How many Mutually Unbiased Bases can exist in Complex Space of Dimension *d* ?

Jonathan Jedwab

Department of Mathematics, Simon Fraser University

Joint work with Lily Yen

Department of Mathematics & Statistics, Capilano University

Outline

- Mutually unbiased bases
- Motivation
- Central question
- Product construction
- Latin squares construction
- Dimension 6
- Zauner's conjecture
- Weiner's dichotomy
- Unextendible sets

Jonathan Jedwab

Mutually Unbiased Bases

(	1	1	1	1	1	1	)
(	1	ω	ω^2	1	ω	ω^2	)
(	1	ω^2	ω	1	ω^2	ω	)
(	1	1	1	-1	-1	-1	)
(	1	ω	ω^2	-1	$-\omega$	$-\omega^2$	)
(	1	ω^2	ω	-1	$-\omega^2$	$-\omega$	)

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

$$(\ 1 \quad \omega^2 \quad \omega \quad 1 \quad \omega^2 \quad \omega\ )$$

$$(\ \overline{1} \quad \overline{\omega^2} \quad \overline{\omega} \quad \overline{-1} \quad \overline{-\omega^2} \quad \overline{-\omega}\ )$$

Hermitian inner product of vectors is

$$1\cdot\overline{(1)} + \omega^2\cdot\overline{(\omega^2)} + \omega\cdot\overline{(\omega)} + 1\cdot\overline{(-1)} + \omega^2\cdot\overline{(-\omega^2)} + \omega\cdot\overline{(-\omega)} = 0$$

Hermitian inner product of every two distinct vectors is 0:

the vectors form an orthogonal basis for $\mathbb{C}^6$

Jonathan Jedwab
18 April 2016

Mutually Unbiased Bases

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

1	1	1	1	1	1
1	ω	ω^2	1	ω	ω^2
1	ω^2	ω	1	ω^2	ω
1	1	1	-1	-1	-1
1	ω	ω^2	-1	$-\omega$	$-\omega^2$
1	ω^2	ω	-1	$-\omega^2$	$-\omega$

1	1	ω	i	i	$i\omega$
1	ω	1	i	$i\omega$	i
1	ω^2	ω^2	i	$i\omega^2$	$i\omega^2$
1	1	ω	$-i$	$-i$	$-i\omega^2$
1	ω	1	$-i$	$-i\omega$	$-i$
1	ω^2	ω^2	$-i$	$-i\omega^2$	$-i\omega^2$

$$(\ 1 \quad \omega^2 \quad \omega \quad 1 \quad \omega^2 \quad \omega\ )$$

$$(\ \overline{1} \quad \overline{\omega} \quad \overline{1} \quad \overline{i} \quad \overline{i\omega} \quad \overline{i}\ )$$

Hermitian inner product of vectors is $(1-i)(1+2\omega)$, of magnitude $\sqrt{6}$

Jonathan Jedwab
18 April 2016

Mutually Unbiased Bases

(	1	1	1	1	1	1	)
(	1	ω	ω^2	1	ω	ω^2	)
(	1	ω^2	ω	1	ω^2	ω	)
(	1	1	1	-1	-1	-1	)
(	1	ω	ω^2	-1	$-\omega$	$-\omega^2$	)
(	1	ω^2	ω	-1	$-\omega^2$	$-\omega$	)

(	1	1	ω	i	i	$i\omega$	)
(	1	ω	1	i	$i\omega$	i	)
(	1	ω^2	ω^2	i	$i\omega^2$	$i\omega^2$	)
(	1	1	ω	$-i$	$-i$	$-i\omega^2$	)
(	1	ω	1	$-i$	$-i\omega$	$-i$	)
(	1	ω^2	ω^2	$-i$	$-i\omega^2$	$-i\omega^2$	)

Hermitian inner product of every two vectors from distinct orthogonal bases has constant magnitude:

the two bases are mutually unbiased

Mutually Unbiased Bases

1	1	1	1	1	1
1	ω	ω^2	1	ω	ω^2
1	ω^2	ω	1	ω^2	ω
1	1	1	-1	-1	-1
1	ω	ω^2	-1	$-\omega$	$-\omega^2$
1	ω^2	ω	-1	$-\omega^2$	$-\omega$

$\sqrt{6}$	0	0	0	0	0
0	$\sqrt{6}$	0	0	0	0
0	0	$\sqrt{6}$	0	0	0
0	0	0	$\sqrt{6}$	0	0
0	0	0	0	$\sqrt{6}$	0
0	0	0	0	0	$\sqrt{6}$

1	1	ω	i	i	$i\omega$
1	ω	1	i	$i\omega$	i
1	ω^2	ω^2	i	$i\omega^2$	$i\omega^2$
1	1	ω	$-i$	$-i$	$-i\omega^2$
1	ω	1	$-i$	$-i\omega$	$-i$
1	ω^2	ω^2	$-i$	$-i\omega^2$	$-i\omega^2$

3 mutually unbiased bases (MUBs) in $\mathbb{C}^6$

Jonathan Jedwab
18 April 2016

Mutually Unbiased Bases

- Schwinger (1960): when a quantum system is prepared in a state belonging to one basis, all outcomes of measurement with respect to any other basis are equally probable

- Many applications in quantum physics
  - ⋆ secure quantum key exchange (Bennett Brassard 1984)
  - ⋆ quantum state determination (Ivanović 1981)
  - ⋆ quantum state reconstruction (Wootters Fields 1989)
  - ⋆ detection of quantum entanglement (Spengler et al 2012)

Mutually Unbiased Bases

- 2010 MUBs survey (Durt Englert Bengtsson Życzkowski) contains almost 200 references!

