Universidade Técnica de Lisboa

Instituto Superior Técnico

Departamento de Matemática

Mutually Unbiased bases: a brief survey

Pedro Vitória

Mathematics Project

Licenciatura em Matemática Aplicada e Computação

Supervisors:

Prof. P. Mateus e Prof. Y. Omar

July 2008

Abstract

Mutually unbiased bases have important applications in Quantum Computation and more specifically in quantum state determination and quantum key distribution. However these applications rely on the existence of a complete set of such bases.

Even though they're being studied since the 1970's the problem of finding a complete set of mutually unbiased bases is only solved for dimensions which are a power of a prime. It remains open for other dimensions but recently there has been found strong numerical evidence that such a set doesn't exist in dimension 6.

Similar results in combinatorics, namely in latin squares and in finite projective planes, inspire two conjectures that may shade some light on the subject.

In this survey we prove the existence of complete sets of mutually unbiased bases in prime power dimensions and refer the numerical approach to this problem in the case of dimension 6. We also determine upper and lower bounds on the number of mutually unbiased bases and refer the conjectures between mutually unbiased bases, latin squares and finite projective planes.

Contents

Acknowledgments

I would like to thank my supervisors for their time, help and guidance. A special thanks goes to Yasser Omar for introducing me to the world of Quantum Information by means of his short course "Introduction to Quantum Information and Quantum Computation" given at IST in the fall semester of 07/08.

I would also like to thank Wootters who kindly sent us a copy of his and Fields' article, [1].

Chapter 1

Introduction

The mathematical framework for Quantum Mechanics is a complex Hilbert space (usually of infinite dimension). Quantum information deals with systems of finite dimension, so the setting for this work will be a complex Hilbert space of dimension d, $\mathbb{C}^d$. [1]

The state of a quantum system is completely specified by its density matrix, ρ. The density matrix is a positive definite operator on $\mathcal{H}$ with unitary trace, thus it is hermitian.

To determine a complex matrix we need to specify $2d^2$ real numbers. The requirement of hermiticity cuts this number by two and the unitary trace cuts one more degree of freedom. Hence to determine a density matrix we need $d^2 - 1$ real numbers.

The problem of quantum tomography is to determine the quantum state, i.e. the density matrix, of an unknown system. This can be done by measuring an ensemble of identically prepared systems and, in general, will not be free of some statistical error. Two questions arise at this point: Given a measurement and assuming an initial probability distribution for the unknown state how can we extract an estimate for the density matrix? What are the measurements that minimize the statistical error?

Complete collections of mutually unbiased bases, when available, answer the second question as we will see shortly.

In the following we will consider only projective measurements. Given a non-degenerate observable, A, the projective measurement associated with it will have d possible outcomes, each with a certain probability. Thus by measuring an ensemble of equivalent unknown systems we will be able to estimate those probabilities and this way we can impose $d-1$ conditions on the $d^2 - 1$ numbers needed to fully specify the system (only $d - 1$ because the probabilities sum to 1). This way we will need at least $\frac{d^2-1}{d-1} = d + 1$ measurements to determine an unknown system. In the optimal case the

[1] For a brief introduction to quantum mechanics, Dirac's bra-ket notation or the density operator formalism we refer the reader to the appendix.

chosen measurements are as uncorrelated to each other as possible and we can hope to need only $d+1$ measurements.

Example 1.1. *Let* $\rho = a_{00}|0\rangle\langle 0| + a_{10}|1\rangle\langle 0| + a_{01}|0\rangle\langle 1| + a_{11}|1\rangle\langle 1|$ *be a generic density operator, and consider two more bases for* $\mathcal{H}_2$*:*

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

In these bases we have:

$$\begin{aligned}\rho &= |+\rangle\langle +| \frac{a_{00} + a_{10} + a_{01} + a_{11}}{2} + ... \\ &= |\bar{0}\rangle\langle \bar{0}| \frac{a_{00} + a_{11} + i(-a_{10} + a_{01})}{2} + ...\end{aligned}$$

Now consider the following observables:

- $A_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$
- $A_1 = |+\rangle\langle +| + |-\rangle\langle -|$
- $A_2 = |\bar{0}\rangle\langle \bar{0}| + |\bar{1}\rangle\langle \bar{1}|$

If we know that measuring ρ *with observables* A_0, A_1, A_2 *results in* $|0\rangle, |+\rangle, |\bar{0}\rangle$ *with probability* p_0, p_1, p_2*, respectively, then:*

$$\begin{aligned} a_{00} &= p_0 \\ a_{00} + a_{10} + a_{01} + a_{11} &= 2p_1 \\ a_{00} + a_{11} + i(-a_{10} + a_{01}) &= 2p_2 \end{aligned}$$

Thus we conclude that:

$$\begin{aligned} a_{00} &= 1 - a_{11} = p_0 \\ a_{10} = a_{01}^* &= \frac{(2p_1 - 1) + i(2p_2 - 1)}{2} \end{aligned}$$

Hence the considered observables are enough to determine the state of an unknown 2-dimensional system.

It was proved in [1] that if we have a set of $d+1$ observables $\{A_0, ..., A_d\}$ with spectral decomposition $A_i = \sum_j \lambda_j^i P_j^i$ such that

$$tr(P_i^r P_j^s) = \frac{1}{d}, \tag{1.1}$$

for all $i, j, r \neq s$ then the set of associated measurements is not only minimal but also optimal, in the sense that it minimizes the statistical error (assuming an uniform probability distribution for the state of the unknown system).

Example 1.2. *In the previous example:*

- $P_0^0 = |0\rangle\langle 0|$, $P_1^0 = |1\rangle\langle 1|$,
- $P_0^1 = |+\rangle\langle +|$, $P_1^1 = |-\rangle\langle -|$,
- $P_0^2 = |\bar{0}\rangle\langle \bar{0}|$, $P_1^2 = |\bar{1}\rangle\langle \bar{1}|$,

and condition (1.1) can readily checked to be true.

If we let $\{|\varphi_k^i\rangle\}_{k=0,...,d-1}$ denote the normalized eigenvectors of the observable A_i then property (1.1) can be restated as follows:

$$|\langle\varphi_r^i|\varphi_s^i\rangle| = \frac{1}{\sqrt{d}}, \tag{1.2}$$

for all $i, j, r \neq s$. This leads to our first and most important definition:

Definition 1.3. *Let $\mathcal{B}_1 = \{|\varphi_1\rangle, ..., |\varphi_d\rangle\}$ and $\mathcal{B}_2 = \{|\phi_1\rangle, ..., |\phi_d\rangle\}$ be orthonormal bases in the d-dimensional state space. Then they are said to be* mutually unbiased *if and only if $|\langle\varphi_i|\phi_j\rangle| = \frac{1}{\sqrt{d}}$ for all i, j. A set $\{\mathcal{B}_1, ..., \mathcal{B}_m\}$ of orthonormal bases of $\mathbb{C}^d$ is said to be a set of mutually unbiased bases,* MUB*, if and only if, for every $i \neq j$, $\mathcal{B}_i$ is mutually unbiased with $\mathcal{B}_j$.*

In a certain sense mutually unbiased bases are as "far" as possible from each other thus the projective measurements associated with them are as uncorrelated as possible. We have already seen that this bases are relevant for quantum state determination. They are also important in quantum cryptography, [2] and [3], namely in extensions of the BB84 protocol[2] to d-dimensional systems, because information codified in mutually unbiased bases will not be much correlated.

Example 1.4. *Let $d = 2$ and consider the bases consisting of the eigenvectors of the observables from example 1.1:*

$$\mathcal{B}_0 = \{|0\rangle, |1\rangle\}, \mathcal{B}_1 = \{|+\rangle, |-\rangle\}, \mathcal{B}_2 = \{|\bar{0}\rangle, |\bar{1}\rangle\}.$$

Then $\mathcal{B}_0, \mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased.

Since we need at least $d + 1$ measurements to fully determine a general quantum state we're interested in knowing when there are collections of $d + 1$ or more mutually unbiased bases. A collection of $d + 1$ MUB is called a complete set of mutually unbiased bases.

Problem 1.5 (MUB problem)**.** *Given d, does there exist a complete set of mutually unbiased bases in $\mathbb{C}_d$?*

[2]Check the appendix for the details for this protocol of Quantum Key Distribution.

This question was first answered by Ivanovic for $d = p$ a prime [4] and then by Wootters and Fields for $d = p^m$ a power of a prime [1]. For composite d this remains an open problem.

The main purpose of this work is to explore the properties of this bases, namely prove the existence theorems (following [5]) and determine upper and lower bounds for the number of possible mutually unbiased bases. We will start by solving the MUB problem for prime dimensions and then we will use some of the ingredients of this proof to solve the problem when the dimension is a power of a prime. Then we will determine upper and lower bounds on the maximum number of bases in a set of MUB, thus proving that complete sets are actually maximal. Next, we present strong numerical evidence for a negative solution to problem 1.5 when $d = 6$. We will finish by stating two conjectures relating MUB, latin squares and Projective Planes.

Chapter 2

The MUB problem for prime dimensions

As stated in the Introduction we begin by solving problem 1.5 in the case of prime dimensions, following [5].

In the following the arithmetic of the indexes is taken to be modulo d.

