5th Workshop on Real and Complex Hadamard Matrices and Applications
Alfréd Rényi Institute of Mathematics, Budapest
10–14 July 2017

Small Unextendible Sets of Mutually Unbiased Hadamard Matrices (MUHs)

arXiv:1611.08962

Markus Grassl

Markus.Grassl@mpl.mpg.de

11 July 2017

MAX PLANCK INSTITUTE
for the science of light

Mutually Unbiased Bases (MUBs)

- orthonormal bases $\mathcal{B}^{(j)} := \{|\psi_k^j\rangle : k = 1, \ldots, d\} \subset \mathbb{C}^d$
- basis states are "mutually unbiased":

$$|\langle\psi_k^j|\psi_m^l\rangle|^2 = \begin{cases} 1/d & \text{for } j \neq l, \\ \delta_{k,m} & \text{for } j = l. \end{cases}$$

- at most $d+1$ MUBs in dimension d
- constructions for $d+1$ MUBs only known for prime powers $d = p^e$
- lower bounds [Klappenecker & Rötteler, quant-ph/0309120]:

$$N(m \cdot n) \geq \min\{N(m), N(n)\} \geq 3$$

$$N(p_1^{e_1} p_2^{e_2} \ldots p_\ell^{e_\ell}) \geq \min_i p_i^{e_i} + 1$$

m MOLS of order $d \Longrightarrow m+2$ MUBs in dimension d^2

[Wocjan & Beth, quant-ph/0407081]

MUBs and Complex Hadamard Matrices

- the first basis $\mathcal{B}^{(1)}$ can always be chosen to be the standard basis
- any other basis $\mathcal{B}^{(i)}$ corresponds to a complex Hadamard matrix $\mathcal{H}^{(i)}$, i.e., a unitary matrix where all entries have constant modulus (unbiasedness wrt. to standard basis)
- the second basis $\mathcal{B}^{(2)}$ can always be chosen to be a dephased complex Hadamard matrix, i.e., first column/row have entries $1/\sqrt{d}$
- mutually unbiasedness of the bases implies that

$$\overline{\left(\mathcal{H}^{(i)}\right)}^{t}\mathcal{H}^{(j)} = d \cdot \mathcal{H}^{(i,j)},$$

i..e., the "product" of any two Hadamard matrices is again a (rescaled) Hadamard matrix (Mutually Unbiased Hadamard Matrices (MUH))

MUBs and Unitary Error Bases

[S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, & F. Vatan, quant-ph/0103162]

Theorem:

There exists k MUBs in dimension d if and only if there are $k(d-1)$ traceless, mutually orthogonal unitary matrices $U_{j,t} \in U(d, \mathbb{C})$ that can be partitioned into k sets of commuting matrices:

$$\mathcal{B} = \mathcal{C}_1 \cup \ldots \cup \mathcal{C}_k, \qquad \text{where } \mathcal{C}_j \cap \mathcal{C}_l = \emptyset \text{ and } |\mathcal{C}_j| = d-1$$

Each of the k orthogonal bases is given by the common eigenstates of the commuting matrices in one class $\mathcal{C}_j$.

Ansatz:

Use the Weyl-Heisenberg group or the generalized Pauli group

Weyl-Heisenberg Group

- generators: $$H_d := \langle X, Z \rangle$$

  where $X := \sum_{j=0}^{d-1} |j+1\rangle\langle j|$ and $Z := \sum_{j=0}^{d-1} \omega_d^j |j\rangle\langle j|$

  $$\omega_d := \exp(2\pi i/d)$$

- relations:

$$\left(\omega_d^c X^a Z^b\right)\left(\omega_d^{c'} X^{a'} Z^{b'}\right) = \omega_d^{a'b-b'a}\left(\omega_d^{c'} X^{a'} Z^{b'}\right)\left(\omega_d^c X^a Z^b\right)$$

- basis:

$$H_d/\zeta(H_d) = \left\{X^a Z^b \colon a, b \in \{0, \ldots, d-1\}\right\} \cong \mathbb{Z}_d \times \mathbb{Z}_d$$