- Close connections with many other combinatorial structures
  - ⋆ finite projective planes (Saniga Planat Rosu 2004)
  - ⋆ mutually orthogonal Latin squares (Wocjan Beth 2005)
  - ⋆ relative difference sets (Godsil Roy 2009)
  - ⋆ complex Hadamard matrices (Szöllősi 2011)
  - ⋆ complex equiangular lines (Jedwab Wiebe 2015+)

3 MUBs in $\mathbb{C}^2$

$(\ \sqrt{2} \quad 0\ )$
$(\ 0 \quad \sqrt{2}\ )$

$(\ 1 \quad 1\ )$
$(\ 1 \quad -1\ )$

$(\ 1 \quad i\ )$
$(\ 1 \quad -i\ )$

Jonathan Jedwab
18 April 2016

4 MUBs in $\mathbb{C}^3$

($\sqrt{3}$	0	0)
(0	$\sqrt{3}$	0)
(0	0	$\sqrt{3}$)

(1	1	1)
(1	ω	ω^2)
(1	ω^2	ω)

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

(1	1	ω)
(1	ω	1)
(1	ω^2	ω^2)

(1	1	ω^2)
(1	ω	ω)
(1	ω^2	1)

Jonathan Jedwab
18 April 2016

5 MUBs in $\mathbb{C}^4$

$$\begin{pmatrix} 2 & 0 & 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 2 & 0 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 & 2 & 0 \end{pmatrix}$$
$$\begin{pmatrix} 0 & 0 & 0 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 & -1 & -1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & -1 & 1 & -1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 & i & -i \end{pmatrix}$$
$$\begin{pmatrix} 1 & 1 & -i & i \end{pmatrix}$$
$$\begin{pmatrix} 1 & -1 & i & i \end{pmatrix}$$
$$\begin{pmatrix} 1 & -1 & -i & -i \end{pmatrix}$$

$$\begin{pmatrix} 1 & i & 1 & -i \end{pmatrix}$$
$$\begin{pmatrix} 1 & i & -1 & i \end{pmatrix}$$
$$\begin{pmatrix} 1 & -i & 1 & i \end{pmatrix}$$
$$\begin{pmatrix} 1 & -i & -1 & -i \end{pmatrix}$$

$$\begin{pmatrix} 1 & i & i & -1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & i & -i & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & -i & i & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & -i & -i & -1 \end{pmatrix}$$

Jonathan Jedwab
18 April 2016

How Many MUBs can exist in $\mathbb{C}^d$?

- At most $d+1$ (Delsarte Goethals Seidel 1975)
  - ⋆ proof using Jacobi polynomials, or else linear algebra

- Constructions of $d+1$ MUBs in $\mathbb{C}^d$ for all prime powers d
  - ⋆ finite fields (Wootters Fields 1989)
  - ⋆ eigenbases of operators in Weyl-Heisenberg group
  - ⋆ estimation of exponential sums
  - ⋆ relative difference sets, planar functions, symplectic spreads, complex Hadamard matrices,…

How Many MUBs can exist in $\mathbb{C}^d$?

- $\mu(d) \le d+1$ (Delsarte Goethals Seidel 1975)

- $\mu(d) = d+1$ for prime powers d (Wootters Fields 1989)

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

How Many MUBs can exist in $\mathbb{C}^d$?

d	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(d) \leq$	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(d) \geq$	3	4	5	6		8	9	10		12		14

14	15	16	17	18	19	20	21	22	23	24	25	26
15	16	17	18	19	20	21	22	23	24	25	26	27
		17	18		20				24		26	

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Jonathan Jedwab
18 April 2016

How Many MUBs can exist in $\mathbb{C}^d$?

- $\mu(d) \leq d+1$ (Delsarte Goethals Seidel 1975)

- $\mu(d) = d+1$ for prime powers d (Wootters Fields 1989)

- $\mu(d)$ is unknown for every non-prime-power $d > 1$

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Jonathan Jedwab
18 April 2016

10 Most Annoying Questions

- How many mutually unbiased bases are there in non-prime-power dimensions?

#8 of *The ten most annoying questions in quantum computing*, Scott Aaronson's blog, 2006

#3 of *The NEW ten most annoying questions in quantum computing*, Scott Aaronson's blog, 2014

Product Construction

$$\begin{pmatrix} \sqrt{3} & 0 & 0 \\ 0 & A & 0 \\ 0 & 0 & \sqrt{3} \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & 1 \\ 1 & B & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$$

4 MUBs in $\mathbb{C}^3$

$$\begin{pmatrix} 1 & 1 & \omega \\ 1 & C & 1 \\ 1 & \omega^2 & \omega^2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & D & \omega \\ 1 & \omega^2 & 1 \end{pmatrix}$$

Product Construction

$$\begin{pmatrix} \sqrt{2} & 0 \\ 0 & \sqrt{2} \end{pmatrix} \qquad \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$$

3 MUBs in $\mathbb{C}^2$

$$\otimes \qquad \otimes \qquad \otimes$$

$$A \qquad B \qquad C$$

3 MUBs in $\mathbb{C}^3$

$$\downarrow \qquad \downarrow \qquad \downarrow$$

$$\begin{pmatrix} \sqrt{2}A & 0 \\ 0 & \sqrt{2}A \end{pmatrix} \qquad \begin{pmatrix} B & B \\ B & -B \end{pmatrix} \qquad \begin{pmatrix} C & iC \\ C & -iC \end{pmatrix}$$

