Searching for mutually unbiased bases in non-prime power dimensions

Dardo Goyeneche & Fernando Chavez

Pontificia Universidad Católica
Santiago de Chile, Chile

Gustavo Lara

Universidad de Antofagasta
Antofagasta, Chile

8th Workshop on Design Theory, Hadamard Matrices and Applications
Sevilla, España - May 28, 2025

QUDIT
Quantum Development of Information Theory

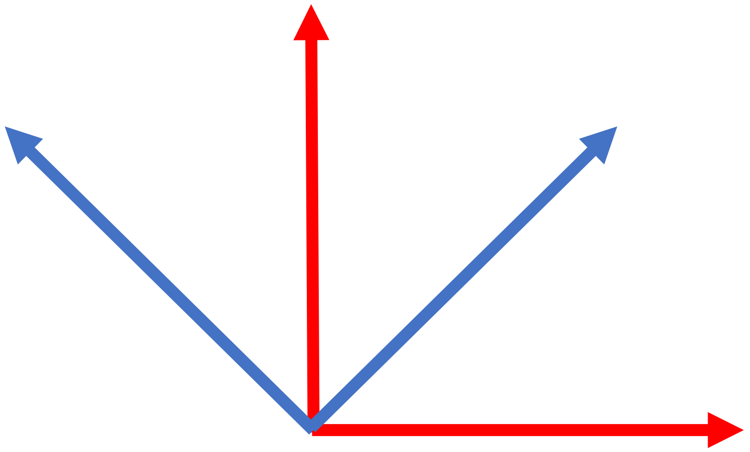
Mutually unbiased bases

Two orthonormal bases $\{\phi_j\}$ and $\{\psi_{j'}\}$ defined in $\mathbb{C}^d$ are unbiased if

$$\left|\langle\phi_j|\psi_{j'}\rangle\right|^2 = \frac{1}{d},$$

for every $j, j' = 1, \dots d$.

We say that m orthonormal bases $\{\phi_j^k\}, k = 1, \dots, m,$ are mutually unbiased (MU) if they are pairwise unbiased.



{{1,0}; {0,1}}

{{1,1};{1,-1}}

Maximal number of MU bases

$$\#MU\ bases\ in\ \mathbb{C}^d \leq d+1$$

In prime power dimensions $d = p_1^{r_1}$, there are $d+1$ MU bases

When $d \neq p_1^{r_1}$, nobody knows the maximal number of MU bases (e.g. $d = 6$)

$$d = p_1^{r_1} p_2^{r_2} p_3^{r_3} \ldots \ (p_1^{r_1} < p_2^{r_2} < p_3^{r_3} \ldots)$$

$$\#MU\ bases\ in\ \mathbb{C}^d \geq p_1^{r_1} + 1$$

The lower bound is not tight!

$$\#MU\ bases\ in\ \mathbb{C}^d \geq p_1^{r_1} + 1$$

$w + 2$ MU bases can be constructed in any square dimension $d = s^2$ provided that there are w mutually orthogonal Latin squares of order s.

There are 4 MOLS of order 26

Wocjan, P., & Beth, T. (2005). New construction of mutually unbiased bases in square dimensions. Quantum Information & Computation, 5(2), 93-101.

Ch. J. Colbourn and J. H. Dinitz, editors. The CRC Handbook of Combinatorial Designs. CRC Press, Boca Raton FL, 1996.

When $d = 26^2 = 2^2\ 13^2,\ \ p_1^{r_1} + 1 = 4 + 1 = 5$

but 6 MU bases are known

$$d = p_1^{r_1} p_2^{r_2} p_3^{r_3} \ldots \ (p_1^{r_1} < p_2^{r_2} < p_3^{r_3} \ldots)$$

$$p_1^{r_1} + 1 \leq \#MU\ bases\ in\ \mathbb{C}^d \leq d + 1$$

Key question

Is the upper bound tight in non-prime power dimensions?

Key question for our work

Is the lower bound tight in relatively low dimensions?

$$d \leq 30$$

Flatness imposition operator

Non-linear operator that takes a vector $\varphi \in \mathbb{C}^d$, and an orthonormal basis $A = \{\phi_j\} \subset \mathbb{C}^d$ and produces a normalized vector $T_A\phi$ that is MU to the basis A.

$$\varphi = \sum_{j=1}^{d} \langle \phi_j | \varphi \rangle \, \phi_j$$

Removes the absolute value of projections

Imposes flatness

$$T_A\varphi = \sum_{j=1}^{d} \frac{1}{\sqrt{d}} \frac{\langle \phi_j | \varphi \rangle}{|\langle \phi_j | \varphi \rangle|} \phi_j, \qquad \forall \varphi \in \mathbb{C}^d$$

Important fact:
Phases do not change

φ is flat with respect to the basis A if and only if $T_A\varphi = \varphi$

Goyeneche, D. M., & de La Torre, A. C. (2008). State determination: An iterative algorithm. *Physical Review A* **77**(4), 042116.

