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

Prabha Mandayam
Chennai Mathematical Institute

Aspects of Mathematics
The Institute of Mathematical Sciences
Mutually Unbiased Bases: an introduction
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
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
Let $\mathbb{H}^d$ be a finite-dimensional Hilbert space\(^1\). State space of any finite quantum system.

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

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

---

\(^1\)Complex inner product space, which is complete.
Let $\mathbb{H}^d$ be a finite-dimensional Hilbert space\(^1\). State space of any finite quantum system.

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

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

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

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

All outcomes are *equally* probable!

---

\(^1\)Complex inner product space, which is complete.
Pauli matrices $X, Z$ on $\mathbb{C}^2$:

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

Eigenbases of $Z, X$:

$$B_Z = \{|0\rangle, |1\rangle\}; \quad B_X = \left\{ |+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \quad |\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \right\}$$
Mutually Unbiased Bases : Examples

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

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

  Eigenbases of $Z, X$:

  $\mathcal{B}_Z = \{|0\rangle, |1\rangle\}; \quad \mathcal{B}_X = \left\{|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}}, \ |-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}$

- 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 \( \mathbb{C}^2 \):

\[
Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}; \quad X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\]

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

- 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 \( Y \)

\[
Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \mathcal{B}_Y = \left\{ \frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}} \right\}
\]
MUBs : Existence and Constructions
A pair of mutually unbiased bases

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

- Choose any reference basis – $\{\lvert 0 \rangle, \lvert 1 \rangle, \ldots, \lvert d-1 \rangle \}$ – Computational Basis
- Discrete quantum Fourier transform:

$$
\tilde{k} = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{-i2\pi jk/d} \lvert j \rangle
$$
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:
    $$\lvert \tilde{k}\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{-i\frac{2\pi j k}{d}} \lvert j\rangle$$

- The bases $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ and $\{\lvert 0\rangle, \lvert 1\rangle, \ldots, \lvert d-1\rangle\}$ are mutually unbiased:
  $$\langle j | \tilde{k}\rangle = \frac{1}{\sqrt{d}} e^{-i\frac{2\pi j k}{d}}, \forall j, k = 0, 1, \ldots, d - 1.$$
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 $\{ |\tilde{0}\rangle, |\tilde{1}\rangle, \ldots, |d-1\rangle \}$ 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:
  $$ \mathcal{X} |j\rangle = |(j + 1)\text{mod } d\rangle; \quad \mathcal{Z} |j\rangle = e^{i2\pi j/d} |j\rangle, \text{ with } (\mathcal{X})^d = (\mathcal{Z})^d = I. $$

Eigenbases of $\mathcal{X}$ and $\mathcal{Z}$ are mutually unbiased!
Three MUBs in $\mathbb{C}^d$ : eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{X}\mathcal{Z}\}$. (Generalized Pauli operators)
Three MUBs in $\mathbb{C}^d$: eigenbases of $\{X, Z, XZ\}$. (Generalized Pauli operators)

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

Can we construct more MUBs in $\mathbb{C}^d$ using higher products $(X)^m(Z)^n$? Yes, when $d$ is prime!

**Lemma 1:** Let $B = \{|b_0\rangle, |b_1\rangle, \ldots, |b_{d-1}\rangle\}$ be a basis in $\mathbb{C}^d$. If there exists a unitary operator

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

then, the eigenbasis of $V$ is mutually unbiased with the basis $B$. 
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