3 MUBs in $\mathbb{C}^6$

Jonathan Jedwab
18 April 2016

Product Construction

$$
\left[\begin{array}{ccc|ccc}
1 & 1 & 1 & 1 & 1 & 1 \\
1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\
1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\
\hline
1 & 1 & 1 & -1 & -1 & -1 \\
1 & \omega & \omega^2 & -1 & -\omega & -\omega^2 \\
1 & \omega^2 & \omega & -1 & -\omega^2 & -\omega
\end{array}\right]
$$

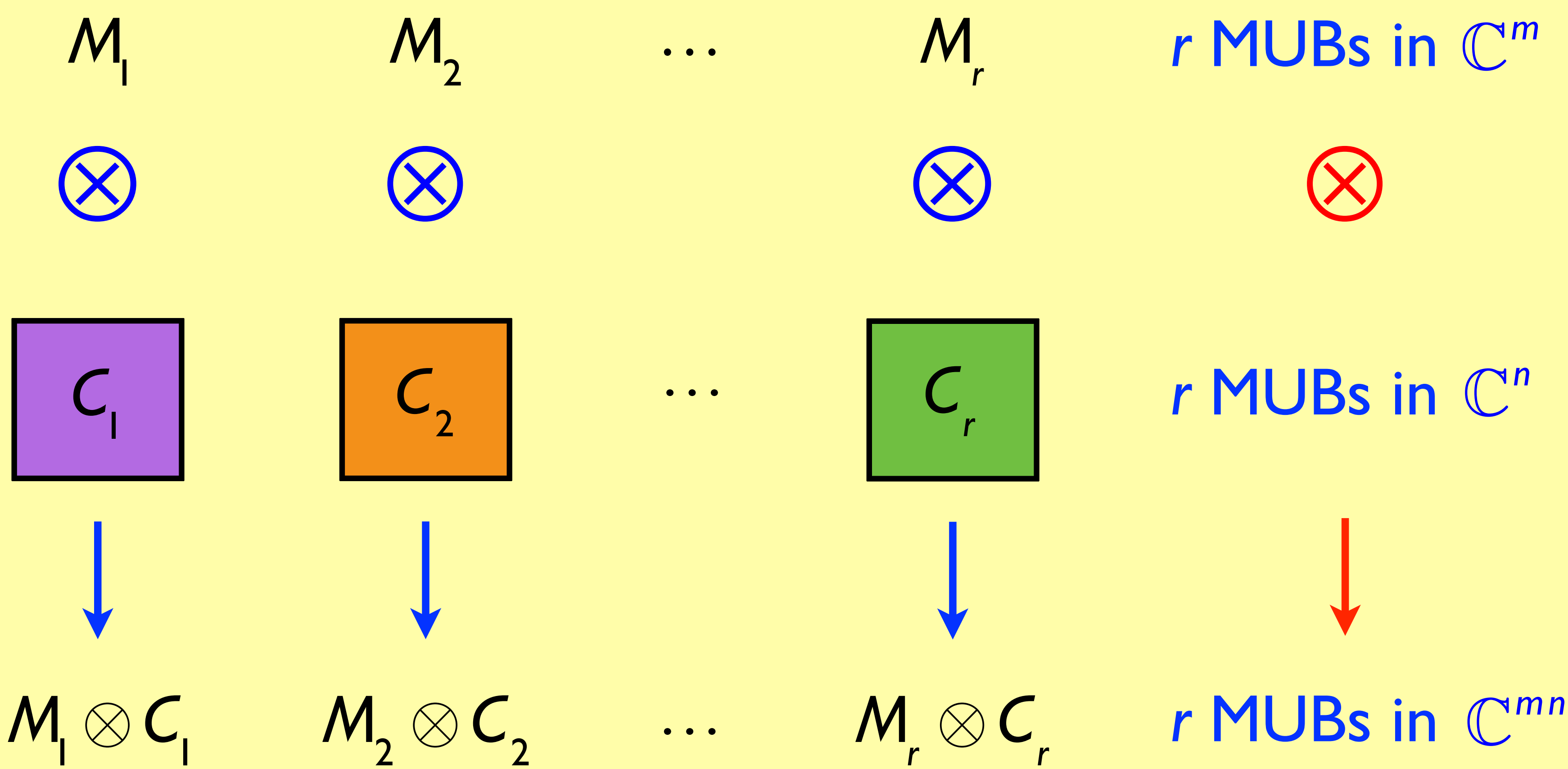
$$
\left[\begin{array}{ccc|ccc}
\sqrt{6} & 0 & 0 & 0 & 0 & 0 \\
0 & \sqrt{6} & 0 & 0 & 0 & 0 \\
0 & 0 & \sqrt{6} & 0 & 0 & 0 \\
\hline
0 & 0 & 0 & \sqrt{6} & 0 & 0 \\
0 & 0 & 0 & 0 & \sqrt{6} & 0 \\
0 & 0 & 0 & 0 & 0 & \sqrt{6}
\end{array}\right]
$$

$$
\left[\begin{array}{ccc|ccc}
1 & 1 & \omega & i & i & i\omega \\
1 & \omega & 1 & i & i\omega & i \\
1 & \omega^2 & \omega^2 & i & i\omega^2 & i\omega^2 \\
\hline
1 & 1 & \omega & -i & -i & -i\omega^2 \\
1 & \omega & 1 & -i & -i\omega & -i \\
1 & \omega^2 & \omega^2 & -i & -i\omega^2 & -i\omega^2
\end{array}\right]
$$

