ON MUTUALLY UNBIASED BASES

by

Rahim Taghikhani

A Thesis submitted to the Faculty of Graduate Studies of

The University of Manitoba

in partial fulfilment of the requirements for the degree of

MASTER OF SCIENCE

Department of Mathematics

University of Manitoba

Winnipeg, Manitoba

Abstract

Two orthonormal bases $\mathcal{B}_1 = \{\mathbf{u}_1, \ldots, \mathbf{u}_d\}$ and $\mathcal{B}_2 = \{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$ in the complex space of dimension d, $\mathbb{C}^d$, are said to be mutually unbiased if the square of the magnitude of the inner product of any vector in $\mathcal{B}_1$ with any vector in $\mathcal{B}_2$ is equal to the reciprocal of the dimension d, in other words $|\langle \mathbf{u}_i, \mathbf{v}_j \rangle|^2 = \frac{1}{d}$, for $i, j = \{1, \ldots, d\}$. Mutually unbiased bases are used for optimal state determination of mixed quantum states [42].

It is known that in any dimension d, the number of mutually unbiased bases is at most $d + 1$ [1]. Ivanovic [22] found a complete set of mutually unbiased bases for prime dimensions. His construction was generalized by Wootters and Fields [42] for prime power dimensions. There is a strong connection between maximally commuting bases of orthogonal unitary matrices and mutually unbiased bases. Based on this connection, there exits a constructive proof of the existence of a complete set of mutually unbiased bases for prime power dimensions [1]. This thesis is an exploration on construction of mutually unbiased bases.

Acknowledgment

I would like to express my sincere gratitude to my advisor Prof. Robert Craigen for his continuous support of my Masters study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me while I did research and wrote this thesis. Besides my advisor, I would like to thank the rest of my thesis committee: Prof. Ben Li and Prof. Jaydeep Chipalkatti, for their encouragement and insightful comments.

Last but not least, I would like to thank my family: my parents Hadi and Zahra, for supporting me spiritually throughout my life and my brother Vahid and my sister Tahereh.

TABLE OF CONTENTS

Chapter 1

INTRODUCTION

Definition 1.1. *The **dot product** of row vectors* $\mathbf{u}$ *and* $\mathbf{v}$ *in complex vector space of dimension* d, $\mathbb{C}^d$, *is defined by*

$$\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}\mathbf{v}^* = \sum_{j=1}^{d} u_j \overline{v_j},$$

where u_j *and* v_j *are the* j*th components of* $\mathbf{u}$ *and* $\mathbf{v}$ *respectively. Two vectors* $\mathbf{u}$ *and* $\mathbf{v}$ *are **orthogonal** if* $\langle \mathbf{u}, \mathbf{v} \rangle = 0$.

Definition 1.2. *A **basis** $\mathcal{B}$ for a vector space $\mathcal{H}$ over a field $\mathbb{F}$ is a set of linearly independent vectors such that any vector in the space can be given as a linear combination of the vectors of $\mathcal{B}$. Basis $\mathcal{B}$ is **orthonormal** if all vectors in $\mathcal{B}$ are mutually orthogonal and of unit length.*

1.1 Quantum Systems

In physics, a **quantum state** is a set of mathematical variables that describes a quantum system. For example, the set of 4 numbers (n, l, m_l, m_s) are parameters that define the state of an electron within a hydrogen atom as follows

(1) n is the principal quantum number,

(2) l is the azimuthal quantum number,

(3) m_l is the magnetic quantum number,

(4) m_s is the spin projection quantum number.

For details see [12].

If d parameters are used to identify a state of a quantum system, they can be presented as a vector in d-dimensional space $\mathcal{H}$. Thus every state of the system corresponds to a vector from $\mathcal{H}$. This vector is called a **ket vector** or **pure state**, and is denoted as a d-tuple

$$|\psi\rangle = (\psi_1, \psi_2, \ldots, \psi_d)\,.$$

The Hermitian adjoint of $|\psi\rangle$ is denoted by $\langle\psi|$, and can be expressed in matrix terms as

$$\langle\psi| = \begin{pmatrix} \overline{\psi_1} \\ \overline{\psi_2} \\ \vdots \\ \overline{\psi_d} \end{pmatrix}.$$

In this context we shall distinguish vectors by bold typeface, $\mathbf{v}$, and the Hermitian adjoint of $\mathbf{v}$ by $\mathbf{v}^*$.