The core theorem in this section is the following:

Theorem 2.1. *Let $\mathcal{B}_1 = \{|\varphi_0\rangle, ..., |\varphi_{d-1}\rangle\}$ be an orthonormal bases of $\mathbb{C}^d$. Suppose that there is an unitary operator V such that $V|\varphi_j\rangle = \beta_j |\varphi_{j+l}\rangle$ where $|\beta_j| = 1$ and $\mathrm{mcd}(l, d) = 1$. If $\mathcal{B}_2 = \{|\psi_0\rangle, ..., |\psi_{d-1}\rangle\}$ is the orthonormal bases consisting of the eigenvectors of V then $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased.*

Proof. Suppose that the eigenvector $|\psi_i\rangle$ is associated with the eigenvalue λ_i, that is $V|\psi_i\rangle = \lambda_i |\psi_i\rangle$. Since V is unitary we have $V^{-1} = V^\dagger$ so $V^\dagger |\psi_i\rangle = \lambda_i^{-1} |\psi_i\rangle$ and:

$$\left\langle \varphi_j \left| V^\dagger \right| \psi_i \right\rangle = \lambda_i^{-1} \langle \varphi_j | \psi_i \rangle , \tag{2.1}$$

$$\langle \psi_i | V | \varphi_j \rangle = \beta_j \langle \psi_i | \varphi_{j+l} \rangle \tag{2.2}$$

Combining these two equations we get:

$$\langle \varphi_j | \psi_i \rangle^* = \lambda_i^* \left\langle \varphi_j \left| V^\dagger \right| \psi_i \right\rangle^* = \lambda_i^* \langle \psi_i | V | \varphi_j \rangle = \lambda_i^* \beta_j \langle \psi_i | \varphi_{j+l} \rangle \tag{2.3}$$

Noting that $|\lambda_i| = |\beta_j| = 1$ and applying last equation several times we conclude that:

$$|\langle \psi_i | \varphi_j \rangle| = |\langle \psi_i | \varphi_{j+l} \rangle| = |\langle \psi_i | \varphi_{j+2l} \rangle| = ... = \left|\left\langle \psi_i \left| \varphi_{j+(d-1)l} \right\rangle\right| \tag{2.4}$$

Since $\mathrm{mcd}(l, d) = 1$ we have $\{l, 2l, ..., dl\} = \{0, 1, ..., d-1\} \mod d$. Taking $j = 0$:

$$|\langle \psi_i | \varphi_0 \rangle| = |\langle \psi_i | \varphi_1 \rangle| = ... = |\langle \psi_i | \varphi_{d-1} \rangle| \tag{2.5}$$

Because $\mathcal{B}_1$ and $\mathcal{B}_2$ are orthonormal bases we know that $1 = \||\psi_i\rangle\|^2 = \sum_j |\langle\psi_i|\varphi_j\rangle|^2$.

Therefore

$$|\langle\psi_i|\varphi_j\rangle|^2 = \frac{1}{d},\ 0 \leq j \leq d-1 \tag{2.6}$$

□

Notice that the condition $\text{mcd}(l, d) = 1$ is trivially true when d is a prime and $l < d$.

Our main goal now is to find d unitary matrices that apply cyclic shifts on the standard bases $\{|0\rangle, ..., |d-1\rangle\}$ and on each other eigenvectors, because if we do then, by the previous theorem, the sets consisting of the eigenvectors of those matrices together with the canonical basis form a complete set of MUB. In a certain sense, those matrices will be generalizations of the Pauli matrices.

Proposition 2.2. *The matrices:*

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.7}$$

called the Pauli matrices are unitary and:

- $\sigma_x |i\rangle = |i+1\rangle$
- $\sigma_z |i\rangle = (-1)^i |i\rangle$
- $\sigma_y = i\sigma_x\sigma_z$

Let $\omega_d = e^{\frac{2\pi i}{d}}$ and consider the following operators, X_d and Z_d, defined by:

$$X_d |i\rangle = |i+1\rangle, \tag{2.8}$$

$$Z_d |i\rangle = \omega_d^i |i\rangle \tag{2.9}$$

We can think of X_d and Z_d as a generalization of σ_x and σ_y, respectively, hence we will call them Pauli matrices. These operators have the following properties:

- They're unitary
- $(X_d)^d = (Z_d)^d = I_d$, where I_d is the identity operator of $\mathbb{C}^d$
- $(X_d)^l (Z_d)^k |i\rangle = \omega_d^{ik} |i+l\rangle$, hence by theorem 3.3 the bases consisting of the eigenvectors of $X_d(Z_d)^k$ are mutually unbiased with the standard basis.
- $\{\omega_d^i (X_d)^j (Z_d)^k : 0 \leq i, j, k \leq d-1\}$ is a multiplicative group with d^3 elements

- $X_2 = \sigma_x$, $Z_2 = \sigma_z$ and $X_2 Z_2 = -i\sigma_y$.

We're interested in the operators $X_d(Z_d)^k$. We determine their eigenvectors, for certain values of d, in the following lemma:

Lemma 2.3. *Let d be odd. Then the eigenvectors of $X(Z_d)^k$ are* [1]*:*

$$\left|\psi_t^k\right\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} \left|j\right\rangle, \tag{2.10}$$

where $s_j = j + ... + (d-1), 0 \leq t \leq d-1$

Proof. The proof involves only one computation:

$$\begin{aligned}
X_d(Z_d)^k \left|\psi_t^k\right\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} X_d(Z_d)^k \left|j\right\rangle \\
&= \frac{1}{\sqrt{d}} \left(\sum_{j=0}^{d-2} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} \omega_d^{kj} \left|j+1\right\rangle + \omega_d^t (\omega_d^{-k})^{d-1} \omega_d^{k(d-1)} \left|0\right\rangle \right) \\
&= \frac{\omega_d^t}{\sqrt{d}} \left(\sum_{j=0}^{d-2} (\omega_d^t)^{d-(j+1)} (\omega_d^{-k})^{s_{j+1}} \left|j+1\right\rangle + \left|0\right\rangle \right) \\
&= \frac{\omega_d^t}{\sqrt{d}} \left(\sum_{j=1}^{d-1} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} \left|j\right\rangle + (\omega_d^t)^d (\omega_d^{-k})^{s_0} \left|0\right\rangle \right) \\
&= \frac{\omega_d^t}{\sqrt{d}} \left(\sum_{j=0}^{d-1} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} \left|j\right\rangle \right) \\
&= \omega_d^t \left|\psi_t^k\right\rangle,
\end{aligned}$$

where in the 4^{th} equality we noticed that $\omega_d^d = 1$ and $\omega_d^{s_0} = \omega_d^{\frac{d(d-1)}{2}} = 1$, because when d is odd $d | \frac{d(d-1)}{2}$. □

Next we determine the action of $X_d(Z_d)^l$ on the eigenvectors of $X_d(Z_d)^l$:

Lemma 2.4. *Let d be odd. Then:*

$$X_d(Z_d)^l \left|\psi_t^k\right\rangle = \omega_d^{t+k-l} \left|\psi_{t+k-l}^k\right\rangle \tag{2.11}$$

[1] This theorem is stated in [5] as true for all prime numbers but this is false because it fails for $d = 2$. When we apply it in the case $d = 2$ we conclude that $\left|\psi_0^1\right\rangle = \frac{-1}{\sqrt{2}}(\left|0\right\rangle + \left|1\right\rangle)$ which is not an eigenvector of $X_2 Z_2 = -i\sigma_y$. The eigenvectors of $X_2 Z_2$ are $\left|0\right\rangle$ and $\left|1\right\rangle$.

Proof. Again the proof is a computation:

$$\begin{aligned}
X_d(Z_d)^l \left|\psi_t^k\right\rangle &= \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} X_d(Z_d)^l |j\rangle \\
&= \frac{1}{\sqrt{d}} \left(\sum_{j=0}^{d-2} (\omega_d^t)^{d-j} (\omega_d^{-k})^{s_j} \omega_d^{lj} |j+1\rangle + \omega_d^t (\omega_d^{-k})^{d-1} \omega_d^{l(d-1)} |0\rangle \right) \\
&= \frac{\omega_d^{t+k-l}}{\sqrt{d}} \left(\sum_{j=0}^{d-2} (\omega_d^t)^{d-(j+1)} (\omega_d^{-k})^{s_{j+1}} \omega_d^{(l-k)(j+1)} |j+1\rangle + |0\rangle \right) \\
&= \frac{\omega_d^{t+k-l}}{\sqrt{d}} \left(\sum_{j=1}^{d-1} (\omega_d^{t+k-l})^{d-j} (\omega_d^{-k})^{s_j} |j\rangle + |0\rangle \right) \\
&= \omega_d^{t+k-l} \left|\psi_{t+k-l}^k\right\rangle
\end{aligned}$$

In the last equality we noticed again that $\omega_d^{s_0} = 1$. □

Combining this result with (3.3) we get the main result of this chapter:

Theorem 2.5. *For any prime d the set of bases consisting of the normalized eigenvectors of*

$$Z_d, X_d, X_d Z_d, X_d (Z_d)^2, ..., X_d (Z_d)^{d-1}$$

forms a set of $d+1$ mutually unbiased bases.

Proof. Since lemma 2.4 only applies to d odd we will have to consider separately the cases $d = 2$ and d an odd prime.

1^{st} *case:* $d = 2$

In this case we will just exhibit $Z_2, X_2, X_2 Z_2$ and its eigenvectors. Then the theorem can readily seen to be true:

- $Z_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ has eigenvectors $\{|0\rangle, |1\rangle\}$.
- $X_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has eigenvectors $\{\frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\}$.
- $X_2 Z_2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has eigenvectors $\{\frac{|0\rangle+i|1\rangle}{\sqrt{2}}, \frac{|0\rangle-i|1\rangle}{\sqrt{2}}\}$.

2^{nd} *case: d is an odd prime*

Let $\mathcal{B}_d^k$ denote the base consisting of the normalized eigenvectors of $X_d(Z_d)^k$ and $\mathcal{B}_d$ denote the standard basis.

Since d is a prime we have $\text{mcd}(k-l,d)=1$ thus by theorem 3.3 we conclude that $\mathcal{B}_d^k$ and $\mathcal{B}_d^l$ are mutually unbiased, for all $k \neq l$.

The eigenvectors of Z_d are the elements of the standard basis and we already know that this base is mutually unbiased with any of the $\mathcal{B}_d^k$, hence we conclude the proof. □

Example 2.6. *Let $d=3$, $\omega_3 = e^{\frac{2\pi i}{3}}$. Then the eigenvectors of the following 4 matrices form a set of 4 mutually unbiased bases:*

$$Z_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, X_3 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, X_3Z_3 = \begin{pmatrix} 0 & 0 & \omega_3^2 \\ 1 & 0 & 0 \\ 0 & \omega_3 & 0 \end{pmatrix}, X_3(Z_3)^2 = \begin{pmatrix} 0 & 0 & \omega_3 \\ 1 & 0 & 0 \\ 0 & \omega_3^2 & 0 \end{pmatrix}.$$

If we make the usual identification: $|0\rangle = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix}^T$, $|1\rangle = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}^T$, $|2\rangle = \begin{pmatrix} 0 & 0 & 1 \end{pmatrix}^T$ then the bases are:

- $\mathcal{B}_3 = \{|0\rangle, |1\rangle, |2\rangle\}$
- $\mathcal{B}_3^0 = \{\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + |2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + \omega_3^2|1\rangle + \omega_3|2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + \omega_3|1\rangle + \omega_3^2|2\rangle)\}$
- $\mathcal{B}_3^1 = \{\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + \omega_3|2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + \omega_3^2|1\rangle + \omega_3^2|2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + \omega_3|1\rangle + |2\rangle)\}$
- $\mathcal{B}_3^2 = \{\frac{1}{\sqrt{3}}(|0\rangle + |1\rangle + \omega_3^2|2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + \omega_3^2|1\rangle + |2\rangle), \frac{1}{\sqrt{3}}(|0\rangle + \omega_3|1\rangle + \omega_3|2\rangle)\}$

Notice that in the previous theorem the requirement of d being a prime was needed to have $\text{mcd}(k-l,d)=1$ for all k,l. If we discard this condition and choose k and l carefully we will still be able to determine a collection (though a smaller one) of mutually unbiased bases.