3 MUBs in $\mathbb{C}^6$

Product Construction

- Klappenecker Rötteler 2004



$$\mu(mn) \geq \min(\mu(m), \mu(n))$$

Product Construction

Construct MUBs in dimension $d = 3^4 \cdot 5^3 \cdot 7^2 \cdot 11^2$

$3^4 + 1$ MUBs in $\mathbb{C}^{3^4}$

$5^3 + 1$ MUBs in $\mathbb{C}^{5^3}$

$7^2 + 1$ MUBs in $\mathbb{C}^{7^2}$

$3^4 + 1$ MUBs in $\mathbb{C}^{3^4 \cdot 5^3}$

$11^2 + 1$ MUBs in $\mathbb{C}^{11^2}$

$7^2 + 1$ MUBs in $\mathbb{C}^{3^4 \cdot 5^3 \cdot 7^2}$

$7^2 + 1$ MUBs in $\mathbb{C}^{3^4 \cdot 5^3 \cdot 7^2 \cdot 11^2}$

$$\mu(mn) \geq \min(\mu(m), \mu(n))$$

Jonathan Jedwab
18 April 2016

How Many MUBs can exist in $\mathbb{C}^d$?

- $\mu(d) \leq d+1$ (Delsarte Goethals Seidel 1975)

- $\mu(d) = d+1$ for prime powers d (Wootters Fields 1989)

- $\mu(d) \geq 1+$(smallest prime power in factorisation of d) (Klappenecker Rötteler 2004)

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Jonathan Jedwab
18 April 2016

How Many MUBs can exist in $\mathbb{C}^d$?

d	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(d) \leq$	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(d) \geq$	3	4	5	6	3	8	9	10	3	12	4	14

d	14	15	16	17	18	19	20	21	22	23	24	25	26
$\mu(d) \leq$	15	16	17	18	19	20	21	22	23	24	25	26	27
$\mu(d) \geq$	3	4	17	18	3	20	5	4	3	24	4	26	3

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Jonathan Jedwab
18 April 2016

Latin Squares Construction

1	**2**	**3**
3	**1**	**2**
2	**3**	**1**

1	**2**	**3**
2	**3**	**1**
3	**1**	**2**

11	**22**	**33**
32	**13**	**21**
23	**31**	**12**

2 mutually orthogonal
Latin squares of order 3

Jonathan Jedwab
18 April 2016

Latin Squares Construction

1	2	3	1	0	0	0	1	0	0	0	1
3	1	2	0	2	0	0	0	2	2	0	0
2	3	1	0	0	3	3	0	0	0	3	0

1	2	3	1	0	0	0	0	1	0	1	0
2	3	1	0	2	0	2	0	0	0	0	2
3	1	2	0	0	3	0	3	0	3	0	0

1	2	3	1	0	0	1	0	0	1	0	0
1	2	3	0	2	0	0	2	0	0	2	0
1	2	3	0	0	3	0	0	3	0	0	3

1	1	1	1	1	1	0	0	0	0	0	0
2	2	2	0	0	0	2	2	2	0	0	0
3	3	3	0	0	0	0	0	0	3	3	3

Jonathan Jedwab
18 April 2016

Latin Squares Construction

1	0	0	0	1	0	0	0	1
0	2	0	0	0	2	2	0	0
0	0	3	3	0	0	0	3	0

1	1	1
1	ω	ω^2
1	ω^2	ω

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

(	1	0	0	0	1	0	0	0	1	)
(	1	0	0	0	ω	0	0	0	ω^2	)
(	1	0	0	0	ω^2	0	0	0	ω	)
(	0	1	0	0	0	1	1	0	0	)
(	0	1	0	0	0	ω	ω^2	0	0	)
(	0	1	0	0	0	ω^2	ω	0	0	)
(	0	0	1	1	0	0	0	1	0	)
(	0	0	1	ω	0	0	0	ω^2	0	)
(	0	0	1	ω^2	0	0	0	ω	0	)

Basis 1

Latin Squares Construction

1	0	0	0	0	1	0	1	0
0	2	0	2	0	0	0	0	2
0	0	3	0	3	0	3	0	0

1	1	1
1	ω	ω^2
1	ω^2	ω

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

(	1	0	0	0	0	1	0	1	0	)
(	1	0	0	0	0	ω	0	ω^2	0	)
(	1	0	0	0	0	ω^2	0	ω	0	)
(	0	1	0	1	0	0	0	0	1	)
(	0	1	0	ω	0	0	0	0	ω^2	)
(	0	1	0	ω^2	0	0	0	0	ω	)
(	0	0	1	0	1	0	1	0	0	)
(	0	0	1	0	ω	0	ω^2	0	0	)
(	0	0	1	0	ω^2	0	ω	0	0	)

Basis 2

Latin Squares Construction

1	0	0	1	0	0	1	0	0
0	2	0	0	2	0	0	2	0
0	0	3	0	0	3	0	0	3

1	1	1
1	ω	ω^2
1	ω^2	ω

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

(	1	0	0	1	0	0	1	0	0	)
(	1	0	0	ω	0	0	ω^2	0	0	)
(	1	0	0	ω^2	0	0	ω	0	0	)
(	0	1	0	0	1	0	0	1	0	)
(	0	1	0	0	ω	0	0	ω^2	0	)
(	0	1	0	0	ω^2	0	0	ω	0	)
(	0	0	1	0	0	1	0	0	1	)
(	0	0	1	0	0	ω	0	0	ω^2	)
(	0	0	1	0	0	ω^2	0	0	ω	)

