Mutually Unbiased Bases: complementary observables in finite-dimensional Hilbert spaces

Prabha Mandayam
Chennai Mathematical Institute

Aspects of Mathematics
The Institute of Mathematical Sciences

Outline

- Mutually Unbiased Bases: an introduction

Outline

- Mutually Unbiased Bases: an introduction
- Existence and Constructions :
  - Generators of the Weyl-Heisenberg group in prime dimensions
  - maximal sets of MUBs prime-powered dimensions: partitions of unitary operator basis

Outline

- Mutually Unbiased Bases: an introduction
- Existence and Constructions :
  - Generators of the Weyl-Heisenberg group in prime dimensions
  - maximal sets of MUBs prime-powered dimensions: partitions of unitary operator basis
- Applications: Quantum State Tomography and Quantum Cryptography

Outline

- Mutually Unbiased Bases: an introduction
- Existence and Constructions :
  - Generators of the Weyl-Heisenberg group in prime dimensions
  - maximal sets of MUBs prime-powered dimensions: partitions of unitary operator basis
- Applications: Quantum State Tomography and Quantum Cryptography
- Maximal sets in other composite dimensions?
  Unextendible sets of MUBs

Mutually Unbiased Bases

- Let $\mathbb{H}^d$ be a finite-dimensional Hilbert space[1].
  State space of any finite quantum system.
- **Definition**:- Two orthonormal bases $\mathcal{A} \equiv \{|a_0\rangle, |a_1\rangle, ..., |a_{d-1}\rangle\}$ and $\mathcal{B} \equiv \{|b_0\rangle, |b_1\rangle, ..., |b_{d-1}\rangle\}$ in $\mathbb{H}^d$ are *mutually unbiased* if

$$| \langle a_i | b_j \rangle | = \frac{1}{\sqrt{d}}, \ \forall \, i, j = 0, 1, \ldots, d-1.$$

[1] Complex inner product space, which is complete.

Mutually Unbiased Bases

- Let $\mathbb{H}^d$ be a finite-dimensional Hilbert space[1].
  State space of any finite quantum system.

- **Definition**:- Two orthonormal bases $\mathcal{A} \equiv \{|a_0\rangle, |a_1\rangle, ..., |a_{d-1}\rangle\}$ and $\mathcal{B} \equiv \{|b_0\rangle, |b_1\rangle, ..., |b_{d-1}\rangle\}$ in $\mathbb{H}^d$ are *mutually unbiased* if

$$|\langle a_i|b_j\rangle| = \frac{1}{\sqrt{d}}, \ \forall\, i, j = 0, 1, \ldots, d-1.$$

- **Complementary Observables:** If a physical system is *prepared* in an eigenstate of basis $\mathcal{A}$ (say $|a_i\rangle$), and *measured* in basis $\mathcal{B}$, the probability of outcome j is:

$$p(j||a_i\rangle) \ := \ |\langle b_j|a_i\rangle|^2 = \frac{1}{d}, \ \forall j.$$

  All outcomes are *equally* probable!

[1] Complex inner product space, which is complete.

Mutually Unbiased Bases : Examples

- Pauli matrices X, Z on $\mathbb{C}^2$:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Eigenbases of Z, X :
$\mathcal{B}_Z = \{|0\rangle, |1\rangle\}$; $\mathcal{B}_X = \left\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\ ,\ |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$

Mutually Unbiased Bases : Examples

- Pauli matrices X, Z on $\mathbb{C}^2$:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

  Eigenbases of Z, X :
  $\mathcal{B}_Z = \{|0\rangle, |1\rangle\}$; $\mathcal{B}_X = \left\{ |+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}} \, , \, |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\}$

- A set of k mutually unbiased bases (MUBs): a set of orthonormal bases $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k\}$ in $\mathbb{H}^d$, where every pair of bases in the set is mutually unbiased.

Mutually Unbiased Bases : Examples

- Pauli matrices X, Z on $\mathbb{C}^2$:

$$Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \qquad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

  Eigenbases of Z, X :
  $\mathcal{B}_Z = \{|0\rangle, |1\rangle\}$; $\mathcal{B}_X = \left\{|+\rangle = \frac{|0\rangle+|1\rangle}{\sqrt{2}}\ ,\ |-\rangle = \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$

- A set of k mutually unbiased bases (MUBs): a set of orthonormal bases $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_k\}$ in $\mathbb{H}^d$, where every pair of bases in the set is mutually unbiased.

- A third MUB in $\mathbb{C}^2$: eigenbasis of Y

$$Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix},\ \mathcal{B}_Y = \left\{\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right\}$$

MUBs : Existence and Constructions

A pair of mutually unbiased bases

- There exist a pair of MUBs in $\mathbb{C}^d$, for *any* dimension d.

A pair of mutually unbiased bases

- There exist a pair of MUBs in $\mathbb{C}^d$, for *any* dimension d.
  - Choose any reference basis – $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ – Computational Basis

A pair of mutually unbiased bases

- There exist a pair of MUBs in $\mathbb{C}^d$, for *any* dimension d.
  - Choose any reference basis – $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ – Computational Basis
  - Discrete quantum Fourier transform:

$$|\tilde{k}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{-i2\pi jk/d} |j\rangle$$

A pair of mutually unbiased bases

- There exist a pair of MUBs in $\mathbb{C}^d$, for *any* dimension d.
  - Choose any reference basis – $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ – Computational Basis
  - Discrete quantum Fourier transform:

$$|\tilde{k}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{-i2\pi jk/d} |j\rangle$$

  - The bases $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ and $\{|\tilde{0}\rangle, |\tilde{1}\rangle, \ldots, |d \tilde{-} 1\rangle\}$ are mutually unbiased:

$$\langle j|\tilde{k}\rangle = \frac{1}{\sqrt{d}} e^{-i2\pi jk/d}, \ \forall \ j, k = 0, 1, \ldots, d-1.$$

A pair of mutually unbiased bases

- There exist a pair of MUBs in $\mathbb{C}^d$, for *any* dimension d.
  - Choose any reference basis – $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ – Computational Basis
  - Discrete quantum Fourier transform:

$$|\tilde{k}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{-i2\pi jk/d} |j\rangle$$

  - The bases $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ and $\{|\tilde{0}\rangle, |\tilde{1}\rangle, \ldots, |d \tilde{-} 1\rangle\}$ are mutually unbiased:

$$\langle j|\tilde{k}\rangle = \frac{1}{\sqrt{d}} e^{-i2\pi jk/d}, \; \forall \; j,k = 0,1,\ldots,d-1.$$

- Define the cyclic operators:

$$\mathcal{X}|j\rangle = |(j+1) \mathrm{mod}\, d\rangle; \; \mathcal{Z}|j\rangle = e^{i2\pi j/d}|j\rangle, \; with \; (\mathcal{X})^d = (\mathcal{Z})^d = \mathbb{I}.$$

Eigenbases of $\mathcal{X}$ and $\mathcal{Z}$ are mutually unbiased!

MUBs in prime dimensions using $\mathcal{X}$ and $\mathcal{Z}$

- Three MUBs in $\mathbb{C}^d$: eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$. (Generalized Pauli operators)

MUBs in prime dimensions using $\mathcal{X}$ and $\mathcal{Z}$

- Three MUBs in $\mathbb{C}^d$: eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$. (Generalized Pauli operators)
- Can we construct more MUBs in $\mathbb{C}^d$ using higher products $(\mathcal{X})^m(\mathcal{Z})^n$? Yes, when d is *prime*!

MUBs in prime dimensions using $\mathcal{X}$ and $\mathcal{Z}$

- Three MUBs in $\mathbb{C}^d$: eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$. (Generalized Pauli operators)
- Can we construct more MUBs in $\mathbb{C}^d$ using higher products $(\mathcal{X})^m(\mathcal{Z})^n$? Yes, when d is *prime*!
- **Lemma 1:** Let $\mathcal{B} = \{|b_0\rangle, |b_1\rangle, \ldots, |b_{d-1}\rangle\}$ be a basis in $\mathbb{C}^d$. If there exists a unitary operator

  $$V : \; V|b_i\rangle = \beta_i |b_{(i+1) \bmod d}\rangle, \; |\beta_i| = 1,$$

  then, the eigenbasis of V is mutually unbiased with the basis $\mathcal{B}$.