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

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

- **Proof:** Let $V|v_i\rangle = \lambda_i|v_i\rangle$, $i = 0, 1, \ldots, d-1$. ($|\lambda_i| = 1$)

  $$|\langle v_i | b_j \rangle| = |\langle v_i | V | b_j \rangle| = |\langle v_i | b_{(j+1)\mod d} \rangle|, \ \forall \ i, j.$$

  $$\Rightarrow |\langle v_i | b_0 \rangle| = |\langle v_i | b_1 \rangle| = \ldots = |\langle v_i | b_{d-1} \rangle|, \ \forall i.$$

  $$\Rightarrow |\langle v_i | b_j \rangle|^2 = \frac{1}{d}, \ \forall i, j. \ (\sum_j |\langle v_i | b_j \rangle|^2 = 1, \ \forall i.)$$
Consider the operators \( \{X, Z, XZ, X(Z)^2, \ldots, X(Z)^{d-1}\} \) over \( \mathbb{C}^d \). They are unitary and cyclic, i.e., \( (X(Z)^k)^d = I \) for \( 0 \leq k \leq d - 1 \).
Consider the operators \( \{X, Z, XZ, X(Z)^2, \ldots, X(Z)^{d-1}\} \) over \( \mathbb{C}^d \).

They are unitary and cyclic, i.e., \( (X(Z)^k)^d = I \) for \( 0 \leq k \leq d - 1 \).

\[
X(Z)^k |j\rangle = \left( e^{i2\pi j/d} \right)^k |(j + 1) \mod d \rangle.
\]

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

\[
X(Z)^l |\psi^{(k)}_t\rangle = \left( e^{i2\pi /d} \right)^{t+k-l} |\psi^{(k)}_{t+k-l} \rangle.
\]
Consider the operators \( \{X, Z, XZ, X(Z)^2, \ldots, X(Z)^{d-1}\} \) over \( \mathbb{C}^d \). They are unitary and cyclic, i.e., \( (X(Z)^k)^d = I \) for \( 0 \leq k \leq d - 1 \).

\[
X(Z)^k |j\rangle = (e^{i2\pi j/d})^k |(j + 1)\text{mod } d\rangle.
\]

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

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

**Lemma 2**: When \( d \) is prime, the eigenvectors of \( X(Z)^k \) are cyclically shifted under the action of \( X(Z)^l \), for all \( l \neq k \) (\( 0 \leq l, k \leq d - 1 \)).
Consider the operators \( \{X, Z, XZ, X(Z)^2, \ldots, X(Z)^{d-1}\} \) over \( \mathbb{C}^d \). They are unitary and cyclic, i.e., \( (X(Z)^k)^d = I \) for \( 0 \leq k \leq d - 1 \).

\[
X(Z)^k |j\rangle = (e^{i2\pi j/d})^k |(j + 1) \text{mod } d\rangle.
\]

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

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

**Lemma 2:** When \( d \) is prime, the eigenvectors of \( X(Z)^k \) are cyclically shifted under the action of \( X(Z)^l \), 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 \( \{X, Z, XZ, X(Z)^2, \ldots, X(Z)^{d-1}\} \) 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 $\mathcal{X}, \mathcal{Z}, \mathcal{XZ}$. Identical to the Pauli eigenbases!

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

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

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 $X, Z, XZ$. Identical to the Pauli eigenbases!
- In $\mathbb{C}^3$: the eigenbases of $\{X, X, XZ, XZ^2\}$ 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 $\{X(Z)^k\}$ have shorter periods. Eg. $(Z^p)^q = I$.
  - Cyclic shift property no longer holds.
$d + 1$ MUBs in prime dimensions: Examples

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

- In $\mathbb{C}^3$ : the eigenbases of $\{\mathcal{X}, \mathcal{XZ}, \mathcal{XZ^2}\}$ 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. $(\mathcal{Z}^p)^q = I$.
  - Cyclic shift property no longer holds.
  - Numerical evidence shows, we obtain no more than 3 MUBs using this approach: the eigenbases of $\{\mathcal{X}, \mathcal{Z}, \mathcal{XZ}\}$. 