Basis 3

Latin Squares Construction

1	1	1	0	0	0	0	0	0
0	0	0	2	2	2	0	0	0
0	0	0	0	0	0	3	3	3

1	1	1
1	ω	ω^2
1	ω^2	ω

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

(	1	1	1	0	0	0	0	0	0	)
(	1	ω	ω^2	0	0	0	0	0	0	)
(	1	ω^2	ω	0	0	0	0	0	0	)
(	0	0	0	1	1	1	0	0	0	)
(	0	0	0	1	ω	ω^2	0	0	0	)
(	0	0	0	1	ω^2	ω	0	0	0	)
(	0	0	0	0	0	0	1	1	1	)
(	0	0	0	0	0	0	1	ω	ω^2	)
(	0	0	0	0	0	0	1	ω^2	ω	)

Basis 4

Jonathan Jedwab
18 April 2016

Latin Squares Construction

1	2	3
3	1	2
2	3	1

1	2	3
2	3	1
3	1	2

11	22	33
32	13	21
23	31	12

2 mutually orthogonal
Latin squares of order 3

Constructed 2+2 MUBs in $\mathbb{C}^{3^2}$

A *B* *C* *D*

Jonathan Jedwab
18 April 2016

Latin Squares Construction

- If there are w mutually orthogonal Latin squares of order s then there are $w+2$ MUBs in $\mathbb{C}^{s^2}$ (Wocjan Beth 2005)
  - ⋆ 4 mutually orthogonal Latin squares of order 26 gives 6 MUBs in $\mathbb{C}^{2^2 \cdot 13^2}$ (product construction gives only 5)
  - ⋆ combine with 8 MUBs in $\mathbb{C}^7$ using product construction to give 6 MUBs in $\mathbb{C}^{2^2 \cdot 13^2 \cdot 7}$
  - ⋆ improves on production construction alone for infinitely many dimensions

$$\mu(mn) \geq \min(\mu(m), \mu(n))$$

How Many MUBs can exist in $\mathbb{C}^d$?

d	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(d) \leq$	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(d) \geq$	3	4	5	6	3	8	9	10	3	12	4	14

14	15	16	17	18	19	20	21	22	23	24	25	26
15	16	17	18	19	20	21	22	23	24	25	26	27
3	4	17	18	3	20	5	4	3	24	4	26	3

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Jonathan Jedwab
18 April 2016

3 MUBs in $\mathbb{C}^6$

(	$\sqrt{6}$	0	0	0	0	0	)
(	0	$\sqrt{6}$	0	0	0	0	)
(	0	0	$\sqrt{6}$	0	0	0	)
(	0	0	0	$\sqrt{6}$	0	0	)
(	0	0	0	0	$\sqrt{6}$	0	)
(	0	0	0	0	0	$\sqrt{6}$	)

Basis 1

Jonathan Jedwab
18 April 2016

3 MUBs in $\mathbb{C}^6$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & \frac{-(1-i\sqrt{3})}{2} & \frac{-(1+i\sqrt{3})}{2} & 1 & \frac{-(1-i\sqrt{3})}{2} & \frac{-(1+i\sqrt{3})}{2} \end{pmatrix}$$

$$\begin{pmatrix} 1 & \frac{-(1+i\sqrt{3})}{2} & \frac{-(1-i\sqrt{3})}{2} & 1 & \frac{-(1+i\sqrt{3})}{2} & \frac{-(1-i\sqrt{3})}{2} \end{pmatrix}$$

$$\begin{pmatrix} \frac{2+i}{\sqrt{5}} & \frac{\sqrt{2}(1+i)(\sqrt{3}-i)}{4} & \frac{\sqrt{2}(1+i)(\sqrt{3}+i)}{4} & \frac{-(2+i)}{\sqrt{5}} & \frac{-\sqrt{2}(1-i)(1+i\sqrt{3})}{4} & \frac{\sqrt{2}(1-i)(1-i\sqrt{3})}{4} \end{pmatrix}$$

$$\begin{pmatrix} \frac{2+i}{\sqrt{5}} & \frac{-(1-i)}{\sqrt{2}} & \frac{1-i}{\sqrt{2}} & \frac{-(2+i)}{\sqrt{5}} & \frac{1-i}{\sqrt{2}} & \frac{-(1-i)}{\sqrt{2}} \end{pmatrix}$$

$$\begin{pmatrix} \frac{2+i}{\sqrt{5}} & \frac{\sqrt{2}(1-i)(1-i\sqrt{3})}{4} & \frac{\sqrt{2}(1-i)(1+i\sqrt{3})}{4} & \frac{-(2+i)}{\sqrt{5}} & \frac{\sqrt{2}(1+i)(\sqrt{3}+i)}{4} & \frac{\sqrt{2}(1+i)(\sqrt{3}-i)}{4} \end{pmatrix}$$