In order to describe a quantum system whose state is not completely known, a mixed state tool called the **density operator** or **statistical operator** was developed by

Von Neumann [37]. If a quantum system is in one of the states $\mathbf{u}_i \in \mathbb{C}^d$, $1 \leq i \leq d$, $\|\mathbf{u}_i\| = 1$, with respective probabilities $p_i \in [0,1]$, then set $\{p_i, \mathbf{u}_i\}$ is called an **ensemble of pure states** and the density operator is defined by

$$\rho = \sum_{i=1}^{d} p_i \mathbf{u}_i^* \mathbf{u}_i, \quad \sum_{i=1}^{d} p_i = 1.$$

ρ is a $d \times d$ matrix containing d^2 entries which can be identified by $d^2 - 1$ parameters. Density matrices provide a more general way of describing a quantum system than pure states. Moreover, pure states represent special cases of density matrices. An **observable** is an Hermitian matrix of the form

$$A = \sum_{i=1}^{d} \lambda_i \mathbf{v}_i^* \mathbf{v}_i, \tag{1.1}$$

where $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ is an orthonormal basis in $\mathbb{C}^d$ and each $\lambda_i \in \mathbb{C}$. A **measurement** corresponding to the observable A on ρ is given by

$$\mathrm{Tr}(A\rho) = \sum_{i=1}^{d} \sum_{j=1}^{d} \lambda_i p_j |\langle \mathbf{v}_i, \mathbf{u}_j \rangle|^2. \tag{1.2}$$

It is well known that in a d-dimensional state space, it is enough to have $d+1$ observables of the form (1.1) to determine a density matrix of a quantum system [10]. Wooters and Fields [42] showed that if we find $d+1$ observable, $A_1, A_2, \ldots, A_{d+1}$, where the kth observable is given by

$$A_k = \sum_{i=1}^{d} \lambda_i^k \mathbf{v}^{*k}{}_i \mathbf{v}_i^k, \quad k = 1, 2, \ldots, d+1 \tag{1.3}$$

where for each k, $\{\mathbf{v}_1^k, \mathbf{v}_2^k, \ldots, \mathbf{v}_d^k\}$ is an orthonormal basis in $\mathbb{C}^d$, each $\lambda_i^k \in \mathbb{C}$, and for all $i, j \in \{1, 2, \ldots, d\}$ and $k, l \in \{1, 2, \ldots, d+1\}$, $k \neq l$ such that

$$|\langle \mathbf{v}_i^k, \mathbf{v}_j^l \rangle|^2 = \frac{1}{d}, \tag{1.4}$$

then we have an optimal set of measurements–meaning that the probability of error of finding the state of the quantum system is minimized.

For example, let

$$\rho = \frac{1}{2} \begin{pmatrix} 1+a & b-ic \\ b+ic & 1-a \end{pmatrix}$$

be the density matrix of a quantum system. Define observables A_1, A_2 and A_3 as follows

$$A_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \end{pmatrix} - \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \end{pmatrix},$$

$$A_2 = \frac{1}{2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 \\ -1 \end{pmatrix} \begin{pmatrix} 1 & -1 \end{pmatrix},$$

$$A_3 = \frac{1}{2} \begin{pmatrix} 1 \\ i \end{pmatrix} \begin{pmatrix} 1 & -i \end{pmatrix} - \frac{1}{2} \begin{pmatrix} 1 \\ -i \end{pmatrix} \begin{pmatrix} 1 & i \end{pmatrix}.$$

Then the measurements on ρ using (1.2) are $\mathrm{Tr}(A_1\rho) = a$, $\mathrm{Tr}(A_2\rho) = b$, $\mathrm{Tr}(A_3\rho) = c$. Thus ρ is identified by A_1, A_2 and A_3.

The argued property of the bases in (1.4) leads to the following definition.

Definition 1.3. *Let $\mathcal{B} = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_d\}$ and $\mathcal{B}' = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ be two orthonormal bases in $\mathbb{C}^d$. They are said to be* ***mutually unbiased bases*** *(MUB) if and only if*

$$|\langle \mathbf{u}_i, \mathbf{v}_j \rangle|^2 = \frac{1}{d}, \tag{1.5}$$

for all $i, j \in \{1, \ldots, d\}$.

