eman ta zabal zazu
Universidad del País Vasco
Euskal Herriko Unibertsitatea
ZIENTZIA ETA TEKNOLOGIA FAKULTATEA
FACULTAD DE CIENCIA Y TECNOLOGÍA

Bachelor's Thesis
Degree in Physics

The Mutually Unbiased Bases problem via the Bloch representation

Author:
Daniel Bedialauneta Rodríguez

Supervisors:
Jens Siewert

Leioa, 17th June 2021

CONTENTS

1. INTRODUCTION 1
1.1. Motivation and objectives of this thesis 1
1.2. Dirac notation and basic notions for finite dimensional Hilbert spaces 2
1.3. The Mutually Unbiased Bases problem 3
1.4. The qubit and the Bloch sphere 5
2. GENERAL PROPERTIES IN $\mathcal{H}_D$ 8
2.1. Properties of mutually unbiased bases and example for $d = 3$ 8
2.2. The Fourier basis 9
2.3. Properties of the Bloch representation 10
2.4. Orthogonality and mutual unbiasedness of Bloch vectors 12
3. MUB GENERATION IN PRIME DIMENSION 16
3.1. The Weyl basis 16
3.2. Computational and Fourier bases in terms of the Weyl basis 18
3.3. W matrix 21
3.4. Proof for the existence of $d + 1$ MUBs in prime dimension 24
3.5. Bloch vector structure 27
4. CONCLUSIONS 30
4.1. Future work 30
A. TRACE OF AN OUTER PRODUCT 31
B. COMMUTATION RELATIONS BETWEEN THE W MATRIX AND THE WEYL MATRICES $D_{J,K}$ 32
BIBLIOGRAPHY 34

1. INTRODUCTION

1.1. Motivation and objectives of this thesis

Since it appeared, quantum mechanics has allowed us to understand a very wide range of phenomena and has also proven successful in creating useful applications. Many of these stem from the field of solid-state physics, since it explains how semiconductors or magnetism in solids work on a fundamental level.

The very well-known transistor, for example, which usually serves as a switch or as an amplifier of electrical signals, is a semiconductor device whose design relies on the knowledge of the energy-bands of semiconductors. Without them, current microprocessors would not exist.

Other applications arise from the understanding of light-matter interactions or stimulated emission of light, which are also related to solid-state physics. For example, laser diodes are a semiconductor device which, when subjected to an electrical current, emit light of a certain wavelength. The wavelength of the coherently emitted light depends on the semiconductor material. Laser diodes are used as the sources of light in fiber optics communication.

How quantum mechanics has shed light on the theoretical grounds of these previously unexplained behaviours presented by nature is called by some authors the 'First Quantum Revolution'. This is in contrast to the 'Second Quantum Revolution' [1], which is now developing at a very fast rate, and which aims at engineering artificial systems that take advantage of purely quantum phenomena, such as superposition, entanglement, the uncertainty principle, etc. The Second Quantum Revolution usually refers to the emerging technologies in the fields of quantum computation, quantum metrology, quantum communication and quantum control, among others, all of which are backed up by Quantum Information Theory. Although Quantum Information Theory sets to studying the new ways of transmitting and processing information using Quantum Mechanics, it is also finding applications in describing entanglement in many-body physics.

Some of these fields, like quantum computation or quantum metrology appeared because of the advantages that quantum mechanics provides over their classical counterpart. As an example, we have Shor's algorithm that turns the problem of factoring any integer into its primes into a problem solvable in polynomial time, when using a quantum computer. Another example can be found in quantum cryptography, where cryptographic keys are 'provably immune to attack' [1], thanks to Heisenberg's uncertainty principle.

However, the underlying Quantum Information Theory is far from being complete and still poses open problems of diverse mathematical connections [2]. One of them is the Mutually Unbiased Bases problem, which will be the object of study in this thesis.

Although we will give formal definitions later, we say that two bases in a Hilbert space are mutually unbiased when the probability of transitioning from any vector of one basis to any vector of the other basis is the same independently from which two vectors we choose. Mutually unbiased bases generally play an important role when trying to find or hide information [3]. For example, mutually unbiased bases are useful in quantum cryptography in order to maximize the uncertainty relations that make these protocols safe [4]. Additionally, when trying to determine the full quantum state of a system, i.e, when performing quantum state tomography, one must perform a series of measurements where it is desirable to use mutually unbiased bases to minimize the statistical spread.

In short, mutually unbiased bases are a useful tool in Quantum Information Theory but, how many there exist in a certain Hilbert space is not fully known. In this thesis we would like to give an introduction to the Mutually Unbiased Bases problem in a different manner than usual. We will approach it via the Bloch representation, because it draws a more geometrical picture of the problem. Also, we will try to minimize the amount of mathematical background necessary to understand the problem, as it can get a bit complex in the existing literature. Finally, regarding content, we will limit ourselves to the study of some known results, that is, existence of mutually unbiased bases in a Hilbert space of prime dimension.

1.2. Dirac notation and basic notions for finite dimensional Hilbert spaces

In this section we will present the notation and basic properties that will be used throughout the entire thesis taking inspiration from the Lecture Notes on Quantum Computation by John Preskill [5].

A Hilbert space $\mathcal{H}$ is a vector space over the complex numbers $\mathbb{C}$ which also has an inner product that maps any two vectors to a complex number [6]. Let $|\psi\rangle$ denote a vector of the Hilbert space and $\langle\varphi|\psi\rangle$ the inner product.

The inner product satisfies the following properties

1) It is positive definite if the product is taken between one vector and itself

$$\langle\psi|\psi\rangle > 0, \quad \text{if } |\psi\rangle \neq 0.$$

2) It is linear in its second argument

$$\langle\varphi| (a\,|\psi_1\rangle + b\,|\psi_2\rangle) = a\,\langle\varphi|\psi\rangle + b\,\langle\varphi|\psi\rangle\,.$$

3) It is conjugate symmetric

$$\langle\varphi|\psi\rangle = \langle\psi|\varphi\rangle^* .$$

Combining the second and third properties we get

$$(a\langle\varphi_1| + b\langle\varphi_2|)|\psi\rangle = \Big(\langle\psi|(a|\varphi_1\rangle + b|\varphi_2\rangle)\Big)^* = \Big(a\langle\psi|\varphi_1\rangle + b\langle\psi|\varphi_2\rangle\Big)^* =$$

$$= a^*\langle\psi|\varphi_1\rangle^* + b^*\langle\psi|\varphi_2\rangle^* = a^*\langle\varphi_1|\psi\rangle + b^*\langle\varphi_2|\psi\rangle ,$$

that is, the inner product is antilinear in its first argument.

Finally, let me introduce the outer product $|\varphi\rangle\langle\Psi|$, which is an operator that acts on a vector in the following way

$$\Big(|\varphi\rangle\langle\Psi|\Big)|\phi\rangle = (\langle\Psi|\phi\rangle)|\varphi\rangle .$$

Therefore, the outer product $|\Psi\rangle\langle\Psi|$ between one normalized vector $|\Psi\rangle$ and itself is a projector because $\Big(|\Psi\rangle\langle\Psi|\Big)^2 = |\Psi\rangle\langle\Psi|$. To see this, first note that $\Big(|\Psi\rangle\langle\Psi|\Big)|\phi\rangle = \langle\Psi|\phi\rangle|\Psi\rangle$. Now, let $\Big(|\Psi\rangle\langle\Psi|\Big)^2$ act on the same vector $|\phi\rangle$:

$$\Big(|\Psi\rangle\langle\Psi|\Big)^2|\phi\rangle = \Big(|\Psi\rangle\langle\Psi|\Big)\Big(|\Psi\rangle\langle\Psi|\Big)|\phi\rangle = \langle\Psi|\phi\rangle\Big(|\Psi\rangle\langle\Psi|\Big)|\Psi\rangle = \langle\Psi|\phi\rangle\langle\Psi|\Psi\rangle|\Psi\rangle .$$

Since we defined $|\Psi\rangle$ as a normalized vector, that is, $\langle\Psi|\Psi\rangle = 1$, we obtain

$$\Big(|\Psi\rangle\langle\Psi|\Big)^2|\phi\rangle = \langle\Psi|\phi\rangle\langle\Psi|\Psi\rangle|\Psi\rangle = \langle\Psi|\phi\rangle|\Psi\rangle .$$

1.3. The Mutually Unbiased Bases problem

Definition 1.1. Let $|a\rangle$ and $|b\rangle$ be normalized vectors that belong to a d-dimensional Hilbert space $\mathcal{H}_d$. These two vectors are said to be mutually unbiased if

$$|\langle a|b\rangle|^2 = \frac{1}{d}.$$

Example 1.1. For example, imagine we have an orthonormal basis $\{|0\rangle, |1\rangle\}$ in $\mathcal{H}_2$. Then, the vectors $|0\rangle$ and $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ are mutually unbiased because

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

whose norm squared is $1/2$.

Example 1.2. Now, for a not so trivial example, take the vectors $\frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $\frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle)$. They are mutually unbiased because

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

whose norm squared is $1/2$.

We can extend the definition of mutual unbiasedness to bases.

Definition 1.2. Let $\mathcal{B}_1 = \left\{ |a_i\rangle \right\}_{i=0}^{d-1}$ and $\mathcal{B}_2 = \left\{ |b_i\rangle \right\}_{i=0}^{d-1}$ be two orthonormal bases, we say that they are mutually unbiased if any two vectors belonging to a different basis each are mutually unbiased. This can also be expressed mathematically as

$$\left|\langle a_i|b_j\rangle\right|^2 = \frac{1}{d}, \quad \forall i, j = 0, 1, ..., d-1.$$

It can be easily checked that the bases $\left\{ |0\rangle, |1\rangle \right\}$ and $\left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}$ are mutually unbiased.

Definition 1.3. Moreover, we say that a set $\left\{ \mathcal{B}_1, \mathcal{B}_2, ..., \mathcal{B}_n \right\}$ of n orthonormal bases is mutually unbiased if every possible pair of bases within the set is mutually unbiased.

Continuing with the example in $d = 2$, the set of three orthonormal bases

$$\mathcal{B}_0 = \left\{ |0\rangle, |1\rangle \right\}, \quad \mathcal{B}_1 = \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\},$$

$$\mathcal{B}_2 = \left\{ \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right\}, \tag{1.1}$$

is mutually unbiased.

In fact, it can be proven [7] that, in $d = 2$, one cannot construct a mutually unbiased set of more than 3 bases.

The problem of mutually unbiased bases is concerned with how big you can make a mutually unbiased set of bases in any dimension d, or how it is usually put: how many mutually unbiased bases there are in dimension d.

It is a well-known result that for any dimension d, there exist, at most, $d + 1$ mutually unbiased bases. It is also known that when d is a prime or a power of a prime number ($d = p^k$, for $k \in \mathbb{N}$), $d + 1$ mutually unbiased bases do exist [8]. However, for composite dimensions ($d = 6, 10, 12, ...$) it is not known how many there actually are.