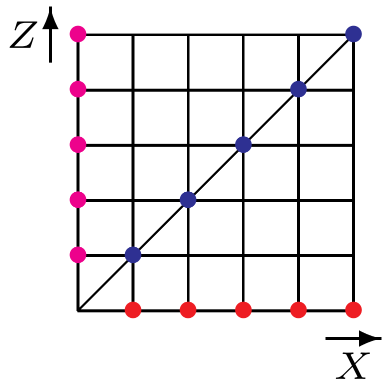
  trace-orthogonal basis of all $d \times d$ matrices

Three MUBs in any Dimension

consider the operators (Weyl-Heisenberg group)

$\{X^a : a = 1,\ldots,d-1\}$, $\{Z^a : a = 1,\ldots,d-1\}$, $\{X^a Z^a : a = 1,\ldots,d-1\}$

- all matrices are mutually orthogonal, the sets are disjoint, the matrices within each set commute
- geometric picture:



$\Longrightarrow$ the eigenvectors of X, Z, and XZ form three MUBs in any dimension

More than 3 MUBs in Dimension 6?

[M. Grassl, On SIC-POVMs and MUBs in Dimension 6, quant-ph/0406175]

Ansatz:

- Start with the eigenvectors of Z and X (computational & Fourier basis).
- Search for a vector $|\psi\rangle$ that is unbiased w.r.t. these 12 vectors.
- W. l. o. g, the first coordinate is $1/\sqrt{6}$.

$\Longrightarrow$ There are exactly 48 solutions for $|\psi\rangle$.

- There are 16 subsets of size 6 that are orthonormal bases.
- None of the vectors is unbiased with respect to one of the 16 bases.

Consequence:

Starting with the eigenvectors of X and Z, we get no more than 3 MUBs in dimension 6.

Unextendible MUBs: Dimension 4

eigenbases of Z and X (Weyl-Heisenberg group)

$$\mathcal{B}^{(1)} := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \qquad \mathcal{B}^{(2)} := \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & i & -1 & -i \\ 1 & -1 & 1 & -1 \\ 1 & -i & -1 & i \end{pmatrix}$$

third basis (row vectors)

$$\mathcal{B}^{(3)} := \frac{1}{2}\begin{pmatrix} 1 & e^{ia} & 1 & -e^{ia} \\ 1 & -e^{ia} & 1 & e^{ia} \\ 1 & e^{ib} & -1 & e^{ib} \\ 1 & -e^{ib} & -1 & -e^{ib} \end{pmatrix} \qquad \text{where } a, b \in [0, \pi)$$

no additional unbiased vector

Unextendible MUBs: Even Dimensions

Unextendible MUBs:

A set of mutually unbiased bases $\{\mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)}\}$ is *unextendible* if there is no other basis that is unbiased with respect to all bases $\mathcal{B}^{(j)}$.

If there is not even a single unbiased[a] vector, the set of MUBs is called *strongly unextendible*.

Conjecture:

For even dimensions $d = 2m$, the eigenbases of X, $Y = XZ$, and Z form a set of three strongly unextendible MUBs, i. e., there is no vector that is unbiased with respect to these three bases.

Verified for $d \leq 12$.

[a] A vector $|\phi\rangle$ is unbiased to a set of vectors $|\psi_i\rangle$ if $|\langle\phi|\psi_i\rangle| = \text{const.}$