Algorithm for finding MU vectors

Define two orthonormal bases $A = \{\varphi_j\}$ and $B = \{\psi_j\}$ in $\mathbb{C}^d$

Define the flatness operators

$$T_A\varphi = \sum_{j=1}^{d} \frac{1}{\sqrt{d}} \frac{\langle \phi_j|\varphi\rangle}{|\langle \phi_j|\varphi\rangle|}\,\phi_j$$

$$\forall \varphi \in \mathbb{C}^d$$

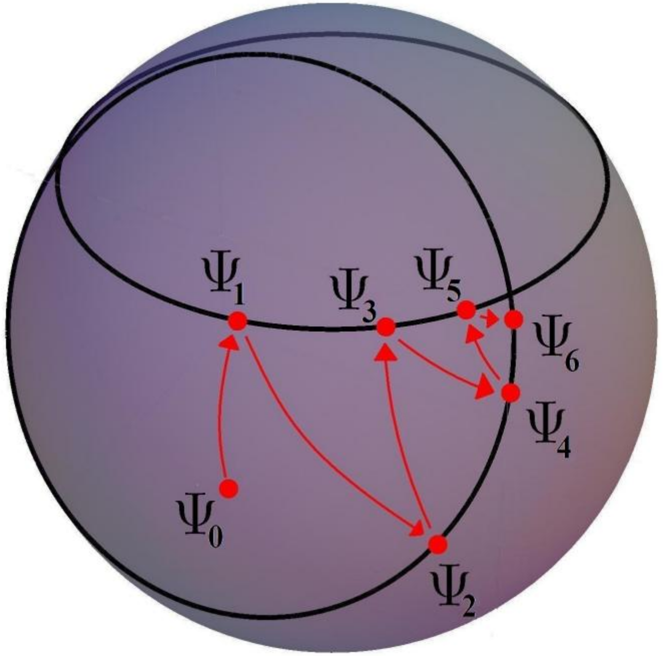
$$T_B\varphi = \sum_{j=1}^{d} \frac{1}{\sqrt{d}} \frac{\langle \psi_j|\varphi\rangle}{|\langle \psi_j|\varphi\rangle|}\,\psi_j$$

Study convergence of the sequence

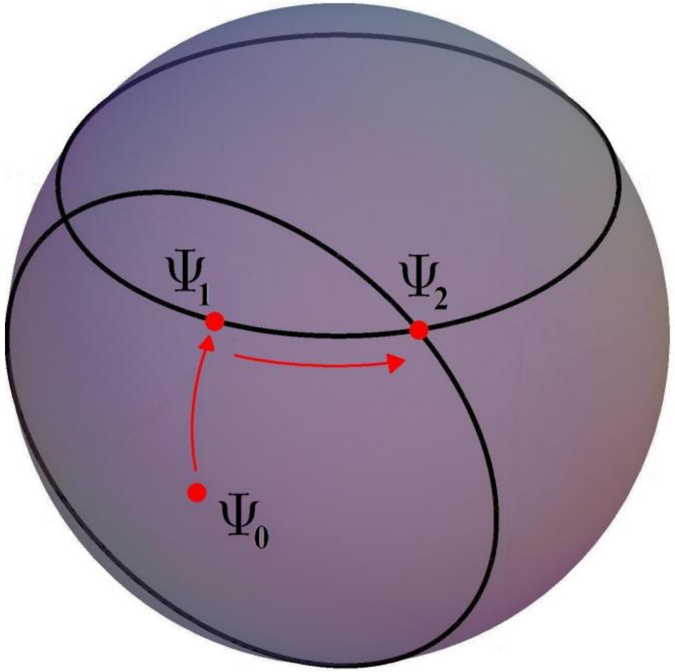
$$\varphi_n = (T_B T_A)^n \varphi_0$$

Goyeneche, D., & de la Torre, A. C. (2014). Quantum tomography meets dynamical systems and bifurcations theory. *J. Math. Phys. 55*(6).

Convergence on the Bloch (Poincaré) sphere



Convergence of the sequence $\varphi_n = (T_B T_A)^n \varphi_0$
when $\{A, B\}$ are not MU



Convergence of the sequence $\varphi_n = (T_B T_A)^n \varphi_0$
when $\{A, B\}$ are MU.
(Flatness corresponds to maximal circles!)

Goyeneche, D., & de la Torre, A. C. (2014). Quantum tomography meets dynamical systems and bifurcations theory. *J. Math. Phys. 55*(6).

Dynamical systems

Desired solutions are common fixed points

$T_A\varphi = T_B\varphi = \varphi$ if and only if φ is MU to the pair of bases $\{A, B\}$

Sweet: MU vectors <u>are always</u> attractive fixed points

Bitter: $T_B T_A\varphi = \varphi$ does not imply $T_A\varphi = T_B\varphi = \varphi$