MUBs: Role in Quantum Information Processing
MUBs form a \textit{minimal} and \textit{optimal} set of orthogonal measurements for quantum state tomography.
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 $\mathcal{B}^j = \{|\psi^j_0\rangle, \ldots, |\psi^j_{d-1}\rangle\}$ yields only $d - 1$ independent probabilities:

$$p(i|\mathcal{B}^j)_\rho := \text{tr}[\rho |\psi^j_i\rangle\langle \psi^j_i|] = \langle \psi^j_i | \rho |\psi^j_i\rangle, \ i = 0, \ldots, d - 1.$$
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 $\mathcal{B}^j = \{|\psi^j_0\rangle, \ldots, |\psi^j_{d-1}\rangle\}$ yields only $d - 1$ independent probabilities:

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

$\Rightarrow$ Need $d + 1$ *distinct* basis sets to obtain $d^2 - 1$ independent probabilities.
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 $\mathcal{B}^j = \{|\psi^j_0\rangle, \ldots, |\psi^j_{d-1}\rangle\}$ yields only $d - 1$ independent probabilities:

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

$\Rightarrow$ 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.
MUBs are the measurement bases that are most incompatible, as quantified by entropic uncertainty relations.
• MUBs are the measurement bases that are most \textit{incompatible}, as quantified by \textit{entropic uncertainty relations}.

• When measuring state $|\phi\rangle \in \mathbb{C}^d$ in the measurement basis $B^j$, probability of the $i^{th}$ outcome is

\[ p(i \mid B^j)|\phi\rangle := |\langle \psi_i^j | \phi \rangle|^2. \]
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

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

Let $H(\mathcal{B}^j || \phi)$ be the *entropy* of the distribution $p(i | \mathcal{B}^j)_\phi$. An entropic *uncertainty* relation (EUR) for the set of bases $\{\mathcal{B}^1, \ldots, \mathcal{B}^L\}$ is:

$$\frac{1}{L} \sum_{j=1}^{L} H(\mathcal{B}^j || \phi) \geq c_{\mathcal{B}^1, \ldots, \mathcal{B}^L}, \ \forall |\phi\rangle$$
MUBs are the measurement bases that are most \textit{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

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

Let $H(\mathcal{B}^j | | \phi\rangle)$ be the entropy of the distribution $p(i | \mathcal{B}^j | \phi)$. An entropic \textit{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 $\mathbb{C}^d$,

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

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

For measurement bases $A = \{|a_1\rangle, \ldots, |a_d\rangle\}$ and $B = \{|b_1\rangle, \ldots, |b_d\rangle\}$ in $\mathbb{C}^d$,

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

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

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 \( A = \{|a_1\rangle, ..., |a_d\rangle\} \) and \( B = \{|b_1\rangle, ..., |b_d\rangle\} \) in \( \mathbb{C}^d \),

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

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

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.
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*.

- 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 $X = x_1x_2 \ldots x_n$, $x_i \in \{0, 1\}$. 
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 \( X = x_1x_2 \ldots x_n, x_i \in \{0, 1\} \).
- **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 $X = x_1x_2 \ldots x_n$, $x_i \in \{0, 1\}$.
- **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**.

- **B** has access to the basis information, **E** does not. By guessing randomly, **E** can typically access only half the key.
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 $X = x_1x_2 \ldots x_n$, $x_i \in \{0, 1\}$.
- 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.

- 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 $mn' - nm' = 0 \text{ mod } d$. 
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 $mn' - nm' = 0 \mod d$.

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

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

$$\mathcal{X} \mathcal{Z} = e^{i 2\pi / d} \mathcal{Z} \mathcal{X}.$$ 

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 $mn' - nm' = 0 \mod d$.

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

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

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

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

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

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

Let $S$ 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 $S \setminus \{I\}$ into Mutually Disjoint Maximal Commuting Classes: $\{C_1, C_2, \ldots, C_L\}$ where, $C_j \subset S \setminus \{I\}$ of size $|C_j| = d - 1$ are such that
There are at most $d$ pairwise orthogonal commuting unitary matrices in $M_d(\mathbb{C})$.