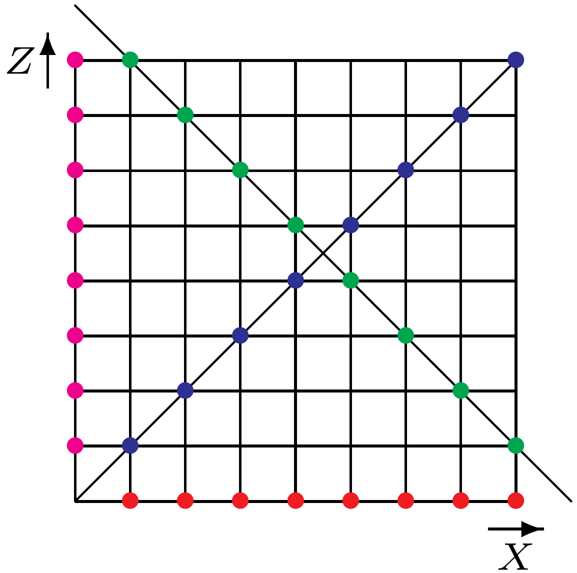
Four MUBs in All Odd Dimensions

four disjoint sets of operators

$$\{X^a : a = 1, \ldots, d-1\} \qquad \{Z^a : a = 1, \ldots, d-1\}$$

$$\{X^a Z^a : a = 1, \ldots, d-1\} \qquad \{X^a Z^{-a} : a = 1, \ldots, d-1\}$$

geometric picture ($d = 9$)



MUBs and Circulant Hadamard Matrices

- the eigenbases of Z and X correspond to the standard basis and the (cyclic) Fourier matrix
- a vector that is unbiased to both the standard basis and the Fourier basis is known as *bi-unimodular sequence*
- cyclic shifts of a bi-unimodular sequence are mutually orthogonal $\Longrightarrow$ circulant Hadamard matrices
- when the dimension is square-free, there are finitely many vectors that are unbiased to the eigenbases of Z and X
- computing all bi-unimodular sequences appears to be extremely difficult (cyclic N roots problem), numerically up to $N \leq 13$

MUBs: Small Prime Dimensions

for $d = 2, 3, 5$, the Fourier matrix is the unique complex Hadamard matrix

- $d = 2$
  there are exactly 2 vectors unbiased to the eigenbases of X and Z, forming the third basis

- $d = 3$
  there are exactly 2×3 vectors unbiased to the eigenbases of X and Z, forming the two other bases

- $d = 5$
  there are exactly 4×5 vectors unbiased to the eigenbases of X and Z, forming the four other bases

$\Longrightarrow$ unique maximal sets of MUBs for $d = 2, 3, 5$

Bachelor Hadamard Matrices

for $d = 6$, there is an isolated complex Hadamard matrix S_6

- for each pair of bases, there are exponentially many unbiased vectors
- here: 90 vectors that are unbiased to I and S_6
  [Stephen Brierley & Stefan Weigert, arXiv:0901.4051]
- but no subset of 6 vectors forms an orthonormal basis
- there is no complex Hadamard matrix that is unbiased to S_6
- in analogy to MOLS, we call such a matrix a *Bachelor Hadamard Matrix*
- so far, $d = 6$ is the only example known to us

Unextendible MUBs: Prime Dimensions $p \geq 7$

If d is prime, the eigenbases of the operators Z and XZ^j for $j = 0, \ldots, d-1$ form $d+1$ mutually unbiased bases.

Dimension 7:

- there are 532 vectors that are unbiased with respect to both the computational and the Fourier basis
- these 532 vectors give rise to 146 orthonormal bases
- among those, there are the six eigenbases of XZ^j for $j = 1, \ldots, 6$

but: together with the computational and Fourier basis, each of the other 140 bases results in a triple of strongly unextendible MUBs

Unextendible MUBs: Prime Dimensions $p \geq 7$

- specific construction that generalizes to other primes $p \geq 7$ yielding a triple of MUBs
- based on bi-unimodular sequences with few different values, depending on quadratic residues/non-residues
- different constructions for $p \equiv 1 \bmod 4$ and $p \equiv -1 \bmod 4$

Conjecture:
For all primes $p \geq 7$, there is a strongly unextendible triple of MUBs.

verified for $p = 7, 11$ and $p = 13$

Unextendible MUBs from Pauli Matrices

[P. Mandayam, S. Bandyopadhyay, M. Grassl, W. K. Wootters, arXiv:1302.3709]

incomplete partitioning of two-qubit Pauli matrices:

$$\mathcal{C}_1 = \{I \otimes X,\ X \otimes I,\ X \otimes X\} \qquad G_1 = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{array}\right)$$

$$\mathcal{C}_2 = \{I \otimes Z,\ Z \otimes I,\ Z \otimes Z\} \qquad G_2 = \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$$

$$\mathcal{C}_3 = \{X \otimes Z, Z \otimes X, Y \otimes Y\} \qquad G_3 = \left(\begin{array}{cc|cc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right)$$

This gives a set of three (real) MUBs that is strongly unextendible.

