

# Mutually Unbiased Bases

**Abdul Fatah**

Faculty of Engineering and Computing

July 2026



Ollscoil  
Teicneolaíochta  
an Atlantaigh

Atlantic  
Technological  
University

# Table of Contents

1	Mutually Unbiased Bases .....	3
1.1	Mutually unbiased bases for $d = 3$ .....	7
1.2	Construction of Mutually Unbiased Bases in $d = 4$ via the Two-Qubit Pauli/Stabilizer Method .....	8
2	Proof that at least three MUBs exist in any dimensions. ....	10
	Bibliography .....	15

# Mutually Unbiased Bases

**Definition 1.1** (Mutually Unbiased Bases): Two bases  $\mathcal{U} = \{|u_i\rangle\}_{i=0}^{d-1}$  and  $\mathcal{V} = \{|v_j\rangle\}_{j=0}^{d-1}$  of the Hilbert space  $\mathbb{C}^d$  are called mutually unbiased when:

$$|\langle u_i | v_j \rangle|^2 = \frac{1}{d}$$

**Definition 1.2** (Set of Mutually Unbiased Bases): A set of  $n$  bases  $S = \{U_i\}_{i=0}^{n-1}$  is called a set of mutually unbiased bases when for each pair of bases  $(U_i, U_j)$  in  $S$ ,  $U_i$  and  $U_j$  are mutually unbiased bases.

**Theorem 1.1** (Horodecki [1]): There are no more than  $d + 1$  mutually unbiased bases in the Hilbert space  $\mathbb{C}^d$ .

*Proof:* ...

□

**Theorem 1.2** (Horodecki [1]): There is a set of three, but not four, mutually unbiased bases in the Hilbert space  $\mathbb{C}^d$  for  $d \geq 2$ .

*Proof:* Suppose we take  $d = 2$ . Then, according to Theorem 1.1, no more than three mutually unbiased bases exist in  $\mathcal{H}_2 (= \mathbb{C}^2)$ , the Hilbert space of dimension two. First we identify a set  $U$  of the three mutually unbiased bases  $U_0, U_1$ , and  $U_2$  so that:

$$U = \{U_0, U_1, U_2\}$$

Then we will show that any other basis can not be unbiased with all three of them.

## Step 1: Defining the first basis (The computational basis)

Our first basis,  $U_0$ , will be the orthonormal computational basis:

$$U_0 = \{|0\rangle, |1\rangle\}$$

This basis corresponds to the eigenbasis of the Pauli-Z operator.

## Step 2: Defining a second mutually unbiased basis

Our second basis must be mutually orthogonal to  $U_0$ :

$$|\langle u_i^0 | u_j^1 \rangle|^2 = \frac{1}{d} = \frac{1}{2}$$

for all  $u_i \in U_0$  and  $u_j \in U_1$ .

It is commonly known [2] that the eigenbases of the Pauli operators are mutually unbiased. So, a good candidate is the Hadamard basis, which corresponds to the eigenbasis of the Pauli-X operator:

$$U_1 = \{|+\rangle, |-\rangle\}$$

where  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  and  $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$ .

The bases  $U_0$  and  $U_1$  are then mutually unbiased:

$$|\langle 0 | + \rangle|^2 = \left| \left\langle 0 \left| \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right. \right\rangle \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

$$|\langle 0 | - \rangle|^2 = \left| \left\langle 0 \left| \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right. \right\rangle \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

$$|\langle 1 | + \rangle|^2 = \left| \left\langle 1 \left| \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right. \right\rangle \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

$$|\langle 1 | - \rangle|^2 = \left| \left\langle 1 \left| \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right. \right\rangle \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2}$$

Since the condition holds for all pairs from  $U_0$  and  $U_1$ , they are mutually unbiased.