Example 2.7. *If $d=p_1p_2$ where $p_1 < p_2$ are odd primes then $\mathcal{B}_d$, $\mathcal{B}_d^0$, $\mathcal{B}_d^1$, ..., $\mathcal{B}_d^{p_1-1}$ are mutually unbiased. This gives a collection of p_1+1 mutually unbiased bases which is known to be the best lower bound for the present case.*

Using this method this is also the biggest collection of mutually unbiased bases we can get.

If we had more matrices with "shifting properties" in the previous example then we would hope to have a bigger collection of mutually unbiased bases. Thus we tried to reformulate lemmas 2.3 and 2.4 for $k \in \mathbb{Q}$ with no success.

Chapter 3

The MUB problem for prime powers

In this chapter we will sketch the proof of the existence of $d+1$ mutually unbiased bases when $d = p^m$ is a power of a prime.

Theorem 3.1. *Let $d = p^m$ where p is a prime. Then there exist $d+1$ mutually unbiased bases in $\mathbb{C}^d$.*

We will not rely directly on theorem 2.5 but we will use some of the ingredients of its proof, namely the matrices defined in (2.8) and (2.9).

For that purpose we will develop, following [5], an interesting connection between MUB's and classes of commuting unitary matrices.

3.1 Mutually unbiased bases and unitary matrices

We begin with a lemma that will be useful:

Lemma 3.2. *For any integers m and n such that $0 < m \leq n$ we have*

$$\sum_{k=0}^{n-1} e^{2\pi i \frac{mk}{n}} = 0 \tag{3.1}$$

Proof. We just need to apply the formula for the sum of a truncated geometric series:

$$\sum_{k=0}^{n-1} \left(e^{2\pi i \frac{m}{n}}\right)^k = \frac{\left(e^{2\pi i \frac{m}{n}}\right)^n - 1}{e^{2\pi i \frac{m}{n}} - 1} = 0$$

□

We now relate MUB and unitary matrices through the following theorem:

Theorem 3.3. *There exist m mutually unbiased bases, $\mathcal{B}_1, ..., \mathcal{B}_m$ in $\mathbb{C}^d$ if and only if there are m classes $\mathcal{C}_1, ..., \mathcal{C}_m$ each consisting of d commuting unitary matrices such that $\mathcal{C}_i \cap \mathcal{C}_j = \{I_d\}$ and matrices in $\mathcal{C}_1 \cup ... \cup \mathcal{C}_m$ are pairwise orthogonal*[1].

For improved readability we separate the proof in two lemmas.

Lemma 3.4. *If there exist m mutually unbiased bases, $\mathcal{B}_1, ..., \mathcal{B}_m$ in $\mathbb{C}^d$ then there are m classes $\mathcal{C}_1, ..., \mathcal{C}_m$ each consisting of d commuting unitary matrices such that $\mathcal{C}_i \cap \mathcal{C}_j = \{I_d\}$ and matrices in $\mathcal{C}_1 \cup ... \cup \mathcal{C}_m$ are pairwise orthogonal.*

Proof. Suppose that $\mathcal{B}_1, ..., \mathcal{B}_m$ are mutually unbiased bases,

$$\mathcal{B}_j = \{\left|\psi_0^j\right\rangle, ..., \left|\psi_{d-1}^j\right\rangle\}$$

Let

$$\mathcal{C}_j = \{U_{j,0}, ..., U_{j,d-1}\}, \tag{3.2}$$

where

$$U_{j,t} = \sum_{k=0}^{d-1} e^{2\pi i \frac{tk}{d}} \left|\psi_k^j\right\rangle \left\langle\psi_k^j\right|, \quad 0 \leq t \leq d-1 \tag{3.3}$$

These matrices are obviously unitary and $U_{j,t}$ commutes with $U_{j,s}$ because both are diagonal with respect to $\mathcal{B}_j$. Notice that $U_{j,0} = I_d$ hence $I_d \in \mathcal{C}_i \cap \mathcal{C}_j$.

We now determine their inner product:

$$\begin{aligned}
\langle U_{j,s}, U_{k,t}\rangle &= Tr\left(U_{j,s}^\dagger U_{k,t}\right) \\
&= \sum_{x=0}^{d-1}\sum_{y=0}^{d-1} e^{2\pi i \frac{ty-sx}{d}} Tr\left(\left|\psi_x^j\right\rangle \left\langle\psi_x^j\right|\psi_y^k\right\rangle \left\langle\psi_y^k\right|\right) \\
&= \sum_{x=0}^{d-1}\sum_{y=0}^{d-1} e^{2\pi i \frac{ty-sx}{d}} \left|\left\langle\psi_x^j\right|\psi_y^k\right\rangle\Big|^2,
\end{aligned} \tag{3.4}$$

so when $j = k$ we have by lemma 3.2:

$$\begin{aligned}
\langle U_{j,s}, U_{j,t}\rangle &= \sum_{x=0}^{d-1}\sum_{y=0}^{d-1} e^{2\pi i \frac{ty-sx}{d}} \delta_{x,y} \\
&= \sum_{x=0}^{d-1} e^{2\pi i x \frac{t-s}{d}} \\
&= d\delta_{t-s},
\end{aligned} \tag{3.5}$$

[1] We consider the Trace inner product for matrices, that is, $\langle A, B\rangle = Tr\left(A^\dagger B\right)$.

and when $j \neq k$:

$$\begin{aligned} \langle U_{j,s}, U_{k,t} \rangle &= \sum_{x=0}^{d-1} \sum_{y=0}^{d-1} \frac{1}{d} e^{2\pi i \frac{ty-sx}{d}} \\ &= d\delta_s \delta_t, \end{aligned} \tag{3.6}$$

so we conclude that $\mathcal{C}_i \cap \mathcal{C}_j = \{I_d\}$ and that the matrices in $\mathcal{C}_1 \cup ... \cup \mathcal{C}_m$ are pairwise orthogonal. □

Lemma 3.5. *If there exist m classes $\mathcal{C}_1, ..., \mathcal{C}_m$ each consisting of d commuting unitary matrices such that $\mathcal{C}_i \cap \mathcal{C}_j = \{I_d\}$ and matrices in $\mathcal{C}_1 \cup ... \cup \mathcal{C}_m$ are pairwise orthogonal then there are m mutually unbiased bases, $\mathcal{B}_1, ..., \mathcal{B}_m$ in $\mathbb{C}^d$.*

Proof. Suppose $\mathcal{C}_1, ..., \mathcal{C}_m$ are m classes of commuting unitary matrices such that $\mathcal{C}_i \cap \mathcal{C}_j = \{I_d\}$ and matrices in $\mathcal{C}_1 \cup ... \cup \mathcal{C}_m$ are pairwise orthogonal.

Let $\mathcal{C}_j = \{U_{j,0}, ..., U_{j,d-1}\}$, $U_{j,0} = I_d$. Then:

$$\begin{aligned} \langle U_{j,s}, U_{k,t} \rangle &= d\delta_s \delta_t, \quad j \neq k \\ \langle U_{j,s}, U_{j,t} \rangle &= d\delta_{s-t} \end{aligned} \tag{3.7}$$

Since all the matrices in the same class commute then they are simultaneously unitarily diagonalizable, i.e. for each j there is a unitary bases $\mathcal{B}_j = \{\left|\psi_0^j\right\rangle, ..., \left|\psi_{d-1}^j\right\rangle\}$ such that:

$$U_{j,t} = \sum_{k=0}^{d-1} \lambda_{j,t,k} \left|\psi_k^j\right\rangle \left\langle\psi_k^j\right| \tag{3.8}$$

Notice that $\lambda_{j,0,k} = 1$ for all j, k.

If we compute the inner product like we did for (3.4) then:

$$\langle U_{j,s}, U_{k,t} \rangle = \sum_{x=0}^{d-1} \sum_{y=0}^{d-1} \lambda_{j,s,x}^* \lambda_{k,t,y} \left|\left\langle\psi_x^j \middle| \psi_y^k\right\rangle\right|^2,$$

hence

$$\sum_{x=0}^{d-1} \sum_{y=0}^{d-1} \lambda_{j,s,x}^* \lambda_{k,t,y} \left|\left\langle\psi_x^j \middle| \psi_y^k\right\rangle\right|^2 = d\delta_{s,t}, \quad j \neq k \tag{3.9}$$

and

$$\sum_{x=0}^{d-1} \lambda_{j,s,x}^* \lambda_{j,t,x} = d\delta_{s,t} \tag{3.10}$$

From (3.10) it follows that Λ_j is unitary where [2]

$$\Lambda_j = \frac{1}{\sqrt{d}} \begin{pmatrix} \lambda_{j,0,0} & \lambda_{j,0,1} & \dots & \lambda_{j,0,d-1} \\ \lambda_{j,1,0} & \lambda_{j,1,1} & \dots & \lambda_{j,1,d-1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{j,d-1,0} & \lambda_{j,d-1,1} & \dots & \lambda_{j,d-1,d-1} \end{pmatrix}.$$

With these matrices the system of equations in (3.9) can then be rewritten as

$$d\Lambda_{j,k}\Psi_{j,k} = D, \tag{3.11}$$

where[3]:

$$\begin{aligned} \Lambda_{j,k} &= \Lambda_j^* \otimes \Lambda_k, \\ \Psi_{j,k} &= \left(\Psi_{1,j,k}|...|\Psi_{d,j,k}\right), \\ \Psi_{i,j,k} &= \left(\left|\left\langle \psi_i^j \middle| \psi_1^k \right\rangle\right|^2, ..., \left|\left\langle \psi_i^j \middle| \psi_d^k \right\rangle\right|^2\right)^T, \\ D &= (d, 0, ..., 0)^T \end{aligned}$$

Since Λ_j and Λ_k are unitary and their first row is the constant vector $\frac{1}{\sqrt{d}}(1, ..., 1)$ it follows that $\Lambda_{j,k}$ is unitary and has a constant first row equal to $\frac{1}{d}(1, ..., 1)$. Hence it follows from $\Psi_{j,k} = \frac{1}{d}\Lambda_{j,k}^{-1} D$ that

$$\left|\left\langle \psi_s^j \middle| \psi_t^k \right\rangle\right|^2 = \frac{1}{d}, \quad j \neq k \tag{3.12}$$

and $\{\mathcal{B}_1, ..., \mathcal{B}_m\}$ is a collection of m mutually unbiased bases. □

Example 3.6. *We will now exhibit 5 classes of 4 unitary commuting matrices in $\mathbb{C}^4$ and extract a set of 5 mutually unbiased bases out of it:*

$$\mathcal{C}_0 = \left\{ Id, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \right\}$$

$$\mathcal{C}_1 = \left\{ Id, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

$$\mathcal{C}_2 = \left\{ Id, \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

[2] In [5] the factor $\frac{1}{\sqrt{d}}$ is missing.