Due to other limiting bounds on the number of mutually unbiased bases, in $d = 6$ there are at least 3 mutually unbiased bases, but no more have been found. It is a conjecture that there only exist 3 mutually unbiased bases in $d = 6$, and finding a correct answer which proves or disproves it is rewarded with the Golden KCIK award [2].

From now on, MUB will stand for mutually unbiased basis.

1.4. The qubit and the Bloch sphere

In $d = 2$, any vector can be written as

$$|\Psi\rangle = a\,|0\rangle + b\,|1\rangle\,, \tag{1.2}$$

where $\left\{|0\rangle, |1\rangle\right\}$ is an orthonormal basis, usually called the computational basis, and $a, b \in \mathbb{C}$.

However, for the vector in (1.2) to represent a physical state it must be normalized, that is, it must satisfy $|a|^2 + |b|^2 = 1$. Let $a = |a|e^{i\varphi_a}$ and $b = |b|e^{i\varphi_b}$, we can rewrite the vector as

$$|\Psi\rangle = e^{i\varphi_a}\Big(|a|\,|0\rangle + |b|e^{i(\varphi_b-\varphi_a)}\,|1\rangle\Big) = e^{i\varphi_a}\Big(|a|\,|0\rangle + e^{i(\varphi_b-\varphi_a)}\sqrt{1-|a|^2}\,|1\rangle\Big).$$

Vectors that differ only by a nonzero complex scalar represent the same physical state. We can then get rid of the $e^{i\varphi_a}$ factor, and by defining $\varphi \equiv \varphi_b - \varphi_a$, we rewrite the state as

$$|\Psi\rangle = |a|\,|0\rangle + e^{i\varphi}\sqrt{1-|a|^2}\,|1\rangle\,.$$

Since $0 \leq |a|^2 \leq 1$, we let $|a| = \cos\frac{\theta}{2}$, with $\theta \in [0, \pi]$ and obtain

$$|\Psi\rangle = \cos\frac{\theta}{2}\,|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}\,|1\rangle\,, \tag{1.3}$$

with $\varphi \in [0, 2\pi]$. Therefore, any quantum state in $d = 2$ can be described by two real parameters $\theta \in [0, \pi]$ and $\varphi \in [0, 2\pi]$. This naturally spans the surface of a sphere with unit radius, which we call the Bloch sphere, Figure 1.1. In the previous section, we pre-

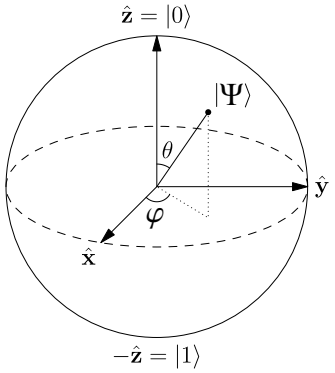

Figure 1.1: Bloch sphere.

sented all mutually unbiased bases in $d = 2$ (Equation (1.1)). By comparing with (1.3), we see that the vectors in $\mathcal{B}_0$ correspond to $\theta = 0$ and $\theta = \pi$, the vectors in $\mathcal{B}_1$ correspond to $(\theta = \pi/2, \varphi = 0)$ and $(\theta = \pi/2, \varphi = \pi)$ and the vectors in $\mathcal{B}_2$ correspond to $(\theta = \pi/2, \varphi = \pi/2)$ and $(\theta = \pi/2, \varphi = 3\pi/2)$. By looking at the Bloch sphere in Figure 1.1, we see that each basis is associated to one of the axes in the sphere, and each vector inside the basis corresponds with one of the ends of the axis.

Note how orthogonal vectors of the same basis belong to the same axis in the Bloch sphere, whereas mutually unbiased vectors from different bases belong to orthogonal axes in the Bloch sphere. In the next chapter we will prove how the Bloch-subspaces spanned by two MUBs are orthogonal for any d.

Let me now introduce another way to arrive at the Bloch picture which will prove useful for the rest of this thesis. For this purpose, we are going to work with projectors instead of kets.

Using the same vector from Equation (1.2), its projector has the following matrix representation

$$|\Psi\rangle\langle\Psi| = \Big(a\,|0\rangle + b\,|1\rangle\Big)\Big(a^*\langle 0| + b^*\langle 1|\Big) = |a|^2\,|0\rangle\langle 0| + ab^*\,|0\rangle\langle 1| + a^*b\,|1\rangle\langle 0| + |b|^2\,|1\rangle\langle 1| =$$

$$= \begin{bmatrix} |a|^2 & ab^* \\ a^*b & |b|^2 \end{bmatrix}.$$

Since for $|\Psi\rangle$ to represent a real physical state it must be normalized, that is, $|a|^2 + |b|^2 = 1$, the trace of the projector satisfies

$$\mathrm{Tr}\Big(\,|\Psi\rangle\langle\Psi|\,\Big) = |a|^2 + |b|^2 = 1.$$

We are now concerned with finding a basis of operators (or a basis of matrices) in terms of which we can express the projector $|\Psi\rangle\langle\Psi|$. One such basis is, of course,

$$|0\rangle\langle 0| = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}, \quad |0\rangle\langle 1| = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad |1\rangle\langle 0| = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}, \quad |1\rangle\langle 1| = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}, \tag{1.4}$$

which we already used. Note how the dimension of the basis has to be 4 in order to describe a general operator in $d = 2$. For any d, the dimension of any vector basis is d, while the dimensions of any operator basis is d^2.

However, to arrive at the Bloch sphere we should use the three Pauli matrices and the identity matrix

$$\sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_0 \equiv \mathbb{1} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},$$

which are all hermitian, unitary and satisfy the following orthogonality condition

$$\mathrm{Tr}\left(\sigma_i^\dagger \sigma_j\right) = 2\delta_{ij}. \tag{1.5}$$

Notice that out of these four matrices, only the identity matrix has nonzero trace: $\mathrm{Tr}\,\mathbb{1} = 2$. This suggests that any projector $|\Psi\rangle\langle\Psi|$ can be cast into the following form

$$|\Psi\rangle\langle\Psi| = \frac{1}{2}\Big(\mathbb{1} + r_x\sigma_x + r_y\sigma_y + r_z\sigma_z\Big), \tag{1.6}$$

in order to satisfy the unit trace of $|\Psi\rangle\langle\Psi|$. The vector of coefficients (r_x, r_y, r_z) associated to the Pauli matrices is called Bloch vector. Following from the orthogonality condition (1.5), the Bloch coordinates are given by

$$r_i = \mathrm{Tr}\Big(\sigma_i^\dagger |\Psi\rangle\langle\Psi|\Big). \tag{1.7}$$

It can be proven (see Section 2.4) that the magnitude of the Bloch vector (in $d = 2$) is unity, so it naturally spans the surface of a unit sphere.

For example, it is easy to see that the projector $|0\rangle\langle 0|$ is given by

$$|0\rangle\langle 0| = \frac{1}{2}\Big(\mathbb{1} + \sigma_z\Big),$$

which corresponds to a $(0, 0, 1)$ Bloch vector, whereas the $|1\rangle\langle 1|$ projector gives the $(0, 0, -1)$ Bloch vector

$$|1\rangle\langle 1| = \frac{1}{2}\Big(\mathbb{1} - \sigma_z\Big).$$

For a more 'complex' example, the projector associated to the state $\frac{1}{\sqrt{2}}\Big(|0\rangle - i|1\rangle\Big)$ can be expressed in terms of the four matrices as follows

$$\left[\frac{1}{\sqrt{2}}\Big(|0\rangle - i|1\rangle\Big)\right]\left[\frac{1}{\sqrt{2}}\Big(\langle 0| + i\langle 1|\Big)\right] = \begin{bmatrix} \frac{1}{2} & \frac{i}{2} \\ -\frac{i}{2} & \frac{1}{2} \end{bmatrix} = \frac{1}{2}\Big(\mathbb{1} - \sigma_y\Big),$$

which corresponds to a $(0, -1, 0)$ Bloch vector.

As a result, we obtain the same Bloch sphere representation from Figure 1.1. Although the two representations of the Bloch sphere that we have used, (1.3) and (1.6), might seem somewhat redundant, this is only the case for $d = 2$. When one goes to higher dimensions, the representation of MUBs via Bloch vectors becomes geometrically appealing because of the fact that Bloch vectors that belong to different MUBs are orthogonal. This result will also be demonstrated in the next chapter.

2. GENERAL PROPERTIES IN $\mathcal{H}_D$

2.1. Properties of mutually unbiased bases and example for $d = 3$

In the previous chapter, we saw how some geometrical properties arise in relation to mutual unbiasedness. We will now give all the mutually unbiased bases in $d = 3$ so that they will serve as examples throughout the chapter.

For visualization purposes, we will represent each basis in $d \times d$ matrix form, where the elements of each column are the coordinates of each vector of the basis (in terms of the computational basis). So, for example, the $\mathcal{B}_1$ basis in (1.1) can be written as

$$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}.$$

The first basis of any set of mutually unbiased bases can always be taken to be the computational basis $\{|j\rangle\}_{j=0}^{d-1}$ which, in matrix form, is written as the identity

$$\mathcal{B}_0 = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix}.$$

Now, for any vector $|\varphi\rangle = \sum_{j=0}^{d-1} c_j |j\rangle$ to be mutually unbiased to $\mathcal{B}_0$ it must satisfy

$$|\langle j|\varphi\rangle| = \left|c_j\right| = \frac{1}{\sqrt{d}}, \qquad j = 0, 1, ..., d-1, \tag{2.1}$$

which means that the coefficients' modulus are completely determined and only the phases θ_j such that

$$|\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{i\theta_j} |j\rangle, \tag{2.2}$$

are left to be specified in order to build the rest of the MU bases.

As we said in Section 1.3, there exist $d + 1$ mutually unbiased bases in prime dimensions. Since $d = 3$ is prime, we will have 4 mutually unbiased bases, of which we take the computational basis $\{|0\rangle, |1\rangle, |2\rangle\}$ as the first one

$$\mathcal{B}_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

The remaining three bases are

$$\mathcal{B}_1 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \quad \mathcal{B}_2 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{bmatrix}, \quad \mathcal{B}_3 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{bmatrix}, \tag{2.3}$$

where $\omega \equiv e^{2\pi i/d}$, and here $d = 3$. We will denote $|i\rangle_j$ the i-th vector of the j-th mutually unbiased basis, where $i = 0, ..., d-1$ and $j = 0, ..., d$.

A couple of things are worth noting here. Firstly, all bases are orthonormal, and all elements are nonzero and of modulus $1/\sqrt{d}$ in accordance with (2.1). Also, the phase θ_0 of every vector (first element of each column) can always be taken to be zero. Finally, all phases of the first vector of the second basis, $\mathcal{B}_1$, can be chosen to be zero. These impositions hold for any dimension d and not only $d = 3$ (see for example (1.1)).