Definition 1.3 can be generalized for more than two bases. m orthonormal bases $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m$ are mutually unbiased bases if each pair of the bases are mutually unbiased bases.

Example 1.4. *For $d = 2$, the following are 3 MUBs*

$$\mathcal{B}_1 = \{(1,0), (0,1)\}, \quad \mathcal{B}_2 = \left\{ \frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(1,-1) \right\}, \quad \mathcal{B}_3 = \left\{ \frac{1}{\sqrt{2}}(1,i), \frac{1}{\sqrt{2}}(1,-i) \right\}.$$

1.2 The MUB problem

Mutually unbiased bases have a special role in determining the state of a finite-dimensional quantum system. One application of mutually unbiased bases is that they minimize the error in determining the state of a finite-dimensional quantum system from measurements as described in Section 1.1. See [9] and [10] for more details.

Mutually unbiased bases were introduced in the literature of quantum mechanics in 1960 in the work of Schwinger [34]. Ivanovic [22] provided a construction of $d + 1$

mutually unbiased bases for odd prime d-dimensional spaces. It was also shown in [22] that $d+1$ is an upper bound for the number of MUBs in $\mathbb{C}^d$. When this bound is attained, we say a **complete set** of MUBs of dimension d exists. Complete sets of MUBs exist in all prime power dimensions [42] but it is unknown whether they can be attained in non-prime power dimensions.

Although the notion arises from a problem concerning physical systems, MUBs are a mathematical structure, and will be treated as such. There are still many open problems and conjectures. For example, is there a complete set of mutually unbiased bases of dimension 6? The main question in the study of MUBs is: for a given dimension d, what is the maximum number of MUBs? Zauner's conjecture [44] states that there exists a complete set of $d+1$ MUBs in dimension d if and only if d is a prime power.

1.3 Outline

In Chapter 2 we will discuss constructions of MUBs and also the relationship between MUBs and special classes of unitary matrices. Then we introduce Pauli matrices and Spin matrices— unitary matrices which provide the conditions that lead to the MUBs construction. Moreover, in Chapter 2 we give a construction of MUBs using difference sets. In Chapter 3 we will consider the connection between MUBs and 2-designs and show that they are equivalent. In Chapter 4 we give a combinatorial construction

based on Latin Squares. Finally in Chapter 5 we will discuss the case of real MUBs.

Chapter 2

CONSTRUCTION OF MUTUALLY UNBIASED BASES

In this chapter we demonstrate a construction of MUBs using orthogonal unitary matrices and some algebraic constructions for MUBs.

2.1 Construction of MUBs using Pauli matrices

Definition 2.1. *Let $M_d(\mathbb{C})$ be the set of $d \times d$ complex matrices. We say $U \in M_d(\mathbb{C})$ is **unitary matrix** if $UU^* = \mathbb{I}_d$, where $U^* = \overline{U}^T$, and $\mathbb{I}_d$ is the identity matrix of order d. The operator $*$ is called **Hermitian adjoint**. If $U = U^*$, then U is **Hermitian**.*

It is well known that if U is a $d \times d$ unitary matrix, then U has d orthonormal eigenvectors in $\mathbb{C}^d$ (see [20]).

Theorem 2.2 ([1])**.** *Let $\mathcal{B}_1 = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ be an orthonormal basis in $\mathbb{C}^d$. Suppose there is a unitary matrix U such that $U\mathbf{v}_i = \beta_i \mathbf{v}_{i+1}$, where $\beta_i \in \mathbb{C}$, $|\beta_i|$=1, $1 \leq i \leq d$, and $\mathbf{v}_{d+1} = \mathbf{v}_1$. Assume that the orthonormal basis $\mathcal{B}_2 = \{\mathbf{w}_1, \mathbf{w}_2, \ldots, \mathbf{w}_d\}$ consists of orthonormal eigenvectors of U. Then $\mathcal{B}_1$ and $\mathcal{B}_2$ are MUBs.*