[3] $(a|b)$ denotes the concatenation of vectors a and b.

$$\mathcal{C}_3 = \left\{ Id, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

$$\mathcal{C}_4 = \left\{ Id, \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

We now need to find 5 unitary matrices $U_0, ..., U_4$ such that U_i simultaneously diagonalizes all the matrices in $\mathcal{C}_i$. Then the columns of U_i will be the elements of $\mathcal{B}_i$. Since all the matrices in $\mathcal{C}_0$ are diagonal we have $U_0 = I_d$, hence $\mathcal{B}_0$ is the standard bases of $\mathbb{C}^4$. As for the other U_i:

$$U_1 = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & -1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \end{pmatrix}, \qquad U_2 = \frac{1}{2}\begin{pmatrix} 1 & i & i & -1 \\ 1 & -i & -i & -1 \\ 1 & i & -i & 1 \\ 1 & -i & i & 1 \end{pmatrix},$$

$$U_3 = \frac{1}{2}\begin{pmatrix} 1 & 1 & -i & i \\ 1 & -1 & i & i \\ 1 & 1 & i & -i \\ 1 & -1 & -i & -i \end{pmatrix}, \qquad U_4 = \frac{1}{2}\begin{pmatrix} 1 & -i & 1 & i \\ 1 & i & -1 & i \\ 1 & i & 1 & -i \\ 1 & -i & -1 & -i \end{pmatrix}$$

The corresponding bases are:

$$\begin{aligned}
\mathcal{B}_0 &= \{ |00\rangle, \ |01\rangle, \ |10\rangle, \ |11\rangle \} \\
\mathcal{B}_1 &= \{ \tfrac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle), \quad \tfrac{1}{2}(|00\rangle - |01\rangle - |10\rangle + |11\rangle), \\
&\quad \tfrac{1}{2}(|00\rangle + |01\rangle - |10\rangle - |11\rangle), \quad \tfrac{1}{2}(|00\rangle - |01\rangle + |10\rangle - |11\rangle) \} \\
\mathcal{B}_2 &= \{ \tfrac{1}{2}(|00\rangle + i\,|01\rangle + i\,|10\rangle - |11\rangle), \quad \tfrac{1}{2}(|00\rangle - i\,|01\rangle - i\,|10\rangle + |11\rangle), \\
&\quad \tfrac{1}{2}(|00\rangle + i\,|01\rangle - i\,|10\rangle + |11\rangle), \quad \tfrac{1}{2}(|00\rangle - i\,|01\rangle + i\,|10\rangle + |11\rangle) \} \\
\mathcal{B}_3 &= \{ \tfrac{1}{2}(|00\rangle + |01\rangle - i\,|10\rangle + i\,|11\rangle), \quad \tfrac{1}{2}(|00\rangle - |01\rangle + i\,|10\rangle + i\,|11\rangle), \\
&\quad \tfrac{1}{2}(|00\rangle + |01\rangle + i\,|10\rangle - i\,|11\rangle), \quad \tfrac{1}{2}(|00\rangle - |01\rangle - i\,|10\rangle - i\,|11\rangle) \} \\
\mathcal{B}_4 &= \{ \tfrac{1}{2}(|00\rangle - i\,|01\rangle + |10\rangle + i\,|11\rangle), \quad \tfrac{1}{2}(|00\rangle + i\,|01\rangle - |10\rangle + i\,|11\rangle), \\
&\quad \tfrac{1}{2}(|00\rangle + i\,|01\rangle + |10\rangle - i\,|11\rangle), \quad \tfrac{1}{2}(|00\rangle - i\,|01\rangle - |10\rangle - i\,|11\rangle) \}.
\end{aligned}$$

We will now use Theorem 3.3 to solve the MUB problem, by proving the existence of $d+1$ such classes of commuting matrices. The matrices constituting these classes will be tensor products of the Pauli matrices developed in the previous chapter.

The intuition behind this approach is the following: we see a system of $\mathbb{C}^{p^m}$ as consisting of m subsystems of $\mathbb{C}^p$ and we already know that for each such subsystem we need only Pauli measurements to determine it. Hence by considering tensor products of these we produce a collection of enough

measurements to fully determine the system. Now these measurements are seen to fall into p^m+1 commuting unitary classes and since that commuting operators give no extra information we conclude that only p^m+1 measurements are needed.

3.2 Tensors of Pauli Matrices

We begin with some notation. As explained the unitary operators that we will consider are:

$$U = (X_p)^{k_1}(Z_p)^{l_1} \otimes ... \otimes (X_p)^{k_m}(Z_p)^{l_m}, \qquad 0 \leq k_i, l_i \leq p-1 \tag{3.13}$$

To describe such an operator we need only two vectors of $(\mathbb{F}_p)^m$, $\alpha = (k_1, ..., k_m)$ and $\beta = (l_1, ..., l_m)$, hence we will denote U by

$$X_p(\alpha)Z_p(\beta)$$

It is interesting to notice that with this notation the action of $X_p(\alpha)Z_p(\beta)$ in $\mathbb{C}^{p^m}$ is totally similar to that of $(X_p)^k(Z_p)^l$ in $\mathbb{C}^p$:

$$X_p(\alpha)Z_p(\beta)\left|i\right\rangle = \omega_p^{i\cdot\beta}\left|i+\alpha\right\rangle, \tag{3.14}$$

where $\left|i\right\rangle = \left|i_1, ..., i_m\right\rangle$ is an element of the standard basis of $\mathbb{C}^p \otimes ... \otimes \mathbb{C}^p = \mathbb{C}^{p^m}$, $(i_1, ..., i_m) \in (\mathbb{F}_p)^m$. Equivalently:

$$X_p(\alpha)Z_p(\beta) = \sum_{i\in(\mathbb{F}_p)^m} \omega_p^{i\cdot\beta}\left|i+\alpha\right\rangle\left\langle i\right| \tag{3.15}$$

It is now easy to check the orthogonality of these matrices:

Lemma 3.7. *If $(\alpha,\beta) \neq (\alpha',\beta')$ then $U = X_p(\alpha)Z_p(\beta)$ and $U' = X_p(\alpha')Z_p(\beta')$ are orthogonal.*

Proof.

$$\begin{aligned}
\left\langle U, U'\right\rangle &= Tr(U^\dagger U') \\
&= Tr\left(\sum_{i\in(\mathbb{F}_p)^m}\sum_{j\in(\mathbb{F}_p)^m} \omega_p^{j\cdot\beta'-i\cdot\beta}\left|i\right\rangle\left\langle i+\alpha\middle|j+\alpha'\right\rangle\left\langle j\right|\right) \\
&= \sum_{i\in(\mathbb{F}_p)^m}\sum_{j\in(\mathbb{F}_p)^m} \omega_p^{j\cdot\beta'-i\cdot\beta}\left\langle i+\alpha\middle|j+\alpha'\right\rangle Tr\left(\left|i\right\rangle\left\langle j\right|\right) \\
&= \sum_{i\in(\mathbb{F}_p)^m}\sum_{j\in(\mathbb{F}_p)^m} \omega_p^{j\cdot\beta'-i\cdot\beta}\left\langle i+\alpha\middle|j+\alpha'\right\rangle\left\langle j\middle|i\right\rangle \\
&= \sum_{i\in(\mathbb{F}_p)^m} \omega_p^{i\cdot(\beta'-\beta)}\left\langle i+\alpha\middle|i+\alpha'\right\rangle
\end{aligned}$$

When $\alpha \neq \alpha'$ we have $\langle i+\alpha \,|i+\alpha'\rangle = 0$ hence $\langle U, U'\rangle = 0$. If $\alpha = \alpha'$ then $\beta \neq \beta'$ so

$$\langle U, U'\rangle = \sum_{i\in(\mathbb{F}_p)^m} \omega_p^{i\cdot(\beta'-\beta)},$$

and we have by lemma 3.2 that $\langle U, U'\rangle = 0$. □

Since we are interested in constructing classes of commuting matrices we need to know when these matrices commute.

Lemma 3.8. *$X_p(\alpha)Z_p(\beta)$ and $X_p(\alpha')Z_p(\beta')$ commute if and only if*

$$\alpha\cdot\beta' - \alpha'\cdot\beta = 0, \qquad (\text{mod } p) \tag{3.16}$$

Proof. We will determine when $(X_p)^k(Z_p)^l$ commutes with $(X_p)^{k'}(Z_p)^{l'}$. From this the lemma will follow. Let $[A,B] = AB - BA$ denote the commutator of 2 operators. Then

$$\begin{aligned}\left[(X_p)^k(Z_p)^l, (X_p)^{k'}(Z_p)^{l'}\right]|i\rangle &= (X_p)^k(Z_p)^l\left(\omega_p^{il'}\left|i+k'\right\rangle\right) - (X_p)^{k'}(Z_p)^{l'}\left(\omega_p^{il}\left|i+k\right\rangle\right)\\ &= \omega_p^{il'}\omega_p^{(i+k')l}\left|i+k'+k\right\rangle - \omega_p^{il}\omega_p^{(i+k)l'}\left|i+k+k'\right\rangle\\ &= \omega_p^{i(l+l')}(\omega_p^{k'l} - \omega_p^{kl'})\left|i+k+k'\right\rangle,\end{aligned}$$

so $\left[(X_p)^k(Z_p)^l, (X_p)^{k'}(Z_p)^{l'}\right] = 0$ if and only if $kl' - k'l = 0, (\text{mod } p)$.