## Step 3: Defining a third mutually unbiased basis

Now, we seek a third basis  $U_2$  that is unbiased with both  $U_0$  and  $U_1$ . Again, the eigenbasis of the Pauli-Y operator works.

$$U_2 = \{|+i\rangle, |-i\rangle\}$$

where  $|+i\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$  and  $|-i\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle)$ . Then  $U_2$  is mutually unbiased with  $U_0$ :

$$\begin{aligned}
|\langle 0|+i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \right\rangle \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2} \\
|\langle 0|-i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right\rangle \right|^2 = \left| \frac{1}{\sqrt{2}} \right|^2 = \frac{1}{2} \\
|\langle 1|+i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \right\rangle \right|^2 = \left| \frac{i}{\sqrt{2}} \right|^2 = \frac{1}{2} \\
|\langle 1|-i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right\rangle \right|^2 = \left| -\frac{i}{\sqrt{2}} \right|^2 = \frac{1}{2}
\end{aligned}$$

Likewise,  $U_2$  is mutually unbiased with  $U_1$ :

$$\begin{aligned}
|\langle +|+i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right\rangle \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \right|^2 = \left| \frac{1+i}{2} \right|^2 = \frac{|1|^2 + |i|^2}{2^2} = \frac{1}{2} \\
|\langle +|-i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle) \right\rangle \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right|^2 = \left| \frac{1-i}{2} \right|^2 = \frac{|1|^2 + |-i|^2}{2^2} = \frac{1}{2} \\
|\langle -|+i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\rangle \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle) \right|^2 = \left| \frac{1-i}{2} \right|^2 = \frac{|1|^2 + |i|^2}{2^2} = \frac{1}{2} \\
|\langle -|-i\rangle|^2 &= \left| \left\langle \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\rangle \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right|^2 = \left| \frac{1+i}{2} \right|^2 = \frac{|1|^2 + |-i|^2}{2^2} = \frac{1}{2}
\end{aligned}$$

Thus, we have found three mutually unbiased bases for  $d = 2$

#### Step 4: Proving a fourth mutually unbiased basis is impossible

Now we show that it's impossible to construct a fourth basis,  $U_3$ , that is unbiased with  $U_0$ ,  $U_1$ , and  $U_2$ .

For any new basis to be unbiased with  $U_0$ , its states must be of the form:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle)$$

where  $0 \leq \varphi < 2\pi$  is a real number.

For this state to also be unbiased with  $U_1$ , we must have

$$|\langle +|\psi\rangle|^2 = \frac{1}{2} \quad \forall \quad |\psi\rangle \in U_2$$

We can then derive the following equation:

$$\begin{aligned}
|\langle +|\psi\rangle|^2 &= \frac{1}{2} \\
\Rightarrow \left| \frac{1}{2}(\langle 0| + \langle 1|)(|0\rangle + e^{i\varphi}|1\rangle) \right|^2 &= \frac{1}{2} \\
\Rightarrow \left| \frac{1 + e^{i\varphi}}{2} \right|^2 &= \frac{1}{2} \\
\Rightarrow \frac{1}{2^2} |1 + e^{i\varphi}|^2 &= \frac{1}{2} \\
\Rightarrow |1 + e^{i\varphi}|^2 &= 2 \\
\Rightarrow |(1 + \cos(\varphi) + i \sin(\varphi))|^2 &= 2 \\
\Rightarrow (1 + \cos(\varphi))^2 + (\sin(\varphi))^2 &= 2 \\
\Rightarrow 1 + 2 \cos(\varphi) + \cos^2(\varphi) + \sin^2(\varphi) &= 2 \\
\Rightarrow 1 + 2 \cos(\varphi) + 1 &= 2 \\
\Rightarrow \cos(\varphi) &= 0
\end{aligned}$$

Therefore any element  $|\psi\rangle$  in  $U_3$  must be of the form:

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\varphi}|1\rangle) = \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{\pi}{2}}|1\rangle) \text{ or } \frac{1}{\sqrt{2}}(|0\rangle + e^{i\frac{3\pi}{2}}|1\rangle)$$