These degrees of freedom come from how we define two sets of MUBs to be equivalent [7][1]. For example, that all θ_0 can be set to zero is a consequence of the fact that any two vectors $|\varphi_1\rangle$, $|\varphi_2\rangle$, that are mutually unbiased (or orthogonal),

$$|\langle\varphi_1|\varphi_2\rangle| = \frac{1}{\sqrt{d}},$$

will still be mutually unbiased (or orthogonal) if they are multiplied by arbitrary phase factors $e^{i\alpha_1}$, $e^{i\alpha_2}$, respectively

$$\left|\langle e^{i\alpha_1}\varphi_1|e^{i\alpha_2}\varphi_2\rangle\right| = \left|e^{i(\alpha_2-\alpha_1)}\right||\langle\varphi_1|\varphi_2\rangle| = |\langle\varphi_1|\varphi_2\rangle| = \frac{1}{\sqrt{d}}.$$

Therefore, we can factor a global phase out of each vector so that the first coefficients are simply $1/\sqrt{d}$.

2.2. The Fourier basis

The Fourier basis is a simple orthonormal basis that is mutually unbiased to the computational basis for any dimension d. Using the notation established in the previous section, it is given by

$$\mathcal{F} = \frac{1}{\sqrt{d}}\begin{bmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \dots & \omega^{d-1} \\ 1 & \omega^2 & \omega^4 & \omega^6 & \dots & \omega^{2(d-1)} \\ 1 & \omega^3 & \omega^6 & \omega^9 & \dots & \omega^{3(d-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \omega^{d-1} & \omega^{2(d-1)} & \omega^{3(d-1)} & \dots & \omega^{(d-1)(d-1)} \end{bmatrix}, \tag{2.4}$$

where $\omega \equiv e^{2\pi i/d}$. This gives the same basis $\mathcal{B}_1$ from (2.3) for $d = 3$ by noting that $\omega^p = \omega^{p \bmod d}$ with p an integer.

We can write each state individually as

$$|f_i\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{ik}|k\rangle\,. \tag{2.5}$$

[1] Appendix A.

From (2.1), it is obvious that the Fourier basis $\mathcal{F}$ is mutually unbiased to the computational basis. It only remains then to prove that $\mathcal{F}$ is, in fact, orthonormal.

$$\langle f_i|f_j\rangle = \frac{1}{d}\sum_{k=0}^{d-1}\sum_{k'=0}^{d-1}\omega^{-ik}\omega^{jk'}\langle k|k'\rangle\,.$$

Since $\langle k|k'\rangle = \delta_{k,k'}$ we get

$$\langle f_i|f_j\rangle = \frac{1}{d}\sum_{k=0}^{d-1}(\omega^{j-i})^k.$$

If $j = i$, then the sum gives d and we obtain

$$\langle f_i|f_j\rangle = 1.$$

On the other hand, if $i \neq j$, the sum is a geometric progression whose solution is

$$\langle f_i|f_j\rangle = \frac{1}{d}\frac{1-(\omega^{j-i})^d}{1-\omega^{j-i}} = 0,$$

because $\omega^{(i-j)d} = 1$ for any i, j and the numerator cancels. Therefore,

$$\langle f_i|f_j\rangle = \delta_{i,j}.$$

2.3. Properties of the Bloch representation

In the previous chapter we saw how a general projector $|\Psi\rangle\langle\Psi|$ in $d = 2$ can be written in terms of an operator basis (1.6), which in a general dimension d takes the form

$$|\Psi\rangle\langle\Psi| = \frac{1}{d}\Big(\mathbb{1} + \sum_{i=1}^{d^2-1} r_i\lambda_i\Big), \tag{2.6}$$

where the λ_i, $i = 1, ..., d^2 - 1$, are traceless operators (or matrices) which, together with the identity ($\mathrm{Tr}\,\mathbb{1} = d$), form a basis of dimension d^2. One could also denote $\lambda_0 \equiv \mathbb{1}$ with $r_0 = 1$, but we will not do this for now.

We also derived an expression for the coordinates of the associated Bloch vector (1.7), and in a general dimension d this takes the same form

$$r_i = \mathrm{Tr}\left(\lambda_i^\dagger|\Psi\rangle\langle\Psi|\right), \tag{2.7}$$

where we have assumed the orthogonality condition

$$\mathrm{Tr}\left(\lambda_i^\dagger\lambda_j\right) = d\delta_{ij}. \tag{2.8}$$

Finally, we define the vector $(r_1, ..., r_{d^2-1})$ as the Bloch vector of $|\Psi\rangle\langle\Psi|$ in terms of the λ_i, $i = 1, ..., d^2 - 1$.

Example 2.1. The generalized Gell-Mann matrices [9] are a set of $d^2 - 1$ traceless and hermitian matrices which satisfy the orthogonality condition (2.8). In $d = 3$ they are given by

$$X_{01} = \sqrt{\frac{3}{2}}\begin{bmatrix}0 & 1 & 0\\ 1 & 0 & 0\\ 0 & 0 & 0\end{bmatrix}, \quad X_{02} = \sqrt{\frac{3}{2}}\begin{bmatrix}0 & 0 & 1\\ 0 & 0 & 0\\ 1 & 0 & 0\end{bmatrix}, \quad X_{12} = \sqrt{\frac{3}{2}}\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & 1\\ 0 & 1 & 0\end{bmatrix},$$

$$Y_{01} = \sqrt{\frac{3}{2}}\begin{bmatrix}0 & -i & 0\\ i & 0 & 0\\ 0 & 0 & 0\end{bmatrix}, \quad Y_{02} = \sqrt{\frac{3}{2}}\begin{bmatrix}0 & 0 & -i\\ 0 & 0 & 0\\ i & 0 & 0\end{bmatrix}, \quad Y_{12} = \sqrt{\frac{3}{2}}\begin{bmatrix}0 & 0 & 0\\ 0 & 0 & -i\\ 0 & i & 0\end{bmatrix},$$

$$Z_1 = \sqrt{\frac{3}{2}}\begin{bmatrix}1 & 0 & 0\\ 0 & -1 & 0\\ 0 & 0 & 0\end{bmatrix}, \quad Z_2 = \sqrt{\frac{1}{2}}\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & -2\end{bmatrix}.$$

Taking these matrices together with the identity $\mathbb{1}$, we obtain a matrix basis of dimensions 3×3.

Let us take the state $|1\rangle$ from the computational basis. Its projector in matrix form is given by

$$|1\rangle\langle 1| = \begin{bmatrix}0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{bmatrix}$$

This matrix can be written in terms of $\mathbb{1}$ and the generalized Gell-Mann matrices as

$$|1\rangle\langle 1| = \begin{bmatrix}0 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 0\end{bmatrix} = \frac{1}{3}\Big(\mathbb{1} - \sqrt{\frac{3}{2}}Z_1 + \frac{1}{\sqrt{2}}Z_2\Big),$$

with Bloch vector $\big(0, 0, 0, 0, 0, 0, -\sqrt{\frac{3}{2}}, \frac{1}{\sqrt{2}}\big)$.

Alternatively, let us consider the state $|1\rangle_3$ from (2.3). Its projector takes the following matrix form

$${}_3|1\rangle_3\,{}_3\langle 1| = \frac{1}{3}\Big(|0\rangle + \omega|1\rangle + |2\rangle\Big)\Big(\langle 0| + \omega^*\langle 1| + \langle 2|\Big) = \frac{1}{3}\begin{bmatrix}1 & \omega^* & 1\\ \omega & 1 & \omega\\ 1 & \omega^* & 1\end{bmatrix}.$$

This matrix can be written as the following linear combination

$${}_3|1\rangle_3\,{}_3\langle 1| = \frac{1}{3}\Big(\mathbb{1} - \frac{1}{\sqrt{6}}X_{01} + \sqrt{\frac{2}{3}}X_{02} - \frac{1}{\sqrt{6}}X_{12} + \frac{1}{\sqrt{2}}Y_{01} - \frac{1}{\sqrt{2}}Y_{12}\Big),$$

with Bloch vector $\big(-\frac{1}{\sqrt{6}}, \sqrt{\frac{2}{3}}, -\frac{1}{\sqrt{6}}, \frac{1}{\sqrt{2}}, 0, -\frac{1}{\sqrt{2}}, 0, 0\big)$.

The Bloch vectors of $|1\rangle$ and $|1\rangle_3$ are obviously orthogonal.

Consider a state $|i\rangle$ from the computational basis, then the matrix form of its projector $|i\rangle\langle i|$ is all zeros but a one in the i-th position of the diagonal (as seen in Example 2.1). Therefore, the projector can be written as a linear combination of d diagonal matrices.

In contrast, let $|\varphi\rangle$ be mutually unbiased to the computational basis, then it can be written as in (2.2). The projector of such a state is

$$|\varphi\rangle\langle\varphi| = \frac{1}{d}\left(\sum_{i=0}^{d-1}\sum_{j=0}^{d-1} e^{i(\theta_i-\theta_j)}|i\rangle\langle j|\right),$$

which can be separated into two different sums: one of projectors $|i\rangle\langle i|$ and another one of outer products $|i\rangle\langle j|$, with $i \neq j$

$$|\varphi\rangle\langle\varphi| = \frac{1}{d}\left(\sum_{i=0}^{d-1}|i\rangle\langle i| + \sum_{\substack{i,j\\ i\neq j}} e^{i(\theta_i-\theta_j)}|i\rangle\langle j|\right).$$

The first term is precisely the identity matrix, because of the completeness relation, so we end up with

$$|\varphi\rangle\langle\varphi| = \frac{1}{d}\left(\mathbb{1} + \sum_{\substack{i,j\\ i\neq j}} e^{i(\theta_i-\theta_j)}|i\rangle\langle j|\right).$$

The second term, on the other hand, is made up of matrices with zero diagonal (see, for example, Equation (1.4)).

Therefore, any state $|\varphi\rangle$ that is mutually unbiased to the computational basis, its projector (or, rather, its Bloch vector) can be written in terms of matrices with zero diagonal (with the exception of the identity matrix, of course). We already saw an example of this in Example 2.1, where the Bloch vector of the projector $|1\rangle_3\,{}_3\langle 1|$ is written as a linear combination of matrices with zero diagonal.

As a consequence, even though there are many possible bases $\{\mathbb{1}, \lambda_1, ..., \lambda_{d^2-1}\}$ in terms of which we can write projectors, for convenience we will work with bases that can be divided into matrices with nonzero diagonal, to describe projectors of the computational basis; and matrices with zero diagonal, to describe projectors that are unbiased to the computational basis. Specifically, there will be d diagonal matrices including the identity to span the whole diagonal, and $d^2 - d$ matrices with zero diagonal.

2.4. Orthogonality and mutual unbiasedness of Bloch vectors

In this section we are going to show what is the connection between two Bloch vectors associated to different projectors, by means of its dot product.

Let $\rho_1 = |\varphi_1\rangle\langle\varphi_1|$ and $\rho_2 = |\varphi_2\rangle\langle\varphi_2|$ be two projectors that can be written in terms of the $\{\mathbb{1}, \lambda_1, ..., \lambda_{d^2-1}\}$ basis as

$$\rho_1 = |\varphi_1\rangle\langle\varphi_1| = \frac{1}{d}\Big(\mathbb{1} + \sum_{i=1}^{d^2-1} r_{1i}\lambda_i\Big),$$

$$\rho_2 = |\varphi_2\rangle\langle\varphi_2| = \frac{1}{d}\Big(\mathbb{1} + \sum_{j=1}^{d^2-1} r_{2j}\lambda_j\Big),$$

where the r_{1i} and the r_{2j} are complex numbers.

