{C}^d$ with d not a prime power?
    Discussed soon.

6. Are there exponentially many pairwise inequivalent complete sets of MUBs in $\mathbb{C}^d$ for an infinite set of dimensions d?
    Conjecture: Yes. Why not?

7. Are there infinitely many pairwise inequivalent complete sets of MUBs in $\mathbb{C}^d$ for some dimensions d?
    Why not? Yes, this contradicts any relationship with planes.

Skipped in this talk:

- Many (but **definitely nothing like** "most") of the above examples come from commutative semifields.
- Extraspecial groups and their faithful irreducible representations are an essential part of this subject.
- Characteristic 2 MUBs
- Characteristic 2 orthogonal geometries
- Codes (nonlinear over $\mathbb{Z}_2$ or linear over $\mathbb{Z}_4$)

Incomplete but maximal sets of MUBs

- $d = p^n$, $V = \mathbb{Z}_p^n$, with dot product
- $p > 2$, $\zeta \in \mathbb{C}$ primitive pth root of 1
- standard orthonormal basis $\mathcal{B}_\infty := \{e_v \mid v \in V\}$ of $\mathbb{C}^d$
- $\mathcal{K}$: a set of $d' \le d = p^n$ symmetric $n \times n$ matrices M over $\mathbb{Z}_p$
- $\mathcal{B}_M^{\mathcal{K}} := \{e_{a,M} \mid a \in V\}, M \in \mathcal{K}$, where

$$e_{a,M} := \frac{1}{\sqrt{d}} \sum_{v \in V} \zeta^{a \cdot v + vM \cdot v/2} e_v .$$

Once again:

$$\mathcal{B}^{\mathcal{K}} := \{\mathcal{B}_\infty\} \cup \left\{\mathcal{B}_M^{\mathcal{K}} \mid M \in \mathcal{K}\right\} \text{ is a set of MUBs}$$

$\iff$ the difference of any two members of $\mathcal{K}$ is nonsingular.

So this is not about complete sets of MUBs, just sets of d' MUBs constructed in a certain way.

Question: Can such a set $\mathcal{K}$ be increased to a set of p^n matrices?

Answer: Rarely (this approach rarely leads to affine planes)

Greed doesn't work

Greed doesn't work

- There are many maximal sets of 3 MUBs.
- There is a maximal set of 2 MUBs (dimension 6).
  (complex Hadamard matrix: Moorhouse, Tao)

Those were very small sets. Soon: smallish sets.

Large maximal sets of MUBs:

Greed doesn't work

- There are many maximal sets of 3 MUBs.
- There is a maximal set of 2 MUBs (dimension 6).
  (complex Hadamard matrix: Moorhouse, Tao)

Those were very small sets. Soon: smallish sets.

Large maximal sets of MUBs:

- (Szántó) Maximal sets of size $p^2 - p + 2$ in $\mathbb{C}^{p^2}$, $p \equiv 3 \bmod 4$.
- (Jedwab-Yen) Maximal sets of size $2^{m-1} + 1$ in $\mathbb{C}^{2^m}$.

Greed doesn't work

- There are many maximal sets of 3 MUBs.
- There is a maximal set of 2 MUBs (dimension 6).
  (complex Hadamard matrix: Moorhouse, Tao)

Those were very small sets. Soon: smallish sets.

Large maximal sets of MUBs:

- (Szántó) Maximal sets of size $p^2 - p + 2$ in $\mathbb{C}^{p^2}$, $p \equiv 3 \bmod 4$.
- (Jedwab-Yen) Maximal sets of size $2^{m-1} + 1$ in $\mathbb{C}^{2^m}$.

Needed: Understanding maximality in order to obtain many examples of very different sizes. Various things can be maximized, e.g.:

- Maximal sets $\mathcal{K}$ of d' symmetric matrices over $\mathbb{Z}_p$ with all differences nonsingular (and resulting sets of $d' + 1$ MUBs)
- Maximal sets of MUBs

The first of these has interested me more: finite geometry.
The second is where new ideas are needed, especially needed are reasonably general results that say:
set of MUBs from suitable maximal set $\mathcal{K}$ is a maximal set of MUBs.

From Grassl's tables of $d' + 1$ MUBs coming from maximal sets $\mathcal{K}$ of d' symmetric $n \times n$ matrices

$d = p^n$	p	n	size $d' + 1$	
4	2	2	3,5	complete list
8	2	3	5,9	complete list
16	2	4	5,8,9,11,13,17	complete list
32	2	5	9,...,15,17,33	
64	2	6	9, ...,47,49,51,57,65	
9	3	2	5,8,10	complete list
27	3	3	10,...,20,28	complete list
81	3	4	18,...,68,70,73,74,82	
25	5	2	13,...,20,22,24,26	complete list
125	5	3	27,...,90,101,126	