Let $S$ 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 $S \setminus \{I\}$ into Mutually Disjoint Maximal Commuting Classes: $\{C_1, C_2, \ldots, C_L\}$ where, $C_j \subset S \setminus \{I\}$ of size $|C_j| = d - 1$ are such that

(a) the elements of $C_j$ commute for all $1 \leq j \leq L$, and,

(b) $C_j \cap C_k = \emptyset$ for all $j \neq k$. 
There are at most $d$ pairwise orthogonal commuting unitary matrices in $\mathbb{M}_d(\mathbb{C})$.

Let $S$ 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 $S \setminus \{I\}$ into Mutually Disjoint Maximal Commuting Classes: $\{C_1, C_2, \ldots, C_L\}$ where, $C_j \subset S \setminus \{I\}$ of size $|C_j| = d - 1$ are such that

(a) the elements of $C_j$ commute for all $1 \leq j \leq L$, and,

(b) $C_j \cap C_k = \emptyset$ for all $j \neq k$.

**Theorem 1:** The common eigenbases of each of $\{C_1, C_2, \ldots, C_L\}$ form a set of $L$ mutually unbiased bases.
Proof of Theorem 1

- Consider a maximal commuting class $C_j$ ($1 \leq j \leq d + 1$):

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

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

- Consider a maximal commuting class $C_j$ ($1 \leq j \leq d + 1$):
  
  $$C_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\}, \ (U_{j,0} = I)$$

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

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

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

- Consider a maximal commuting class $C_j$ ($1 \leq j \leq d + 1$):

  $C_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\}$, ($U_{j,0} = I$)

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

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

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

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

$$\sum_{i=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{i,j}^s \lambda_{l,k}^t |\langle \psi^j_i| \psi^k_l\rangle|^2 = d \delta_{s,0} \delta_{t,0}, \forall 0 \leq s, t \leq d - 1.$$
Consider a maximal commuting class $C_j$ ($1 \leq j \leq d + 1$):

$$C_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\}, \ (U_{j,0} = I)$$

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

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

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

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

$$\sum_{i=0}^{d-1} \sum_{l=0}^{d-1} \lambda_{i}^{j,s} \lambda_{l}^{k,t} |\langle \psi^j_i| \psi^k_l\rangle|^2 = d \delta_{s,0} \delta_{t,0}, \ \forall 0 \leq s, t \leq d - 1.$$ 

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

$$|\langle \psi^j_i| \psi^k_l\rangle|^2 = \frac{1}{d}, \ \forall 0 \leq i, l \leq d.$$

Proof of Theorem 1
Proof of Theorem 1

Consider a maximal commuting class $C_j$ ($1 \leq j \leq d + 1$):

$$C_j = \{U_{j,0}, U_{j,1}, U_{j,2}, \ldots, U_{j,d-1}\}, \ (U_{j,0} = I)$$

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

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

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

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

$$\sum_{i=0}^{d-1} \sum_{l=0}^{d-1} \lambda^j_i s \lambda^k_l t |\langle \psi^j_i| \psi^k_l\rangle|^2 = d \delta_{s,0} \delta_{t,0}, \ \forall 0 \leq s, t \leq d - 1.$$ 

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

$$|\langle \psi^j_i| \psi^k_l\rangle|^2 = \frac{1}{d}, \ \forall 0 \leq i, l \leq d.$$ 

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

Prabha Mandayam (CMI)
Conversely, let \( \{B^1, B^2, \ldots, B^L\} \) 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.
Conversely, let \( \{B^1, B^2, \ldots, B^L\} \) 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 \( B^j \equiv \{|\psi_0^j\rangle, |\psi_1^j\rangle, \ldots, |\psi_{d-1}^j\rangle\} \). Then,

\[
|\langle \psi_i^j | \psi_l^k \rangle|^2 = \frac{1}{d}, \quad \forall \; j \neq k, \; \forall \; 0 \leq i, l \leq d - 1.
\]
Conversely, let \( \{B^1, B^2, \ldots, B^L\} \) 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 \( B^j \equiv \{ |\psi^j_0 \rangle, |\psi^j_1 \rangle, \ldots, |\psi^j_{d-1} \rangle \} \). Then,

\[
|\langle \psi^j_i | \psi^k_l \rangle|^2 = \frac{1}{d}, \quad \forall \ j \neq k, \forall \ 0 \leq i, l \leq d - 1.
\]