In general:
A set of MUBs from a partitioning of unitary operators is *weakly unextendible* if one cannot add another eigenbasis of those unitary operators.

Weakly Unextendible MUBs

A set of mutually unbiased bases $\{\mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)}\}$ is *unextendible* if there is no other basis that is unbiased with respect to all bases $\mathcal{B}^{(j)}$.

If there is not even a single unbiased[a] vector, the set of MUBs is called *strongly unextendible*.

A set of mutually unbiased bases constructed via eigenbases of generalized Pauli matrices is *weakly unextendible* if no other eigenbasis of Pauli matrices can be added.

Weakly unextendible MUBs can be obtained from so-called maximal symplectic partial spreads over finite fields.

[a] A vector $|\phi\rangle$ is unbiased to a set of vectors $|\psi_i\rangle$ if $|\langle\phi|\psi_i\rangle| = \text{const}$.

MAX PLANCK INSTITUTE for the science of light

Symplectic Spreads

totally isotropic subspace:

- subspace $S_i \leq \mathbb{F}_q^{2n}$ such that $S_i = S_i^\star$
- symplectic self-dual code $[2n, n, d]_q$ or $(n, q^n, d)_{q^2}$
- quantum code $[\![n, 0, d]\!]_q$ (graph state)

symplectic spread

collection of totally isotropic subspaces S_i with trivial intersection:

- $S_i \cap S_j = \{\mathbf{0}\}$ $(i \neq j)$
- $S_i + S_j = \mathbb{F}_q^{2n}$ $(i \neq j)$

maximal partial spread

collection of subspaces S_i that cannot be enlarged

Some Known Results

- maximal size of a (complete) symplectic spread in $\mathbb{F}_q^{2n}$ is $q^n + 1$
- complete spreads exists for all prime powers q and n
  - $n = 1$: take the lines through the origin in the affine space $\mathbb{F}_q^2$
  - $n > 1$: expand the spread in $\mathbb{F}_{q^n}^2$ using a symmetric basis of $\mathbb{F}_{q^n}$ as matrix algebra over $\mathbb{F}_q$
- maximal partial symplectic spreads have mainly been studied for the case $n = 2$ using generalized quadrangles (e.g., by the group in Ghent)

I did not find much information on maximal partial symplectic spreads for $n > 2$, but

[William M. Kantor, "On maximal symplectic partial spreads", arXiv:1601.04194]

MAX PLANCK INSTITUTE for the science of light

Defining Conditions for Symplectic Spreads

Normal Form of Generators:

$$G_\infty = \left(\ 0 \,\middle|\, I\ \right) \qquad \text{or} \qquad G_i = \left(\ I \,\middle|\, A_i\ \right), \quad A_i = A_i^t \text{ (symmetric)}$$

Proof:

- transitive action of symplectic group allows choice of G_∞
- joint row span of G_∞ and G_i is the full space $\Longrightarrow G_i = (I|A_i)$
- $S_i = S_i^\star \Longrightarrow A_i$ is symmetric

Defining Conditions for Symplectic Spreads:

$$S_i + S_j = \mathbb{F}_q^{2n} \Longleftrightarrow \det\left(\begin{array}{c|c} I & A_i \\ I & A_j \end{array}\right) \neq 0 \Longleftrightarrow \det(A_i - A_j) \neq 0$$

$$\Longleftrightarrow (\det(A_i - A_j))^{q-1} = 1$$

Smallest Maximal Partial Spread

[M. Cimráková, S. De Winter, V. Fack, and L. Storme, 2007]

Theorem There is a maximal partial symplectic spread of size $q+1$ for $q = 2^m$ and $n = 2$, and there is no smaller maximal partial symplectic spread.