There are more attractive fixed points than MU vectors

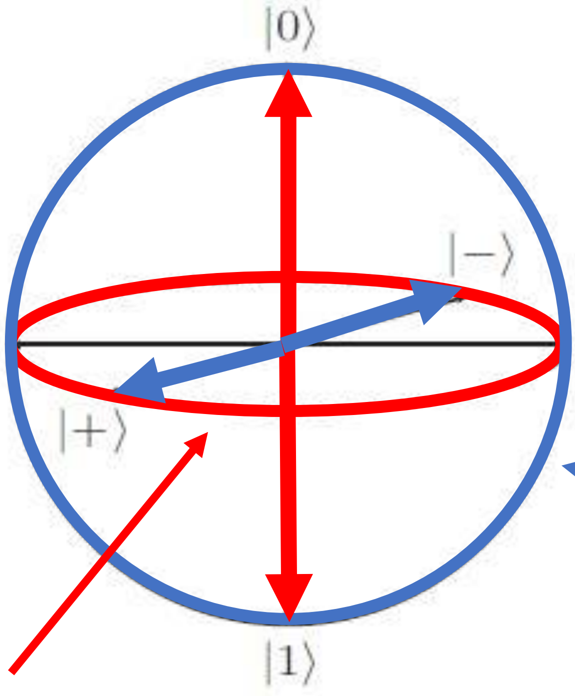
Goyeneche, D., & de la Torre, A. C. (2014). Quantum tomography meets dynamical systems and bifurcations theory. *J. Math. Phys. 55*(6).

Convergence on the Bloch (Poincaré) sphere

Common fixed point 1

Common fixed point 2

{1,-i} = $|-i\rangle$



$|+i\rangle$ **= {1,i}**

Set of fixed points for T_B

B={{1,1};{1,-1}}

Set of fixed points for T_A

A={{1,0}; {0,1}}

C={{1,i};{1,-i}}

3 MU bases in $\mathbb{C}^2$
A, B, C

How to reach the desired fixed points?

Smart approach: Common fixed point theorems

Problem:

Common fixed point theorems from the literature seem not to be useful for us. State a suitable theorem seems to be hard.

Quick and dirty approach: Discard undesired solutions and keep trying.

Problem: The fraction desired/undesired solutions is very small in not-so-small dimensions ($d > 10$), so most of the time the algorithm is discarding undesired fixed points.

Our approach

Metrics in the probability space

Hellinger distance

$$D_A(\Phi, \Psi) = \sqrt{\sum_{k=0}^{d-1} (\sqrt{p_k} - \sqrt{q_k})^2},$$

$where$

$$p_k = |\langle \varphi_k, \Phi \rangle|^2 \ and \ q_k = |\langle \varphi_k, \Psi \rangle|^2,$$

$for \ every \ k = 0, \ldots, d-1.$

Distributional “distance”

$$\mathcal{D}_{A^1 \ldots A^m}(\Phi, \Psi) = \sqrt{\frac{1}{m} \sum_{j=1}^{m} D^2_{A^j}(\Phi, \Psi)}.$$

Properties of the distributional "distance"

1. $\mathcal{D}_{A^1 \dots A^m}(\Phi, \Psi) = 0$ iff $|\langle \varphi_k^j, \Phi \rangle| = |\langle \varphi_k^j, \Psi \rangle|$, for every $j = 1, \dots, m$, $k = 0, \dots, d-1$.

2. $\mathcal{D}_{A^1 \dots A^m}(\Phi, \Psi) = \mathcal{D}_{A^1 \dots A^m}(\Psi, \Phi) \ \ \forall \Phi, \Psi \in \mathcal{H}$.

3. $\mathcal{D}_{A^1 \dots A^m}(\Phi, \Psi) \leq \mathcal{D}_{A^1 \dots A^m}(\Phi, \Xi) + \mathcal{D}_{A^1 \dots A^m}(\Xi, \Psi) \ \ \forall \Phi, \Psi, \Xi \in \mathcal{H}$.

Metric in the Hilbert space

Bures metric for pure states

$$d(\Phi, \Psi) = \sqrt{2 - 2|\langle \Phi, \Psi \rangle|}.$$

Note that $d(\Phi, \Psi) = d\left(\Phi, e^{i\alpha}\Psi\right)$, for any $\alpha \in [0, 2\pi)$

Property

$$d(\Phi, \Psi) \geq \mathcal{D}_{A^1 \ldots A^m}(\Phi, \Psi), \ \forall \Phi, \Psi \in \mathcal{H}.$$

Two different elements can have the same (flat) probability distributions

What’s new in our current approach?

Efficient coding in Python

Use GPU to accelerate simulations

Chao2 to estimate the number of undetected MU vectors

Two workstations available at QuDIT

(1 workstation with exclusive dedication to the MU bases problem)

Results

Preliminar studies

Dim	Second Basis	# MU Vectors	Distributional metric	Max Clique
6	F_6	48	$< 10^{-15}$	16 size 6
	$S_6^{(0)}$	90	$< 10^{-16}$	90 size 1
	$C_6^{(0)}$	52	$< 5 * 10^{-16}$	1 size 4
	$D_6^{(1)}$	120	$< 10^{-15}$	10 size 6
	$B_6^{(1)}$	84	$< 10^{-15}$	1 size 6
	$M_6^{(1)}$	8	$< 2 * 10^{-16}$	4 size 2
	$K_6^{(2)}$	56	$< 4 * 10^{-16}$	52 size 2
	$K_6^{(3)}$	48	$< 10^{-16}$	24 size 2