Finally, for the state to also be unbiased with  $U_2$ . Checking the condition for  $\varphi = \frac{\pi}{2}$  we get:

$$\begin{aligned}
|\psi\rangle &= |0\rangle + i|1\rangle = |+i\rangle \\
\Rightarrow |\langle +i|\psi\rangle|^2 &= \left| \frac{1}{2}(\langle 0| - i\langle 1|)(|0\rangle + i|1\rangle) \right|^2 \\
&= \left| \frac{1 - i^2}{2} \right|^2 = 1
\end{aligned}$$

For a mutually unbiased basis, this should equal  $\frac{1}{2}$ . Therefore,  $|\psi\rangle$  cannot be an element of  $U_2$ .

Likewise:

$$\begin{aligned}
|\psi\rangle &= |0\rangle - i|1\rangle = |-i\rangle \\
\Rightarrow |\langle +i|\psi\rangle|^2 &= \left| \frac{1}{2}(\langle 0| - i\langle 1|)(|0\rangle - i|1\rangle) \right|^2 \\
&= \left| \frac{1 + i^2}{2} \right|^2 = 1
\end{aligned}$$

Therefore, no 4th basis for  $d=2$  can exist. □

## 1.1 Mutually unbiased bases for $d = 3$

We can construct mutually unbiased bases for  $d = 3$  with various well established methods, such as:

### 1.1.1 Weyl-Heisenberg (or generalized Pauli operator):

It is the standard technique for prime dimensions. It uses the shift and phase operators  $X$  and  $Z$ , along with their products  $XZ^a$  for  $a = 0, 1, \dots, d - 1$ , to generate eigenbases that are mutually unbiased. This method scales well with prime  $d$  and is algebraically elegant.

Generalized Pauli (Weyl) operators on  $C^3$

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

$$X = [(0, 1, 0), (0, 0, 1), (1, 0, 0), ]$$

$$Z = [(1, 0, 0), (0, \omega, 0), (0, 0, \omega^2), ]$$

$$B_Z = [(1, 0, 0), (0, 1, 0), (0, 0, 1), ]$$

$$B_X = \frac{1}{\sqrt{3}} * [(1, 1, 1), (1, \omega, \omega^2), (1, \omega^2, \omega), ]$$

$$B_{\{XZ\}} = \frac{1}{\sqrt{3}} * [(1, 1, 1), (1, \omega, \omega^2), (\omega, 1, \omega^2), ]$$

$$B_{\{XZ^2\}} = \frac{1}{\sqrt{3}} * [(1, 1, 1), (1, \omega, \omega^2), (\omega^2, \omega, 1), ]$$

### 1.1.2 Finite field (Galois Field) method:

It is another powerful approach, particularly useful for both prime and prime power dimensions. This method uses structure from finite fields  $F_d$ , which exist for prime  $d$ . It defines MUB vectors using field-theoretic constructions involving quadratic and linear phase terms. This method is highly generalizable and connects quantum information with abstract algebra.

### 1.1.3 Geometric approach:

It is based on finite projective planes and complex Hadamard matrices, provides a combinatorial and geometric perspective. MUBs correspond to lines in projective geometry over finite fields. While this method is mathematically rich and generalizable, it is often more suitable for larger or composite dimensions.

### 1.1.4 Fourier matrix and its diagonal phase-shifted versions:

Starting with the Discrete Fourier Transform (DFT) matrix  $F$ , one can multiply it by diagonal matrices of the form  $D_a = \{\text{diag}\}(1, \omega^a, \omega^{2a})$  to generate additional MUBs. This is particularly convenient for small dimensions like  $d = 3$ , though less structured for general cases.

The **Fourier matrix** and simple phase shifts. For  $d = 3$ , the Discrete Fourier Transform (DFT) matrix is

$$F = \frac{1}{\sqrt{3}} * [(1, 1, 1), (1, \omega, \omega^2), (1, \omega^2, \omega)]$$

where  $\omega = e^{2\pi\frac{i}{3}}$  is a primitive third root of unity. The columns of  $F$  form one unbiased basis.