Construct the unitaries

\[
U^j_{j,s} = \sum_{l=0}^{d-1} e^{2\pi i s l/d} |\psi^j_l \rangle \langle \psi^j_l|, \quad \forall \ 0 \leq s \leq d - 1, \ 1 \leq j \leq L.
\]

Clearly, \( U^j_{j,s} \) and \( U^j_{j,t} \) commute for every \( j \).
Conversely, let \( \{B^1, B^2, \ldots, B^L\} \) 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 \( B^j \equiv \{ |\psi^j_0\rangle, |\psi^j_1\rangle, \ldots, |\psi^j_{d-1}\rangle \} \). Then,

\[
|\langle \psi^j_i | \psi^k_l \rangle|^2 = \frac{1}{d}, \forall j \neq k, \forall 0 \leq i, l \leq d - 1.
\]

Construct the unitaries

\[
U_{j,s} = \sum_{l=0}^{d-1} e^{2\pi isl/d} |\psi^j_l\rangle \langle \psi^j_l|, \forall 0 \leq s \leq d - 1, 1 \leq j \leq L.
\]

Clearly, \( U_{j,s} \) and \( U_{j,t} \) commute for every \( j \).

These unitaries are indeed mutually orthogonal:

\[
\text{tr}[U^\dagger_{j,s} U_{k,t}] = \sum_{l,m=0}^{d-1} e^{2\pi i (tl-sm)/d} |\langle \psi^j_l | \psi^k_m \rangle|^2
\]

\[
\Rightarrow \text{tr}[U^\dagger_{j,s} U_{j,t}] = d \delta_{s,t}, \quad \text{tr}[U^\dagger_{j,s} U_{k,t}] = 0, j \neq k, (s, t) \neq (0, 0).
\]
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, $N(d) \leq d + 1$. 
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, $U_i \in \{I, X, Y, Z\}$.
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, $U_i \in \{\mathbb{I}, X, Y, Z\}$.

- $S_1 = \{Y \otimes \mathbb{I}, \mathbb{I} \otimes Y, Y \otimes Y\}$
- $S_2 = \{Y \otimes Z, Z \otimes X, X \otimes Y\}$
- $S_3 = \{Z \otimes \mathbb{I}, \mathbb{I} \otimes Z, Z \otimes Z\}$
- $S_4 = \{X \otimes \mathbb{I}, \mathbb{I} \otimes X, X \otimes X\}$
- $S_5 = \{X \otimes Z, Z \otimes Y, Y \otimes X\}$.

Common eigenbases of $S_1, S_2, \ldots, S_5$ form a set of 5 MUBs in $\mathbb{C}^4$. 
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, $U_i \in \{I, X, Y, Z\}$.

\[
\begin{align*}
S_1 &= \{Y \otimes I, I \otimes Y, Y \otimes Y\} \\
S_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\} \\
S_3 &= \{Z \otimes I, I \otimes Z, Z \otimes Z\} \\
S_4 &= \{X \otimes I, I \otimes X, X \otimes X\} \\
S_5 &= \{X \otimes Z, Z \otimes Y, Y \otimes X\}.
\end{align*}
\]

Common eigenbases of $S_1, S_2, \ldots, S_5$ form a set of 5 MUBs in $\mathbb{C}^4$.

This partitioning is not unique!
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.
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 $\mathbb{C}^d = \mathbb{C}^p \otimes \mathbb{C}^p \ldots \otimes \mathbb{C}^p$. $n$ times

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

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, $U_i = (\mathcal{X})^{k_i} (\mathcal{Z})^{l_i}$, $0 \leq k_i, l_i \leq p - 1$. 


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 $\mathbb{C}^d = \mathbb{C}^p \otimes \mathbb{C}^p \ldots \otimes \mathbb{C}^p$.