16 triplets $\{\mathbb{I}, F_6, H_i\}$

90 vectors (no triplet)

10 triplets $\{\mathbb{I}, D_6(0), H_i\}$

Preliminar studies

Dim	Second Basis	# MU Vectors	Distributional metric	Max Clique
6	F_6	48	$< 10^{-15}$	16 size 6
	$S_6^{(0)}$	90	$< 10^{-16}$	90 size 1
	$C_6^{(0)}$	52	$< 5 * 10^{-16}$	1 size 4
	$D_6^{(1)}$	120	$< 10^{-15}$	10 size 6
	$B_6^{(1)}$	84	$< 10^{-15}$	1 size 6
	$M_6^{(1)}$	8	$< 2 * 10^{-16}$	4 size 2
	$K_6^{(2)}$	56	$< 4 * 10^{-16}$	52 size 2
	$K_6^{(3)}$	48	$< 10^{-16}$	24 size 2
11	F_{11}	110	$< 10^{-15}$	10 size 11
	$C_{11A}^{(0)}$	3021	$< 10^{-15}$	3021 size 1
	$C_{11B}^{(0)}$	3006	$< 10^{-15}$	3006 size 1
	$N_{11A}^{(0)}$	3143	$< 10^{-15}$	3143 size 1
	$N_{11B}^{(0)}$	3077	$< 10^{-15}$	3077 size 1
	$Q_{11A}^{(0)}$	3006	$< 10^{-12}$	3006 size 1
	$Q_{11B}^{(0)}$	2553	$< 10^{-12}$	2553 size 1

16 triplets $\{\mathbb{I}, F_6, H_i\}$

90 vectors (no triplet)

10 triplets $\{\mathbb{I}, D_6(0), H_i\}$

Equivalent?

Bruzda – Tadej – Życzkowski catalog

$F_{11}^{(0)} = F_{11} \in BH(11,11)$

$C_{11\Sigma\,:\,\Sigma\in\{A,B\}}^{(0)}$

$N_{11A}^{(0)}$

$N_{11B}^{(0)}$

$Q_{11\Sigma\,:\,\Sigma\in\{A,B\}}^{(0)}$

48 MU vectors to F_6

$$a = \frac{1-\sqrt{3}}{2} + i\sqrt{\frac{\sqrt{3}}{2}}$$

$$X|\varphi_k\rangle = |\varphi_{k+1}\rangle, \text{ and } Z|\varphi_k\rangle = \omega^k|\varphi_k\rangle$$

$$\omega = e^{2\pi i/6}$$

$$\tau = -e^{i\pi/6}$$

$$D_p = \tau^{p_1 p_2} X^{p_1} Z^{p_2}$$

$\{D_{(\mu,0)} v_1\}_{\mu\in\mathbb{Z}_6}$ (6 elements)

$\{D_{(\mu,0)} v_2)\}_{\mu\in\mathbb{Z}_6}$ (6 elements)

$\{D_{(\mu,\mu\nu)} v_3\}_{\mu,\nu\in\mathbb{Z}_6}.$ (36 elements)

$$\begin{aligned}
v_1 &= \frac{1}{\sqrt{6}}(1, i, \omega^4, i, 1, i\omega^4),\\
v_2 &= \frac{1}{\sqrt{6}}(1, -i, \omega^2, -i, 1, -i\omega^2),\\
v_3 &= \frac{1}{\sqrt{6}}(1, ia, a^2, -ia^2, -a, -i),
\end{aligned}$$

Goyeneche, D. (2013). Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension 6. *J. Phys. A: Math & Theor.*, *46*(10), 105301.