Even though any projector is hermitian, that is, $\Big(|\Psi\rangle\langle\Psi|\Big)^\dagger = |\Psi\rangle\langle\Psi|$, we can still write

$$\rho_1^\dagger = \Big(|\varphi_1\rangle\langle\varphi_1|\Big)^\dagger = \frac{1}{d}\Big(\mathbb{1} + \sum_{i=1}^{d^2-1} r_{1i}^*\lambda_i^\dagger\Big).$$

Therefore, the operator $\rho_1^\dagger\rho_2$ is

$$\rho_1^\dagger\rho_2 = \frac{1}{d^2}\Big(\mathbb{1} + \sum_{i=1}^{d^2-1} r_{1i}^*\lambda_i^\dagger + \sum_{j=1}^{d^2-1} r_{2j}\lambda_j + \sum_{i,j} r_{1i}^* r_{2j}\lambda_i^\dagger\lambda_j\Big).$$

We now take the trace of this expression and obtain

$$\mathrm{Tr}\,(\rho_1^\dagger\rho_2) = \frac{1}{d^2}\Big(d + \sum_{i,j} r_{1i}^* r_{2j}\,\mathrm{Tr}\,\Big(\lambda_i^\dagger\lambda_j\Big)\Big),$$

where we have used the fact that the trace is a linear operator, that is,

$$\mathrm{Tr}\,(A + B) = \mathrm{Tr}\,A + \mathrm{Tr}\,B, \qquad \mathrm{Tr}\,(cA) = c\,\mathrm{Tr}\,A,$$

for any square matrix A and B and any scalar c, and that the trace of each element of the basis is

$$\mathrm{Tr}\,\mathbb{1} = d, \qquad \mathrm{Tr}\,\lambda_i = \mathrm{Tr}\,\lambda_i^\dagger = 0, \quad i = 1, ..., d^2 - 1.$$

Finally, using the orthogonality condition $\mathrm{Tr}\,(\lambda_i^\dagger\lambda_j) = d\delta_{ij}$ we obtain

$$\mathrm{Tr}\,(\rho_1^\dagger\rho_2) = \frac{1}{d}\Big(1 + \sum_{i=1}^{d^2-1} r_{1i}^* r_{2i}\Big).$$

Notice that the sum is actually the scalar product between the Bloch vectors of the two projectors. Let $\vec{P}_1 = (r_{11}, ..., r_{1,d^2-1})$ and $\vec{P}_2 = (r_{21}, ..., r_{2,d^2-1})$, then we have

$$\mathrm{Tr}\,(\rho_1^\dagger\rho_2) = \frac{1}{d}\Big(1 + \vec{P}_1^* \cdot \vec{P}_2\Big).$$

On the other hand, the trace of two projectors is

$$\mathrm{Tr}\,(\rho_1^\dagger\rho_2) = \mathrm{Tr}\Big(|\varphi_1\rangle\langle\varphi_1|\varphi_2\rangle\langle\varphi_2|\Big) = \langle\varphi_1|\varphi_2\rangle\,\mathrm{Tr}\,|\varphi_1\rangle\langle\varphi_2|.$$

Since $\mathrm{Tr}\,|\varphi_1\rangle\langle\varphi_2| = \langle\varphi_2|\varphi_1\rangle$ (see Appendix A), we have

$$\mathrm{Tr}\,(\rho_1^\dagger \rho_2) = |\langle\varphi_1|\varphi_2\rangle|^2.$$

We can now relate the two expressions obtained for $\mathrm{Tr}\,(\rho_1^\dagger \rho_2)$

$$|\langle\varphi_1|\varphi_2\rangle|^2 = \frac{1}{d}\Big(1 + \vec{P}_1^{\,*} \cdot \vec{P}_2\Big).$$

If $|\varphi_1\rangle = |\varphi_2\rangle$ the inner product $|\langle\varphi_1|\varphi_2\rangle|^2$ is one and we obtain the modulus of the Bloch vector

$$|\vec{P}|^2 = d - 1. \tag{2.9}$$

If $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are orthogonal then $\langle\varphi_1|\varphi_2\rangle = 0$ and we have

$$\vec{P}_1^{\,*} \cdot \vec{P}_2 = -1. \tag{2.10}$$

Since $\vec{P}_1^{\,*} \cdot \vec{P}_2 = |\vec{P}_1^{\,*}||\vec{P}_2| \cos\theta$ and both Bloch vectors have modulus $\sqrt{d-1}$, then

$$\cos\theta = -\frac{1}{d-1}. \tag{2.11}$$

Finally, if $|\varphi_1\rangle$ and $|\varphi_2\rangle$ are mutually unbiased, then $|\langle\varphi_1|\varphi_2\rangle|^2 = 1/d$, so

$$\vec{P}_1^{\,*} \cdot \vec{P}_2 = 0. \tag{2.12}$$

This last equation proves the result we have encountered previously that the Bloch vectors associated to two mutually unbiased states are orthogonal.

More generally, any mutually unbiased basis has a set of Bloch vectors that span a 'Bloch subspace' which is orthogonal to the 'Bloch subspace' of any other mutually unbiased basis.

Additionally, from Equation (2.11) we have that the projection of a Bloch vector onto any other Bloch vector from the same Bloch subspace is constant.

Example 2.2. From Equation (2.11), we get that in $d = 2$ the angle between Bloch vectors belonging to the same mutually unbiased basis is $\cos\theta = -1 \rightarrow \theta = \pi$. We already saw this in Section (1.4), where each mutually unbiased basis corresponded to an axis in the Bloch sphere, and the two ends of each axis represented the states that make up the basis. The Bloch subspace is a line.

In $d = 3$, we get that $\cos\theta = -1/2$, so $\theta = 2\pi/3$. Since each mutually unbiased basis contains 3 Bloch vectors and 3 vectors that are separated by an angle $2\pi/3$ must be in the same plane (see Figure 2.1), the Bloch subspaces are planes. Although we cannot draw any Bloch sphere equivalent for $d = 3$ because the dimension of the Bloch vector[2] is $d^2 - 1 = 8$, knowing that the set of $d + 1 = 4$ MUBs results in 4 planes perpendicular to each other makes it 'easier' to picture.

[2]Note that in $d = 2$, the dimension of the Bloch vector is $d^2 - 1 = 3$, so we can draw a Bloch sphere.

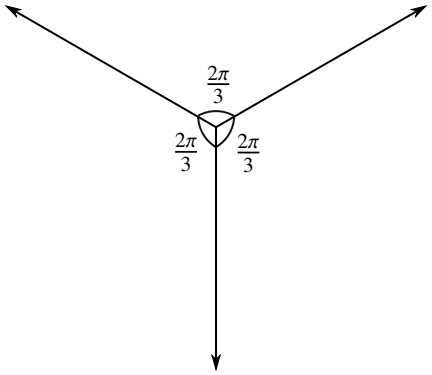

Figure 2.1: Bloch vectors from a Bloch subspace in $d = 3$.

At this point, we can give a sense of why in any dimension d the maximum possible number of MUBs is $d + 1$.[3] As we saw in Example 2.2, although each MUB gives d Bloch vectors, the Bloch subspace spanned by these is of dimension $d-1$. The dimension of the total Bloch space is $d^2 - 1 = (d + 1)(d - 1)$, and since these Bloch subspaces are all orthogonal to each other, the total Bloch space can contain $d+1$ such subspaces at most.

In order to obtain a rigorous proof, we would have to show that Bloch subspaces are indeed of dimension $d - 1$, but we will not do this here. It is not complicated to show that one of these d Bloch vectors can be written as a linear combination of the rest. In fact, let $\{\vec{P}_0, \vec{P}_1, P_2, ..., \vec{P}_{d-1}\}$ be the set of d Bloch vectors associated to one of the MUBs, then the vector $\vec{P}_0$ can be written as the linear combination

$$\vec{P}_0 = -\sum_{i=1}^{d-1} \vec{P}_i,$$

and it is easy to see that it satisfies conditions (2.9) and (2.10), so the Bloch subspace is at most of dimension $d - 1$.

[3] Which is not to say that these MUBs exist.

3. MUB GENERATION IN PRIME DIMENSION

3.1. The Weyl basis

In Example 2.1, we saw one possible basis in terms of which to write Bloch vectors, the generalized Gell-Mann basis. There is another basis, the Weyl basis [3], that gives Bloch vectors a nice structure in prime dimensions.

The Weyl basis is constructed from two operators Z and X that act on the computational basis in the following way

$$Z\,|j\rangle = \omega^j\,|j\rangle\,, \qquad X\,|j\rangle = |j+1 \mod d\rangle\,, \qquad j = 0, ..., d-1,$$

where $\omega \equiv e^{2\pi i/d}$ (in this definition of ω, the number i is the imaginary unit). In other words, X is a circular shifting operator and Z is diagonal in the computational basis. Also, the action of Z^k and X^k on the computational basis is

$$Z^k\,|j\rangle = \omega^{jk}\,|j\rangle\,, \qquad X^k\,|j\rangle = |j+k \mod d\rangle\,, \qquad j = 0, ..., d-1, \tag{3.1}$$

where k is any integer, positive or negative. Notice that (3.1) gives the inverses of Z and X if $k = -1$.

Since $\omega^{jd} = 1$ and $(j + d \mod d) = j$, from (3.1) we have that

$$Z^d = X^d = \mathbb{1}. \tag{3.2}$$

These operators can be defined without acting on any state as follows

$$Z^k = \sum_{j=0}^{d-1} \omega^{jk}\,|j\rangle\langle j|\,, \qquad X^k = \sum_{j=0}^{d-1} |j+k \mod d\rangle\langle j|\,. \tag{3.3}$$

The operators Z^k and X^k for any integer k are unitary, that is

$$(Z^k)^\dagger = Z^{-k}, \qquad (X^k)^\dagger = X^{-k}.$$

This is easy to see from (3.3) by noting that $\left(\,|a\rangle\langle b|\,\right)^\dagger = |b\rangle\langle a|$.