From this and from the linearity of the tensor product it follows that $X_p(\alpha)Z_p(\beta)$ and $X_p(\alpha')Z_p(\beta')$ commute if and only if

$$\sum_{j=1}^m k_j l'_j - \sum_{j=1}^m k'_j l_j = 0, \qquad (\text{mod } p)$$

□

We can think of each pair (α,β) as an element $u = (\alpha|\beta) \in (\mathbb{F}_p)^{2m}$. Then formula (3.16) defines a symplectic product (bilinear, skew-symmetric and non-degenerate) in $(\mathbb{F}_p)^{2m}$:

$$(\alpha|\beta)\circ(\alpha'|\beta') = \alpha\cdot\beta' - \alpha'\cdot\beta \tag{3.17}$$

If we now remember Theorem 3.3 in the light of these new results and notation we see that we have reduced the problem of finding p^m+1 mutually unbiased bases to the following:

Problem 3.9. *Find p^m+1 classes $C_j = \{u_1^j, ..., u_{p^m}^j\} \subset (\mathbb{F}_p)^{2m}$ such that:*

1. *$C_j \cap C_i = \{0\}$*
2. *$u, v \in C_j \Rightarrow u \circ v = 0$.*

If we let each C_j be a linear subspace (of dimension m) spanned by some basis $B_j = \{b_1^j, ..., b_m^j\}$ then condition 1 tells us that $B_i \cup B_j$ spans $(\mathbb{F}_p)^{2m}$ and condition 2 tells us that each C_j is isotropic[4], hence lagrangian (and by the linearity of the symplectic product this condition needs only to be checked on the basis B_j).

3.3 The solution to the MUB problem for prime powers

To find the spaces needed to solve problem 3.9 two approaches can be taken and both rely on an extra structure in the space $(\mathbb{F}_p)^m$: the structure of a field. As is known from algebra, $\mathbb{F}_{p^m}$ is a field and a vector space of dimension m over $\mathbb{F}_p$ hence it can be thought of as $(\mathbb{F}_p)^m$ with an additional structure of vector multiplication (just like $\mathbb{C}$ can be thought of $\mathbb{R}^2$ with the complex product).

In the first approach due to Bandyopadhyay *et al*, [5], we let $b_i^0 = (0|e_i)$ and $b_i^k = (e_i|\beta_i^k)$ and try to determine β_i^k such that conditions 1 and 2 of problem 3.9 are satisfied. In this particular case:

- $C_0 \cap C_i = \{0\}$
- $b_i^0 \circ b_j^0 = 0$
- $b_i^k \circ b_j^k = \left(\beta_j^k\right)_i - \left(\beta_i^k\right)_j$

Thus if we let $(A^k)_{ij} = \left(\beta_i^k\right)_j$ then condition 2 is satisfied if and only if $A^k \in \mathcal{M}_{m\times m}(\mathbb{F}_p)$ is symmetric. Regarding condition 1 of the same problem we have the following lemma:

Lemma 3.10. *Let $b_i^k = (e_i|\beta_i^k)$. The set $\{b_1^k, ..., b_m^k, b_i^l, ..., b_m^l\}$ consists of $2m$ linearly independent vectors if and only if the vectors $\beta_1^k - \beta_1^l, ..., \beta_m^k - \beta_m^l$ are linearly independent.*

Proof. We have

$$\sum_{i=1}^{m} c_i b_i^k + d_i b_i^l = \sum_{i=1}^{m} c_i(e_i|\beta_i^k) + d_i(e_i|\beta_i^l) = 0,$$

if and only if

$$c_i = -d_i \text{ and } \sum_{i=1}^{m} c_i(0|\beta_i^k - \beta_i^l) = 0,$$

[4]If (V, Ω) is a symplectic vector space and $A \subset V$ is a subspace we say that A is isotropic if it is contained in its symplectic orthogonal, that is $A \subset A^\Omega$. A is lagrangian if it is isotropic and $\dim(A) = \dim(V)/2$.

if and only if

$$c_i = -d_i \text{ and } \sum_{i=1}^{m} c_i \left(\beta_i^k - \beta_i^l\right) = 0,$$

and the lemma follows. □

Thus condition 1 of problem 3.9 is satisfied if and only if for any $k \neq l$, $\det(A^k - A^l) \neq 0$ and the problem is solved if we find p^m symmetric matrices with this property. For this it is enough to find m symmetric matrices $M_1, ..., M_m$ such that $\sum_{j=1}^{m} c_j M_j$ is also nonsingular for every non-vanishing $(c_1, ..., c_m) \in (\mathbb{F}_p)^m$. Because then we can take the p^m matrices A^k to be

$$\sum_{j=1}^{m} c_j M_j, \qquad (c_1, ..., c_m) \in (\mathbb{F}_p)^m \tag{3.18}$$

Example 3.11. *In this example we consider the particular case $m = 1$. In this case we need to determine only one nonsingular 1×1 matrix, M_1, in $\mathbb{F}_p$:*

$$M_1 = [1],$$

Then:

$$A_1 = M_1 = [1], ..., A_{p-1} = (p-1)M_1 = [p-1], A_p = [0],$$

and the bases $B_j = \{b_1^j\}, j = 1, ..., p$ are determined:

$$b_1^0 = (0,1), b_1^1 = (1,1), ..., b_1^{p-1} = (1, p-1), ...b_1^p = (1,0)$$

Now the set C_j spanned by B_j determines a class of commuting unitary matrices $\mathcal{C}_j$:

$$\mathcal{C}_0 = \{Z_p^k : k \in \mathbb{F}_p\},$$

$$\mathcal{C}_j = \{X_p^k (Z_p^j)^k : k \in \mathbb{F}_p\}, \qquad j = 1, ..., p$$

All the matrices in the same class, $\mathcal{C}_j$, are simultaneously diagonalizable by some unitary matrix U_j. The columns of U_j determine a basis $\mathcal{B}_j$ and we know by the proof of theorem 3.3 that all these bases are mutually unbiased. Since each class, $\mathcal{C}_j$, only consists of powers of the same matrix it follows that they all have the same eigenvectors. Thus $\mathcal{B}_j$ is just the set of eigenvectors of any of the matrices in $\mathcal{C}_j$. In particular the eigenvectors of

$$Z_p, X_p Z_p, ..., X_p Z_p^{p-1}, X_p$$

are mutually unbiased.

Previous example captures the result from Theorem 2.5 (without the need to separate the even and odd dimensions) so the previous chapter could be omitted. We chose not to do so because the two methodologies are essentially different and reveal two different ways of constructing sets of mutually unbiased bases.

To determine the matrices M_j in the general case, found by Wootters and Fields [1], we take a basis $\gamma_1, ..., \gamma_m$ of $\mathbb{F}_{p^m}$ as a vector space over $\mathbb{F}_p$. Then the product $\gamma_i \gamma_j$ can be written uniquely in this base as

$$\gamma_i \gamma_j = \sum_{l=1}^{m} s_{ij}^l \gamma_l, \tag{3.19}$$

and we take $(M_l)_{ij} = s_{ij}^l$. The symmetry of this matrices follows directly from the commutativity of $\mathbb{F}_{p^m}$. Their non-singularity is not that easy to verify and requires finite fields theory.

Example 3.12. *We now follow the results of this chapter in an algorithmic way to construct a set of mutually unbiased bases in the simplest case* $p = 2$, $m = 2$.

We start by construction the field $\mathbb{F}_{p^m}$ *as usual, that is* $\mathbb{F}_{p^m} = \frac{\mathbb{F}_p[x]}{<p(x)>}$ *where* $p(x)$ *is an irreducible polynomial of degree* m *in* $\mathbb{F}_p$. *In this case* $p(x) = 1 + x + x^2$ *and:*

$$\mathbb{F}_{p^m} = \{0, 1, i, i+1\},$$

where $i = [x]$ *satisfies* $i^2 = [x^2] = [x + 1] = i + 1$. *As a bases of this space over* $\mathbb{F}_p$ *we can take* $\gamma_1 = 1, \gamma_2 = i$. *Then we write the product with respect to this bases as in (3.19):*

$$\gamma_1\gamma_2 = \gamma_2, \qquad \gamma_1\gamma_1 = \gamma_1, \qquad \gamma_2\gamma_2 = \gamma_1 + \gamma_2,$$

and find:

$$M_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad M_2 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

hence the matrices A^k *given by (3.18) are:*

$$A^1 = M_1, \qquad A^2 = M_2, \qquad A^3 = M_1 + M_2, \qquad A^4 = 0.$$

Remember that the i-th row of A^k *is* β_i^k, *so we have just determined all the* B_j *and consequently the* C_j*:*

$$C_0 = \left\{ \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}^T, \begin{pmatrix} 0 & 0 & 1 & 0 \end{pmatrix}^T, \begin{pmatrix} 0 & 0 & 0 & 1 \end{pmatrix}^T, \begin{pmatrix} 0 & 0 & 1 & 1 \end{pmatrix}^T \right\},$$

$$C_1 = \left\{ \begin{pmatrix} 0 & 0 & 0 & 0 \end{pmatrix}^T, \begin{pmatrix} 1 & 0 & 1 & 0 \end{pmatrix}^T, \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix}^T, \begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}^T \right\},$$

$$C_2 = \left\{ \begin{pmatrix}0&0&0&0\end{pmatrix}^T, \begin{pmatrix}1&0&0&1\end{pmatrix}^T, \begin{pmatrix}0&1&1&1\end{pmatrix}^T, \begin{pmatrix}1&1&1&0\end{pmatrix}^T \right\},$$
$$C_3 = \left\{ \begin{pmatrix}0&0&0&0\end{pmatrix}^T, \begin{pmatrix}1&0&1&1\end{pmatrix}^T, \begin{pmatrix}0&1&1&0\end{pmatrix}^T, \begin{pmatrix}1&1&0&1\end{pmatrix}^T \right\},$$
$$C_4 = \left\{ \begin{pmatrix}0&0&0&0\end{pmatrix}^T, \begin{pmatrix}1&0&0&0\end{pmatrix}^T, \begin{pmatrix}0&1&0&0\end{pmatrix}^T, \begin{pmatrix}1&1&0&0\end{pmatrix}^T \right\}.$$

Remember that each of this 4-dimensional vector is of the form $(\alpha|\beta)$ and recall the definition of $X_p(\alpha)Z_p(\beta)$ in (3.13).