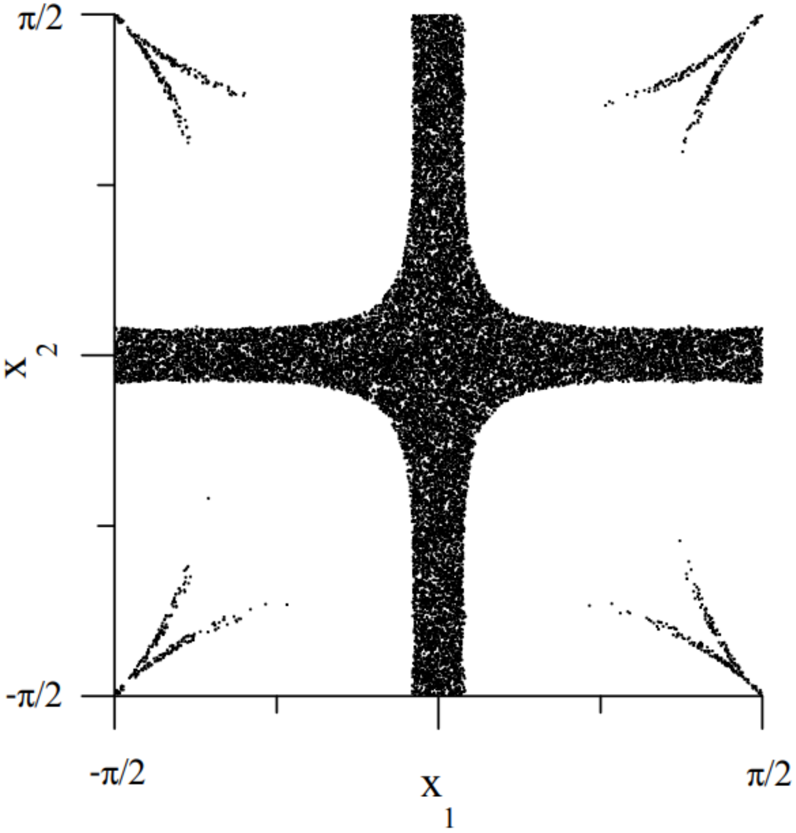
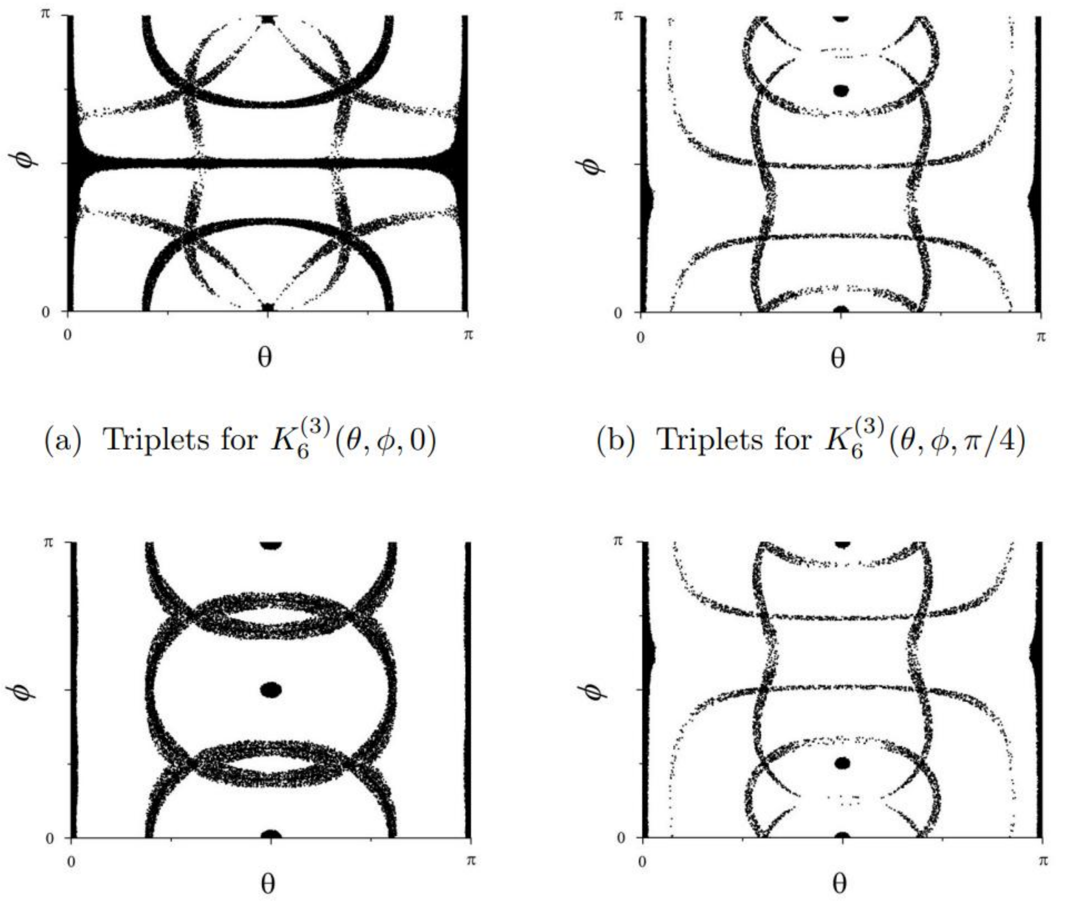


FIG. 1: Triplets of MU bases from $K_6^{(2)}$. A dot at the point (x_1, x_2) indicates that the pair $\{\mathbb{I}, K_6^{(2)}(x_1, x_2)\}$ can be extended to a triplet of MU bases.

Goyeneche, D. (2013). Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension 6. *J. Phys. A: Math & Theor.*, *46*(10), 105301.