Proof. Let U be a unitary matrix which applies a cyclic shift modulo a phase on the elements of the basis $\mathcal{B}_1$, i.e., $U\mathbf{v}_i = \beta_i \mathbf{v}_{i+1}$. Let $U\mathbf{w}_i = \lambda_i \mathbf{w}_i$, where λ_i is an

eigenvalue of U. Since U is unitary, $|\lambda_i| = 1$. For every $1 \leq j \leq d$, the inner product of $\mathbf{w}_j$ and $\mathbf{v}_1$ is

$$\begin{aligned} |\langle \mathbf{w}_j, \mathbf{v}_1 \rangle| &= |\langle U\mathbf{w}_j, U\mathbf{v}_1 \rangle| \\ &= |\lambda_j \langle \mathbf{w}_j, U\mathbf{v}_1 \rangle| \\ &= |\beta_1^* \langle \mathbf{w}_j, \mathbf{v}_2 \rangle| \\ &= |\langle \mathbf{w}_j, \mathbf{v}_2 \rangle|. \end{aligned}$$

Continuing in this fashion we obtain

$$|\langle \mathbf{w}_j, \mathbf{v}_1 \rangle| = |\langle \mathbf{w}_j, \mathbf{v}_i \rangle|, \quad \text{for } 1 \leq i \leq d.$$

Since $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ is an orthonormal basis in $\mathbb{C}^d$ then

$$\mathbf{w}_j = \sum_{i=1}^{d} \langle \mathbf{w}_j, \mathbf{v}_i \rangle \mathbf{v}_i.$$

Therefore

$$\begin{aligned} \langle \mathbf{w}_j, \mathbf{w}_j \rangle &= \sum_{i=1}^{d} |\langle \mathbf{w}_j, \mathbf{v}_i \rangle|^2 \\ &= \sum_{i=1}^{d} |\langle \mathbf{w}_j, \mathbf{v}_1 \rangle|^2 \\ &= d|\langle \mathbf{w}_j, \mathbf{v}_1 \rangle|^2 \\ &= 1. \end{aligned}$$

Thus, $|\langle \mathbf{w}_j, \mathbf{v}_i \rangle|^2 = \dfrac{1}{d}$, for all $1 \leq i, j \leq d$. So $\mathcal{B}_1$ and $\mathcal{B}_2$ are MUBs. □

By Theorem 2.2 if we find a unitary matrix U that acts on an orthonormal basis $\mathcal{B}$ by shifting vectors in $\mathcal{B}$ cyclically up to a unit complex number, then the set of eigenvectors of U and $\mathcal{B}$ are MUBs. In this section we examine a special class of unitary matrices called Pauli matrices that satisfy the hypothesis of Theorem 2.2. Results are due to S. Bandyopadhyay et al [1].

Definition 2.3. *The **Pauli matrices** are a set of four 2×2 complex matrices which are Hermitian and unitary. These are usually indicated by the Greek letter σ as follows*

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

For any prime number p, Pauli matrices σ_x and σ_z are generalized by

$$P = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & \cdots & 0 & 1 & 0 \end{pmatrix}_{p\times p}, \quad Q = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{p-1} \end{pmatrix}_{p\times p},$$

where $\omega = e^{2\pi i/p}$.

Let $\{\mathbf{e}_0, \mathbf{e}_1, \ldots, \mathbf{e}_{p-1}\}$ be the standard basis for $\mathbb{C}^p$. All algebraic operations in the indices are reduced modulo p which is a prime number. It is easy to see that

$$P\mathbf{e}_j = \mathbf{e}_{j+1}, \quad Q\mathbf{e}_j = \omega^j \mathbf{e}_j, \quad PQ^k\mathbf{e}_j = (\omega^k)^j \mathbf{e}_{j+1}. \tag{2.1}$$

The following lemma characterizes the eigenvectors of PQ^k for every $0 \leq k \leq p-1$.

Lemma 2.4 ([1]). *For $k \in \mathbb{Z}_p$, the eigenvectors of PQ^k are*

$$\mathbf{w}_t^k = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^t)^{p-j} (\omega^{-k})^{s_j} \mathbf{e}_j, \qquad 0 \leq t \leq p-1, \tag{2.2}$$

where $s_j = j + \cdots + p - 1$.