Proof (maximality):

generators: $G_\infty = \left(\begin{array}{cc|cc} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right)$ and $G_\alpha = \left(\begin{array}{cc|cc} 1 & 0 & 0 & \alpha \\ 0 & 1 & \alpha & 0 \end{array}\right)$, $\alpha \in \mathbb{F}_q$

additional generator $G' = \left(\begin{array}{cc|cc} 1 & 0 & x_{00} & x_{01} \\ 0 & 1 & x_{01} & x_{11} \end{array}\right)$

condition: $\det \begin{pmatrix} x_{00} & x_{01} - \alpha \\ x_{01} - \alpha & x_{11} \end{pmatrix} = x_{00}x_{11} + x_{01}^2 + \alpha^2 \neq 0$ for all $\alpha \in \mathbb{F}_q$

MAX PLANCK INSTITUTE
for the science of light

Small Maximal Partial Spreads

Theorem For q an even prime power, the expansion of the smallest maximal partial spread of size $q^m + 1$ in $\mathbb{F}_{q^m}^4$ yields a maximal partial spread in $\mathbb{F}_q^{4m}$.

Corollary For $n = 2m$ qubits, there exists a weakly unextendibile set of MUBs of size $2^m + 1$, i.e., the size of the set is $\sqrt{d} + 1$, where $d = 2^{2m}$.

This seems to be the smallest possible (weakly) unextendible set of MUBs formed from eigenvactors of Pauli matrices.

But there is a candidate of size $61 < 2^6 + 1 = 65$ for $d = 8^4 = 2^{12}$

Construction I: Subfield Expansion

Take a maximal partial spread in $\mathbb{F}_{q^m}^{2n}$ and expand it to obtain a partial spread in $\mathbb{F}_q^{2mn}$.

Problem:

A maximal partial spread over an extension field need not remain maximal when represented over a subfield:

- $q = 4 = 2^2$, $n = 3$: size 17
- $q = 9 = 3^2$, $n = 2$: size 22, 23, 24, 25, and 29

Moreover, this does not yield maximal partial spreads in $\mathbb{F}_q^{2n}$, n prime.

$\Longrightarrow$ Find criteria to decide when the expansion remains to be maximal.

Construction II: Extension

Given generators

$$G_\infty = \left(\begin{array}{c|c} 0 & I \end{array} \right), \quad \text{and} \quad G_i = \left(\begin{array}{c|c} I & A_i \end{array} \right)$$

find a symmetric matrix X with

$$\det(X - A_i) \neq 0 \Longleftrightarrow (\det(X - A_i))^{q-1} = 1$$

$\Longrightarrow$ system of polynomial equations for the symmetric matrix X

$\Longrightarrow$ compute Gröbner basis

$\Longrightarrow$ proves maximality or provides candidates for extension

MAX PLANCK INSTITUTE
for the science of light

Exhaustive & Heuristic Search

exhaustive search

- graph $\mathcal{G}$ with all symmetric matrices as vertices
- edge between A_i and A_j iff $\det(A_i - A_j) \neq 0$
- maximal cliques in $\mathcal{G}$ of size m correspond to maximal partial spreads of size $m+1$ (use `cliquer`)

heuristic search

- start with a spread $\mathcal{S} = \{S_\infty, S_1, \ldots, S_m\}$
- pick a symmetric matrix A such that $S' \notin \mathcal{S}$, S' the row span of $\left(\begin{array}{c|c} I & A \end{array} \right)$
- keep those $S_i \in \mathcal{S}$ that intersect trivially with S'
- compute maximal extension of this partial spread