MUBs in prime dimensions using $\mathcal{X}$ and $\mathcal{Z}$

- Three MUBs in $\mathbb{C}^d$: eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$. (Generalized Pauli operators)
- Can we construct more MUBs in $\mathbb{C}^d$ using higher products $(\mathcal{X})^m(\mathcal{Z})^n$? Yes, when d is *prime*!
- **Lemma 1:** Let $\mathcal{B} = \{|b_0\rangle, |b_1\rangle, \ldots, |b_{d-1}\rangle\}$ be a basis in $\mathbb{C}^d$. If there exists a unitary operator

$$V \,:\; V|b_i\rangle = \beta_i|b_{(i+1)\bmod d}\rangle,\; |\beta_i| = 1,$$

  then, the eigenbasis of V is mutually unbiased with the basis $\mathcal{B}$.
- *Proof:* Let $V|v_i\rangle = \lambda_i|v_i\rangle$, $i = 0, 1, \ldots, d-1$. ($|\lambda_i| = 1$)

$$\begin{aligned} |\langle v_i|b_j\rangle| &= |\langle v_i|V|b_j\rangle| = |\langle v_i|b_{(j+1)\mathrm{mod} d}\rangle|, \;\forall\, i, j. \\ \Rightarrow |\langle v_i|b_0\rangle| &= |\langle v_i|b_1\rangle| = \ldots = |\langle v_i|b_{d-1}\rangle|, \;\forall i. \\ \Rightarrow |\langle v_i|b_j\rangle|^2 &= \frac{1}{d}, \;\forall i, j. \quad (\sum_j |\langle v_i|b_j\rangle|^2 = 1, \;\forall i.) \end{aligned}$$

$(d+1)$ MUBs in prime dimensions

- Consider the operators $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}, \mathcal{X}(\mathcal{Z})^2, \ldots, \mathcal{X}(\mathcal{Z})^{d-1}\}$ over $\mathbb{C}^d$. They are unitary and cyclic, i.e., $(\mathcal{X}(\mathcal{Z})^k)^d = \mathbb{I}$ for $0 \leq k \leq d-1$.

$(d+1)$ MUBs in prime dimensions

- Consider the operators $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}, \mathcal{X}(\mathcal{Z})^2, \ldots, \mathcal{X}(\mathcal{Z})^{d-1}\}$ over $\mathbb{C}^d$. They are unitary and cyclic, i.e., $(\mathcal{X}(\mathcal{Z})^k)^d = \mathbb{I}$ for $0 \leq k \leq d-1$.

$$\mathcal{X}(\mathcal{Z})^k|j\rangle = (e^{i2\pi j/d})^k|(j+1) \bmod d\rangle.$$

- If $|\psi_t^{(k)}\rangle, t = 0, 1, \ldots, d-1$ denote eigenstates of $\mathcal{X}(\mathcal{Z})^k$, for prime d,

$$\mathcal{X}(\mathcal{Z})^l|\psi_t^{(k)}\rangle = (e^{i2\pi/d})^{t+k-l}|\psi_{t+k-l}^{(k)}\rangle.$$

- Consider the operators $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}, \mathcal{X}(\mathcal{Z})^2, \ldots, \mathcal{X}(\mathcal{Z})^{d-1}\}$ over $\mathbb{C}^d$. They are unitary and cyclic, i.e., $(\mathcal{X}(\mathcal{Z})^k)^d = \mathbb{I}$ for $0 \leq k \leq d-1$.

$$\mathcal{X}(\mathcal{Z})^k|j\rangle = (e^{i2\pi j/d})^k|(j+1)\mathrm{mod}\, d\rangle.$$

- If $|\psi_t^{(k)}\rangle, t = 0, 1, \ldots, d-1$ denote eigenstates of $\mathcal{X}(\mathcal{Z})^k$, for prime d,

$$\mathcal{X}(\mathcal{Z})^l|\psi_t^{(k)}\rangle = (e^{i2\pi/d})^{t+k-l}|\psi_{t+k-l}^{(k)}\rangle.$$

- **Lemma 2 :** When d is prime, the eigenvectors of $\mathcal{X}(\mathcal{Z})^k$ are cyclically shifted under the action of $\mathcal{X}(\mathcal{Z})^l$, for all $l \neq k$ ($0 \leq l, k \leq d-1$).

$(d+1)$ MUBs in prime dimensions

- Consider the operators $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}, \mathcal{X}(\mathcal{Z})^2, \ldots, \mathcal{X}(\mathcal{Z})^{d-1}\}$ over $\mathbb{C}^d$. They are unitary and cyclic, i.e., $(\mathcal{X}(\mathcal{Z})^k)^d = \mathbb{I}$ for $0 \leq k \leq d-1$.

$$\mathcal{X}(\mathcal{Z})^k|j\rangle = (e^{i2\pi j/d})^k|(j+1) \bmod d\rangle.$$

- If $|\psi_t^{(k)}\rangle, t = 0, 1, \ldots, d-1$ denote eigenstates of $\mathcal{X}(\mathcal{Z})^k$, for prime d,

$$\mathcal{X}(\mathcal{Z})^l|\psi_t^{(k)}\rangle = (e^{i2\pi/d})^{t+k-l}|\psi_{t+k-l}^{(k)}\rangle.$$

- **Lemma 2 :** When d is prime, the eigenvectors of $\mathcal{X}(\mathcal{Z})^k$ are cyclically shifted under the action of $\mathcal{X}(\mathcal{Z})^l$, for all $l \neq k$ ($0 \leq l, k \leq d-1$).

- From Lemmas 1 & 2: For any prime d, the set of bases comprising eigenvectors of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}, \mathcal{X}(\mathcal{Z})^2, \ldots, \mathcal{X}(\mathcal{Z})^{d-1}\}$ is a set of $d+1$ MUBs in $\mathbb{C}^d$.

$d+1$ MUBs in prime dimensions: Examples

- In $\mathbb{C}^2$: the eigenbases of $\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}$. Identical to the Pauli eigenbases!

$d+1$ MUBs in prime dimensions: Examples

- In $\mathbb{C}^2$: the eigenbases of $\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}$. Identical to the Pauli eigenbases!
- In $\mathbb{C}^3$: the eigenbases of $\{\mathcal{X}, \mathcal{X}, \mathcal{X}\mathcal{Z}, \mathcal{X}\mathcal{Z}^2\}$ form a set of 4 MUBs.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix},$$

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

$d+1$ MUBs in prime dimensions: Examples

- In $\mathbb{C}^2$: the eigenbases of $\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}$. Identical to the Pauli eigenbases!
- In $\mathbb{C}^3$: the eigenbases of $\{\mathcal{X}, \mathcal{X}, \mathcal{X}\mathcal{Z}, \mathcal{X}\mathcal{Z}^2\}$ form a set of 4 MUBs.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix},$$

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

- Composite dimensions: $d = pq$ $(p, q > 1)$
  - The operators $\{\mathcal{X}(\mathcal{Z})^k\}$ have shorter periods. Eg. $(\mathcal{Z}^p)^q = \mathbb{I}$.

$d+1$ MUBs in prime dimensions: Examples

- In $\mathbb{C}^2$: the eigenbases of $\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}$. Identical to the Pauli eigenbases!
- In $\mathbb{C}^3$: the eigenbases of $\{\mathcal{X}, \mathcal{X}, \mathcal{X}\mathcal{Z}, \mathcal{X}\mathcal{Z}^2\}$ form a set of 4 MUBs.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix},$$

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

- Composite dimensions: $d = pq$ $(p, q > 1)$
  - The operators $\{\mathcal{X}(\mathcal{Z})^k\}$ have shorter periods. Eg. $(\mathcal{Z}^p)^q = \mathbb{I}$.
  - Cyclic shift property no longer holds.

$d + 1$ MUBs in prime dimensions: Examples

- In $\mathbb{C}^2$: the eigenbases of $\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}$. Identical to the Pauli eigenbases!
- In $\mathbb{C}^3$: the eigenbases of $\{\mathcal{X}, \mathcal{X}, \mathcal{X}\mathcal{Z}, \mathcal{X}\mathcal{Z}^2\}$ form a set of 4 MUBs.

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix},$$

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

- Composite dimensions: $d = pq$ $(p, q > 1)$
  - The operators $\{\mathcal{X}(\mathcal{Z})^k\}$ have shorter periods. Eg. $(\mathcal{Z}^p)^q = \mathbb{I}$.
  - Cyclic shift property no longer holds.
  - Numerical evidence shows, we obtain no more than 3 MUBs using this approach: the eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$.