Finally, the commutation relation between Z and X is

$$ZX = \omega XZ,$$

from which we get the more general relation

$$Z^jX^k = \omega^{jk}X^kZ^j. \tag{3.4}$$

Example 3.1. Here we show the matrix form of some operators Z^k and X^k in $d = 5$.

$$Z = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega^2 & 0 & 0 \\ 0 & 0 & 0 & \omega^3 & 0 \\ 0 & 0 & 0 & 0 & \omega^4 \end{bmatrix}, \qquad X^0 = \mathbb{1} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix},$$

$$X^1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix}, \qquad X^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix},$$

$$X^3 = X^{-2} = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \end{bmatrix}, \qquad X^4 = X^{-1} = \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{bmatrix},$$

$$ZX^2 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & \omega \\ \omega^2 & 0 & 0 & 0 & 0 \\ 0 & \omega^3 & 0 & 0 & 0 \\ 0 & 0 & \omega^4 & 0 & 0 \end{bmatrix}, \qquad X^0 + X^1 + X^2 + X^3 + X^4 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

The Weyl basis is the set of d^2 operators $D_{j,k}$, with $j, k = 0, ..., d-1$, where each operator is given by

$$D_{j,k} = Z^j X^k \omega^{-jk/2}. \tag{3.5}$$

There are d diagonal but traceless matrices $D_{j,0}$, with $j = 0, ..., d-1$ and $d^2 - d$ matrices $D_{j,k}$ with $k = 1, ..., d-1$ that have zero diagonal. This is because the X^k have zero diagonal, and multiplying them by a diagonal matrix Z^j will maintain the zero diagonal.

The adjoint of $D_{j,k}$ is given by

$$(D_{j,k})^\dagger = (Z^j X^k \omega^{-jk/2})^\dagger = (\omega^{-jk/2})^\dagger (X^k)^\dagger (Z^j)^\dagger = \omega^{jk/2} X^{-k} Z^{-j}.$$

Therefore, these operators are also unitary because

$$D_{j,k}^\dagger D_{j,k} = D_{j,k} D_{j,k}^\dagger = \mathbb{1}. \tag{3.6}$$

On the other hand, the product of $D_{j,k}^\dagger$ and $D_{j',k'}$ yields

$$D_{j,k}^\dagger D_{j',k'} = \omega^{(jk - j'k')/2} X^{-k} Z^{j'-j} X^{k'},$$

and using (3.4) we obtain

$$D_{j,k}^{\dagger} D_{j',k'} = \omega^{(jk-j'k')/2} \omega^{k(j'-j)} Z^{j'-j} X^{k'-k} = \omega^{(j'k-jk')/2} D_{j'-j,k'-k}, \tag{3.7}$$

which is a traceless matrix if $j' \neq j$ or $k' \neq k$. Therefore, the Weyl basis operators satisfy the orthogonality condition

$$\mathrm{Tr}\left(D_{j,k}^{\dagger} D_{j',k'}\right) = d\delta_{j,j'}\delta_{k,k'}, \qquad j,k,j',k' = 0,...,d-1. \tag{3.8}$$

While it is not relevant for now, we should mention here what happens to the orthogonality condition when one considers operators $D_{p,q}$ where p and q do not necessarily belong to $0,...,d-1$.

Consider

$$D_{p,q}^{\dagger} D_{p',q'} = \omega^{(p'q-pq')/2} D_{p'-p,q'-q}, \tag{3.9}$$

the matrix $D_{p'-p,q'-q}$ is traceless unless $p'-p = nd$ and $q'-q = md$ are some multiple of d, in which case

$$D_{nd,md} \propto Z^{nd} X^{md} = \mathbb{1}.$$

Therefore, we can say for certain that

$$\mathrm{Tr}\left(D_{p,q}^{\dagger} D_{p',q'}\right) \propto d\delta_{p'-p \mod d,0}\delta_{q'-q \mod d,0}, \tag{3.10}$$

but whether the proportionality constant is 1 as in (3.8) or not is more complicated. To give an example, take $p = 1$, $q = 0$, $p' = d+1$ and $q' = d$ then, from (3.7), we have

$$D_{1,0}^{\dagger} D_{d+1,d} = \omega^{-d/2} D_{d,d}.$$

From (3.5) we have that $D_{d,d} = \omega^{-d^2/2}\mathbb{1} \neq \mathbb{1}$ so, by substituting, the previous expression becomes

$$D_{1,0}^{\dagger} D_{d+1,d} = \omega^{-d(d+1)/2}\mathbb{1} = e^{-\pi i(d+1)}\mathbb{1} = (-1)^{d+1}\mathbb{1},$$

so

$$\mathrm{Tr}\left(D_{1,0}^{\dagger} D_{d+1,d}\right) = (-1)^{d+1} d.$$

In other words, the definition of the Weyl operators $D_{p,q}$ in (3.5), when p and q do not belong to $0,...,d-1$, give rise to possibly unexpected phase factors.

3.2. Computational and Fourier bases in terms of the Weyl basis

In this section we are going to express the projectors of the computational and Fourier bases as linear combinations of Weyl operators. This will be useful in the next section when we generate all MUBs in prime dimension.

Similarly to (2.6), we know that any projector $|\Psi\rangle\langle\Psi|$ can be written in terms of the Weyl operators as

$$|\Psi\rangle\langle\Psi| = \frac{1}{d}\sum_{j=0}^{d-1}\sum_{k=0}^{d-1} r_{j,k} D_{j,k}, \tag{3.11}$$

where we have hidden the identity matrix term inside the sum as $r_{0,0}D_{0,0} = \mathbb{1}$.

Let us start with the projector $|0\rangle\langle 0|$. Since its matrix form is diagonal, we only need the diagonal terms in the sum in (3.11), i.e., the $D_{j,0}$. Therefore,

$$|0\rangle\langle 0| = \frac{1}{d}\sum_{j=0} r_{j,0} D_{j,0} = \frac{1}{d}\sum_{j=0}^{d-1} r_{j,0} Z^j.$$

From (2.7), the $r_{j,0}$ are given by

$$r_{j,0} = \mathrm{Tr}\left(Z^{-j}|0\rangle\langle 0|\right). \tag{3.12}$$

Using (3.3) the operator $Z^{-j}|0\rangle\langle 0|$ is

$$Z^{-j}|0\rangle\langle 0| = \sum_{k=0}^{d-1} \omega^{-jk}|k\rangle\langle k|0\rangle\langle 0|.$$

Since $\langle k|0\rangle = \delta_{k,0}$, then

$$Z^{-j}|0\rangle\langle 0| = |0\rangle\langle 0|.$$

Substituting in (3.12) we obtain

$$r_{j,0} = \mathrm{Tr}\left(|0\rangle\langle 0|\right) = 1,$$

so the first projector of the computational basis is simply

$$|0\rangle\langle 0| = \frac{1}{d}\sum_{j=0}^{d-1} Z^j. \tag{3.13}$$

From (3.1), we can write any projector of the computational basis as

$$|i\rangle\langle i| = X^i|0\rangle\langle 0|(X^i)^\dagger = X^i|0\rangle\langle 0|X^{-i}.$$

Substituting (3.13) we get

$$|i\rangle\langle i| = \frac{1}{d}\sum_{j=0}^{d-1} X^i Z^j X^{-i},$$

and using the commutation relation (3.4) we obtain

$$|i\rangle\langle i| = \frac{1}{d}\sum_{j=0}^{d-1} \omega^{-ij} Z^j X^i X^{-i} = \frac{1}{d}\sum_{j=0}^{d-1} \omega^{-ij} Z^j. \tag{3.14}$$

Regarding the projectors of the Fourier basis, recall (2.5). The projector $|f_0\rangle\langle f_0|$ is then

$$|f_0\rangle\langle f_0| = \frac{1}{d}\sum_{k=0}^{d-1}\sum_{k'=0}^{d-1} |k'\rangle\langle k|,$$

whose matrix form is simply

$$|f_0\rangle\langle f_0| = \frac{1}{d}\begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ 1 & 1 & 1 & \dots & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & \dots & 1 \end{bmatrix}$$

which is the same matrix we saw in Example 3.1 for the sum of the X matrices in $d = 5$ but with a factor $1/d$. Therefore, we can write

$$|f_0\rangle\langle f_0| = \frac{1}{d}\sum_{j=0}^{d-1} X^j.$$

Using (2.5) and (3.1) we see that $|f_i\rangle = Z^i|f_0\rangle$ because

$$|f_i\rangle = Z^i|f_0\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1} Z^i|k\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{ik}|k\rangle,$$

and we then obtain a general expression for a projector $|f_i\rangle\langle f_i|$ of the Fourier basis

$$|f_i\rangle\langle f_i| = Z^i|f_0\rangle\langle f_0|(Z^i)^\dagger = Z^i|f_0\rangle\langle f_0|Z^{-i} = \frac{1}{d}Z^i\Big(\sum_{j=0}^{d-1} X^j\Big)Z^{-i} = \frac{1}{d}\sum_{j=0}^{d-1} Z^iX^jZ^{-i},$$

and using the commutation relation (3.4) we get

$$|f_i\rangle\langle f_i| = \frac{1}{d}\sum_{j=0}^{d-1}\omega^{ij}X^j, \tag{3.15}$$

where the X^j could also be written as $D_{0,j}$.

It is very interesting to see that the projectors associated to the computational basis and the Fourier basis, (3.14) and (3.15), are expressed in terms of only $d-1$ operators $D_{j,k}$ and the identity $D_{0,0}$. Moreover, the contributing operators to the computational basis are the $D_{j,0}$, whereas in the case of the Fourier basis it is the $D_{0,j}$ that contribute. In other words, they do not share any operators in the expansion except for the identity $D_{0,0}$. Therefore, their respective Bloch vectors are clearly orthogonal.

Example 3.2. Here we give some examples of Bloch vectors in the Weyl basis in $d = 3$.

The projector $|2\rangle\langle 2|$ from the computational basis is

$$|2\rangle\langle 2| = \frac{1}{3}\Big(\mathbb{1} + \omega^{-2}Z^1 + \omega^{-4}Z^2\Big).$$

Because $\omega^3 = 1$, by noting that $\omega^{-2} = \omega^3\omega^{-2} = \omega$ and that, similarly, $\omega^{-4} = \omega^{-1} = \omega^2$, we obtain

$$|2\rangle\langle 2| = \frac{1}{3}\Big(\mathbb{1} + \omega Z^1 + \omega^2 Z^2\Big) = \frac{1}{3}\Big(\mathbb{1} + \omega D_{1,0} + \omega^2 D_{2,0}\Big).$$

If we order the coordinates in the Bloch vector as $(r_{0,1}, r_{0,2}, r_{1,0}, r_{1,1}, r_{1,2}, r_{2,0}, r_{2,1}, r_{2,2})$, then the Bloch vector associated to $|2\rangle\langle 2|$ is

$$\vec{P}_{|2\rangle\langle 2|} = (0, 0, \omega, 0, 0, \omega^2, 0, 0).$$

Now, let us take the projector $|f_1\rangle\langle f_1|$ from the Fourier basis. Then, the linear combination of Weyl operators is

$$|f_1\rangle\langle f_1| = \frac{1}{3}\Big(\mathbb{1} + \omega X^1 + \omega^2 X^2\Big) = \frac{1}{3}\Big(\mathbb{1} + \omega D_{0,1} + \omega^2 D_{0,2}\Big),$$

and the Bloch vector is

$$\vec{P}_{|f_1\rangle\langle f_1|} = (\omega, \omega^2, 0, 0, 0, 0, 0, 0).$$

The two Bloch vectors are clearly orthogonal.