MAX PLANCK INSTITUTE
for the science of light

Maximal Symplectic Partial Spreads

$d = q^n$	q	n	size	remark
4	2	2	$3, 5$	complete
8	2	3	$5, 9$	complete
16	2	4	$5, 8, 9, 11, 13, 17$	complete
16	4	2	$5, 9, 11, 13, 17$	complete
32	2	5	$9, \ldots, 15, 17, 33$	
64	2	6	$9, 13, \ldots, 47, 49, 51, 57, 65$	
64	4	3	$17, \ldots, 43, 49, 65$	
64	8	2	$9, 17, 21, \ldots, 47, 49, 51, 57, 65$	
128	2	7	$21, \ldots, 31, 33, 35, 37, 39, 45, 49, 53, 57, 61, 65, 129$	
256	2	8	$17, 28, \ldots, 205, 209, 211, 213, 214, 215, 225, 227, 241, 257$	
256	4	4	$17, 33, 35, \ldots, 205, 209, 211, 213, 214, 215, 225, 227, 241, 257$	
256	16	2	$17, 33, 46, \ldots, 205, 209, 211, 213, 214, 215, 225, 227, 241, 257$	new values

Maximal Symplectic Partial Spreads (cont.)

$d = q^n$	q	n	size	remark
9	3	2	$5, 8, 10$	complete
27	3	3	$10, \ldots, 20, 28$	complete
81	3	4	$18, \ldots, 68, 70, 73, 74, 82$	
81	9	2	$22, \ldots, 68, 70, 73, 74, 82$	
243	3	5	$32, \ldots, 120, 123, 154, 163, 244$	
25	5	2	$13, \ldots, 20, 22, 24, 26$	complete
125	5	3	$27, \ldots, 90, 101, 126$	
49	7	2	$14, 17, \ldots, 42, 44, 48, 50$	
121	11	2	$28, \ldots, 106, 109, 110, 112, 120, 122$	new values
169	13	2	$40, \ldots, 140, 145, 146, 148, 158, 170$	new values
289	17	2	$67, \ldots, 238, 241, \ldots, 248, 257, 258, 260, 274, 290$	new values
361	19	2	$82, \ldots, 302, 307, \ldots, 314, 325, 326, 328, 344, 362$	new values

MAX PLANCK INSTITUTE
for the science of light

Small Sets of Unextendible MUBs

d	smallest set known	largest set known	other sizes
2	3	3	
3	4	4	
4	3	5	
5	6	6	
6	2	3	
7	3	8	
8	3	9	5
9	3	10	$4, 5, 8$
10	3	3	
11	3	12	
12	3	4	
13	3	14	
14	3 (?)	3	
15	3 (?)	4	
16	3 (?)	17	$5, 8, 9, 11, 13$

Average Entropy of MUB Measurements

- measuring the state $|\psi\rangle$ in the basis $\mathcal{B}^{(j)}$ results in a probability distribution P_j with Shannon entropy $H(\mathcal{B}^{(j)}, |\psi\rangle)$
- entropic (un)certainty relations