Basis 2

Jonathan Jedwab
18 April 2016

3 MUBs in $\mathbb{C}^6$

$$\left(\frac{1+i\sqrt{5}}{\sqrt{6}} \quad \frac{(1+i\sqrt{2})(\sqrt{3}-i)}{\sqrt{12}} \quad \frac{(1-i\sqrt{2})(\sqrt{3}+i)}{\sqrt{12}} \quad \frac{1-i\sqrt{5}}{\sqrt{6}} \quad \frac{-(1-i\sqrt{2})(\sqrt{3}-i)}{\sqrt{12}} \quad \frac{-(1+i\sqrt{2})(\sqrt{3}+i)}{\sqrt{12}} \right)$$

$$\left(\frac{1+i\sqrt{5}}{\sqrt{6}} \quad \frac{(-\sqrt{2}+i)}{\sqrt{3}} \quad \frac{-(\sqrt{2}+i)}{\sqrt{3}} \quad \frac{1-i\sqrt{5}}{\sqrt{6}} \quad \frac{-(\sqrt{2}+i)}{\sqrt{3}} \quad \frac{(-\sqrt{2}+i)}{\sqrt{3}} \right)$$

$$\left(\frac{1+i\sqrt{5}}{\sqrt{6}} \quad \frac{-(1+i\sqrt{2})(\sqrt{3}+i)}{\sqrt{12}} \quad \frac{-(1-i\sqrt{2})(\sqrt{3}-i)}{\sqrt{12}} \quad \frac{1-i\sqrt{5}}{\sqrt{6}} \quad \frac{(1-i\sqrt{2})(\sqrt{3}+i)}{\sqrt{12}} \quad \frac{(1+i\sqrt{2})(\sqrt{3}-i)}{\sqrt{12}} \right)$$

$$\left(\frac{(2+i)(1+i\sqrt{5})}{\sqrt{30}} \quad \frac{(1-i)(\sqrt{2}-i)}{\sqrt{6}} \quad \frac{(-1+i)(\sqrt{2}+i)}{\sqrt{6}} \quad \frac{(2+i)(-1+i\sqrt{5})}{\sqrt{30}} \quad \frac{(-1+i)(\sqrt{2}+i)}{\sqrt{6}} \quad \frac{(1-i)(\sqrt{2}-i)}{\sqrt{6}} \right)$$

$$\left(\frac{(2+i)(1+i\sqrt{5})}{\sqrt{30}} \quad \frac{(1+i)(\sqrt{2}-i)(\sqrt{3}+i)}{\sqrt{24}} \quad \frac{(1+i)(\sqrt{2}+i)(\sqrt{3}-i)}{\sqrt{24}} \quad \frac{(2+i)(-1+i\sqrt{5})}{\sqrt{30}} \quad \frac{-(1+i)(\sqrt{2}+i)(\sqrt{3}+i)}{\sqrt{24}} \quad \frac{-(1+i)(\sqrt{2}-i)(\sqrt{3}-i)}{\sqrt{24}} \right)$$

$$\left(\frac{(2+i)(1+i\sqrt{5})}{\sqrt{30}} \quad \frac{(1+i)(\sqrt{2}-i)(-\sqrt{3}+i)}{\sqrt{24}} \quad \frac{-(1+i)(\sqrt{2}+i)(\sqrt{3}+i)}{\sqrt{24}} \quad \frac{(2+i)(-1+i\sqrt{5})}{\sqrt{30}} \quad \frac{(1+i)(\sqrt{2}+i)(\sqrt{3}-i)}{\sqrt{24}} \quad \frac{(1+i)(\sqrt{2}-i)(\sqrt{3}+i)}{\sqrt{24}} \right)$$

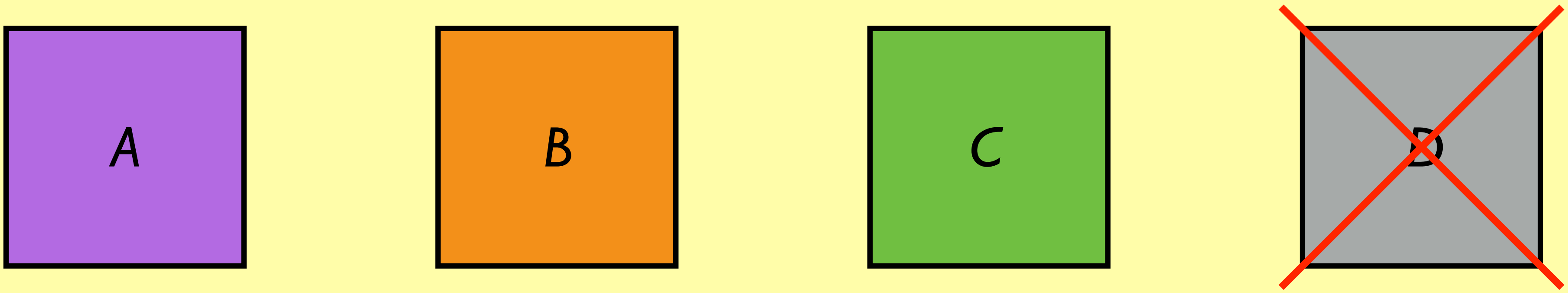
Basis 3

Jonathan Jedwab
18 April 2016

3 MUBs in $\mathbb{C}^6$

- Infinitely many sets of 3 MUBs in $\mathbb{C}^6$
  - ⋆ one-parameter family (Zauner 1999)
  - ⋆ another one-parameter family (Jaming Matolcsi Móra Szöllősi Weiner 2009): "Even in the [simplest case] the calculations are rather long and cumbersome, and not very instructive"
  - ⋆ two-parameter family (Szöllősi 2010)
- But no known construction of set of 4 MUBs in $\mathbb{C}^6$