To generate more bases, we multiply  $F$  by diagonal matrices of the form

$$D_a = \text{diag}(1, \omega^a, \omega^{2a}), \quad a = 1, 2.$$

The sets of vectors from  $F$ ,  $FD_1$ , and  $FD_2$  give the remaining mutually unbiased bases, together with the standard computational basis.

This approach is straightforward for small prime dimensions like  $d = 3$ .

**Computational basis  $B_0$**

$$B_0 = [(1, 0, 0), (0, 1, 0), (0, 0, 1)]$$

**Fourier basis  $B_1$  (columns of  $F$ )**

$$B_1 = \frac{1}{\sqrt{3}} * [(1, 1, 1), (1, \omega, \omega^2), (1, \omega^2, \omega)]$$

**Quadratic-phase Fourier  $B_2 = \text{diag}(1, \omega, \omega) \times B_1$**

$$B_2 = \frac{1}{\sqrt{3}} * [(1, 1, 1), (\omega, \omega^2, 1), (\omega, 1, \omega^2)]$$

**Quadratic-phase Fourier  $B_3 = \text{diag}(1, \omega^2, \omega^2) \times B_1$**

$$B_3 = \frac{1}{\sqrt{3}} * [(1, 1, 1), (\omega^2, 1, \omega), (\omega^2, \omega, 1)]$$

### 1.1.5 Brute-force numerical or symbolic approach

It is possible to use a brute-force numerical or symbolic approach, solving the orthonormality and unbiasedness conditions directly. While this method offers hands-on intuition and is useful for validation, it becomes computationally impractical as the dimension increases.

## 1.2 Construction of Mutually Unbiased Bases in $d = 4$ via the Two-Qubit Pauli/Stabilizer Method

For a Hilbert space of dimension  $d$ , at most  $d + 1$  mutually unbiased bases (MUBs) can exist; this maximum is achieved for prime powers. Since  $4 = 2^2$ , we can construct five MUBs in  $C^4$ .

Let the single-qubit Pauli operators be



$$X = [[0, 1], [1, 0]],$$

$$Y = [[0, -i], [i, 0]],$$

$$Z = [[1, 0], [0, -1]].$$

The computational basis for two qubits ordered as:  $|00\rangle, |01\rangle, |10\rangle, |11\rangle$ .

### 1.2.1 Commuting partition used

One convenient disjoint partition of the 15 non-identity Paulis into five maximal commuting sets is:

$$S_1 = \{Z \otimes I, I \otimes Z, Z \otimes Z\}$$

$$S_2 = \{X \otimes I, I \otimes X, X \otimes X\}$$

$$S_3 = \{Y \otimes I, I \otimes Y, Y \otimes Y\}$$

$$S_4 = \{X \otimes Y, Y \otimes Z, Z \otimes X\}$$

$$S_5 = \{X \otimes Z, Z \otimes Y, Y \otimes X\}$$

# Proof that at least three MUBs exist in any dimensions.

**Theorem 2.1** (At least three mutually unbiased bases exist [3], [4], [5]): For any dimension  $d \geq 2$ , there exist three pairwise mutually unbiased bases (MUBs) in Hilbert space  $\mathbb{C}^d$ .

*Proof:*

## Road-map for proof:

1. Constructing 3 MUBs for all powers of 2,  $d = 2^a$  using Pauli eigenbases  $\{X, Y, Z\}$  on  $a$  qubits.
2. Constructing 3 MUBs for all odd dimensions  $d = m$  using Weyl operators and a quadratic Gauss-sum argument
  - (Weyl operators are generalized Pauli matrices  $X, Z$ )
  - (A Gauss sum is a finite sum of roots of unity).
3. Using a tensor-product lemma to combine the odd and even parts will give new 3 pairwise MUBs for any  $d = 2^a m$  where  $m$  is odd.