(a) Triplets for $K_6^{(3)}(\theta, \phi, 0)$

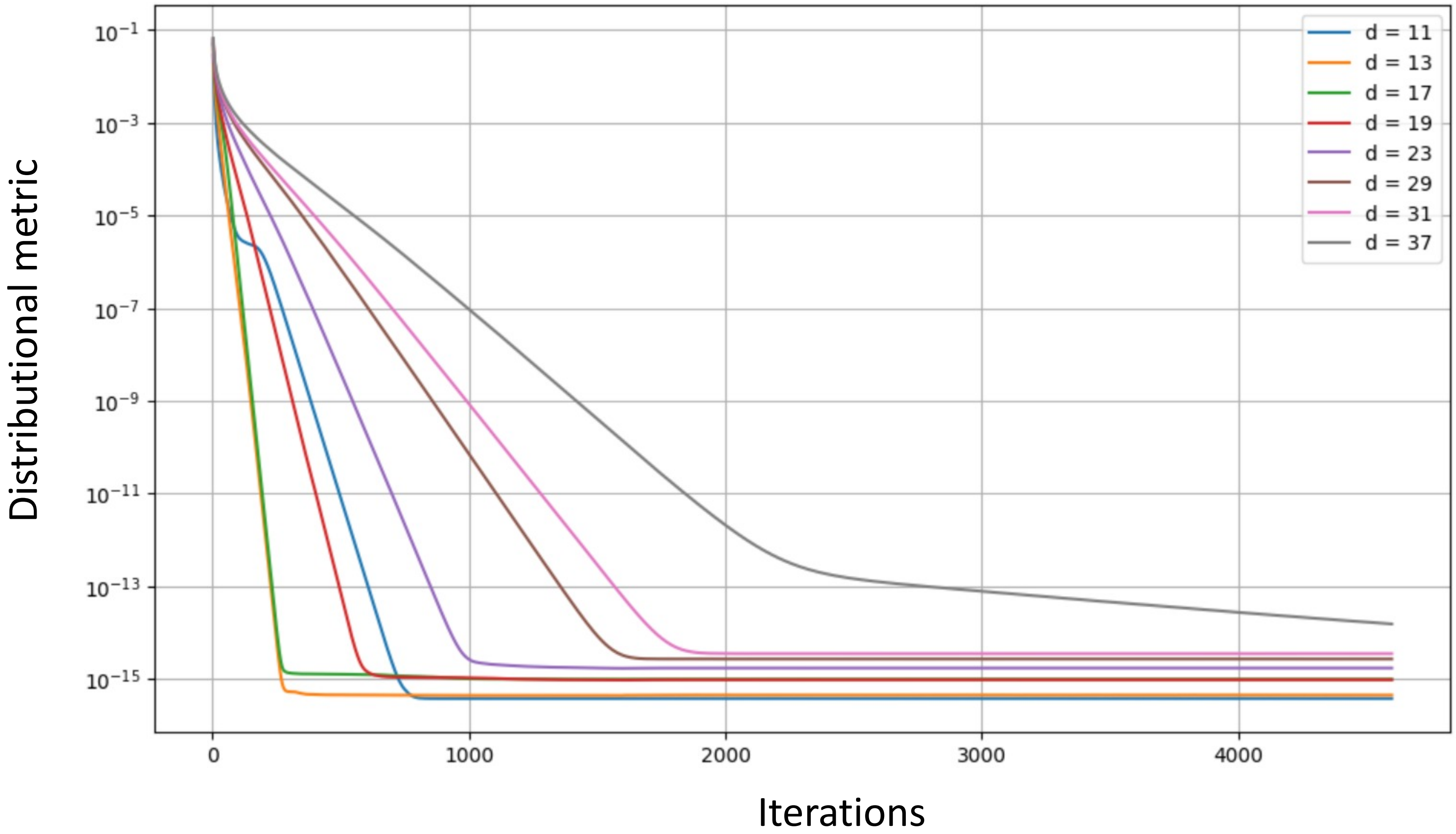
(b) Triplets for $K_6^{(3)}(\theta, \phi, \pi/4)$