MUBs : Role in Quantum Information Processing

Identifying an unknown quantum state

- MUBs form a *minimal* and *optimal* set of orthogonal measurements for **quantum state tomography**.

Identifying an unknown quantum state

- MUBs form a *minimal* and *optimal* set of orthogonal measurements for **quantum state tomography**.
  - To specify a general density matrix $\rho \in \mathbb{C}^d$: need $d^2 - 1$ real parameters.
  - Measurement in one orthonormal basis $\mathcal{B}^j = \{|\psi_0^j\rangle, \ldots, |\psi_{d-1}^j\rangle\}$ yields only $d-1$ independent probabilities:

$$p(i|\mathcal{B}^j)_\rho := \mathrm{tr}[\rho|\psi_i^j\rangle\langle\psi_i^j|] = \langle\psi_i^j|\rho|\psi_i^j\rangle, \; i = 0, \ldots, d-1.$$

Identifying an unknown quantum state

- MUBs form a *minimal* and *optimal* set of orthogonal measurements for **quantum state tomography**.
  - To specify a general density matrix $\rho \in \mathbb{C}^d$: need $d^2 - 1$ real parameters.
  - Measurement in one orthonormal basis $\mathcal{B}^j = \{|\psi_0^j\rangle, \ldots, |\psi_{d-1}^j\rangle\}$ yields only $d-1$ independent probabilities:

$$p(i|\mathcal{B}^j)_\rho := \mathrm{tr}[\rho|\psi_i^j\rangle\langle\psi_i^j|] = \langle\psi_i^j|\rho|\psi_i^j\rangle, \ i = 0, \ldots, d-1.$$

$\Rightarrow$ Need $d+1$ *distinct* basis sets to obtain $d^2 - 1$ independent probabilities.

Identifying an unknown quantum state

- MUBs form a *minimal* and *optimal* set of orthogonal measurements for **quantum state tomography**.
  - To specify a general density matrix $\rho \in \mathbb{C}^d$: need $d^2 - 1$ real parameters.
  - Measurement in one orthonormal basis $\mathcal{B}^j = \{|\psi_0^j\rangle, \ldots, |\psi_{d-1}^j\rangle\}$ yields only $d - 1$ independent probabilities:

$$p(i|\mathcal{B}^j)_\rho := \mathrm{tr}[\rho|\psi_i^j\rangle\langle\psi_i^j|] = \langle\psi_i^j|\rho|\psi_i^j\rangle,\ i = 0, \ldots, d-1.$$

  $\Rightarrow$ Need $d + 1$ *distinct* basis sets to obtain $d^2 - 1$ independent probabilities.

- Mutual unbiasedness implies that statistical errors are minimized when measuring finite samples.

Incompatibility and Complementarity - I

- MUBs are the measurement bases that are most *incompatible*, as quantified by **entropic uncertainty relations**.

Incompatibility and Complementarity - I

- MUBs are the measurement bases that are most *incompatible*, as quantified by **entropic uncertainty relations**.
- When measuring state $|\phi\rangle \in \mathbb{C}^d$ in the measurement basis $\mathcal{B}^j$, probability of the i^{th} outcome is

$$p(i\,|\,\mathcal{B}^j)_{|\phi\rangle} := |\langle\psi_i^j|\phi\rangle|^2.$$

Incompatibility and Complementarity - I

- MUBs are the measurement bases that are most *incompatible*, as quantified by **entropic uncertainty relations**.
- When measuring state $|\phi\rangle \in \mathbb{C}^d$ in the measurement basis $\mathcal{B}^j$, probability of the i^{th} outcome is
$$p(i\,|\,\mathcal{B}^j)_{|\phi\rangle} := |\langle\psi_i^j|\phi\rangle|^2.$$
- Let $H(\mathcal{B}^j||\phi\rangle)$ be the entropy of the distribution $p(i\,|\,\mathcal{B}^j)_{|\phi\rangle}$.
An entropic *uncertainty* relation (EUR) for the set of bases $\{\mathcal{B}^1, \ldots, \mathcal{B}^L\}$ is:
$$\frac{1}{L}\sum_{j=1}^{L} H(\mathcal{B}^j||\phi\rangle) \geq c_{\mathcal{B}^1,\ldots,\mathcal{B}^L},\ \forall|\phi\rangle$$

Incompatibility and Complementarity - I

- MUBs are the measurement bases that are most *incompatible*, as quantified by **entropic uncertainty relations**.
- When measuring state $|\phi\rangle \in \mathbb{C}^d$ in the measurement basis $\mathcal{B}^j$, probability of the i^{th} outcome is
$$p(i \,|\, \mathcal{B}^j)_{|\phi\rangle} := |\langle\psi_i^j|\phi\rangle|^2.$$
- Let $H(\mathcal{B}^j||\phi\rangle)$ be the entropy of the distribution $p(i \,|\, \mathcal{B}^j)_{|\phi\rangle}$.
An entropic *uncertainty* relation (EUR) for the set of bases $\{\mathcal{B}^1, \ldots, \mathcal{B}^L\}$ is:
$$\frac{1}{L}\sum_{j=1}^{L} H(\mathcal{B}^j||\phi\rangle) \geq c_{\mathcal{B}^1,\ldots,\mathcal{B}^L},\ \forall|\phi\rangle$$
- Lower bound $c_{\mathcal{B}^1,\ldots,\mathcal{B}^L}$ captures the mutual incompatibility of the set $\{\mathcal{B}^1, \ldots, \mathcal{B}^L\}$.

- **Example :** Massen and Uffink bound :-
  For measurement bases $\mathcal{A} = \{|a_1\rangle, ..., |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, ..., |b_d\rangle\}$ in $\mathbb{C}^d$,

  $$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq -\log c(\mathcal{A},\mathcal{B})$$

  where $c(\mathcal{A},\mathcal{B}) := \max|\langle a|b\rangle|, \; \forall\, |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}$.

Incompatibility and Complementarity - II

- **Example :** Massen and Uffink bound :-
  For measurement bases $\mathcal{A} = \{|a_1\rangle, ..., |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, ..., |b_d\rangle\}$ in $\mathbb{C}^d$,

$$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq -\log c(\mathcal{A}, \mathcal{B})$$

  where $c(\mathcal{A}, \mathcal{B}) := \max |\langle a|b\rangle|, \ \forall \ |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}$.

- Maximum value of RHS is attained when $|\langle a|b\rangle| = \frac{1}{\sqrt{d}}, \ \forall |a\rangle, |b\rangle$: Strongest possible uncertainty relation is satisfied when the bases are *mutually unbiased*.

- **Example :** Massen and Uffink bound :-
  For measurement bases $\mathcal{A} = \{|a_1\rangle, ..., |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, ..., |b_d\rangle\}$ in $\mathbb{C}^d$,

  $$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq -\log c(\mathcal{A}, \mathcal{B})$$

  where $c(\mathcal{A}, \mathcal{B}) := \max |\langle a|b\rangle|, \ \forall \ |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}$.

- Maximum value of RHS is attained when $|\langle a|b\rangle| = \frac{1}{\sqrt{d}}, \ \forall |a\rangle, |b\rangle$: Strongest possible uncertainty relation is satisfied when the bases are *mutually unbiased*.

- For measurements involving more than 2 bases, to obtain strong uncertainty relations, the bases must be mutually unbiased -
  MUBs are a *necessary* condition to achieve maximal incompatibility with multiple bases.

- **Example :** Massen and Uffink bound :-
  For measurement bases $\mathcal{A} = \{|a_1\rangle, ..., |a_d\rangle\}$ and $\mathcal{B} = \{|b_1\rangle, ..., |b_d\rangle\}$ in $\mathbb{C}^d$,

$$\frac{1}{2}\left(H(\mathcal{A}||\psi\rangle) + H(\mathcal{B}||\psi\rangle)\right) \geq -\log c(\mathcal{A}, \mathcal{B})$$

  where $c(\mathcal{A}, \mathcal{B}) := \max|\langle a|b\rangle|, \ \forall\ |a\rangle \in \mathcal{A}, |b\rangle \in \mathcal{B}$.

- Maximum value of RHS is attained when $|\langle a|b\rangle| = \frac{1}{\sqrt{d}}, \ \forall |a\rangle, |b\rangle$: Strongest possible uncertainty relation is satisfied when the bases are *mutually unbiased*.