Everything here in point 1 and 2 is in MUBs literature separately, we just need to combine them using the tensor-product lemma in point 3.

## Step 1: Power of 2, $d = 2^a$ (Even dimensions)

For a single qubit ( $d = 2$ ), the eigenbases of  $Z$ ,  $X$ , and  $Y$  are pairwise MUB.

For  $a$  qubits ( $d = 2^a$ ), take product bases

$$\mathcal{B}_z^{(a)} = \text{eigenbases of } Z^{\otimes a}, \quad \mathcal{B}_x^{(a)} = \text{eigenbases of } X^{\otimes a}, \quad \mathcal{B}_y^{(a)} = \text{eigenbases of } Y^{\otimes a}$$

If  $|\Phi\rangle$  and  $|\psi\rangle$  are single qubit vectors from different Pauli eigenbases,  $|\langle\Phi|\psi\rangle|^2 = 1/\sqrt{2}$  and for tensor products across  $a$  qubits, the inner products factorize, so the magnitude becomes  $(1/\sqrt{2})^a = 1/\sqrt{2^a}$ . Thus these three bases MUB in  $2^a$ .

## Step 2: three MUBs from Odd dimensions, $d = m$ from $\{Z, X, XZ\}$

General Pauli operators (Weyl operators) on  $\mathbb{C}^d$ , We fix computational  $Z$  - basis  $\{|0\rangle, |1\rangle, \dots, |d-1\rangle\}$  with  $\langle j|l\rangle = \delta_{j,l}$  (Kronecker delta) and  $\omega = e^{2\pi i/d}$ .

$$Z|j\rangle = \omega^j|j\rangle \quad X|j\rangle = |(j+1) \bmod d\rangle$$

Two immediate facts:

1.  $Z$  is diagonal in the computational basis.
2.  $X$  is cyclic shift operator (unitary,  $X^d = I$ ), and  $XZ = \omega ZX$ .

### Phase operator $Z$

Its matrix form is  $Z = \text{diag}\{\omega^0, \omega^1, \dots, \omega^{d-1}\}$

Suppose  $d = 3$ , then  $Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}$

### Shift operator $X$

suppose  $d = 3$ , then  $X|0\rangle = |1\rangle$ ,  $X|1\rangle = |2\rangle$ ,  $X|2\rangle = |0\rangle$ .

$X = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$  For convenience the  $X$  matrix is often written as  $X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$

#### 2.0.1 $Z$ and $X$ are mutually Unbiased:

Fourier Vectors (i.e.  $X$ -eigenbasis)

$$|x_k\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \omega^{jk} |j\rangle$$

Compute  $\langle j|x_k\rangle$

$$\langle j|x_k\rangle = \langle j|\frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{lk} |l\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{jk} \langle j|l\rangle.$$

use orthonormality  $\langle j|l\rangle = \delta_{j,l}$  to pick out  $l = j$  term:

$$\langle j|x_k\rangle = \frac{1}{\sqrt{d}} \omega^{jk} = \frac{1}{\sqrt{d}}.$$

because  $|\omega^{jk}| = 1$ , its magnitude squared is

$$|\langle j|x_k\rangle|^2 = \frac{1}{d}.$$

the kronecker delta makes every term zero except when  $j = l$ , and the remaining term has unit modulus.

Similarly, it also works for reverse overlap:  $\langle x_{k'}|j\rangle = (\langle j|x_{k'}\rangle)^* = \frac{1}{\sqrt{d}} \omega^{-jk}$ . same magnitude  $1/\sqrt{d}$ .

**In terms of Matrices:** The  $d \times d$  Fourier matrix  $F$  columns are the  $X$ -eigenbasis, with entries  $F_{j,k} = \frac{1}{\sqrt{d}} \omega^{jk}$ . The vector  $|x_k\rangle$  is just the  $k$ -th column of  $F$ , so  $\langle j|x_k\rangle$  is the  $(j, k)$  entry of  $\frac{1}{\sqrt{d}} \omega^{jk}$ .