As a last example, consider $|f_2\rangle\langle f_2|$. The expansion in Weyl operators is

$$|f_2\rangle\langle f_2| = \frac{1}{3}\Big(\mathbb{1} + \omega^2 D_{0,1} + \omega^4 D_{0,2}\Big) = \frac{1}{3}\Big(\mathbb{1} + \omega^2 D_{0,1} + \omega D_{0,2}\Big),$$

and its Bloch vector is

$$\vec{P}_{|f_2\rangle\langle f_2|} = (\omega^2, \omega, 0, 0, 0, 0, 0, 0).$$

The inner product between these two Bloch vectors is

$$\vec{P}^{*}_{|f_1\rangle\langle f_1|} \cdot \vec{P}_{|f_2\rangle\langle f_2|} = \omega^{-1} \cdot \omega^2 + \omega^{-2} \cdot \omega = \omega + \omega^{-1} = e^{2\pi i/3} + e^{-2\pi i/3} = -1,$$

as predicted by (2.10).

3.3. W matrix

For the reader's ease, we recall here all MUBs for $d = 3$ that were given in (2.3)

$$\mathcal{B}_0 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

$$\mathcal{B}_1 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \quad \mathcal{B}_2 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{bmatrix}, \quad \mathcal{B}_3 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{bmatrix},$$

where $\mathcal{B}_0$ is the computational basis and $\mathcal{B}_1$ is the Fourier basis.

If we look closely, we find that we can get the bases $\mathcal{B}_2$ and $\mathcal{B}_3$ simply by multiplying the Fourier basis with the following W matrix on the left

$$W = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{bmatrix}. \tag{3.16}$$

In other words, let $|i\rangle_l$ denote the i-th state of the l-th basis, then

$$W|i\rangle_1 = |i\rangle_2, \qquad W^2|i\rangle_1 = |i\rangle_3, \qquad W^3 = \mathbb{1}.$$

Example 3.3. Consider the following state from the Fourier basis

$$|2\rangle_1 = \frac{1}{\sqrt{3}}\Big(|0\rangle + \omega^2 |1\rangle + \omega |2\rangle \Big),$$

then

$$|2\rangle_2 = W |2\rangle_1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{bmatrix} \begin{bmatrix} 1 \\ \omega^2 \\ \omega \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ \omega^2 \end{bmatrix}.$$

Also, to get $|2\rangle_3$ we do

$$|2\rangle_3 = W^2 |2\rangle_1 = W |2\rangle_2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ \omega^2 \end{bmatrix} = \begin{bmatrix} 1 \\ \omega \\ 1 \end{bmatrix}.$$

If we apply W to $|2\rangle_3$, we get

$$W |2\rangle_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{bmatrix} \begin{bmatrix} 1 \\ \omega \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ \omega^2 \\ \omega \end{bmatrix} = |2\rangle_1 .$$

Now, we would like to know if there exist similar W diagonal matrices for all d which, given the Fourier basis, produce the rest of the MUBs, and what is their structure. Although this is a very ambitious question, we can state two properties that the W matrix must have.

The first property of W is a consequence of the fact that all MUB vectors must be of the form (2.2) so that they are unbiased to the computational basis. This forces the diagonal W matrix to only have elements of unit modulus.

More formally, let W be

$$W = \sum_{k=0}^{d-1} g_k |k\rangle \langle k| .$$

When W acts on a vector $|\varphi\rangle$ of the form (2.2) we obtain

$$W |\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \sum_{k=0}^{d-1} g_k e^{i\theta_j} |k\rangle \langle k|j\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} g_j e^{i\theta_j} |j\rangle ,$$

which only satisfies (2.2) if $\left|g_j\right| = 1$, for $j = 0, ..., d-1$. Therefore, the matrix W is a diagonal matrix of complex exponentials

$$W = \sum_{k=0}^{d-1} e^{i\alpha_k} |k\rangle \langle k| .$$

The second property is a consequence of the fact that the vector $W |\varphi\rangle$ must be unbiased to $|\varphi\rangle$, that is, $|\langle\varphi|W|\varphi\rangle| = 1/\sqrt{d}$. Let us compute $\langle\varphi|W|\varphi\rangle$

$$\langle\varphi|W|\varphi\rangle = \frac{1}{d}\Big(\sum_{j=0}^{d-1} e^{-i\theta_j} \langle i| \Big)\Big(\sum_{k=0}^{d-1} e^{i\alpha_k} e^{i\theta_k} |k\rangle \Big) = \frac{1}{d} \sum_{j=0}^{d-1} e^{i\alpha_j} = \frac{1}{d} \operatorname{Tr} W.$$

Therefore,

$$|\mathrm{Tr}\, W| = \sqrt{d}.$$

However, we can still add more restrictions, as any $W^m |\varphi\rangle$ must also be unbiased to $|\varphi\rangle$, as long as $m = 1, ..., d-1$. By noting that $W^m |\varphi\rangle$ is

$$W^m |\varphi\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} e^{im\alpha_j} e^{i\theta_j} |j\rangle ,$$

and by computing $\langle\varphi|W^m|\varphi\rangle$ as before, it is easy to see that we obtain the restriction

$$|\mathrm{Tr}\, W^m| = \sqrt{d}, \qquad m = 1, ..., d-1.$$

Finally, since $W^d = \mathbb{1}$ we also get the condition

$$\mathrm{Tr}\, W^d = d \Rightarrow \sum_{j=0}^{d-1} e^{id\alpha_j} = d.$$

This last result suggests that, instead of considering general complex exponentials $e^{i\alpha_j}$, we could try with integer powers of ω (i.e., ω^{n_j}), since $\omega^{dn_j} = 1$, independently from n_j and, therefore, $\sum_{j=0}^{d-1} \omega^{dn_j} = d$.

A possible candidate is the following W matrix

$$W = \sum_{n=0}^{d-1} \omega^{n^2} |n\rangle \langle n| . \tag{3.17}$$

The trace of W^m is given by

$$\mathrm{Tr}\, W^m = \sum_{n=0}^{d-1} \omega^{mn^2} = \sum_{n=0}^{d-1} e^{2\pi i m n^2/d}, \qquad m = 1, ..., d-1. \tag{3.18}$$

This is a specific case of a Gauss sum. Because of the mathematical complexity behind this field of number theory, we will not go into much detail and simply state the following.

It can be proven that the absolute value of the Gauss sum in (3.18) *is* $\sqrt{d}$ *for all* $m = 1, ..., d-1$ *only if* d *is a prime number* [10].

Obviously, the fact that the specific form of W from (3.17) only admits prime dimensions for its trace to have modulus $\sqrt{d}$ does not imply that there does not exist any other W that satisfies it for any dimension d.

In any case, it is rather disappointing that the proof for one of the most interesting results from the Mutually Unbiased Bases problem (i.e., prime dimensions do admit $d+1$ MUBs) is not shown in this thesis. Therefore, in the next section we will show an alternative proof that the matrix W from (3.17) does indeed generate all MUBs in any prime dimension d.

Example 3.4. The W matrix from (3.17) is the same as (3.16) for $d = 3$

$$W = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^4 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega \end{bmatrix}.$$

3.4. Proof for the existence of $d + 1$ MUBs in prime dimension

We already showed that in any dimension d, the computational and the Fourier bases form a mutually unbiased set of two bases. We will now prove that consecutive actions of the W matrix operator, defined in (3.17), on the Fourier basis leads to the remaining $d - 1$ mutually unbiased bases if d is an odd prime.

We will denote $|k\rangle_n \equiv W^{n-1} |k\rangle_1$, where $|k\rangle_1$ is the k-th vector from the Fourier basis. The vector $|k\rangle_n$ should be the k-th vector of the n-th mutually unbiased basis. Therefore, we must prove the following

$$\left| {}_m\langle j|i\rangle_l \right|^2 = \begin{cases} \frac{1}{d}, & \text{if } m \neq l, \\ 0, & \text{if } m = l \text{ and } i \neq j, \\ 1, & \text{if } m = l \text{ and } i = j, \end{cases} \tag{3.19}$$

where $i, j = 0, ..., d - 1$ and $l, m = 1, ..., d$. The first statement is simply the unbiasedness condition between different bases, while the second and third mean that the generated bases are orthonormal.

From the result proved in Appendix A, the quantity in (3.19) can also be written as the trace of the composition of the two projectors

$$\left| {}_m\langle j|i\rangle_l \right|^2 = \mathrm{Tr}\Big(|i\rangle_l \, {}_l\langle i|j\rangle_m \, {}_j\langle j| \Big).$$

By definition, $|k\rangle_n = W^{n-1} |k\rangle_1$, and so ${}_n\langle k| = {}_1\langle k| \, W^{-(n-1)}$. Therefore,

$$\left| {}_m\langle j|i\rangle_l \right|^2 = \mathrm{Tr}\Big(W^{l-1} |i\rangle_1 \, {}_1\langle i| \, W^{-(l-1)} W^{m-1} |j\rangle_1 \, {}_1\langle j| \, W^{-(m-1)} \Big).$$

Using the expression presented in (3.15) for the Fourier projectors

$$|i\rangle_1 \, {}_1\langle i| = \frac{1}{d} \sum_{j=0}^{d-1} \omega^{ij} D_{0,j},$$

and substituting in the derivation at hand we obtain

$$\left| {}_m\langle j|i\rangle_l \right|^2 = \mathrm{Tr}\Big(W^{l-1} \Big(\frac{1}{d} \sum_{k=0}^{d-1} \omega^{ik} D_{0,k} \Big) W^{-(l-1)} W^{m-1} \Big(\frac{1}{d} \sum_{k'=0}^{d-1} \omega^{jk'} D_{0,k'} \Big) W^{-(m-1)} \Big).$$

By linearity of the trace we have

$$\left|{}_m\langle j|i\rangle_l\right|^2 = \frac{1}{d^2}\sum_{k,k'}\omega^{ik}\omega^{jk'}\,\mathrm{Tr}\left[W^{l-1}D_{0,k}W^{-(l-1)}W^{m-1}D_{0,k'}W^{-(m-1)}\right].$$

At this stage, we must use the following commutation relation

$$W^n D_{j,k} W^{-n} = D_{j+2nk,k},$$

whose proof, in order not to disturb the current narrative, is discussed in Appendix B. This is, actually, the only time when we use the explicit form of W defined in (3.17). Therefore, we end up with the following expression

$$\left|{}_m\langle j|i\rangle_l\right|^2 = \frac{1}{d^2}\sum_{k,k'}\omega^{ik}\omega^{jk'}\,\mathrm{Tr}\left[D_{2(l-1)k,k}D_{2(m-1)k',k'}\right],$$

and using the property $D_{j,k} = D^\dagger_{-j,-k}$ we have

$$\left|{}_m\langle j|i\rangle_l\right|^2 = \frac{1}{d^2}\sum_{k,k'}\omega^{ik}\omega^{jk'}\,\mathrm{Tr}\left[D^\dagger_{-2(l-1)k,-k}D_{2(m-1)k',k'}\right].$$

This expression for the trace cannot be directly replaced with the orthogonality condition (3.8) because here, the subidinces do not necessarily lie in $0, ..., d-1$. Using (3.9) we find that

$$D^\dagger_{-2(l-1)k,-k}D_{2(m-1)k',k'} = \omega^{kk'(l-m)}D_{2(m-1)k'+2(l-1)k,k'+k},$$

and using (3.5) we have

$$D^\dagger_{-2(l-1)k,-k}D_{2(m-1)k',k'} = \omega^{kk'(l-m)}\omega^{-(k'+k)(k'(m-1)+k(l-1))}Z^{2(m-1)k'+2(l-1)k}X^{k'+k}. \tag{3.20}$$

Here we notice what we already stated in (3.10), that is, the trace of the expression above is nonzero only when the following two conditions are satisfied

$$k'+k \mod d = 0, \tag{3.21a}$$

$$2(m-1)k' + 2(l-1)k \mod d = 0 \tag{3.21b}$$

Since $k', k = 0, ..., d-1$, the condition (3.21a) is satisfied either when $k = k' = 0$ or when $k' + k = d$. If $k = k' = 0$, then the second condition (3.21b) is also satisfied. On the other hand, if $k' = d - k$, then the second condition becomes

$$2k(l-m) \mod d = 0. \tag{3.22}$$

Here, the obvious solution is $l = m$ but, at first sight, it is not clear whether there are more. The answer is that $l = m$ is a unique solution $\forall k = 0, ..., d-1$ if and only if d is an odd prime number. This is best seen with some examples. Although, first notice that, since $l, m = 1, ..., d$, the factor $l - m$ can take the range of values $-(d-1), ..., 0, ..., d-1$. That is, both k and $l - m$ can only take values that are strictly lower than d in magnitude.