- For measurements involving more than 2 bases, to obtain strong uncertainty relations, the bases must be mutually unbiased -
  MUBs are a *necessary* condition to achieve maximal incompatibility with multiple bases.

- Security of quantum cryptographic protocols relies on this property of MUBs.

- **Quantum Key Distribution –**
  The participants (A and B) want to generate a *secret key* about which an eavesdropper (E) cannot obtain significant information.

- **Quantum Key Distribution –**
  The participants (A and B) want to generate a *secret key* about which an eavesdropper (E) cannot obtain significant information.

- **Example** of a protocol using states in $\mathbb{C}^2$ (qubits):

- **Quantum Key Distribution –**
  The participants (A and B) want to generate a *secret key* about which an eavesdropper (E) cannot obtain significant information.

- **Example** of a protocol using states in $\mathbb{C}^2$ (qubits):
  - **Key:** n-bit string $X = x_1 x_2 \ldots x_n$, $x_i \in \{0, 1\}$.

- **Quantum Key Distribution –**
  The participants (A and B) want to generate a *secret key* about which an eavesdropper (E) cannot obtain significant information.

- **Example** of a protocol using states in $\mathbb{C}^2$ (qubits):
  - **Key:** n-bit string $X = x_1 x_2 \ldots x_n$, $x_i \in \{0, 1\}$.
  - **A** *encodes* each bit x_i in an eigenstate of one a pair of complementary bases, $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ in $\mathbb{C}^2$:

$$x_i \rightarrow |x_i\rangle \text{ or } x_i \rightarrow (|x_i\rangle + |\bar{x}_i\rangle)/\sqrt{2}.$$

  Then, sends the encoded state to **B**.

- **Quantum Key Distribution –**
  The participants (A and B) want to generate a *secret key* about which an eavesdropper (E) cannot obtain significant information.

- **Example** of a protocol using states in $\mathbb{C}^2$ (qubits):

  - **Key:** n-bit string $X = x_1 x_2 \ldots x_n$, $x_i \in \{0, 1\}$.

  - **A** *encodes* each bit x_i in an eigenstate of one a pair of complementary bases, $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ in $\mathbb{C}^2$:

    $$x_i \to |x_i\rangle \text{ or } x_i \to (|x_i\rangle + |\bar{x}_i\rangle)/\sqrt{2}.$$

    Then, sends the encoded state to **B**.

  - **B** has access to the basis information, **E** does not. By guessing randomly, **E** can typically access only *half* the key.

MUBs in Quantum Cryptography

- **Quantum Key Distribution –**
  The participants (A and B) want to generate a *secret key* about which an eavesdropper (E) cannot obtain significant information.

- **Example** of a protocol using states in $\mathbb{C}^2$ (qubits):

  - **Key:** n-bit string $X = x_1 x_2 \ldots x_n$, $x_i \in \{0, 1\}$.

  - **A** *encodes* each bit x_i in an eigenstate of one a pair of complementary bases, $\{|0\rangle, |1\rangle\}$ or $\{|+\rangle, |-\rangle\}$ in $\mathbb{C}^2$:

    $$x_i \to |x_i\rangle \text{ or } x_i \to (|x_i\rangle + |\bar{x}_i\rangle)/\sqrt{2}.$$

    Then, sends the encoded state to **B**.

  - **B** has access to the basis information, **E** does not. By guessing randomly, **E** can typically access only *half* the key.

- Amount of information **E** has about the *key* is a measure of incompatibility of the set of bases used by **A**.

The case of prime-power dimensions

The Weyl-Heisenberg Group

- **Weyl-Heisenberg group** $\mathcal{H}_d$ **:** Finite non-abelian group generated by the cyclic shift operator $\mathcal{X}$ and the phase operator $\mathcal{Z}$. They satisfy the Weyl commutation rule:

$$\mathcal{X}\mathcal{Z} = e^{i2\pi/d}\mathcal{Z}\mathcal{X}.$$

The Weyl-Heisenberg Group

- **Weyl-Heisenberg group** $\mathcal{H}_d$ **:** Finite non-abelian group generated by the cyclic shift operator $\mathcal{X}$ and the phase operator $\mathcal{Z}$. They satisfy the Weyl commutation rule:

$$\mathcal{X}\mathcal{Z} = e^{i2\pi/d}\mathcal{Z}\mathcal{X}.$$

- Each element of $\mathcal{H}_d$ can be uniquely represented (upto a phase) as $U_{m,n} = (\mathcal{X})^m(\mathcal{Z})^n$, $0 \leq m, n \leq d-1$. $U_{m',n'}$ and $U_{m,n}$ commute iff $mn' - nm' = 0 \bmod d$.

The Weyl-Heisenberg Group

- **Weyl-Heisenberg group** $\mathcal{H}_d$ **:** Finite non-abelian group generated by the cyclic shift operator $\mathcal{X}$ and the phase operator $\mathcal{Z}$. They satisfy the Weyl commutation rule:

$$\mathcal{X}\mathcal{Z} = e^{i2\pi/d}\mathcal{Z}\mathcal{X}.$$

- Each element of $\mathcal{H}_d$ can be uniquely represented (upto a phase) as $U_{m,n} = (\mathcal{X})^m(\mathcal{Z})^n$, $0 \leq m, n \leq d-1$. $U_{m',n'}$ and $U_{m,n}$ commute iff $mn' - nm' = 0 \bmod d$.

- $\mathcal{H}_d$ is a group of unitary operators, closed under multiplication:

$$U_{m,n}U_{m',n'} = U_{(m+m')\bmod d,(n+n')\bmod d}.$$

The Weyl-Heisenberg Group

- **Weyl-Heisenberg group** $\mathcal{H}_d$ **:** Finite non-abelian group generated by the cyclic shift operator $\mathcal{X}$ and the phase operator $\mathcal{Z}$. They satisfy the Weyl commutation rule:

$$\mathcal{X}\mathcal{Z} = e^{i2\pi/d}\mathcal{Z}\mathcal{X}.$$

- Each element of $\mathcal{H}_d$ can be uniquely represented (upto a phase) as $U_{m,n} = (\mathcal{X})^m(\mathcal{Z})^n$, $0 \leq m, n \leq d-1$. $U_{m',n'}$ and $U_{m,n}$ commute iff $mn' - nm' = 0 \bmod d$.

- $\mathcal{H}_d$ is a group of unitary operators, closed under multiplication:

$$U_{m,n}U_{m',n'} = U_{(m+m')\bmod d,(n+n')\bmod d}.$$

- The elements of $\mathcal{H}_d$ are pairwise trace orthogonal:

$$\mathrm{tr}[(\mathcal{X}^m\mathcal{Z}^n)(\mathcal{X}^{m'}\mathcal{Z}^{n'})] = \delta_{mm'}\delta_{nn'}.$$

  The operators $\{U_{m,n}\}$ form a ON basis for the space of $d \times d$ complex matrices $\mathbb{M}_d(\mathbb{C})$.

- There are at most d pairwise orthogonal commuting unitary matrices in $\mathbb{M}_d(\mathbb{C})$.

Unitary Operator Basis and MUBs - I

- There are at most d pairwise orthogonal commuting unitary matrices in $\mathbb{M}_d(\mathbb{C})$.
- Let $\mathcal{S}$ be a set of d^2 mutually orthogonal unitary operators acting on $\mathbb{C}^d$ (unitary basis for the space of $d \times d$ matrices).

Unitary Operator Basis and MUBs - I

- There are at most d pairwise orthogonal commuting unitary matrices in $\mathbb{M}_d(\mathbb{C})$.
- Let $\mathcal{S}$ be a set of d^2 mutually orthogonal unitary operators acting on $\mathbb{C}^d$ (unitary basis for the space of $d \times d$ matrices).
- Suppose there exists a partitioning of $\mathcal{S} \setminus \{\mathbb{I}\}$ into Mutually Disjoint Maximal Commuting Classes: $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ where, $\mathcal{C}_j \subset \mathcal{S} \setminus \{\mathbb{I}\}$ of size $|\mathcal{C}_j| = d - 1$ are such that

Unitary Operator Basis and MUBs - I

- There are at most d pairwise orthogonal commuting unitary matrices in $\mathbb{M}_d(\mathbb{C})$.
- Let $\mathcal{S}$ be a set of d^2 mutually orthogonal unitary operators acting on $\mathbb{C}^d$ (unitary basis for the space of $d \times d$ matrices).
- Suppose there exists a partitioning of $\mathcal{S} \setminus \{\mathbb{I}\}$ into Mutually Disjoint Maximal Commuting Classes: $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ where, $\mathcal{C}_j \subset \mathcal{S} \setminus \{\mathbb{I}\}$ of size $|\mathcal{C}_j| = d - 1$ are such that
  - (a) the elements of $\mathcal{C}_j$ commute for all $1 \leq j \leq L$, and,
  - (b) $\mathcal{C}_j \cap \mathcal{C}_k = \emptyset$ for all $j \neq k$.