If we let $Y = X_pZ_p$ and I be the identity matrix the following are 5 classes of commuting unitary matrices as in Theorem 3.3:

$$\begin{aligned}
\mathcal{C}_0 &= \{ Z\otimes I,\, I\otimes Z,\, Z\otimes Z \}, \\
\mathcal{C}_1 &= \{ X\otimes I,\, I\otimes X,\, X\otimes X \}, \\
\mathcal{C}_2 &= \{ Y\otimes I,\, I\otimes Y,\, Y\otimes Y \}, \\
\mathcal{C}_3 &= \{ X\otimes Z,\, Z\otimes Y,\, Y\otimes X \}, \\
\mathcal{C}_4 &= \{ Y\otimes Z,\, Z\otimes X,\, X\otimes Y \},
\end{aligned}$$

which are the matrices of example 3.6 and as we have seen they determine a set of 5 mutually unbiased bases.

The second approach is due to Pittenger and Rubin [6] and consists in looking to $(\mathbb{F}_p)^{2m}$ as $(\mathbb{F}_{p^m})^2$. They then consider a symplectic structure in $(\mathbb{F}_{p^m})^2$ given by:

$$(\alpha,\beta)\circ(\alpha',\beta') = \beta\alpha' - \alpha\beta'^{5}, \tag{3.20}$$

and find p^m+1 lagrangian subspaces with only $(0,0)$ in common:

$$\begin{aligned}
C_\alpha &= \{(\beta,\beta\alpha) : \beta\in\mathbb{F}_{p^m}\}, \qquad \alpha\in\mathbb{F}_{p^m} \\
C_\infty &= \{(0,\beta) : \beta\in\mathbb{F}_{p^m}\}
\end{aligned} \tag{3.21}$$

To finish they relate the two symplectic structures and define the classes C_k of problem 3.9 in terms of C_α and C_∞.

[5] $\alpha\beta$ denotes the product of α and β in $\mathbb{F}_{p^m}$.

Chapter 4

Upper and lower bounds

In this chapter we determine upper and lower bounds for the number of elements in a set of mutually unbiased bases in $\mathbb{C}^d$. The upper bound will be a simple corollary of Theorem 3.3 while the lower bound will be a consequence of Theorem 3.1.

We begin with the upper bound:

Theorem 4.1. *A set of mutually unbiased bases in $\mathbb{C}^d$ contains at most $d+1$ bases.*

Proof. Suppose $\{\mathcal{B}_1, ..., \mathcal{B}_m\}$ is a set of mutually unbiased bases. Then by Theorem 3.3 there are m classes $\mathcal{C}_1, ..., \mathcal{C}_m$ of unitary matrices such that $\mathcal{C}_i \cap \mathcal{C}_j = \{Id\}$ and matrices in $\mathcal{C}_1 \cup ... \cup \mathcal{C}_m$ are pairwise orthogonal. Thus there are $m(d-1)+1$ matrices in $\mathcal{C}_1 \cup ... \cup \mathcal{C}_m$ and they are linearly independent. Since the space $\mathbb{M}_d(\mathbb{C})$ has dimension d^2 we conclude that $m(d-1)+1 \leq d^2$ hence $m \leq d+1$. □

The previous Theorem shows that complete sets of mutually unbiased bases are actually maximal.

As for the lower bound we will decompose the space in subsystems each with dimension equal to a power of a prime and then apply Theorem 3.1.

Theorem 4.2. *Suppose $d = p_1^{e_1} ... p_n^{e_n}$ is the prime factorisation of d and let $d_i = p_i^{e_i}$, $d' = \min_i\{d_i\}$. Then there is a set of $d'+1$ mutually unbiased bases in $\mathbb{C}^d$.*

Proof. We have $\mathbb{C}^d = \mathbb{C}^{d_1} \otimes ... \otimes \mathbb{C}^{d_n}$ and by Theorem 3.1 there is a set of $d_i + 1$ mutually unbiased bases in $\mathbb{C}^{d_i}$ for each i, $\left\{\mathcal{B}_0^i, ..., \mathcal{B}_{d_i}^i\right\}$. Let

$$\mathcal{B}_j^i = \{\left|(\varphi_j^i)_0\right\rangle, ..., \left|(\varphi_j^i)_{d_i-1}\right\rangle\},$$

and

$$\left|\varphi_k^j\right\rangle = \left|(\varphi_{j_1}^1)_{k_1}\right\rangle \otimes ... \otimes \left|(\varphi_{j_n}^n)_{k_n}\right\rangle, \tag{4.1}$$

where $j = (j_1, ..., j_n), 0 \leq j_i \leq d_i$ and $k = (k_1, ..., k_n), 0 \leq k_i \leq d_i - 1$.

Then

$$\mathcal{B}_j = \{\varphi_k^j : k = (k_1, ..., k_n), 0 \leq k_i \leq d_i - 1\} \tag{4.2}$$

is a bases for $\mathbb{C}^d$ and

$$\begin{aligned} \left\langle \varphi_k^j \middle| \varphi_{k'}^{j'} \right\rangle &= \left\langle (\varphi_{j_1}^1)_{k_1} \middle| (\varphi_{j_1'}^1)_{k_1'} \right\rangle ... \left\langle (\varphi_{j_n}^n)_{k_n} \middle| (\varphi_{j_n'}^n)_{k_n'} \right\rangle \\ &= \begin{cases} 0, & \text{if } \exists i : j_i = j_i', k_i \neq k_i' \\ \frac{1}{\sqrt{d}} \prod_{i=1}^n \sqrt{d_i}^{\delta_{j_i - j_i'}}, & \text{otherwise} \end{cases} \end{aligned} \tag{4.3}$$

so all the vectors in $\mathcal{B}_j$ are orthonormal and $\mathcal{B}_j$ is mutually unbiased with $\mathcal{B}_{j'}$ if and only if for every i, $j_i \neq j_i'$. Thus it is possible to extract d' and only d' mutually unbiased bases from (4.2). □

Example 4.3. *If we take $d = 6$ then $d_1 = 2$ and $d_2 = 3$ so $d' = 2$ and we conclude that there are at least 3 mutually unbiased bases in $\mathbb{C}^6$. Those can be constructed from the mutually unbiased bases of $\mathbb{C}^2$, $\mathcal{B}_2, \mathcal{B}_2^1, \mathcal{B}_2^2$, and the ones from $\mathbb{C}^3$, $\mathcal{B}_3, \mathcal{B}_3^1, \mathcal{B}_3^2, \mathcal{B}_3^3$, presented respectively in Theorem 2.5 and in example 2.6. We just need to pair them together without repetitions, for example: $(\mathcal{B}_2, \mathcal{B}_3)$, $(\mathcal{B}_2^1, \mathcal{B}_3^1)$ and $(\mathcal{B}_2^2, \mathcal{B}_3^2)$.*

Chapter 5

The MUB problem for composite dimensions

As stated in the Introduction there is no know answer to the MUB problem in the case of composite dimensions.

The lowest such d is 6 and for this particular dimension P. Butterly and W. Hall have attacked the problem numerically in a recent paper, [7], and showed strong evidence for a negative answer. Their approach is based on a reformulation of the problem in terms of a minimization problem which they then attack with computational algorithms.

They start by relating mutually unbiased bases and unitary matrices in yet another way. Let $\mathcal{B}_1 = \{|\varphi_1^1\rangle, ..., |\varphi_d^1\rangle\}$, $\mathcal{B}_2 = \{|\varphi_1^2\rangle, ..., |\varphi_d^2\rangle\}$ be two bases and let U_i be the matrix that changes bases from $\mathcal{B}_i$ to the standard bases, that is, U_i is such that $\left|\varphi_j^i\right\rangle = \sum_{k=1}^d U_{kj}^i |k\rangle$. Then:

$$\left(U_1^\dagger U_2\right)_{ij} = \langle \varphi_i^1 | \varphi_j^2 \rangle , \tag{5.1}$$

and so $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased if and only if

$$\left|\left(U_1^\dagger U_2\right)_{ij}\right|^2 = \frac{1}{d}, \qquad \forall 1 \leq i,j \leq d \tag{5.2}$$

Thus we can represent M mutually unbiased bases by M unitary matrices, $U_1, ..., U_M$, such that every pair checks this last condition. By a suitable change of bases we can suppose that one of this matrices is the identity matrix, $U_M = I_d$.

Then Butterly and Hall construct a function of $M-1$ unitary matrices that has a global minimum exactly when they constitute a set of matrices with property 5.2:

$$f(U_1, ..., U_{M-1}) = \sum_{1 \leq k < l \leq M-1} \sum_{i,j=1}^{d} \left(\left| \left(U_k^\dagger U_l\right)_{ij} \right|^2 - \frac{1}{d} \right)^2 \tag{5.3}$$

The problem of finding M mutually unbiased bases in $\mathbb{C}^d$ is thus reduced to that of finding a global minimum of (5.3) through all unitary matrices $U_1, ..., U_{M-1}$. This is a conditioned optimization problem which can be turned into an unrestricted one by recalling that every unitary matrix U can be written as the exponential of a hermitian matrix, $U = e^{iH}$. The function which is to be minimized is then

$$f(e^{iH_1}, ..., e^{iH_{M-1}}), \tag{5.4}$$

where $H_1, ..., H_{M-1}$ run through all the hermitian matrices. Since each hermitian matrix is determined by d^2 real numbers the function to be minimized has $(M-1)d^2$ variables.

In their paper Butterly and Hall search for sets of 4 and $d+1$ mutually unbiased bases in dimensions $d = 2, 3, 4, 5, 6, 7$. The algorithm used finds local extrema rather than global hence they run it many times from randomised starting points.

In their tests they were able to find sets of $d+1$ mutually unbiased bases in dimensions $d = 2, 3, 4, 5$ and sets of 4 mutually unbiased bases when $d = 4$ with a success rate of over 99.8% (in 2500 tests). They also found sets of 4 mutually unbiased bases in dimension $d = 5$ with a success rate of 60,4% and sets of 8 and 4 mutually unbiased bases when $d = 7$ at a much lower success rate of around 1%. Yet they found no set of 4 nor 7 mutually unbiased bases in dimension $d = 6$ (even though they ran 10000 tests to find sets of 4 mutually unbiased bases). This is strong numerical evidence for the non existence of more than 3 mutually unbiased bases in $\mathbb{C}^6$.

Chapter 6

Other approaches

In this chapter we connect mutually unbiased bases to combinatorics by means of two conjectures about Latin squares and Finite Geometry.