Proof. By direct calculation and using (2.1)

$$\begin{aligned} PQ^k \mathbf{w}_t^k &= \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^t)^{p-j} (\omega^{-k})^{s_j} (\omega^k)^j \mathbf{e}_{j+1} \\ &= \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^t)^{p-j} (\omega^{-k})^{s_{j+1}} \mathbf{e}_{j+1} \\ &= \frac{1}{\sqrt{p}} \sum_{m=1}^{p} (\omega^t)^{p-m+1} (\omega^{-k})^{s_m} \mathbf{e}_m \\ &= \omega^t \frac{1}{\sqrt{p}} \sum_{m=1}^{p} (\omega^t)^{p-m} (\omega^{-k})^{s_m} \mathbf{e}_m \qquad (2.3) \\ &= \omega^t \mathbf{w}_t^k. \end{aligned}$$

Equality (2.3) is because $\mathbf{e}_p = \mathbf{e}_0$. Thus, $\mathbf{w}_t^k$, $t \in \mathbb{Z}_p$, are eigenvectors of PQ^k. □

It is easy to check that for each $k \in \mathbb{Z}_p$, PQ^k is unitary. Moreover, the set of eigenvectors of PQ^k, $\mathcal{B}_k = \{\mathbf{w}_t^k : t \in \mathbb{Z}_p\}$ is an orthonormal basis for $\mathbb{C}^p$. We show that each unitary matrix $U = PQ^l$ permutes vectors in $\mathcal{B}_k$ up to the scalar factor $\beta_t^k = \omega^{t+k-l}$, which has norm 1, as follows

$$PQ^l \mathbf{w}_t^k = \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^t)^{p-j} (\omega^{-k})^{s_j} (\omega^l)^j \mathbf{e}_{j+1}$$

$$
\begin{aligned}
&= \frac{1}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^t)^{p-j+1} (\omega^{-k})^{s_{j-1}} (\omega^l)^{j-1} \mathbf{e}_j \\
&= \frac{\omega^{t-l}}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^t)^{p-j} (\omega^{-k})^{s_j} (\omega^k)^{j-1} (\omega^l)^j \mathbf{e}_j \\
&= \frac{\omega^{t+k-l}}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^t)^{d-j} (\omega^{-k})^{s_j} (\omega^{l-k})^j \mathbf{e}_j \\
&= \frac{\omega^{t+k-l}}{\sqrt{p}} \sum_{j=0}^{p-1} (\omega^{t+k-l})^{p-j} (\omega^{-k})^{s_j} \mathbf{e}_j \\
&= \omega^{t+k-l} \mathbf{w}_{t+k-l}^k. \qquad (2.4)
\end{aligned}
$$

Fixing $k, l \in \mathbb{Z}_p$, let $\mathcal{B}_k = \{\mathbf{w}_t^k : t \in \mathbb{Z}_p\}$ and $\mathcal{B}_l = \{\mathbf{w}_t^l : t \in \mathbb{Z}_p\}$ that is, the set of eigenvectors of PQ^k and PQ^l, respectively. According to (2.4), $U = PQ^l$ acts on $\mathcal{B}_k$ by permuting $\mathbf{w}_t^k$ to $\mathbf{w}_{t+k-l}^k$, up to a scalar factor ω^{t+k-l}, for each $t \in \mathbb{Z}_p$. Writing $b = k - l$, then U cyclically permutes vectors $\mathbf{w}_t^k, \mathbf{w}_{t+b}^k, \mathbf{w}_{t+2b}^k, \ldots, \mathbf{w}_{t+(p-1)b}^k$, up to a scalar factor, for $U\mathbf{w}_{t+(p-1)b}^k = \omega^{t+pb}\mathbf{w}_{t+pb}^k = \omega^t \mathbf{w}_t^k$.

Further, if $k \neq l$ then $\{0, b, 2b, \ldots, (p-1)b\} = \mathbb{Z}_p$, since p is prime, and so U cyclically permutes the orthonormal basis $\mathcal{B}_k$ up to a scalar factor. By Theorem 2.2, the basis $\mathbb{B}_l$ of eigenvectors of U and the basis $\mathcal{B}_k$ are mutually unbiased. Thus

$$
P, Q, PQ, PQ^2, \ldots, PQ^{p-1} \qquad (2.5)
$$

provide a set of $p + 1$ MUBs in $\mathbb{C}^p$.