Example 3.5. If d is an even number, then it is easy to see that there exist more solutions. Let $d = 4$, then the values $k = 2$, $l = 4$, $m = 2$ satisfy (3.22). Moreover, let $d = 2$ the only even prime number, then the combination $k = 1$, $l = 2$ and $m = 1$ also satisfies (3.22).

Example 3.6. Let d be an odd prime number. Since d has no divisors other than 1 and itself, and since both k and $|l-m|$ are lower than d, there are no more solutions than $l = m$. Take $d = 5$, for example. Then, we have $k = 0, ..., 4$ and $l - m = -4, ..., 0, ...4$. There are no numbers here with which to produce a multiple of 5 in order to satisfy (3.22).

Example 3.7. Let $d = 9$, then, $k = 0, ..., 8$ and $l - m = -8, ..., 0, ..., 8$. A possible solution to (3.22) is simply $k = 3$ and $l - m = 3$. Although it is true that, for example, in the specific case of $k = 1$ there are no other solutions than $l = m$, what we are interested in is whether the solution $l = m$ is unique *for all* $k = 0, ..., d - 1$, and this is only accomplished when d is an odd prime.

In short, the only way to satisfy both conditions (3.21a) and (3.21b) when d is an odd prime is either $k = k' = 0$ or $k + k' = d$ and $l = m$. In any of these two cases, it turns out that the ω factors in (3.20) are unity, and so we can safely say that

$$\mathrm{Tr}\left[D^{\dagger}_{-2(l-1)k,-k} D_{2(m-1)k',k'}\right] = d(\delta_{k,0}\delta_{k',0} + \delta_{k',d-k}\delta_{l,m}),$$

if d is an odd prime.

Going back to the proof and substituting this orthogonality condition, we obtain

$$\left|{}_m\langle j|i\rangle_l\right|^2 = \frac{1}{d^2}\sum_{k,k'} \omega^{ik}\omega^{jk'} d(\delta_{k,0}\delta_{k',0} + \delta_{k',d-k}\delta_{l,m}) =$$

$$= \frac{1}{d} + \frac{1}{d}\delta_{l,m}\sum_{k=1}^{d-1} \omega^{ik}\omega^{j(d-k)}.$$

Since $\omega^{jd} = 1$, then the sum becomes $\sum_{k=1}^{d-1} \omega^{(i-j)k}$. This sum resembles the one discussed at the end of Section 2.2 with the only difference that it starts in $k = 1$. By adding and subtracting a 1 to the sum we obtain

$$\sum_{k=1}^{d-1} \omega^{(i-j)k} = -1 + \sum_{k=0}^{d-1} \omega^{(i-j)k} = -1 + d\delta_{i,j}.$$

Therefore,

$$\left|{}_m\langle j|i\rangle_l\right|^2 = \frac{1}{d} + \frac{1}{d}\delta_{l,m}(-1 + d\delta_{i,j}).$$

This is exactly the result (3.19) we aimed at proving.

Example 3.8. Now that we have a method for obtaining every mutually unbiased basis in an odd dimension, let us apply it to $d = 5$ and obtain the 6 bases. The W matrix in $d = 5$

is

$$W = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega^4 & 0 & 0 \\ 0 & 0 & 0 & \omega^9 & 0 \\ 0 & 0 & 0 & 0 & \omega^{16} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & \omega & 0 & 0 & 0 \\ 0 & 0 & \omega^4 & 0 & 0 \\ 0 & 0 & 0 & \omega^4 & 0 \\ 0 & 0 & 0 & 0 & \omega \end{bmatrix},$$

and, from (2.4), the computational and Fourier bases can be written as

$$\mathcal{B}_1 = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}, \qquad \mathcal{B}_2 = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega^6 & \omega^8 \\ 1 & \omega^3 & \omega^6 & \omega^9 & \omega^{12} \\ 1 & \omega^4 & \omega^8 & \omega^{12} & \omega^{16} \end{bmatrix} = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & \omega^3 & \omega^4 \\ 1 & \omega^2 & \omega^4 & \omega & \omega^3 \\ 1 & \omega^3 & \omega & \omega^4 & \omega^2 \\ 1 & \omega^4 & \omega^3 & \omega^2 & \omega \end{bmatrix}.$$

The remaining bases can be obtained by consecutively multiplying W to $\mathcal{B}_2$ on the left

$$\mathcal{B}_3 = W\mathcal{B}_2 = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega & \omega^2 & \omega^3 & \omega^4 & 1 \\ \omega^4 & \omega & \omega^3 & 1 & \omega^2 \\ \omega^4 & \omega^2 & 1 & \omega^3 & \omega \\ \omega & 1 & \omega^4 & \omega^3 & \omega^2 \end{bmatrix},$$

$$\mathcal{B}_4 = W\mathcal{B}_3 = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^2 & \omega^3 & \omega^4 & 1 & \omega \\ \omega^3 & 1 & \omega^2 & \omega^4 & \omega \\ \omega^3 & \omega & \omega^4 & \omega^2 & 1 \\ \omega^2 & \omega & 1 & \omega^4 & \omega^3 \end{bmatrix},$$

$$\mathcal{B}_5 = W\mathcal{B}_4 = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^3 & \omega^4 & 1 & \omega & \omega^2 \\ \omega^2 & \omega^4 & \omega & \omega^3 & 1 \\ \omega^2 & 1 & \omega^3 & \omega & \omega^4 \\ \omega^3 & \omega^2 & \omega & 1 & \omega^4 \end{bmatrix},$$

$$\mathcal{B}_6 = W\mathcal{B}_5 = \frac{1}{\sqrt{5}} \begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ \omega^4 & 1 & \omega & \omega^2 & \omega^3 \\ \omega & \omega^3 & 1 & \omega^2 & \omega^4 \\ \omega & \omega^4 & \omega^2 & 1 & \omega^3 \\ \omega^4 & \omega^3 & \omega^2 & \omega & 1 \end{bmatrix}.$$

These are the same bases that are obtained in [7].

3.5. Bloch vector structure

In this section we are going to look at a nice property of Bloch vectors that we already saw in Example 3.2. Consider the i-th projector from the l-th mutually unbiased basis,

with $l = 1, ..., d$, which can be written as

$$|i\rangle_l \ {}_l\langle i| = W^{l-1} \, |i\rangle_1 \ {}_1\langle i| \, W^{-(l-1)}.$$

Using (3.15) we can rewrite it as

$$|i\rangle_l \ {}_l\langle i| = \frac{1}{d} \sum_{k=0}^{d-1} \omega^{ik} W^{l-1} D_{0,k} W^{-(l-1)}.$$

Here, we can use the commutation relation (B.3) and obtain

$$|i\rangle_l \ {}_l\langle i| = \frac{1}{d} \sum_{k=0}^{d-1} \omega^{ik} D_{2(l-1)k,k}. \tag{3.23}$$

In Example 3.2 we saw that Bloch vectors that are associated to different mutually unbiased bases do not share any Weyl operators (except $D_{0,0}$) in terms of which the projectors can be written, and so the Bloch vectors are very visibly orthogonal. On the other hand, we also saw that Bloch vectors associated to the same basis share all Weyl operators. This last claim is obvious from (3.23), because the $D_{2(l-1)k,k}$ do not depend on i.

However, regarding the first claim, we would have to prove that the Weyl operators $D_{2(l-1)k,k}$ and $D_{2(l'-1)k,k}$ are always different if $l' \neq l$. Remember that this is not necessarily the case as $D_{p,q} \propto D_{p \mod d, q \mod d}$. Formally, we would have to prove that the equation

$$2(l-1)k \mod d = b \tag{3.24}$$

has a unique solution $\forall k = 0, ..., d-1$. Although we will not prove it, this is only the case when d is an odd prime [11].

Example 3.9. Take $d = 3$. In addition to the computational basis, there exist other 3 mutually unbiased bases given by

$$|i\rangle_1 \ {}_1\langle i| = \frac{1}{d}\Big(D_{0,0} + \omega^i D_{0,1} + \omega^{2i} D_{0,2}\Big), \qquad i = 0, ..., d-1,$$

$$|i\rangle_2 \ {}_2\langle i| = \frac{1}{d}\Big(D_{0,0} + \omega^i D_{2,1} + \omega^{2i} D_{4,2}\Big), \qquad i = 0, ..., d-1,$$

$$|i\rangle_3 \ {}_3\langle i| = \frac{1}{d}\Big(D_{0,0} + \omega^i D_{4,1} + \omega^{2i} D_{8,2}\Big), \qquad i = 0, ..., d-1,$$

Using (3.5), some of the Weyl operators can be rewritten as

$$D_{4,2} = D_{1,2}, \qquad D_{4,1} = \omega^{-3/2} D_{1,1}, \qquad D_{8,2} = D_{2,2}.$$

so the previous mutually unbiased bases are

$$|i\rangle_1 \ {}_1\langle i| = \frac{1}{d}\Big(D_{0,0} + \omega^i D_{0,1} + \omega^{2i} D_{0,2}\Big), \qquad i = 0, ..., d-1,$$

$$|i\rangle_2 \ {}_2\langle i| = \frac{1}{d}\Big(D_{0,0} + \omega^i D_{2,1} + \omega^{2i} D_{1,2}\Big), \qquad i = 0, ..., d-1,$$

$$|i\rangle_3\ {}_3\langle i| = \frac{1}{d}\Big(D_{0,0} + \omega^i\omega^{-3/2}D_{1,1} + \omega^{2i}D_{2,2}\Big), \qquad i = 0, ..., d-1.$$

We can see that no Weyl operators except for $D_{0,0}$ are repeated. The associated Bloch vectors are

$$\begin{aligned}
\vec{P}_{|i\rangle_1\ {}_1\langle i|} &= (\omega^i, \omega^{2i}, 0, 0, 0, 0, 0, 0), && i = 0, ..., d-1,\\
\vec{P}_{|i\rangle_2\ {}_2\langle i|} &= (0, 0, 0, 0, \omega^{2i}, 0, \omega^i, 0), && i = 0, ..., d-1,\\
\vec{P}_{|i\rangle_3\ {}_3\langle i|} &= (0, 0, 0, \omega^{-3/2+i}, 0, 0, 0, \omega^{2i}), && i = 0, ..., d-1,
\end{aligned}$$

which are visibly orthogonal.