Unitary Operator Basis and MUBs - I

- There are at most d pairwise orthogonal commuting unitary matrices in $\mathbb{M}_d(\mathbb{C})$.
- Let $\mathcal{S}$ be a set of d^2 mutually orthogonal unitary operators acting on $\mathbb{C}^d$ (unitary basis for the space of $d \times d$ matrices).
- Suppose there exists a partitioning of $\mathcal{S} \setminus \{\mathbb{I}\}$ into Mutually Disjoint Maximal Commuting Classes: $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ where, $\mathcal{C}_j \subset \mathcal{S} \setminus \{\mathbb{I}\}$ of size $|\mathcal{C}_j| = d - 1$ are such that
  - (a) the elements of $\mathcal{C}_j$ commute for all $1 \leq j \leq L$, and,
  - (b) $\mathcal{C}_j \cap \mathcal{C}_k = \emptyset$ for all $j \neq k$.
- **Theorem 1:** The common eigenbases of each of $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ form a set of L mutually unbiased bases.

Proof of Theorem 1

- Consider a maximal commuting class $\mathcal{C}_j$ $(1 \leq j \leq d+1)$:

$$\mathcal{C}_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\},\ (U_{j,0} = \mathbb{I})$$

Let $\mathcal{B}^j = \{|\psi_i^j\rangle,\ i = 0, 1, \ldots, d-1\}$ be the associated basis.

Proof of Theorem 1

- Consider a maximal commuting class $\mathcal{C}_j$ $(1 \leq j \leq d+1)$:

$$\mathcal{C}_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\}, \ (U_{j,0} = \mathbb{I})$$

  Let $\mathcal{B}^j = \{|\psi_i^j\rangle, \ i = 0, 1, \ldots, d-1\}$ be the associated basis.

- Orthogonality of the unitaries implies, for every pair $j \neq k$,

$$\mathrm{tr}[U_{j,s}^{\dagger} U_{k,t}] = d\,\delta_{s,0}\delta_{t,0}, \ \forall 0 \leq s, t \leq d-1.$$

Proof of Theorem 1

- Consider a maximal commuting class $\mathcal{C}_j$ $(1 \leq j \leq d+1)$:

$$\mathcal{C}_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\},\ (U_{j,0} = \mathbb{I})$$

  Let $\mathcal{B}^j = \{|\psi_i^j\rangle,\ i = 0, 1, \ldots, d-1\}$ be the associated basis.

- Orthogonality of the unitaries implies, for every pair $j \neq k$,

$$\mathrm{tr}[U_{j,s}^{\dagger} U_{k,t}] = d\,\delta_{s,0}\delta_{t,0},\ \forall 0 \leq s, t \leq d-1.$$

  Since $U_{j,s} = \sum_{i=0}^{d-1} \lambda_i^{j,s} |\psi_i^j\rangle\langle\psi_i^j|$, this implies,

$$\sum_{i=0}^{d-1}\sum_{l=0}^{d-1} \lambda_i^{j,s}\lambda_l^{k,t} |\langle\psi_i^j|\psi_l^k\rangle|^2 = d\,\delta_{s,0}\,\delta_{t,0},\ \forall 0 \leq s, t \leq d-1.$$

Proof of Theorem 1

- Consider a maximal commuting class $\mathcal{C}_j$ $(1 \leq j \leq d+1)$:

$$\mathcal{C}_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\}, \ (U_{j,0} = \mathbb{I})$$

Let $\mathcal{B}^j = \{|\psi_i^j\rangle, \ i = 0, 1, \ldots, d-1\}$ be the associated basis.

- Orthogonality of the unitaries implies, for every pair $j \neq k$,

$$\mathrm{tr}[U_{j,s}^\dagger U_{k,t}] = d\,\delta_{s,0}\delta_{t,0}, \ \forall 0 \leq s, t \leq d-1.$$

Since $U_{j,s} = \sum_{i=0}^{d-1} \lambda_i^{j,s} |\psi_i^j\rangle\langle\psi_i^j|$, this implies,

$$\sum_{i=0}^{d-1}\sum_{l=0}^{d-1} \lambda_i^{j,s}\lambda_l^{k,t} |\langle\psi_i^j|\psi_l^k\rangle|^2 = d\,\delta_{s,0}\,\delta_{t,0}, \ \forall 0 \leq s, t \leq d-1.$$

- Inverting this system of equations, for every $j \neq k$,

$$|\langle\psi_i^j|\psi_l^k\rangle|^2 = \frac{1}{d}, \forall\ 0 \leq i, l \leq d.$$

Proof of Theorem 1

- Consider a maximal commuting class $\mathcal{C}_j$ $(1 \leq j \leq d+1)$:

$$\mathcal{C}_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\}, \; (U_{j,0} = \mathbb{I})$$

Let $\mathcal{B}^j = \{|\psi_i^j\rangle, \; i = 0, 1, \ldots, d-1\}$ be the associated basis.

- Orthogonality of the unitaries implies, for every pair $j \neq k$,

$$\mathrm{tr}[U_{j,s}^\dagger U_{k,t}] = d\,\delta_{s,0}\delta_{t,0}, \; \forall 0 \leq s, t \leq d-1.$$

Since $U_{j,s} = \sum_{i=0}^{d-1} \lambda_i^{j,s} |\psi_i^j\rangle\langle\psi_i^j|$, this implies,

$$\sum_{i=0}^{d-1}\sum_{l=0}^{d-1} \lambda_i^{j,s}\lambda_l^{k,t}|\langle\psi_i^j|\psi_l^k\rangle|^2 = d\,\delta_{s,0}\,\delta_{t,0}, \; \forall 0 \leq s, t \leq d-1.$$

- Inverting this system of equations, for every $j \neq k$,

$$|\langle\psi_i^j|\psi_l^k\rangle|^2 = \frac{1}{d}, \forall\; 0 \leq i, l \leq d.$$

$\{\mathcal{B}^1, \mathcal{B}^2, \ldots, \mathcal{B}^L\}$ is thus a set of L MUBs in $\mathbb{C}^d$.

Unitary Operator Bases and MUBs - II

- **Conversely**, let $\{\mathcal{B}^1, \mathcal{B}^2, \ldots, \mathcal{B}^L\}$ be a set of L MUBs in $\mathbb{C}^d$. Then, there exists a set of $L(d-1)$ mutually orthogonal unitary operators that can be partitioned into L mutually disjoint maximal commuting classes.

Unitary Operator Bases and MUBs - II

- **Conversely**, let $\{\mathcal{B}^1, \mathcal{B}^2, \ldots, \mathcal{B}^L\}$ be a set of L MUBs in $\mathbb{C}^d$. Then, there exists a set of $L(d-1)$ mutually orthogonal unitary operators that can be partitioned into L mutually disjoint maximal commuting classes.
- *Proof:* Let $\mathcal{B}^j \equiv \{|\psi_0^j\rangle, |\psi_1^j, \ldots, |\psi_{d-1}^j\rangle\}$. Then,

$$|\langle\psi_i^j|\psi_l^k\rangle|^2 = \frac{1}{d}, \;\forall\; j \neq k, \;\forall\; 0 \leq i, l \leq d-1.$$

Unitary Operator Bases and MUBs - II

- **Conversely**, let $\{\mathcal{B}^1, \mathcal{B}^2, \ldots, \mathcal{B}^L\}$ be a set of L MUBs in $\mathbb{C}^d$. Then, there exists a set of $L(d-1)$ mutually orthogonal unitary operators that can be partitioned into L mutually disjoint maximal commuting classes.
- *Proof:* Let $\mathcal{B}^j \equiv \{|\psi_0^j\rangle, |\psi_1^j, \ldots, |\psi_{d-1}^j\rangle\}$. Then,

$$|\langle\psi_i^j|\psi_l^k\rangle|^2 = \frac{1}{d}, \ \forall\, j \neq k, \ \forall\, 0 \leq i, l \leq d-1.$$

- Construct the unitaries

$$U_{j,s} = \sum_{l=0}^{d-1} e^{2\pi i s l/d} |\psi_l^j\rangle\langle\psi_l^j|, \ \forall\, 0 \leq s \leq d-1, \ 1 \leq j \leq L.$$

Clearly, $U_{j,s}$ and $U_{j,t}$ commute for every j.