Example 2.5. *Here are the four MUBs in $\mathbb{C}^3$ we have constructed from the eigen-*

vectors determined in Lemma 2.4

$$\begin{aligned}
\mathcal{B}_0 &= \{(1,0,0),(0,1,0),(0,0,1)\}, \\
\mathcal{B}_1 &= \left\{\frac{1}{\sqrt{3}}(1,1,1),\frac{1}{\sqrt{3}}(1,\omega^2,\omega),\frac{1}{\sqrt{3}}(1,\omega,\omega^2)\right\}, \\
\mathcal{B}_2 &= \left\{\frac{1}{\sqrt{3}}(1,1,\omega),\frac{1}{\sqrt{3}}(1,\omega^2,\omega^2),\frac{1}{\sqrt{3}}(1,\omega,1)\right\}, \\
\mathcal{B}_3 &= \left\{\frac{1}{\sqrt{3}}(1,1,\omega^2),\frac{1}{\sqrt{3}}(1,\omega^2,1),\frac{1}{\sqrt{3}}(1,\omega,\omega)\right\},
\end{aligned}$$

where $\omega = e^{2\pi i/3}$ *and the bases are the eigenvector sets for the following generalized Pauli matrices*

$$Q = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \qquad P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

$$PQ = \begin{pmatrix} 0 & 0 & \omega^2 \\ 1 & 0 & 0 \\ 0 & \omega & 0 \end{pmatrix}, \qquad PQ^2 = \begin{pmatrix} 0 & 0 & \omega \\ 1 & 0 & 0 \\ 0 & \omega^2 & 0 \end{pmatrix}.$$

2.2 MUBs and unitary matrices

In this section the relation between MUBs and a special class of unitary matrices in $M_d(\mathbb{C})$ will be considered.

Let $A = [a_{ij}]$ be a matrix in $M_d(\mathbb{C})$. The **trace** of A is denoted by $\mathrm{Tr}(A)$ and is defined as follows

$$\mathrm{Tr}(A) = \sum_{i=1}^{d} a_{ii}.$$

Define an inner product for all A, $B \in M_d(\mathbb{C})$, by

$$\langle A, B \rangle = \mathrm{Tr}(AB^*). \tag{2.6}$$

Two matrices A and B in $M_d(\mathbb{C})$ are **orthogonal** if $\langle A, B \rangle = 0$.

Theorem 2.6 (Spectral Theorem[20]). *If U is a $d \times d$ Hermitian or unitary matrix, then U can be decomposed as*

$$U = \sum_{i=1}^{d} \lambda_i \mathbf{v}_i^* \mathbf{v}_i,$$

where the λ_is and $\mathbf{v}_i$s are the eigenvalues and eigenvectors of U respectively. Moreover, $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ is an orthonormal basis in $\mathbb{C}^d$.

Definition 2.7. *Let $A = [a_{i,j}]$ be an $m \times n$ matrix and $B = [b_{l,k}]$ be a $p \times q$ matrix with entries in $\mathbb{C}$. The **Kronecker product** of A and B is an $mp \times nq$ matrix denoted by $A \otimes B$, and is defined by*

$$A \otimes B = [a_{i,j}B].$$

For example, let

$$A = \begin{bmatrix} 2 & 0 \\ -1 & 3 \end{bmatrix}, \quad B = \begin{bmatrix} 5 & 3 \\ 2 & -4 \end{bmatrix}.$$

Then

$$A \otimes B = \begin{bmatrix} 10 & 6 & 0 & 0 \\ 4 & -8 & 0 & 0 \\ -5 & -3 & 15 & 9 \\ -2 & 4 & 6 & -12 \end{bmatrix}.$$

Let $d \geq 2$ be an integer and let $\omega = e^{2\pi i/d}$. Since $\omega^d = 1$ and $\omega^d - 1 = (\omega - 1)(1 + \omega^2 + \cdots + \omega^{d-1})$, it is easy to check that for any $0 < k < d$,

$$\sum_{j=1}^{d} \omega^{jk} = 0. \tag{2.7}$$

Lemma 2.8. *The existence of two MUBs $\mathcal{B}_1$ and $\mathcal{B}_2$ is equivalent to existence of two sets $\mathcal{C}_1$ and $\mathcal{C}_2$, each consisting of d commuting $d \times d$ unitary matrices, such that $\mathcal{C}_1 \bigcap \mathcal{C}_2 = \{\mathbb{I}_d\}$ and matrices in $\mathcal{C}_1 \bigcup \mathcal{C}_2$ are mutually orthogonal.*

Proof. Let $\mathcal{C}_1 = \{U_1, U_2, \ldots, U_d = \mathbb{I}_d\}$ and $\mathcal{C}_2 = \{V_1, V_2, \ldots, V_d = \mathbb{I}_d\}$ be sets of $d \times d$ unitary matrices such that matrices in each set commute and the matrices in $\mathcal{C}_1 \bigcup \mathcal{C}_2$ are orthogonal. Since the matrices in each set commute, they share a common basis of eigenvectors [20]. Let $\mathcal{B}_1 = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_d\}$ and $\mathcal{B}_2 = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ be the sets of eigenvectors for matrices in $\mathcal{C}_1$ and $\mathcal{C}_2$ respectively. We claim that $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased bases.