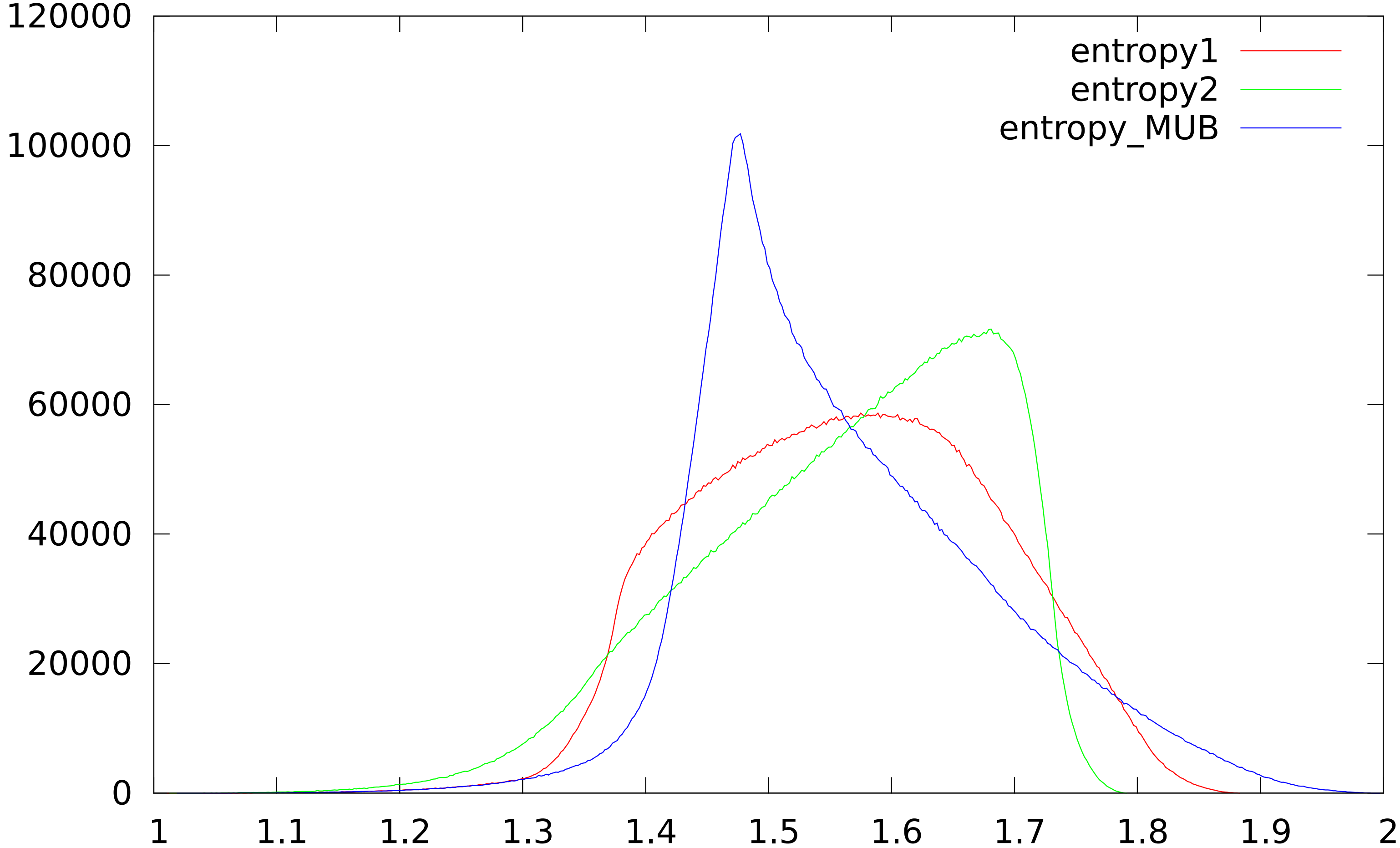
$$lb \leq \frac{1}{M} \sum_{j=1}^{M} H(\mathcal{B}^{(j)}, |\psi\rangle) \leq ub \leq \log d$$

lower bound lb and upper bound ub by minimisation/maximisation over all pure states $|\psi\rangle$