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 $\mathbb{F}_p$: $(k_1, \ldots, k_n|l_1, \ldots, l_n)$. 

Prabha Mandayam (CMI)  
IMSc July’14  
1 July 2014  
21 / 29
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 $\mathbb{C}^d = \mathbb{C}^p \otimes \mathbb{C}^p \ldots \otimes \mathbb{C}^p$. Consider tensor products of $\mathcal{X}$ and $\mathcal{Z}$ acting on $\mathbb{C}^p$.

Unitary basis of operators: $S = \{U_1 \otimes U_2 \otimes \ldots \otimes U_n\}$, 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 $S$ into $d + 1$ mutually disjoint maximal commuting classes $C_i$. A partitioning of $d^2$ elements of the Weyl-Heisenberg group into $d + 1$ Abelian subgroups.
Composite Dimensions: Unextendible MUBs
• In composite dimensions, smaller sets of MUBs have been constructed.
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.
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 \(\{B_1^{r_1}, B_2^{r_2}, \ldots, B_L^{r_m}\}\) for each \(\mathbb{C}^{p_m^{r_m}}\). Then,

\[
\{B_{j_1}^{r_1} \otimes \ldots \otimes B_{j_m}^{r_m} : j = 1, \ldots, L\}
\]

is a set of \(L\) MUBs in \(\mathbb{C}^d\).
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 $d = p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$:

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

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

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

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

Simple consequence: $N(d) \geq 3$ for any $d \geq 2$. Eigenbases of $\{X, Z, XZ\}$.
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 \(\{B^{1,m}, B^{2,m}, \ldots, B^{L,m}\}\) for each \(\mathbb{C}^{p_m^{r_m}}\). Then,

\[
\{B^{j,1} \otimes \ldots \otimes B^{j,m} : j = 1, \ldots, L\}
\]

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

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

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

- 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,

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

- 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 $d = 6$?

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

- 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 \( \{B_1, B_2, \ldots, B_m\} \) in \( \mathbb{C}^d \) is *unextendible* if there does not exist another basis in \( \mathbb{C}^d \) that is unbiased with respect to \( \{B_j, j = 1, \ldots, m\} \).
Definition [Unextendibility]: A set of MUBs \( \{B_1, B_2, \ldots, B_m\} \) in \( \mathbb{C}^d \) is unextendible if there does not exist another basis in \( \mathbb{C}^d \) that is unbiased with respect to \( \{B_j, j = 1, \ldots, m\} \).

Example: In \( d = 6 \), the eigenbases of \( \mathcal{X}, \mathcal{Z} \) and \( \mathcal{XZ} \) are an unextendible set of 3 MUBs.
**Definition [Unextendibility]:** A set of MUBs \( \{B_1, B_2, \ldots, B_m\} \) in \( \mathbb{C}^d \) is *unextendible* if there does not exist another basis in \( \mathbb{C}^d \) that is unbiased with respect to \( \{B_j, j = 1, \ldots, m\} \).

**Example:** In \( d = 6 \), the eigenbases of \( \mathcal{X}, \mathcal{Z} \) and \( \mathcal{XZ} \) are an unextendible set of 3 MUBs.

\[ \Rightarrow \text{Cannot be extended to obtain a complete set of 7 MUBs in } d = 6! \]
Definition [Unextendibility]: A set of MUBs \( \{B_1, B_2, \ldots, B_m\} \) in \( \mathbb{C}^d \) is \textit{unextendible} if there does not exist another basis in \( \mathbb{C}^d \) that is unbiased with respect to \( \{B_j, j = 1, \ldots, m\} \).

Example: In \( d = 6 \), the eigenbases of \( \mathcal{X}, \mathcal{Z} \) and \( \mathcal{XZ} \) 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]: \( \{B_1, B_2, \ldots, B_m\} \) is \textit{strongly unextendible} if there does not exist another vector that is unbiased with respect to \( B_j, j = 1, \ldots, m \).

