Mutually Unbiased Bases

Abdul Fatah

Faculty of Engineering and Computing

July 2026

Ollscoil
Teicneolaíochta
an Atlantaigh

Atlantic
Technological
University

Table of Contents

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:

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

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

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

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

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:

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

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

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

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

Likewise, U_2 is mutually unbiased with U_1:

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

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

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

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

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

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

We can then derive the following equation:

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

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

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

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

$$|\psi\rangle = |0\rangle + i|1\rangle = |+i\rangle$$

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

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

Likewise:

$$|\psi\rangle = |0\rangle - i|1\rangle = |-i\rangle$$

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

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 $a = 0, 1, ..., d - 1$, 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:

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

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

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

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

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

Theorem 1.2.1.1 (At least three mutually unbiased bases): 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)

□

Bibliography

[1] P. Horodecki, Ł. Rudnicki, and K. \ifmmode \dot{Z}\else Ż\fi{}yczkowski, “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.