Suppose  $d = 3$ , then  $|x_0\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}$ ,  $|x_1\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix}$ ,  $|x_2\rangle = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 \\ \omega^2 \\ \omega \end{pmatrix}$ .

then e.g.  $\langle 2|x_1\rangle$  is the third component of  $|x_1\rangle$ , which is  $\langle 2|x_1\rangle = \frac{1}{\sqrt{3}}\omega^{2.1}$ , whose magnitude is  $1/\sqrt{3} \quad \forall \omega^2 = 1$ .

Hence  $Z$  and  $X$  are mutually unbiased.

### Third basis by diagonalizing $XZ$ (odd $d$ )

The trick is a quadratic phase (“Chirp”):

$$|u_k\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{rl^2+kl} |l\rangle, \quad k = 0, 1, \dots, d-1$$

Since  $d$  is odd, 2 has a multiplicative inverse modulo  $d$ . Choose  $r \in \{0, 1, \dots, d-1\}$  such that  $2r \equiv 1 \pmod{d}$ . Equivalently,  $r \equiv \frac{1}{2} \pmod{d}$ .

Quick examples:

$d = 3 : r = (3+1)/2 = 2$ . Check  $2 \cdot 2 = 4 \equiv 1 \pmod{3}$

$d = 5 : r = (5+1)/2 = 3$ . Check  $2 \cdot 3 = 6 \equiv 1 \pmod{5}$

$d = 7 : r = (7+1)/2 = 4$ . Check  $2 \cdot 4 = 8 \equiv 1 \pmod{7}$

These will be eigenvectors of  $XZ$ . Compute  $XZ|l\rangle = Z|l+1\rangle = \omega^{l+1}|l+1\rangle$ , then

$$\begin{aligned} XZ|u_k\rangle &= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{rl^2+kl} Z|l+1\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{rl^2+kl} \omega^{l+1} |l+1\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \omega^{r(m-1)^2+k(m-1)} \omega^m |m\rangle \quad \forall l = m-1, \\ &= \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \omega^{rm^2-2rm+r+km-k} \omega^m |m\rangle \\ &= \frac{1}{\sqrt{d}} \sum_{m=0}^{d-1} \omega^{rm^2+(k-2r+1)m+(r-k)} |m\rangle \end{aligned}$$

Because  $2r \equiv 1 \pmod{d}$ , the coefficient of  $m$  simplifies:  $-2r + k + 1 \equiv k \pmod{d}$ .

Hence

$$XZ|u_k\rangle = \omega^{r-k} \frac{1}{\sqrt{d}} \sum_m \omega^{rm^2+km} |m\rangle = \omega^{r-k} |u_k\rangle. \quad \forall \quad m \rightarrow l.$$

so  $|u_k\rangle$  is an eigenvector of  $XZ$ . Vectors  $\{|u_k\rangle\}_{k=0}^{d-1}$  form the eigenbasis.

### Unbiasedness of $Z$ - basis and $XZ$ - basis:

$$\langle j|u_k\rangle = \frac{1}{\sqrt{d}}\omega^{r+j^2+kj} \Rightarrow |\langle j|u_k\rangle| = \frac{1}{\sqrt{d}}\omega^{-jk} \quad \forall \omega^{-jk} = 1$$

### Unbiasedness of $X$ - basis and $XZ$ - basis:

$$X \text{ - bases are } |x_{k'}\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{lk'} |l\rangle$$

$$XZ \text{ - bases are } |u_k\rangle = \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{rl^2+kl} |l\rangle$$

$$\langle x_{k'}|u_k\rangle = \left\langle \left( \left| \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{lk'} |l\rangle \right\rangle \right) \left| \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{rl^2+kl} |l\rangle \right\rangle \right\rangle$$

$$\langle x_{k'}|u_k\rangle = \frac{1}{\sqrt{d}} \frac{1}{\sqrt{d}} \sum_{l=0}^{d-1} \omega^{(lk')+(rl^2+kl)}$$

$$\langle x_{k'}|u_k\rangle = \frac{1}{d} \sum_{l=0}^{d-1} \omega^{rl^2+(k-k')l}$$