Unitary Operator Bases and MUBs - II

- **Conversely**, let $\{\mathcal{B}^1, \mathcal{B}^2, \ldots, \mathcal{B}^L\}$ be a set of L MUBs in $\mathbb{C}^d$. Then, there exists a set of $L(d-1)$ mutually orthogonal unitary operators that can be partitioned into L mutually disjoint maximal commuting classes.
- *Proof:* Let $\mathcal{B}^j \equiv \{|\psi_0^j\rangle, |\psi_1^j, \ldots, |\psi_{d-1}^j\rangle\}$. Then,
$$|\langle\psi_i^j|\psi_l^k\rangle|^2 = \frac{1}{d}, \; \forall \; j \neq k, \; \forall \; 0 \leq i, l \leq d-1.$$
- Construct the unitaries
$$U_{j,s} = \sum_{l=0}^{d-1} e^{2\pi i s l/d} |\psi_l^j\rangle\langle\psi_l^j|, \; \forall \; 0 \leq s \leq d-1, \; 1 \leq j \leq L.$$
Clearly, $U_{j,s}$ and $U_{j,t}$ commute for every j.
- These unitaries are indeed mutually orthogonal:
$$\mathrm{tr}[U_{j,s}^\dagger U_{k,t}] \quad = \quad \sum_{l,m=0}^{d-1} e^{2\pi i(tl - sm)/d} |\langle\psi_l^j|\psi_m^k\rangle|^2$$
$$\Rightarrow \mathrm{tr}[U_{j,s}^\dagger U_{j,t}] = d\,\delta_{s,t} \quad , \quad \mathrm{tr}[U_{j,s}^\dagger U_{k,t}] = 0, j \neq k, \; (s,t) \neq (0,0).$$

Unitary operator basis and MUBs - III

- **Corollary :** The cardinality of a set of MUBs in $\mathbb{C}^d$ cannot be more than $d+1$.
  Let $N(d)$ be the *maximal* number of MUBs in d-dimensions, then, $N(d) \leq d+1$.

Unitary operator basis and MUBs - III

- **Corollary :** The cardinality of a set of MUBs in $\mathbb{C}^d$ cannot be more than $d+1$.
  Let $N(d)$ be the *maximal* number of MUBs in d-dimensions, then, $N(d) \leq d+1$.
- Example: In $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$, consider the unitary basis of Pauli operators $\{U_i \otimes U_j\}$, where, $U_i \in \{\mathbb{I}, X, Y, Z\}$.

Unitary operator basis and MUBs - III

- **Corollary :** The cardinality of a set of MUBs in $\mathbb{C}^d$ cannot be more than $d+1$.
  Let $N(d)$ be the *maximal* number of MUBs in d-dimensions, then, $N(d) \leq d+1$.

- Example: In $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$, consider the unitary basis of Pauli operators $\{U_i \otimes U_j\}$, where, $U_i \in \{\mathbb{I}, X, Y, Z\}$.

$$\begin{aligned}
\mathcal{S}_1 &= \{Y \otimes \mathbb{I}, \mathbb{I} \otimes Y, Y \otimes Y\} \\
\mathcal{S}_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\} \\
\mathcal{S}_3 &= \{Z \otimes \mathbb{I}, \mathbb{I} \otimes Z, Z \otimes Z\} \\
\mathcal{S}_4 &= \{X \otimes \mathbb{I}, \mathbb{I} \otimes X, X \otimes X\} \\
\mathcal{S}_5 &= \{X \otimes Z, Z \otimes Y, Y \otimes X\}.
\end{aligned}$$

  Common eigenbases of $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_5$ form a set of 5 MUBs in $\mathbb{C}^4$.

Unitary operator basis and MUBs - III

- **Corollary :** The cardinality of a set of MUBs in $\mathbb{C}^d$ cannot be more than $d+1$.
  Let $N(d)$ be the *maximal* number of MUBs in d-dimensions, then, $N(d) \leq d+1$.

- Example: In $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$, consider the unitary basis of Pauli operators $\{U_i \otimes U_j\}$, where, $U_i \in \{\mathbb{I}, X, Y, Z\}$.

$$\begin{aligned}
\mathcal{S}_1 &= \{Y \otimes \mathbb{I}, \mathbb{I} \otimes Y, Y \otimes Y\} \\
\mathcal{S}_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\} \\
\mathcal{S}_3 &= \{Z \otimes \mathbb{I}, \mathbb{I} \otimes Z, Z \otimes Z\} \\
\mathcal{S}_4 &= \{X \otimes \mathbb{I}, \mathbb{I} \otimes X, X \otimes X\} \\
\mathcal{S}_5 &= \{X \otimes Z, Z \otimes Y, Y \otimes X\}.
\end{aligned}$$

  Common eigenbases of $\mathcal{S}_1, \mathcal{S}_2, \ldots, \mathcal{S}_5$ form a set of 5 MUBs in $\mathbb{C}^4$.

- This partitioning is not unique!

MUBs in prime-power dimensions

- In *prime-power dimensions* $d = p^n$, explicit construction of $N(d) = d + 1$ MUBs is known using the operators of the Weyl-Heisenberg group.

MUBs in prime-power dimensions

- In *prime-power dimensions* $d = p^n$, explicit construction of $N(d) = d + 1$ MUBs is known using the operators of the Weyl-Heisenberg group.

- Decompose the Hilbert space as $\mathbb{C}^d = \underbrace{\mathbb{C}^p \otimes \mathbb{C}^p \ldots \otimes \mathbb{C}^p}_{n\,\text{times}}$.

  Consider tensor products of $\mathcal{X}$ and $\mathcal{Z}$ acting on $\mathbb{C}^p$.

MUBs in prime-power dimensions

- In *prime-power dimensions* $d = p^n$, explicit construction of $N(d) = d + 1$ MUBs is known using the operators of the Weyl-Heisenberg group.
- Decompose the Hilbert space as $\mathbb{C}^d = \underbrace{\mathbb{C}^p \otimes \mathbb{C}^p \ldots \otimes \mathbb{C}^p}_{n\,\text{times}}$.

  Consider tensor products of $\mathcal{X}$ and $\mathcal{Z}$ acting on $\mathbb{C}^p$.
- Unitary basis of operators: $\mathcal{S} = \{U_1 \otimes U_2 \otimes \ldots \otimes U_n\}$, where, $U_i = (\mathcal{X})^{k_i}(\mathcal{Z})^{l_i}$, $0 \leq k_i, l_i \leq p - 1$.

MUBs in prime-power dimensions

- In *prime-power dimensions* $d = p^n$, explicit construction of $N(d) = d + 1$ MUBs is known using the operators of the Weyl-Heisenberg group.
- Decompose the Hilbert space as $\mathbb{C}^d = \underbrace{\mathbb{C}^p \otimes \mathbb{C}^p \ldots \otimes \mathbb{C}^p}_{n\,\text{times}}$.

  Consider tensor products of $\mathcal{X}$ and $\mathcal{Z}$ acting on $\mathbb{C}^p$.
- Unitary basis of operators: $\mathcal{S} = \{U_1 \otimes U_2 \otimes \ldots \otimes U_n\}$, where, $U_i = (\mathcal{X})^{k_i}(\mathcal{Z})^{l_i}$, $0 \leq k_i, l_i \leq p-1$.
- Each operator is represented by a vector of length $2n$ over the finite field $\mathbb{F}_p$: $(k_1, \ldots, k_n | l_1, \ldots, l_n)$.

MUBs in prime-power dimensions

- In *prime-power dimensions* $d = p^n$, explicit construction of $N(d) = d + 1$ MUBs is known using the operators of the Weyl-Heisenberg group.