Eigenbases of \( \mathcal{X}, \mathcal{Z} \) and \( \mathcal{XZ} \) in \( d = 6 \) are strongly unextendible.
**Definition [Unextendible Classes]:** A set of $L$ mutually disjoint maximal commuting classes \( \{C_1, C_2, \ldots, C_L\} \) of Pauli operators in \( d = 2^n \) is **unextendible** if another maximal commuting class cannot be formed out of the remaining operators in \( \mathcal{P}_n \setminus \{I \cup \bigcup_{i=1}^{L} C_i\} \).
Definition [Unextendible Classes]: A set of $L$ mutually disjoint maximal commuting classes $\{C_1, C_2, \ldots, C_L\}$ of Pauli operators in $d = 2^n$ is **unextendible** if another maximal commuting class cannot be formed out of the remaining operators in $P_n \setminus \{I \cup \bigcup_{i=1}^{L} C_i\}$.

**Example:** a set of 3 unextendible maximal commuting Pauli classes in $d = 4$.

\[
\begin{align*}
C_1 &= \{Y \otimes Y, I \otimes Y, Y \otimes I\}, \\
C_2 &= \{Y \otimes Z, Z \otimes X, X \otimes Y\}, \\
C_3 &= \{X \otimes I, I \otimes Z, X \otimes Z\}
\end{align*}
\]
**Definition [Unextendible Classes]:** A set of $L$ mutually disjoint maximal commuting classes $\{C_1, C_2, \ldots, C_L\}$ of Pauli operators in $d = 2^n$ is **unextendible** if another maximal commuting class cannot be formed out of the remaining operators in $\mathcal{P}_n \setminus \{I \cup \bigcup_{i=1}^{L} C_i\}$.

**Example:** a set of 3 unextendible maximal commuting Pauli classes in $d = 4$.

\[
C_1 = \{Y \otimes Y, I \otimes Y, Y \otimes I\}, \\
C_2 = \{Y \otimes Z, Z \otimes X, X \otimes Y\}, \\
C_3 = \{X \otimes I, I \otimes Z, X \otimes Z\}
\]

Cannot find one more class of 3 commuting operators from the remaining 6 Pauli operators.
Definition [Unextendible Classes]: A set of $L$ mutually disjoint maximal commuting classes $\{C_1, C_2, \ldots, C_L\}$ of Pauli operators in $d = 2^n$ is unextendible if another maximal commuting class cannot be formed out of the remaining operators in $\mathcal{P}_n \setminus \{I \cup \bigcup_{i=1}^{L} C_i\}$.

Example: a set of 3 unextendible maximal commuting Pauli classes in $d = 4$.

- $C_1 = \{Y \otimes Y, I \otimes Y, Y \otimes I\}$,
- $C_2 = \{Y \otimes Z, Z \otimes X, X \otimes Y\}$,
- $C_3 = \{X \otimes I, I \otimes Z, X \otimes Z\}$

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 $C_{L+1} \subset \mathcal{P}_n \setminus \{I\}$. 
Given any two maximal commuting Pauli classes $C_1$ and $C_2$ in $d = 4$, there always exists a third class $C'_3$, of commuting Paulis such that $\{C_1, C_2, C'_3\}$ constitute an unextendible set of three maximal commuting Pauli classes in $d = 4$. 
Given any two maximal commuting Pauli classes $C_1$ and $C_2$ in $d = 4$, there always exists a third class $C'_3$, of commuting Paulis such that $\{C_1, C_2, C'_3\}$ 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 $d = 8$. 
Given any two maximal commuting Pauli classes $C_1$ and $C_2$ in $d = 4$, there always exists a third class $C_3'$, of commuting Paulis such that $\{C_1, C_2, C_3'\}$ 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.
Given any two maximal commuting Pauli classes $C_1$ and $C_2$ in $d = 4$, there always exists a third class $C'_3$, of commuting Paulis such that $\{C_1, C_2, C'_3\}$ 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


Thank You!