Simplifying the power of  $\omega$  using completing the square technique:

$$rl^2 + (k - k')l = r \left( l + \frac{k - k'}{2r} \right)^2 - \frac{(k - k')^2}{4r}$$

so

$$\langle x_{k'}|u_k\rangle = \frac{\omega^{-\frac{(k-k')^2}{4r}}}{d} \sum_{j=0}^{d-1} \omega^{r \left( l + \frac{k-k'}{2r} \right)^2} = \frac{\omega^{-\frac{(k-k')^2}{4r}}}{d} \sum_{j=0}^{d-1} G(r; d)$$

where  $G(r; d) = \sum_{j=0}^{d-1} \omega^{rj^2}$  is a quadratic Gauss sum. For odd  $d$ , with  $\gcd(r,d)=1$ ,

$$|G(r; d)| = \sqrt{d}$$

Therefore

$$|\langle x_{k'}|u_k\rangle| = \left( \frac{|G(r; d)|}{d} \right) = \frac{1}{\sqrt{d}}$$

This proves that  $XZ$ -eigenbasis unbiased with the  $X$ -eigenbasis. Putting it all together, for odd  $d$ , the three bases  $Z$ -eigenbasis,  $X$ -eigenbasis, and  $XZ$ -eigenbasis are pairwise mutually unbiased.

**Step 3: Tensor-product lemma to combine even and odd parts  $\Rightarrow$  any  $d2^am$  (with  $m$  odd)**

Lemma (Tensor-product MUB):

If  $\{A\}_{i=0}^r$  are MUBs in dimension  $d_1$  and  $\{B\}_{i=0}^r$  are MUBs in dimension  $d_2$ , then  $\{A_i \otimes B_i\}_{i=0}^r$  are MUBs in dimension  $d_1 d_2$ .

**Proof of lemma:** Pick unit vectors  $a \in A_i, a' \in A_j$  and  $b \in B_i, b' \in B_j$ . Then

$$\langle a \otimes b | a' \otimes b' \rangle = \langle a | a' \rangle \langle b | b' \rangle = \frac{1}{\sqrt{d_1}} \cdot \frac{1}{\sqrt{d_2}} = \frac{1}{\sqrt{d_1 d_2}} \quad \forall i \neq j$$

Now we can write any dimension  $d$  as  $d = 2^a m$  (with  $m$  odd).

- Using step 1, to get three MUBs  $\{A_1, A_2, A_3\}$  in  $2^a$ .
- Using step 2, to get three MUBs  $\{B_1, B_2, B_3\}$  in  $m$ .
- Applying the tensor-product lemma, we get three MUBs  $\{A_i \otimes B_i\}_{i=1}^3$  in  $d = 2^a m$ .

□

# Bibliography

- [1] P. Horodecki, Ł. Rudnicki, and K. Życzkowski, “Five Open Problems in Quantum Information Theory,” *PRX Quantum*, vol. 3, no. 1, p. 10101, 2022, doi: 10.1103/PRXQuantum.3.010101.
- [2] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010. doi: 10.1017/cbo9780511976667.
- [3] W. K. Wootters and B. D. Fields, “Optimal state-determination by mutually unbiased measurements,” *Annals of Physics*, vol. 191, no. 2, pp. 363–381, 1989, doi: [https://doi.org/10.1016/0003-4916\(89\)90322-9](https://doi.org/10.1016/0003-4916(89)90322-9).
- [4] I. Ivanovic, “Geometrical description of quantal state determination,” *Journal of Physics A: Mathematical and General*, vol. 14, no. 12, p. 3241, 1981, doi: 10.1088/0305-4470/14/12/019.
- [5] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*, 2nd ed. Cambridge University Press, 2017.