- Decompose the Hilbert space as $\mathbb{C}^d = \underbrace{\mathbb{C}^p \otimes \mathbb{C}^p \ldots \otimes \mathbb{C}^p}_{n \text{ times}}$.

  Consider tensor products of $\mathcal{X}$ and $\mathcal{Z}$ acting on $\mathbb{C}^p$.

- Unitary basis of operators: $\mathcal{S} = \{U_1 \otimes U_2 \otimes \ldots \otimes U_n\}$, where, $U_i = (\mathcal{X})^{k_i}(\mathcal{Z})^{l_i}$, $0 \leq k_i, l_i \leq p - 1$.

- Each operator is represented by a vector of length $2n$ over the finite field $\mathbb{F}_p$: $(k_1, \ldots, k_n | l_1, \ldots, l_n)$.

- There exists a partitioning of $\mathcal{S}$ into $d + 1$ mutually disjoint maximal commuting classes $\mathcal{C}_i$.

  A partitioning of d^2 elements of the Weyl-Heisenberg group into $d + 1$ Abelian subgroups.

Composite Dimensions: Unextendible MUBs

MUBs in composite dimensions

- In composite dimensions, smaller sets of MUBs have been constructed.

MUBs in composite dimensions

- In composite dimensions, smaller sets of MUBs have been constructed.
- Using Mutually Orthogonal Latin Squares in square dimensions ($d = s^2$), we can obtain $\sqrt{d} + 1$ MUBs.

MUBs in composite dimensions

- In composite dimensions, smaller sets of MUBs have been constructed.
- Using Mutually Orthogonal Latin Squares in square dimensions ($d = s^2$), we can obtain $\sqrt{d} + 1$ MUBs.
- **Lower bound** on $N(d)$ for any $d = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$:

$$N(d) \geq \min \{N(p_1^{r_1}), N(p_2^{r_2}), \ldots, N(p_m^{r_m})\}$$

MUBs in composite dimensions

- In composite dimensions, smaller sets of MUBs have been constructed.
- Using Mutually Orthogonal Latin Squares in square dimensions ($d = s^2$), we can obtain $\sqrt{d} + 1$ MUBs.
- **Lower bound** on $N(d)$ for any $d = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$:

$$N(d) \geq \min \{N(p_1^{r_1}), N(p_2^{r_2}), \ldots, N(p_m^{r_m})\}$$

Proof: Let $L = \min_m N(p_m^{r_m})$. Choose L MUBs $\{\mathcal{B}^{1,m}, \mathcal{B}^{2,m}, \ldots, \mathcal{B}^{L,m}\}$ for each $\mathbb{C}^{p_m^{r_m}}$. Then,

$$\{\mathcal{B}^{j,1} \otimes \ldots \otimes \mathcal{B}^{j,m} : j = 1, \ldots, L\}$$

is a set of L MUBs in $\mathbb{C}^d$.

MUBs in composite dimensions

- In composite dimensions, smaller sets of MUBs have been constructed.
- Using Mutually Orthogonal Latin Squares in square dimensions ($d = s^2$), we can obtain $\sqrt{d} + 1$ MUBs.
- **Lower bound** on $N(d)$ for any $d = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$:

$$N(d) \geq \min \{N(p_1^{r_1}), N(p_2^{r_2}), \ldots, N(p_m^{r_m})\}$$

Proof: Let $L = \min_m N(p_m^{r_m})$. Choose L MUBs $\{\mathcal{B}^{1,m}, \mathcal{B}^{2,m}, \ldots, \mathcal{B}^{L,m}\}$ for each $\mathbb{C}^{p_m^{r_m}}$. Then,

$$\{\mathcal{B}^{j,1} \otimes \ldots \otimes \mathcal{B}^{j,m} : j = 1, \ldots, L\}$$

is a set of L MUBs in $\mathbb{C}^d$.

- Simple consequence: $N(d) \geq 3$ for any $d \geq 2$. Eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$.

MUBs in composite dimensions

- In composite dimensions, smaller sets of MUBs have been constructed.
- Using Mutually Orthogonal Latin Squares in square dimensions ($d = s^2$), we can obtain $\sqrt{d} + 1$ MUBs.
- **Lower bound** on $N(d)$ for any $d = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$:

$$N(d) \geq \min \{N(p_1^{r_1}), N(p_2^{r_2}), \ldots, N(p_m^{r_m})\}$$

Proof: Let $L = \min_m N(p_m^{r_m})$. Choose L MUBs $\{\mathcal{B}^{1,m}, \mathcal{B}^{2,m}, \ldots, \mathcal{B}^{L,m}\}$ for each $\mathbb{C}^{p_m^{r_m}}$. Then,

$$\{\mathcal{B}^{j,1} \otimes \ldots \otimes \mathcal{B}^{j,m} : j = 1, \ldots, L\}$$

is a set of L MUBs in $\mathbb{C}^d$.

- Simple consequence: $N(d) \geq 3$ for any $d \geq 2$. Eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$.
- Question of whether a maximal set of MUBs exists in non-prime-power dimensions still remains unresolved.

Maximal set of MUBs in $d = 6$?

- Triples of MUBs have been constructed using:
  - Abelian subgroups of the Weyl-Heisenberg group

Maximal set of MUBs in $d = 6$?

- Triples of MUBs have been constructed using:
  - Abelian subgroups of the Weyl-Heisenberg group
  - Mutually unbiased Hadamard matrices

Maximal set of MUBs in $d = 6$?

- Triples of MUBs have been constructed using:
  - Abelian subgroups of the Weyl-Heisenberg group
  - Mutually unbiased Hadamard matrices
- Complex *Hadamard matrix* H on $\mathbb{C}^d$: a rescaled $d \times d$ unitary matrix,

$$|H_{i,j}| = \frac{1}{\sqrt{d}},\ i,j = 0,1,\ldots,d-1, \quad H^\dagger H = d\,\mathbb{I}.$$

Maximal set of MUBs in $d = 6$?

- Triples of MUBs have been constructed using:
  - Abelian subgroups of the Weyl-Heisenberg group
  - Mutually unbiased Hadamard matrices
- Complex *Hadamard matrix* H on $\mathbb{C}^d$: a rescaled $d \times d$ unitary matrix,

$$|H_{i,j}| = \frac{1}{\sqrt{d}},\ i, j = 0, 1, \ldots, d-1, \quad H^\dagger H = d\,\mathbb{I}.$$

- Two Hadamard matrices H_1, H_2 are mutually unbiased if $H_1^\dagger H_2$ is also Hadamard.

Maximal set of MUBs in $d = 6$?

- Triples of MUBs have been constructed using:
  - Abelian subgroups of the Weyl-Heisenberg group
  - Mutually unbiased Hadamard matrices
- Complex *Hadamard matrix* H on $\mathbb{C}^d$: a rescaled $d \times d$ unitary matrix,

$$|H_{i,j}| = \frac{1}{\sqrt{d}},\ i,j = 0,1,\ldots,d-1, \quad H^\dagger H = d\,\mathbb{I}.$$

- Two Hadamard matrices H_1, H_2 are mutually unbiased if $H_1^\dagger H_2$ is also Hadamard.
  A set of N Hadamard matrices $\Leftrightarrow$ A set of $N+1$ MUBs!

Maximal set of MUBs in $d = 6$?

- Triples of MUBs have been constructed using:
  - Abelian subgroups of the Weyl-Heisenberg group
  - Mutually unbiased Hadamard matrices
- Complex *Hadamard matrix* H on $\mathbb{C}^d$: a rescaled $d \times d$ unitary matrix,

$$|H_{i,j}| = \frac{1}{\sqrt{d}},\ i,j = 0,1,\ldots,d-1, \quad H^\dagger H = d\,\mathbb{I}.$$

- Two Hadamard matrices H_1, H_2 are mutually unbiased if $H_1^\dagger H_2$ is also Hadamard.
  A set of N Hadamard matrices $\Leftrightarrow$ A set of $N+1$ MUBs!
- All known triples of MUBs in $d = 6$ are unextendible to a maximal set!

- **Definition [Unextendibility]:** A set of MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is *unextendible* if there does not exist another basis in $\mathbb{C}^d$ that is unbiased with respect to $\{\mathcal{B}_j, j = 1, \ldots, m\}$.