(c) Triplets for $K_6^{(3)}(\theta, \phi, \pi/2)$

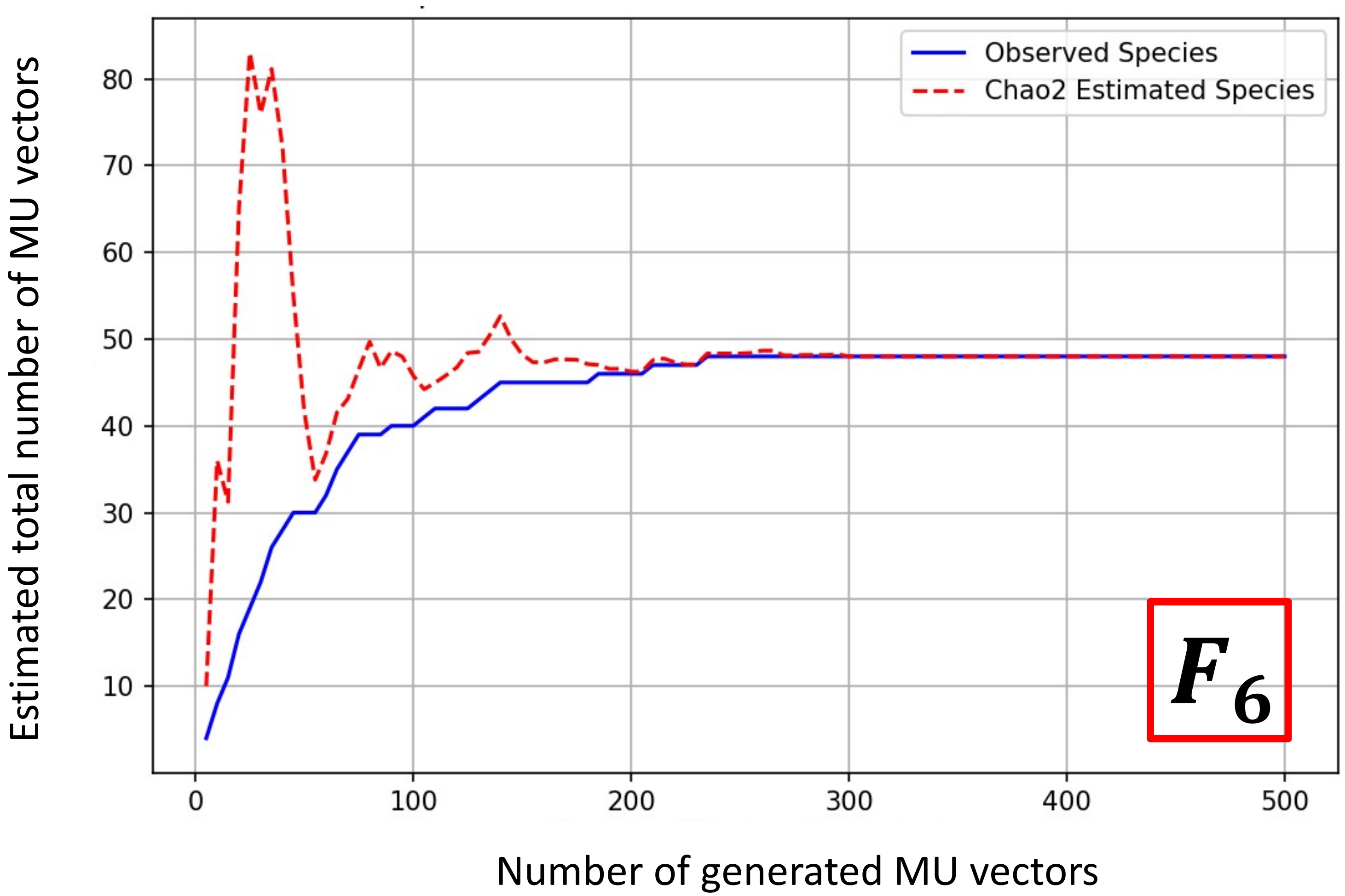
(d) Triplets for $K_6^{(3)}(\theta, \phi, 3\pi/4)$

Goyeneche, D. (2013). Mutually unbiased triplets from non-affine families of complex Hadamard matrices in dimension 6. *J. Phys. A: Math & Theor.*, *46*(10), 105301.

Convergence for vectors MU to $\{\mathbb{I}, F_d\}$



Estimating the total number of MU vectors



Chao2 estimation is a non-parametric method to estimate total species richness from incidence (presence/absence) data across multiple samples, accounting for unseen species based on the number of rare ones.

Chao, A. (1987). Estimating the population size for capture-recapture data with unequal catchability. *Biometrics*, 783-791.

MU vectors for quaternary CHM

https://wiki.aalto.fi/display/QCHmatrices/Home

P. H. J. Lampio, F. Szöllősi, P. R. J. Östergård: The quaternary complex Hadamard matrices of orders 10, 12, and 14. Discrete Math., 313:189–206 (2013).

MU vectors for quaternary CHM

$d = 10$			
m	#v	k	c
10	962	10	1
9	960	10	1
3	989	6	360
1	866	6	16
7	807	6	1
4	859	4	1192
8	743	4	416
6	733	4	416
5	882	4	52
2	894	4	36

10 matrices

m= matrix label
#v= number of vectors
k = size of the largest orthogonal clique
c = number of distinct cliques of that size.

https://wiki.aalto.fi/display/QCHmatrices/Home

P. H. J. Lampio, F. Szöllősi, P. R. J. Östergård: The quaternary complex Hadamard matrices of orders 10, 12, and 14. Discrete Math., 313:189–206 (2013).

MU vectors for quaternary CHM

$d = 10$				$d = 12$			
m	#v	k	c	m	#v	k	c
10	962	**10**	1	28	1360	**12**	64
9	960	**10**	1	182	3943	**12**	36
3	989	6	360	218	3577	**12**	4
1	866	6	16	165	3559	**12**	4
7	807	6	1	168	2730	**12**	2
4	859	4	1192	304	2699	**12**	2
8	743	4	416	213	3720	**12**	1
6	733	4	416	308	3712	**12**	1
5	882	4	52	237	3367	**12**	1
2	894	4	36	248	3334	**12**	1
				203	3446	10	3
				258	3454	9	6
				281	3489	9	3
				187	3390	9	2
				261	3663	8	89
				210	3655	8	60
				282	3392	8	60
				185	2973	8	32
				190	2917	8	32
				94	3175	8	26

10 matrices

319 matrices

m= matrix label
#v= number of vectors
k = size of the largest orthogonal clique
c = number of distinct cliques of that size.

https://wiki.aalto.fi/display/QCHmatrices/Home

P. H. J. Lampio, F. Szöllősi, P. R. J. Östergård: The quaternary complex Hadamard matrices of orders 10, 12, and 14. Discrete Math., 313:189–206 (2013).