6.1 Latin Squares

We will develop an analogy between the problem of finding sets of mutually unbiased bases and that of finding mutually orthogonal latin squares, as in [8]. The analogy between latin squares and mutually unbiased bases was first noticed by Zauner, [9], and more recently by A. Klappenecker and M. Rötteler, [10]. We start with the definition of a latin square:

Definition 6.1. *A latin square of order N is a $N \times N$ matrix filled with N symbols such that each symbol occurs exactly once in each row and each column.*

Two latin squares of the same size, A and B, are orthogonal if all the ordered pairs (A_{ij}, B_{ij}) are different.

Example 6.2. *The following is an example of latin square of order* 3 *filled with the symbols* $1, 2, 3$*:*

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{pmatrix}$$

The language of latin squares is not the best to express the analogy. The language of striations is.

Definition 6.3. *Consider a collection of N^2 points. A striation of this set is a partition in N subsets called lines, each with N points. We say that its order is N.*

Two striations of the same set are said to be mutually unbiased if each line in either of the striations has exactly one point in common with each line of the other.

Example 6.4. *Two mutually unbiased striations of order* 3*:*

$$\begin{pmatrix} \otimes & \odot & \oplus \\ \otimes & \odot & \oplus \\ \otimes & \odot & \oplus \end{pmatrix}, \qquad \begin{pmatrix} \otimes & \otimes & \otimes \\ \odot & \odot & \odot \\ \oplus & \oplus & \oplus \end{pmatrix}$$

If you take the collection of cells of a $N \times N$ matrix you can construct two mutually unbiased striations, the striation of rows and the striation of columns. If you now forget about cells and consider instead any collection of N^2 points where you have two mutually unbiased striations, called rows and columns, then you can define a latin square of order N to be a striation which is unbiased with respect to columns and rows. In this language two orthogonal latin squares are mutually unbiased.

Notice that for each set of M mutually orthogonal latin squares you actually have $M + 2$ mutually orthogonal striations.

If you let $M(N)$ denote the maximum number of mutually unbiased striations of a collection of N^2 points and translate the results of the theory of latin squares to the language of striations then you have the following facts:

- $M(N) \leq N+1$, that is the maximum number of latin squares of order N is $N - 1$,
- If N is a power of a prime then $M(N) = N + 1$,
- $M(6) = 3$,
- If $N - 1$ or $N - 2$ is divisible by four and if N is not a sum of squared integers then $M(N) < N + 1$,
- $M(10) < 11$.

The first two results are just equal to those regarding mutually unbiased bases. Also, according to the last chapter there is strong evidence that the number of mutually unbiased bases in dimension 6 is 3 which again agrees with the third result. We are thus led to conjecture that *the number of mutually unbiased bases in dimension d is the same as the number of mutually unbiased striations of order d, or equivalently, to* 2 *plus the number of mutually orthogonal latin squares of order d.* Maybe the last three facts on striations can shed some light over this conjecture.

6.2 Finite Projective Planes

Now we relate the problem of finding sets of mutually unbiased bases to that of finding finite projective planes, by stating a conjecture of Saniga *et al*, [11].

Definition 6.5. *A projective plane consists of points and lines such that:*

- *For every two points there is only one line that passes through them,*
- *Every two lines intersect at only one point,*
- *There are four points such that no three of them are colinear.*

From the definition it follows that every projective plane has the same number of points as lines. In the case of finite projective planes this number is

$$d^2 + d + 1, \tag{6.1}$$

where d is called the order of the plane.

The analogy between mutually unbiased bases and finite projective planes comes from the fact that all the known finite projective planes have as order a power of a prime, thus leading to the conjecture, [11], that *the non-existence of a projective plane of the given order d implies that there is no set of $d+1$ mutually unbiased bases in the corresponding $\mathbb{C}^d$.*

Actually there is a connection between projective planes and latin squares[1]:

Theorem 6.6. *There exists a finite projective plane of order d if and only if there exists a set of $d-1$ mutually orthogonal latin squares.*

So the conjecture about latin squares implies that of finite projective planes but the former is stronger.

[1]For an account of the proof check for example [12].

Chapter 7

Conclusion

The main concern of this text was to answer the MUB problem, that is, to find sets of $d+1$ mutually unbiased bases in $\mathbb{C}^d$.

We started by answering this problem positively when d is a prime. The approach is that of Bandyopadhyay *et al*, [5], with slight changes that allow us to find (non-complete) sets of MUB in other dimensions. Actually there is a minor mistake in the approach of [5] because as we have noticed the cases of even and odd dimensions need to be considered separately. An essential ingredient in the proof is a class of matrices which can be thought of as generalized Pauli matrices. This proof only works when d is a prime because $\mathbb{Z}_d$ is a field if and only if d is a prime.

We have also addressed the same problem when d is a power of a prime. The approach is once again that of Bandyopadhyay *et al*, which relies on a strong connection between sets of mutually unbiased bases and classes of commuting unitary matrices. A small error in Theorem 3.2 of [5] was detected. This case obviously has as a particular case the previous one and we have considered it separately capturing the same set of MUB as before. This is due to the fact that tensors of the generalized Pauli matrices are also a main ingredient of this approach. The proof of Theorem 3.1, which fills the entire Chapter 3, gives an algorithm for finding complete sets of mutually unbiased bases and we followed it in Example 3.12 for the case $d = 4$.

In other dimensions the MUB problem is still unsolved. Though there is numerical evidence that, for the particular case $d = 6$, the answer is negative. This is the content of Chapter 5 where we explained how this evidence was obtained.

We concluded by emphasizing two possible connections between mutually unbiased bases, latin squares and finite projective planes. These may help solve the MUB problem in the general case.

Appendix A

Quantum computation

We now make a brief introduction to Quantum Computation. It's certainly not the best and its objective is just to make this text self-contained. For a better introduction to the subject we refer the reader to [13] and [14].

A.1 Dirac's bra-ket notation

We start by presenting Dirac's Bra-Ket notation which is widely used in the context of Quantum Mechanics.

Let $\mathcal{H}$ be a vector space with some inner product. We denote the elements of $\mathcal{H}$ by $|\psi\rangle$ and the inner product of $|\psi\rangle$ and $|\varphi\rangle$ by:

$$\langle\varphi\,|\psi\rangle = \langle\psi\,|\varphi\rangle^* \tag{A.1}$$

The inner product of $\mathcal{H}$ determines a canonical identification between $\mathcal{H}$ and its dual, $\mathcal{H}^*$, which assigns to each $|\psi\rangle$ its dual $\langle\psi|$ such that:

$$\langle\psi|\,(|\varphi\rangle) = \langle\psi\,|\varphi\rangle \tag{A.2}$$

We call $|\psi\rangle$ a ket and $\langle\psi|$ a bra, hence the name of the notation.

We represent by $|\psi\rangle\langle\psi'|$ the operator such that

$$|\psi\rangle\left\langle\psi'\right|(|\varphi\rangle) = \left\langle\psi'\,|\varphi\right\rangle|\psi\rangle \tag{A.3}$$

Example A.1. *Let $\mathcal{H} = \mathbb{C}^2$ and let $\{|0\rangle, |1\rangle\}$ be its canonical orthonormal basis:*

$$|0\rangle = (1,0), |1\rangle = (0,1)$$

Let $|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ and $|\varphi\rangle = \gamma\,|0\rangle + \delta\,|1\rangle$. If we use the matricial notation to represent the elements of $\mathcal{H}$ and $\mathcal{H}^*$ in terms of this basis then:

$$|\psi\rangle = \begin{pmatrix}\alpha\\ \beta\end{pmatrix}, \qquad |\varphi\rangle = \begin{pmatrix}\gamma\\ \delta\end{pmatrix}, \qquad \alpha,\beta,\gamma,\delta \in \mathbb{C}$$

$$\langle\psi| = \begin{pmatrix}\alpha^* & \beta^*\end{pmatrix}, \qquad \langle\varphi| = \begin{pmatrix}\gamma^* & \delta^*\end{pmatrix},$$

$$\langle\psi\,|\varphi\rangle = \alpha^*\gamma + \beta^*\delta$$

$$|\psi\rangle\langle\varphi| = \begin{pmatrix}\gamma^*\alpha & \delta^*\alpha \\ \gamma^*\beta & \delta^*\beta\end{pmatrix}$$

A.2 Postulates of Quantum Mechanics

Now we state the postulates of Quantum Mechanics, which are the rules of Quantum Computation.

A.2.1 The state space

Given a physical system the state completely describes it and is the mathematical object by which we represent it. In Classical Mechanics the state is a vector of coordinates of speed and position and in Quantum Mechanics it is a unitary vector in a Hilbert space, $\mathcal{H}$, which we call the state space.

In Quantum Computation we deal usually with state spaces of dimension 2, $\mathcal{H} = \mathbb{C}^2$, (which can represent the spin of a particle or the polarization of a photon) but usually $\mathcal{H}$ is infinite dimensional. The vectors of $\mathcal{H}$ are represented using the Dirac's bra-ket notation, $|\psi\rangle$. Since every state is unitary we have $\langle\psi\,|\psi\rangle = 1$.

In the case of Quantum Computation the canonical orthonormal basis of $\mathbb{C}^2$ (also called the computational bases) is constituted by $|0\rangle$ and $|1\rangle$. Hence any state $|\psi\rangle \in \mathbb{C}^2$ can be written in the form:

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{A.4}$$

where $\alpha, \beta \in \mathbb{C}, |\alpha|^2 + |\beta|^2 = 1$ and this is what we call a qubit.

When we deal with systems of dimension n we usually represent the canonical bases vectors by $|i\rangle\,, i = 0, ..., n-1$.

A.2.2 Evolution

So given a state of a system how can it evolute with time? According to Quantum Mechanics if a system is in a state $|\psi_{t_1}\rangle$ at a given time t_1 then it can only evolute unitarily, that is, in time t_2 it will be in the state:

$$|\psi_{t_2}\rangle = U\,|\psi_{t_1}\rangle\,, \tag{A.5}$$

where U is the unitary operator which dictates the evolution.

Actually this is the discrete version of the postulate of evolution and deals only with discrete variations of time, which is the only thing that

matters for Quantum Computation. It is a particular case of the continuous version which says that $|\psi_t\rangle$ evolves according to the Schrödinger equation:

$$i\hbar\frac{d}{dt}|\psi_t\rangle = H|\psi_t\rangle, \tag{A.6}$$

where H is an operator called the Hamiltonian of the system.