Unextendible Sets of MUBs

- **Definition [Unextendibility]:** A set of MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is *unextendible* if there does not exist another basis in $\mathbb{C}^d$ that is unbiased with respect to $\{\mathcal{B}_j, j = 1, \ldots, m\}$.
- Example: In $d = 6$, the eigenbases of $\mathcal{X}, \mathcal{Z}$ and $\mathcal{X}\mathcal{Z}$ are an unextendible set of 3 MUBs.

Unextendible Sets of MUBs

- **Definition [Unextendibility]:** A set of MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is *unextendible* if there does not exist another basis in $\mathbb{C}^d$ that is unbiased with respect to $\{\mathcal{B}_j, j = 1, \ldots, m\}$.
- Example: In $d = 6$, the eigenbases of $\mathcal{X}, \mathcal{Z}$ and $\mathcal{X}\mathcal{Z}$ are an unextendible set of 3 MUBs.

  $\Rightarrow$ Cannot be extended to obtain a complete set of 7 MUBs in $d = 6$!

Unextendible Sets of MUBs

- **Definition [Unextendibility]:** A set of MUBs $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ in $\mathbb{C}^d$ is *unextendible* if there does not exist another basis in $\mathbb{C}^d$ that is unbiased with respect to $\{\mathcal{B}_j, j = 1, \ldots, m\}$.
- Example: In $d = 6$, the eigenbases of $\mathcal{X}, \mathcal{Z}$ and $\mathcal{X}\mathcal{Z}$ are an unextendible set of 3 MUBs.

  $\Rightarrow$ Cannot be extended to obtain a complete set of 7 MUBs in $d = 6$!
- **Definition [Strongly Unextendiblity]:** $\{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m\}$ is *strongly unextendible* if there does not exist another vector that is unbiased with respect to $\mathcal{B}_j, j = 1, \ldots, m$.

  Eigenbases of $\mathcal{X}, \mathcal{Z}$ and $\mathcal{X}\mathcal{Z}$ in $d = 6$ are strongly unextendible.

Unextendible sets of Pauli Classes

- **Definition [Unextendible Classes]:** A set of L mutually disjoint maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ of Pauli operators in $d = 2^n$ is unextendible if another maximal commuting class cannot be formed out of the remaining operators in $\mathcal{P}_n \setminus \{\mathbb{I} \cup_{i=1}^{L} \mathcal{C}_i\}$.

Unextendible sets of Pauli Classes

- **Definition [Unextendible Classes]:** A set of L mutually disjoint maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ of Pauli operators in $d = 2^n$ is unextendible if another maximal commuting class cannot be formed out of the remaining operators in $\mathcal{P}_n \setminus \{\mathbb{I} \cup_{i=1}^{L} \mathcal{C}_i\}$.
- Example: a set of 3 unextendible maximal commuting Pauli classes in $d = 4$.

$$\begin{aligned} \mathcal{C}_1 &= \{Y \otimes Y, \mathbb{I} \otimes Y, Y \otimes \mathbb{I}\}, \\ \mathcal{C}_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\}, \\ \mathcal{C}_3 &= \{X \otimes \mathbb{I}, \mathbb{I} \otimes Z, X \otimes Z\} \end{aligned}$$

Unextendible sets of Pauli Classes

- **Definition [Unextendible Classes]:** A set of L mutually disjoint maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ of Pauli operators in $d = 2^n$ is unextendible if another maximal commuting class cannot be formed out of the remaining operators in $\mathcal{P}_n \setminus \{\mathbb{I} \cup_{i=1}^{L} \mathcal{C}_i\}$.
- Example: a set of 3 unextendible maximal commuting Pauli classes in $d = 4$.

$$\begin{aligned} \mathcal{C}_1 &= \{Y \otimes Y, \mathbb{I} \otimes Y, Y \otimes \mathbb{I}\}, \\ \mathcal{C}_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\}, \\ \mathcal{C}_3 &= \{X \otimes \mathbb{I}, \mathbb{I} \otimes Z, X \otimes Z\} \end{aligned}$$

Cannot find one more class of 3 commuting operators from the remaining 6 Pauli operators.

Unextendible sets of Pauli Classes

- **Definition [Unextendible Classes]:** A set of L mutually disjoint maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \ldots, \mathcal{C}_L\}$ of Pauli operators in $d = 2^n$ is unextendible if another maximal commuting class cannot be formed out of the remaining operators in $\mathcal{P}_n \setminus \{\mathbb{I} \cup_{i=1}^{L} \mathcal{C}_i\}$.
- Example: a set of 3 unextendible maximal commuting Pauli classes in $d = 4$.

$$
\begin{aligned}
\mathcal{C}_1 &= \{Y \otimes Y, \mathbb{I} \otimes Y, Y \otimes \mathbb{I}\}, \\
\mathcal{C}_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\}, \\
\mathcal{C}_3 &= \{X \otimes \mathbb{I}, \mathbb{I} \otimes Z, X \otimes Z\}
\end{aligned}
$$

  Cannot find one more class of 3 commuting operators from the remaining 6 Pauli operators.
- **Weakly Unextendible Sets:** The common eigenbases of an unextendible set of Pauli classes form a weakly unextendible set of MUBs:
  There does not exist another MUB that can be realized as a common eigenbasis of a maximal commuting class $\mathcal{C}_{L+1} \subset \mathcal{P}_n \setminus \{\mathbb{I}\}$.

Unextendible Sets in $d = 2^n$

- Given any two maximal commuting Pauli classes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $d = 4$, there always exists a third class $\mathcal{C}_3'$, of commuting Paulis such that $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3'\}$ constitute an unextendible set of **three** maximal commuting Pauli classes in $d = 4$.

Unextendible Sets in $d = 2^n$

- Given any two maximal commuting Pauli classes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $d = 4$, there always exists a third class $\mathcal{C}_3'$, of commuting Paulis such that $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3'\}$ constitute an unextendible set of **three** maximal commuting Pauli classes in $d = 4$.

- In $d = 8$, the number of maximal commuting Pauli classes in an unextendible set is exactly 5. $\Rightarrow$ A weakly unextendible set of 5 MUBs in $d = 8$.

Unextendible Sets in $d = 2^n$

- Given any two maximal commuting Pauli classes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $d = 4$, there always exists a third class $\mathcal{C}_3'$, of commuting Paulis such that $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3'\}$ constitute an unextendible set of **three** maximal commuting Pauli classes in $d = 4$.

- In $d = 8$, the number of maximal commuting Pauli classes in an unextendible set is exactly 5. $\Rightarrow$ A weakly unextendible set of 5 MUBs in $d = 8$.

- **Numerical evidence:** Specific examples of unextendible sets of Pauli classes in $d = 4, 8$ lead to *strongly unextendible* MUBs.

Unextendible Sets in $d = 2^n$

- Given any two maximal commuting Pauli classes $\mathcal{C}_1$ and $\mathcal{C}_2$ in $d = 4$, there always exists a third class $\mathcal{C}_3'$, of commuting Paulis such that $\{\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3'\}$ constitute an unextendible set of **three** maximal commuting Pauli classes in $d = 4$.
- In $d = 8$, the number of maximal commuting Pauli classes in an unextendible set is exactly 5. $\Rightarrow$ A weakly unextendible set of 5 MUBs in $d = 8$.
- **Numerical evidence:** Specific examples of unextendible sets of Pauli classes in $d = 4, 8$ lead to *strongly unextendible* MUBs.
- In $d = 2^n$: we conjecture the existence of unextendible sets of $\frac{d}{2} + 1$ maximal commuting Pauli classes.

References

- T.Durt, B.-G.Englert, I. Bengtsson, and K. Żuczkowski, *On mutually unbiased bases* International Journal of Quantum Information, **8**, 535-640 (2010).
- I.D.Ivanovic, JPhys A **14**, 3241 (1981).
- Wootters & Fields, Annals of Phys **191**, 363 (1989).
- S. Bandyopadhyay *et al.* Algorithmica **34**, 512 (2002), Lawrence *et al.* Physical Review A **65**, 032320 (2002).
- C. H. Bennett and G. Brassard, *Quantum Cryptography : Public key distribution and coin tossing*, In IEEE Intl. Conf. on Computers, Systems and Signal Processing
- M. Grassl, *On SIC-POVMs and MUBs in dimension* 6, quant-ph: 0406175.
- M. Combescure, J. Math Phys. **50**, 032104 (2009).
- P. Mandayam, S. Bandyopadhyay, M. Grassl and W.K. Wootters, QIC **14**, 0823 (2014).

Thank You!