MU vectors for quaternary CHM

$d = 10$				$d = 12$				$d = 14$			
m	#v	k	c	m	#v	k	c	m	#v	k	c
10	962	**10**	1	28	1360	**12**	64	185	15132	12	78
9	960	**10**	1	182	3943	**12**	36	588	11230	5	1
3	989	6	360	218	3577	**12**	4	462	11039	4	1
1	866	6	16	165	3559	**12**	4	390	10993	4	1
7	807	6	1	168	2730	**12**	2	232	10813	4	1
4	859	4	1192	304	2699	**12**	2	694	10903	2	40710
8	743	4	416	213	3720	**12**	1	332	10572	2	39327
6	733	4	416	308	3712	**12**	1	160	11316	2	36823
5	882	4	52	237	3367	**12**	1	61	11762	2	32871
2	894	4	36	248	3334	**12**	1	123	11611	2	32696
				203	3446	10	3	453	11321	2	32240
				258	3454	9	6	197	11186	2	31626
				281	3489	9	3	612	12033	2	22512
				187	3390	9	2	137	11776	2	21868
				261	3663	8	89	⋮	⋮	⋮	⋮
				210	3655	8	60				
				282	3392	8	60				
				185	2973	8	32				
				190	2917	8	32				
				94	3175	8	36				

10 matrices

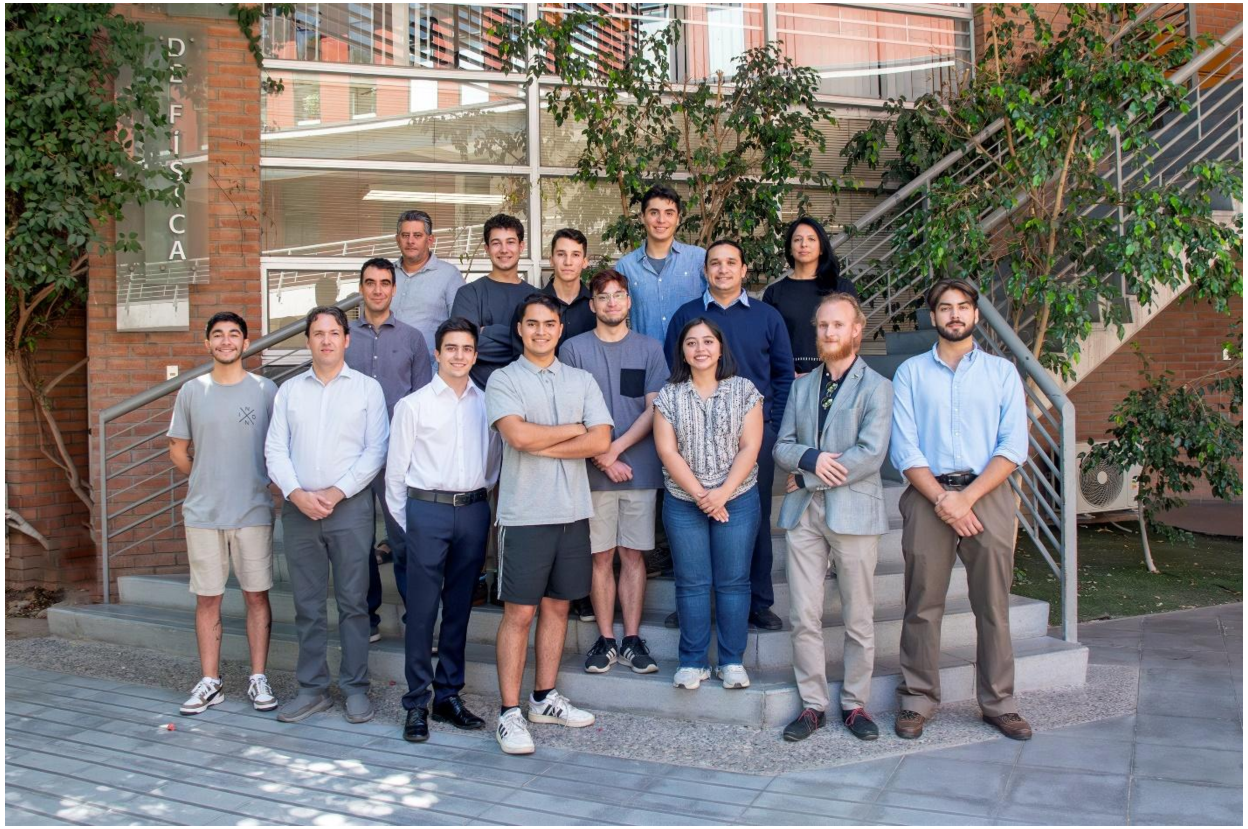
319 matrices

752 matrices

m= matrix label
#v= number of vectors
k = size of the largest orthogonal clique
c = number of distinct cliques of that size.

https://wiki.aalto.fi/display/QCHmatrices/Home

P. H. J. Lampio, F. Szöllősi, P. R. J. Östergård: The quaternary complex Hadamard matrices of orders 10, 12, and 14. Discrete Math., 313:189–206 (2013).



QUDIT

Quantum Development of Information Theory

qudit.cl

@qudit.cl

Acknowledgements:

Grant FONDECyT Regular

nro 1230586, Chile

Many thanks for your attention!