Moreover, let $d = 4$. For example, in the case of $k = 1$ and $b = 2$ we can find two solutions to (3.24): $l = 2$ and $l = 4$. This means that the projectors $|i\rangle_2\ {}_2\langle i|$ and $|i\rangle_4\ {}_4\langle i|$ will share the Weyl operator $D_{2,1}$ so the Bloch vectors are not necessarily orthogonal and so $|i\rangle_2 = W\,|i\rangle_1$ and $|i\rangle_4 = W^3\,|i\rangle_1$ do not necessarily belong to mutually unbiased bases.

4. CONCLUSIONS

The main objective of this thesis was to present an easy-to-follow introduction to the Mutually Unbiased Bases problem that does not rely too much on the mathematical background of the reader. Moreover, we decided to approach the problem using the Bloch representation because of the geometrically appealing structure that emerges. Therefore, we hope this thesis can serve as a reference for any future students who decide to pursue further this interesting problem via the Bloch representation. We will now give an overview of the main results that were shown throughout the thesis.

In Chapter 2, we derived what is the connection between the Bloch vectors associated to different or the same mutually unbiased bases. Specifically, we saw that each MUB defines a $(d-1)$-dimensional subspace, called Bloch subspace, inside a (d^2-1)-dimensional Hilbert space. We also proved that a Bloch subspace is orthogonal to every other Bloch subspace and, therefore, one can only have a maximum of $d+1$ MUBs in a d-dimensional Hilbert space. Furthermore, the inner product between any two Bloch vectors belonging to the same MUB was shown to be constant, which gives the vectors a nice geometrical structure. Since the d^2-1 Hilbert space is three-dimensional when $d=2$, this allows us to draw the usual Bloch sphere whose axes are the Bloch subspaces.

In Chapter 3, we presented the Fourier basis, which is always unbiased to the computational basis, in terms of the Weyl operators and provided a method to obtain the rest of the MUBs when the dimension d is an odd prime. This method consisted in using one particular diagonal matrix that resulted in the next MUB when consecutively applied to the Fourier basis. Finally, we saw that, not only were the Bloch vectors associated to different MUBs orthogonal, but they shared no nonzero components.

4.1. Future work

As we stated at the beginning of this thesis, the existence of $d+1$ mutually unbiased bases has only been shown for prime power dimensions. Nonetheless, all of the proofs rely on explicitly constructing these bases (as we did for odd prime dimensions) and not on an abstract existence proof. As a result, there is still a lot to learn even for prime power dimensions, and as follow-up work, it would be interesting to use the Bloch representation to produce the MUBs in these dimensions. In fact, the dimensions that are a power of 2 are of special interest since they describe a set of qubits, which is the unit of quantum information that people usually work with. In any case, even though we do not actually know, there seems to be a widespread conviction that for $d=6$ there exist a maximum of 3 bases, instead of 7 [4].

A. TRACE OF AN OUTER PRODUCT

Let $|a\rangle$ and $|b\rangle$ be two states that can be written in terms of the computational basis $\{|i\rangle\}_{i=0}^{d-1}$ as follows

$$|a\rangle = \sum_{i=0}^{d-1} a_i |i\rangle , \qquad |b\rangle = \sum_{j=0}^{d-1} b_j |j\rangle ,$$

then its outer product is

$$|a\rangle \langle b| = \sum_{i,j} a_i b_j^* |i\rangle \langle j| .$$

By definition, the trace of an operator A is

$$\mathrm{Tr}\, A = \sum_{k=0}^{d-1} \langle k|A|k\rangle ,$$

so the trace of the outer product $|a\rangle \langle b|$ is

$$\mathrm{Tr}\, |a\rangle \langle b| = \sum_{k=0}^{d-1} \langle k| \left(\sum_{i,j} a_i b_j^* |i\rangle \langle j| \right) |k\rangle = \sum_{i,j,k} a_i b_j^* \langle k|i\rangle \langle j|k\rangle .$$

Since the basis is orthonormal, $\langle k|i\rangle = \delta_{ki}$ and $\langle j|k\rangle = \delta_{jk}$ so we obtain

$$\mathrm{Tr}\, |a\rangle \langle b| = \sum_{i=0}^{d-1} a_i b_i^* ,$$

which is precisely the inner product $\langle b|a\rangle$. Therefore,

$$\boxed{\mathrm{Tr}\, |a\rangle \langle b| = \langle b|a\rangle} .$$

B. COMMUTATION RELATIONS BETWEEN THE W MATRIX AND THE WEYL MATRICES $D_{J,K}$

For this demonstration we are going to use the definitions of X and W that were presented in (3.3) and (3.17), which we write here

$$W = \sum_{k=0}^{d-1} \omega^{k^2} |k\rangle \langle k| , \qquad X^n = \sum_{i=0}^{d-1} |i+n \mod d\rangle \langle i| .$$

By using these definitions, we can write the quantity WX^nW^{-1} as

$$WX^nW^{-1} = \left(\sum_{k=0}^{d-1} \omega^{k^2} |k\rangle \langle k| \right)\left(\sum_{i=0}^{d-1} |i+n \mod d\rangle \langle i| \right)\left(\sum_{k'=0}^{d-1} \omega^{-k'^2} |k'\rangle \langle k'| \right) =$$

$$= \sum_{k,k',i} \omega^{k^2}\omega^{-k'^2} |k\rangle \langle k|i+n \mod d\rangle \langle i|k'\rangle \langle k'| .$$

Since $\langle i|k'\rangle = \delta_{i,k'}$ and $\langle k|i+n \mod d\rangle = \delta_{i+n \mod d,k}$, then we obtain

$$WX^nW^{-1} = \sum_{k'=0} \omega^{(k'+n \mod d)^2}\omega^{-k'^2} |k'+n \mod d\rangle \langle k'| .$$

Here we can make the substitution $\omega^{(k'+n \mod d)^2} = \omega^{(k'+n)}$. To see why, consider the following quantity

$$\omega^{p^2},$$

where p is an integer that has r as a remainder when divided by d, that is, $p = nd + r$, with $n \in \mathbb{Z}$ and $r = 0, ..., d-1$. Substituting we have

$$\omega^{p^2} = \omega^{(nd+r)^2} = \omega^{n^2d^2}\omega^{2nrd}\omega^{r^2} = \omega^{r^2},$$

where the last equality is due to the identity $\omega^d = 1$. Therefore, $\omega^{p^2} = \omega^{r^2} = \omega^{(p \mod d)^2}$. Going back to the proof, we have

$$WX^nW^{-1} = \omega^{n^2} \sum_{k'=0}^{d-1} \omega^{2nk'} |k'+n \mod d\rangle \langle k'| .$$

Looking at the definition of the powers of Z in (3.3) it is easy to see that

$$X^nZ^{2n} = \sum_{k'=0}^{d-1} \omega^{2nk'} |k'+n \mod d\rangle \langle k'| .$$

Therefore,

$$WX^nW^{-1} = \omega^{n^2}X^nZ^{2n}. \tag{B.1}$$

It is now straightforward to obtain an expression for $W^mX^nW^{-m}$. For example, take $m = 2$, using the above equality (B.1) we obtain

$$W^2X^nW^{-2} = WWX^nW^{-1}W^{-1} = W\omega^{n^2}X^nZ^{2n}W^{-1}.$$

Because all diagonal matrices commute among themselves and the powers of both Z and W are diagonal, we have

$$W^2 X^n W^{-2} = \omega^{n^2} W X^n W^{-1} Z^{2n}.$$

Applying (B.1) once again we get

$$W^2 X^n W^{-2} = \omega^{2n^2} X^n Z^{2\cdot 2n}.$$

Therefore, by repeating this process as many times as necessary, we infer the relation

$$W^m X^n W^{-m} = \omega^{mn^2} X^n Z^{2mn}. \tag{B.2}$$

We can now move on and prove the final commutation relation $W^m D_{j,k} W^{-m}$ by using the definition of the $D_{j,k}$ in (3.5):

$$W^m D_{j,k} W^{-m} = W^m Z^j X^k \omega^{-jk/2} W^{-m} = \omega^{-jk/2} Z^j W^m X^k W^{-m}.$$

Using (B.2) we get

$$W^m D_{j,k} W^{-m} = \omega^{-jk/2} \omega^{mk^2} Z^j X^k Z^{2mk}.$$

Finally, using the commutation relation (3.4) we have

$$W^m D_{j,k} W^{-m} = \omega^{-jk/2} \omega^{mk^2} \omega^{-2mk^2} Z^{j+2mk} X^k,$$

which results in the final expression

$$W^m D_{j,k} W^{-m} = D_{j+2mk,k}. \tag{B.3}$$

BIBLIOGRAPHY

[1] A. G. J. MacFarlane, J. P. Dowling, and G. J. Milburn, "Quantum technology: The second quantum revolution," *Philosophical Transactions of the Royal Society of London. Series A: Mathematical, Physical and Engineering Sciences*, vol. 361, no. 1809, pp. 1655–1674, 2003.

[2] P. Horodecki, Ł. Rudnicki, and K. Życzkowski, *Five open problems in quantum information*, 2020. arXiv: 2002.03233 [quant-ph].

[3] I. Bengtsson and K. Życzkowski, *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2017.

[4] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," *International Journal of Quantum Information*, vol. 08, no. 04, pp. 535–640, 2010.

[5] J. Preskill, "Lecture notes for physics 219: Quantum computation," Jan. 1999.

[6] E. H. K. Stromberg, *Real and Abstract Analysis*. Springer, Berlin, Heidelberg, 1965.

[7] S. Brierley, S. Weigert, and I. Bengtsson, "All mutually unbiased bases in dimensions two to five," *Quantum information and computation*, Jul. 2009.

[8] 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.

[9] C. Eltschka and J. Siewert, "Distribution of entanglement and correlations in all finite dimensions," *Quantum*, vol. 2, p. 64, May 2018.

[10] B. Berndt, R. Evans, R. Evans, and K. Williams, *Gauss and Jacobi Sums*, ser. Canadian Mathematical Society series of monographs and advanced texts. Wiley, 1998.

[11] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, ser. Graduate Texts in Mathematics. Springer, New York, NY, 1990.