Unextendible MUBs



3 unextendible MUBs in $\mathbb{C}^d$

Jonathan Jedwab
18 April 2016

Zauner's Conjecture

- Conjecture (Zauner 1999). Every set of 3 MUBs in $\mathbb{C}^6$ is unextendible (so $\mu(6) = 3$)
    - ⋆ "a growing consensus" in favour, yet concluded "We have almost no evidence either way" (Bengtsson 2007)
    - ⋆ holds when one of the 3 MUBs is the standard basis and another is constrained to belong to the "Fourier family $F(a,b)$" (Jaming et al 2009)
    - ⋆ "By now the evidence for [Zauner's] conjecture is overwhelming, but not quite conclusive" (Durt Englert Bengtsson Życzkowski 2010)

Weiner's Dichotomy

- Explicit construction of $(d+1)^{\text{th}}$ MUB from d MUBs in $\mathbb{C}^d$ (Weiner 2013)
  - ⋆ proof uses maximal abelian *-subalgebras
  - ⋆ every set of d MUBs in $\mathbb{C}^d$ is extendible to a set of size $d+1$
  - ⋆ dichotomy: $\mu(d) \neq d$

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

How Many MUBs can exist in $\mathbb{C}^d$?

- $\mu(d) \leq d+1$ (Delsarte Goethals Seidel 1975)

- $\mu(d) = d+1$ for prime powers d (Wootters Fields 1989)

- $\mu(d) \geq 1+$(smallest prime power in factorisation of d) (Klappenecker Rötteler 2004)

- $\mu(d) \neq d$ (Weiner 2013)

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Jonathan Jedwab
18 April 2016

How Many MUBs can exist in $\mathbb{C}^d$?

d	2	3	4	5	6	7	8	9	10	11	12	13
$\mu(d) \leq$	3	4	5	6	7	8	9	10	11	12	13	14
$\mu(d) \geq$	3	4	5	6	3	8	9	10	3	12	4	14
$\mu(d) \neq$					6				10		12	

d	14	15	16	17	18	19	20	21	22	23	24	25	26
$\mu(d) \leq$	15	16	17	18	19	20	21	22	23	24	25	26	27
$\mu(d) \geq$	3	4	17	18	3	20	5	4	3	24	4	26	3
$\mu(d) \neq$	14	15			18		20	21	22		24		26

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

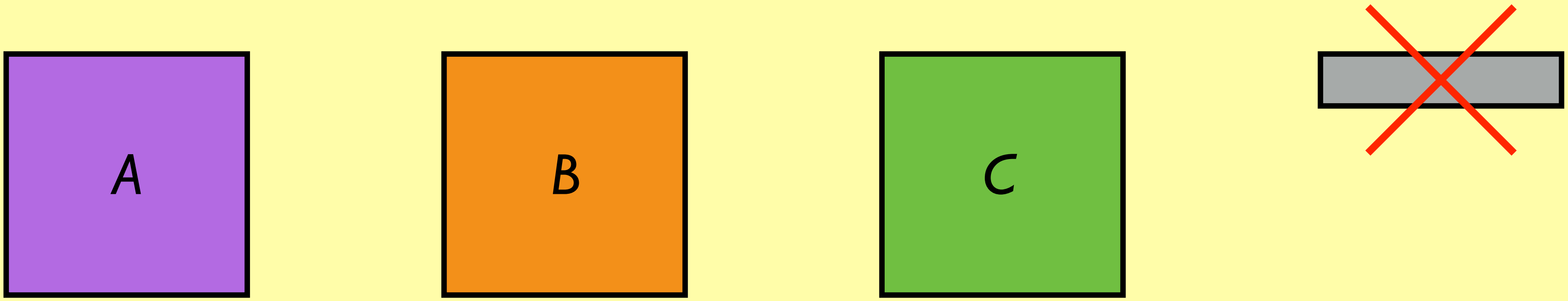
Jonathan Jedwab
18 April 2016

Unextendible MUBs

- How many MUBs can exist in $\mathbb{C}^d$?

- When and why is a set of MUBs unextendible?
  - ⋆ seek simple criterion or insight

Strongly Unextendible MUBs



3 strongly unextendible MUBs in $\mathbb{C}^d$

(Grassl)

Strongly Unextendible MUBs

- How many MUBs can exist in $\mathbb{C}^d$?

- When and why is a set of MUBs unextendible?
    - ⋆ seek simple criterion or insight
    - ⋆ *strongly unextendible* is a more demanding condition, but presumably easier to establish

Strongly Unextendible MUBs

- $\mu(d) \leq d+1$ (Delsarte Goethals Seidel 1975)
  - ⋆ there are at most $d(d+1)$ vectors in $\mathbb{C}^d$ of norm d whose pairwise Hermitian inner products each have magnitude 0 or $\sqrt{d}$
  - ⋆ so every set of $d+1$ MUBs in $\mathbb{C}^d$ is strongly unextendible

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Strongly Unextendible MUBs

$$(\;2\quad 0\quad 0\quad 0\;)$$
$$(\;0\quad 2\quad 0\quad 0\;)$$
$$(\;0\quad 0\quad 2\quad 0\;)$$
$$(\;0\quad 0\quad 0\quad 2\;)$$

$$(\;1\quad 1\quad 1\quad 1\;)$$
$$(\;1\quad 1\quad -1\quad -1\;)$$
$$(\;1\quad -1\quad 1\quad -1\;)$$
$$(\;1\quad -1\quad -1\quad 1\;)$$

$$(\;1\quad 1\quad i\quad -i\;)$$
$$(\;1\quad 1\quad -i\quad i\;)$$
$$(\;1\quad -1\quad i\quad i\;)$$
$$(\;1\quad -1\quad -i\quad -i\;)$$