A.2.3 Observables

An observable is a property of the system which can, in principle, be measured. In this framework it is represented by a self-adjoint operator, A, and its eigenvalues (which are all real) are the possible outcomes of the measurement.

To avoid subtleties we now consider only the finite-dimensional case. Then we know that A has a spectral decomposition:

$$A = \sum_i a_i P_i, \tag{A.7}$$

where each a_i is an eigenvalue of A and P_i is the corresponding orthogonal projection into the eigenspace. This decomposition will be important for the following postulate.

A.2.4 Quantum Measurements

We now state the postulate for projective measurements. This could be stated in a (apparently) more general way involving other types of measurements but since we don't need it for this text we chose the simplest version of the postulate.

According to Quantum Mechanics when we have an observable A, and we measure it on a system at a given state $|\psi\rangle$ then we get as a result one of the eigenvalues of A, a_i, and the state of the system is projected into the corresponding eigenspace, that is, right after the measurement the state of the system is:

$$\frac{P_i|\psi\rangle}{\|P_i|\psi\rangle\|} \tag{A.8}$$

Moreover the outcome a_i is obtained with probability:

$$Prob(a_i) = \|P_i|\psi\rangle\|^2 \tag{A.9}$$

Notice that if we repeat the same measurement twice then we get the same result.

A.2.5 Composite Systems

Now suppose we have more than one physical system. How is the state space of the whole related to that of the parts? Quantum mechanics says that the state space of a composite system is the tensor product of the state spaces of the individual components. Moreover if the system has n components and each is in the state $|\psi_i\rangle$ then the state of the system is:

$$|\psi\rangle = |\psi_1\rangle \otimes ... \otimes |\psi_n\rangle , \tag{A.10}$$

also denoted by $|\psi_1\rangle ... |\psi_n\rangle$ or more shortly $|\psi_1 ... \psi_n\rangle$.

It is worth mentioning that in a composite system not all the states are of the form of A.10 and actually most of them are not. This means that you can have a system that is not totally determined by the information of the states of its subsystems (there is additional information about correlations of states). Hence the information of the sum of the parts is more than the sum of the information of the parts. This leads to the existence of entangled states, which also have application in quantum key distribution.

The most important case of composite systems in Quantum Computation is that of multiple qubits. If we have a system of 2 qubits for instance then the state space will be $\mathcal{H}_2 \otimes \mathcal{H}_2$ and a bases for that space is:

$$\{|00\rangle , |01\rangle , |10\rangle , |11\rangle\}$$

This ends the mathematical formulation of Quantum Mechanics.

A.3 The Density Operator

Now we introduce a tool which is particularly suited to deal with the states of parts of a larger system. This tool is the density operator and will allow us to reformulate the previous postulates in another language.

Suppose you have a system which can be in a state $|\psi_i\rangle$ with probability p_i. Then the density operator of the system is:

$$\rho \equiv \sum_i p_i |\psi_i\rangle \langle\psi_i| \tag{A.11}$$

So instead of representing the state of a system by a vector we will instead use the density operator, also called density matrix. From A.11 it follows that a density matrix is positive definite and has unitary trace.

The density operator can also be thought of as representing an ensemble of systems prepared in state $|\psi_i\rangle$ with probability p_i.

In the simplest case the density operator of the system is $|\psi\rangle \langle\psi|$ so that the system is known to be in state $|\psi\rangle$. If this happens then the system is said to be in a pure state. Otherwise it is said to be in a mixed state.

We now reformulate the postulates in the language of density operators:

1. An isolated physical system is completely described by its density operator.

2. The evolution of a closed quantum system is described by an unitary transformation U. If the initial density operator of the system is ρ then after the evolution it will be:

$$\rho' = U\rho U^\dagger \tag{A.12}$$

3. If you measure an observable A in a system in the state ρ then the outcome will be one of the eigenvalues of A, a_i with probability:

$$Prob(a_i) = Tr(P_i\rho), \tag{A.13}$$

where P_i is the orthogonal projection in the eigenspace corresponding to a_i. Right after the measurement the system's state will be:

$$\rho' = \frac{P_i\rho P_i}{Tr(P_i\rho)} \tag{A.14}$$

4. If you have n systems prepared in the states $\rho_1, ..., \rho_n$ then the state of the total system will be $\rho_1 \otimes ... \otimes \rho_n$.

A.4 Quantum Key Distribution

The purpose of this section is to introduce the reader to Quantum Key Distribution, QKD, by describing the BB84 protocol.

The objective of Key Distribution is for two parties (traditionally called Alice and Bob) to establish a common private key, so they can communicate privately. QKD is a way to achieve this which is provably secure. It relies on some fundamental results from the theory of Quantum Computation, namely[1]:

Theorem A.2 (No-Cloning)**.** *It's impossible to copy a qubit in an unknown state.*

Theorem A.3. *Given a qubit, $|\psi\rangle$, which can be in two non-orthogonal states then any information gain about the state of $|\psi\rangle$ disturbs it: $|\psi\rangle \rightarrow |\psi'\rangle$.*

One of the QKD protocols is BB84.

[1]For an account of the proof of these results check [13].

A.4.1 BB84 protocol

BB84 was developed by C. Bennett and G. Brassard in 1984, [15]. We describe it briefly.

Alice and Bob pretend to establish a binary key between them. This will be done bit by bit and in the process two bases for $\mathbb{C}^2$ will be used to encode the transmited bits: the computational one $\{|0\rangle, |1\rangle\}$ and the diagonal one $\{|+\rangle, |-\rangle\}$, where

$$|\pm\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle) \tag{A.15}$$

The protocol goes as follows:

1. For each bit, Alice starts by choosing randomly one of the two bases in which to encode it. 0 is encoded in $|0\rangle$ or $|+\rangle$ and 1 is encoded in $|1\rangle$ or $|-\rangle$ depending on the chosen basis. She then sends the encoded bit, $|\psi\rangle$, to Bob.

2. Bob receives the qubit sent by Alice which may or may not match the original, depending on interference in the channel, $|\psi'\rangle$. He then chooses randomly a basis to decode the qubit using the same decoding scheme as the encoding. This way Alice and Bob have established a bit between them which is guaranteed to agree if and only if they chose the same bases and there was no interference in the process of transmission.

3. They repeat steps 1 and 2 for each bit they want to share, thus getting a key of length n. Then they publicly communicate the chosen bases in those steps and discard all the bits in which they chose a different basis reducing the size of the key to n'.

4. At this time if there was no interference then the keys of Alice and Bob should be equal. To test this, they choose a sample to compare and discard, thus getting a key of length n''.

5. If the rate of disturbance in the previous test is not acceptable the keys are discarded and the protocol is restarted. Otherwise Alice and Bob proceed with privacy amplification and information reconciliation in order to extract the final key.

Example A.4. *This is an example of the application of the protocol*[2]*:*

[2] $\nrightarrow$ denotes an error in the transmission.

Bit_A	$Base_A$	$Qubit_A$	$\rightarrow$	$Qubit_B$	$Base_B$	Bit_B
0	B_1	$\|0\rangle$	$\rightarrow$	$\|0\rangle$	B_1	0
1	B_2	$\|-\rangle$	$\rightarrow$	$\|-\rangle$	B_1	0
1	B_1	$\|1\rangle$	$\rightarrow$	$\|1\rangle$	B_1	1
0	B_1	$\|0\rangle$	$\nrightarrow$	$\|-\rangle$	B_1	1
1	B_2	$\|-\rangle$	$\rightarrow$	$\|-\rangle$	B_2	1
0	B_1	$\|0\rangle$	$\rightarrow$	$\|-\rangle$	B_1	0
0	B_2	$\|+\rangle$	$\nrightarrow$	$\|-\rangle$	B_2	1
1	B_1	$\|1\rangle$	$\rightarrow$	$\|1\rangle$	B_2	1

After Alice and Bob discard the bits in which their bases were not the same they end with the keys 010100 and 011101 respectively. In this case the rate of error is $1/3$ *and could be due to the noise in the channel or an eventual eavesdropping.*

Bibliography

[1] W. K. Wootters and B. D. Fields. Optimal state-determination by mutually unbiased measurements. *Annals of Physics*, 191:363–381, May 1989.

[2] D. Bruß. Optimal Eavesdropping in Quantum Cryptography with Six States. *Physical Review Letters*, 81:3018–3021, October 1998. `arXiv:quant-ph/9805019`.

[3] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of Quantum Key Distribution Using d-Level Systems. *Physical Review Letters*, 88(12):127902, March 2002. `arXiv:quant-ph/0107130`.

[4] I. D. Ivanovic. Geometrical description of quantal state determination. *Journal of Physics A Mathematical General*, 14:3241–3245, December 1981.

[5] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. A new proof for the existence of mutually unbiased bases. *ArXiv Quantum Physics e-prints*, March 2001. `arXiv:quant-ph/0103162v3`.

[6] A. O. Pittenger and M. H. Rubin. Mutually Unbiased Bases, Generalized Spin Matrices and Separability. *ArXiv Quantum Physics e-prints*, August 2003. `arXiv:quant-ph/0308142`.

[7] P. Butterley and W. Hall. Numerical evidence for the maximum number of mutually unbiased bases in dimension six. *Physics Letters A*, 369:5–8, September 2007. `arXiv:quant-ph/0701122`.

[8] W. K. Wootters. Quantum measurements and finite geometry. *ArXiv Quantum Physics e-prints*, June 2004. `arXiv:quant-ph/0406032`.

[9] G. Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. Diploma thesis, Universität Wien, 1999.

[10] A. Klappenecker and M. Roetteler. Constructions of Mutually Unbiased Bases. *ArXiv Quantum Physics e-prints*, September 2003. `arXiv:quant-ph/0309120`.

[11] M. Saniga, M. Planat, and H. Rosu. Letter to the editor: Mutually unbiased bases and finite projective planes. *Journal of Optics B: Quantum and Semiclassical Optics*, 6:L19–L20, September 2004. arXiv:arXiv:math-ph/0403057.

[12] I. Wanless. *Lecture 7 on Combinatorial Matrices*. Australian Mathematical Sciences Institute Summer School, 2005 edition. Available from: http://wwwmaths.anu.edu.au/events/amsiss05/courses.html#combmat.

[13] M. Nielsen and I. Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, Cambridge, 2000.

[14] J. Preskill. *Lecture Notes on Quantum Computation*. Available from: http://www.theory.caltech.edu/people/preskill/ph229/#lecture.

[15] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, Bangalore, India, December 1984.