MAX PLANCK INSTITUTE for the science of light

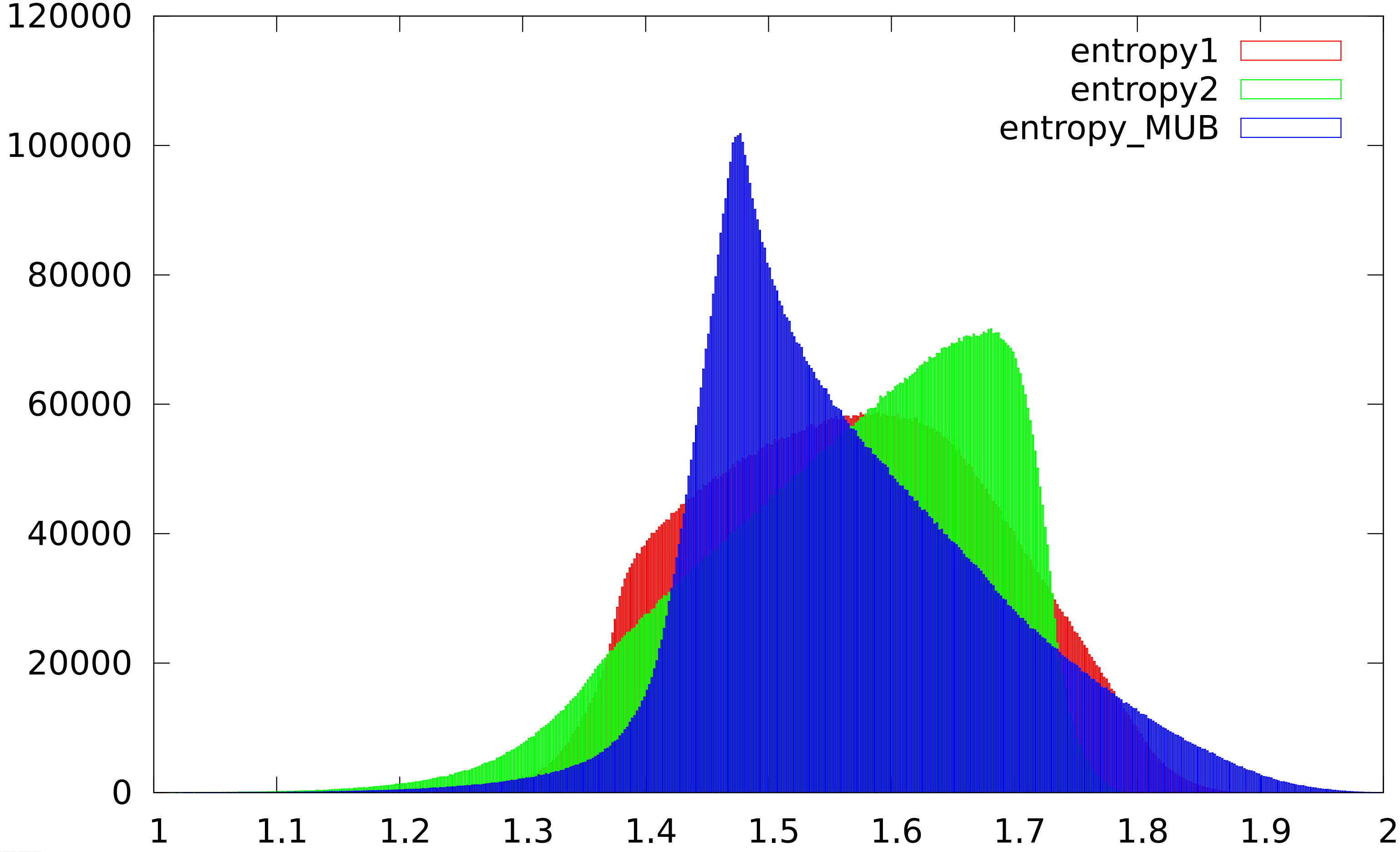
Three MUBs in Dimension 4

distribution of the average entropy for three different sets with $M = 3$ MUBs
10^7 random pure states (Haar measure)



Three MUBs in Dimension 4

distribution of the average entropy for three different sets with $M = 3$ MUBs
10^7 random pure states (Haar measure)



MAX PLANCK INSTITUTE
for the science of light

Conclusion & Outlook

- strongly unextendible triples of MUBs conjectured to exist in even and prime ($p \geq 7$) dimension
- strongly unextendible triple for $d = 9$
- pair of unextendible MUBs in dimension six
- weakly unextendible sets of MUBs from spreads of various sizes

Further directions

- When are weakly unextendible sets of MUBs unextendible?
- Are there Bachelor Hadamard Matrices in other dimensions?
- Find conditions when a set of MUBs is (strongly) unextendible.
  $\Longrightarrow$ [András Szántó, arXiv:1502.05245] using matrix algebras:
  $p^2 - p + 2$ strongly unextendible MUBs for $d = p^2$, $p \equiv 3 \bmod 4$
  $\Longrightarrow$ [J. Jedwab, L. Yen, arXiv:1604.04797] $d = 4^m$, $\frac{1}{2}d + 1$ (real) bases