5 strongly unextendible MUBs in $\mathbb{C}^4$

$$(\;1\quad i\quad 1\quad -i\;)$$
$$(\;1\quad i\quad -1\quad i\;)$$
$$(\;1\quad -i\quad 1\quad i\;)$$
$$(\;1\quad -i\quad -1\quad -i\;)$$

$$(\;1\quad i\quad i\quad -1\;)$$
$$(\;1\quad i\quad -i\quad 1\;)$$
$$(\;1\quad -i\quad i\quad 1\;)$$
$$(\;1\quad -i\quad -i\quad -1\;)$$

Jonathan Jedwab
18 April 2016

Strongly Unextendible MUBs

- Every set of 3 MUBs in $\mathbb{C}^6$ arising from the product construction is strongly unextendible (McNulty Weigert 2012)
  - ⋆ proof relies on classifying all such sets of 3 MUBs in $\mathbb{C}^6$, up to equivalence

r MUBs in $\mathbb{C}^m$

$\otimes$

r MUBs in $\mathbb{C}^n$

↓

r MUBs in $\mathbb{C}^{mn}$

$$\mu(mn) \geq \min(\mu(m), \mu(n))$$

Strongly Unextendible MUBs

- Infinite family of $p^2 - p + 2$ strongly unextendible MUBs in $\mathbb{C}^{p^2}$, for all primes p congruent to 3 modulo 4 (Szántó 2016)
  - ★ proof using complementary decompositions of $M_p \otimes M_p$ (M_p is the algebra of matrices acting on $\mathbb{C}^p$)
  - ★ only known infinite family of dimensions d containing fewer than $\mu(d)$ strongly unextendible MUBs
  - ★ ratio $(p^2 - p + 2)/\mu(p^2) \to 1$ as $p \to \infty$

$\mu(d)$ is largest number of MUBs that can exist in $\mathbb{C}^d$

Strongly Unextendible MUBs

(2	0	0	0)
(0	2	0	0)
(0	0	2	0)
(0	0	0	2)

(1	i	i	-1)
(1	$-i$	$-i$	-1)
(1	$-i$	i	1)
(1	i	$-i$	1)

(1	$-i$	$-i$	1)
(1	$-i$	i	-1)
(1	i	$-i$	-1)
(1	i	i	1)

3 strongly unextendible MUBs in $\mathbb{C}^4$

(Mandayam Bandyopadhyay Grassl Wootters 2014)

Jonathan Jedwab
18 April 2016

Strongly Unextendible MUBs

- 3 strongly unextendible MUBs in $\mathbb{C}^4$ (yet $\mu(4) = 5$)

  5 strongly unextendible MUBs in $\mathbb{C}^8$ (yet $\mu(8) = 9$)

  (Mandayam Bandyopadhyay Grassl Wootters 2014)

  - ⋆ constructed from maximal commuting classes of Pauli operators
  - ⋆ computational proof of strong unextendibility using Gröbner bases
  - ⋆ conjecture: $2^{m-1}+1$ strongly unextendible MUBs in $\mathbb{C}^{2^m}$
  - ⋆ conjecture fails if restrict to Pauli operators (Thas 2014+, using finite geometry)

Strongly Unextendible MUBs

- Conjecture: $2^{m-1}+1$ strongly unextendible MUBs in $\mathbb{C}^{2^m}$ (Mandayam et al 2014)

(2	0	0	0)
(0	2	0	0)
(0	0	2	0)
(0	0	0	2)

(1	1	1	−1)
(1	−1	−1	−1)
(1	−1	1	1)
(1	1	−1	1)

(1	−1	−1	1)
(1	−1	1	−1)
(1	1	−1	−1)
(1	1	1	1)

3 strongly unextendible MUBs in $\mathbb{R}^4$

Strongly Unextendible MUBs

- Conjecture: $2^{m-1}+1$ strongly unextendible MUBs in $\mathbb{C}^{2^m}$ (Mandayam et al 2014)

- At most $\frac{1}{2}d+1$ MUBs in $\mathbb{R}^d$ (Delsarte Goethals Seidel 1975)
  - ⋆ every set of $\frac{1}{2}d+1$ MUBs in $\mathbb{R}^d$ is strongly unextendible over $\mathbb{R}$

- Construction of $\frac{1}{2}d+1$ MUBs in $\mathbb{R}^d$ when $d=2^m$ for even m (Cameron Seidel 1973)
  - ⋆ $2^{m-1}+1$ MUBs in $\mathbb{R}^{2^m}$ for even m

Strongly Unextendible MUBs

- Conjecture: $2^{m-1}+1$ strongly unextendible MUBs in $\mathbb{C}^{2^m}$

- Construction of $2^{m-1}+1$ MUBs in $\mathbb{R}^{2^m}$ for even *m*

- Theorem: these MUBs are strongly unextendible! (Jedwab Yen)
  - ⋆ conjecture holds for all even *m*
  - ⋆ proof using only elementary linear algebra
  - ⋆ ratio $(2^{m-1}+1)/\mu(2^m) \to 1/2$ as $m \to \infty$
  - ⋆ evidence that $\mu(6)=3$ is not convincing

Open Questions

- Does Mandayam et al conjecture hold for odd m ?

- Is Zauner's conjecture that $\mu(6) = 3$ true ?

- What is the smallest size of a (strongly) unextendible set of MUBs in $\mathbb{C}^d$? Can the ratio of unextendible set size to $\mu(d)$ be asymptotically less than 1/2 ?

- Can we find new construction methods for MUBs from combinatorial designs ?