Since matrices in each set are unitary, $\mathcal{B}_1$ and $\mathcal{B}_2$ are orthonormal bases of $\mathbb{C}^d$ [20]. Finally, we show that $|\langle \mathbf{u}_i, \mathbf{v}_j \rangle|^2 = \dfrac{1}{d}$, $1 \leq i, j \leq d$.

Since U_i and V_j are unitary, by Theorem 2.6,

$$U_i = \sum_{k=1}^{d} \lambda_{i,k} \mathbf{u}_k^* \mathbf{u}_k, \quad V_j = \sum_{l=1}^{d} \lambda'_{j,l} \mathbf{v}_l^* \mathbf{v}_l, \quad 1 \leq i, j \leq d, \tag{2.8}$$

where $\lambda_{i,k}$ is the kth eigenvalue of U_i and $\lambda'_{j,l}$ is the lth eigenvalue of V_j. Since $\mathrm{Tr}\left((\mathbf{u}_k^* \mathbf{u}_k)(\mathbf{v}_l^* \mathbf{v}_l)\right) = |\langle \mathbf{u}_k, \mathbf{v}_l \rangle|^2$ and $\mathrm{Tr}(U_i V_j^*) = d\delta_{i,d}\delta_{j,d}$, then

$$\begin{aligned} \mathrm{Tr}(U_i V_j^*) &= \mathrm{Tr}\left(\sum_{k=1}^{d} \lambda_{i,k} \mathbf{u}_k^* \mathbf{u}_k \sum_{l=1}^{d} \overline{\lambda'_{j,l}} \mathbf{v}_l^* \mathbf{v}_l \right) \\ &= \sum_{k=1}^{d} \sum_{l=1}^{d} \lambda_{i,k} \overline{\lambda'_{j,l}} \, \mathrm{Tr}\left((\mathbf{u}_k^* \mathbf{u}_k)(\mathbf{v}_l^* \mathbf{v}_l) \right) \\ &= \sum_{k=1}^{d} \sum_{l=1}^{d} \lambda_{i,k} \overline{\lambda'_{j,l}} |\langle \mathbf{u}_k, \mathbf{v}_l \rangle|^2 \qquad (2.9) \\ &= d\delta_{i,d}\delta_{j,d}. \end{aligned}$$

We may write (2.9) in matrix form. Let M and M' be as follows

$$M = \begin{pmatrix} \lambda_{1,1} & \lambda_{1,2} & \dots & \lambda_{1,d} \\ \lambda_{2,1} & \lambda_{2,2} & \dots & \lambda_{2,d} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{d,1} & \lambda_{d,2} & \dots & \lambda_{d,d} \end{pmatrix}, \quad M' = \begin{pmatrix} \lambda'_{1,1} & \lambda'_{1,2} & \dots & \lambda'_{1,d} \\ \lambda'_{2,1} & \lambda'_{2,2} & \dots & \lambda'_{2,d} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda'_{d,1} & \lambda'_{d,2} & \dots & \lambda'_{d,d} \end{pmatrix},$$

where ith rows of M and M' consist of eigenvalues of $U_i \in \mathcal{C}_1$ and $V_i \in \mathcal{C}_2$ respectively. Since $\mathcal{B}_1$ and $\mathcal{B}_2$ are orthonormal bases in in $\mathbb{C}^d$, it is easy to check that $MM^* = M'M'^* = d\mathbb{I}_d$. Moreover the last rows of M and M' are all 1 because the eigenvalues of $U_d = V_d = \mathbb{I}_d$ are all 1. Let $A = M \otimes M'^*$, then in matrix form (2.9) says

$$AX = D, \tag{2.10}$$

where

$$X = (|\langle \mathbf{u}_1, \mathbf{v}_1\rangle|^2, \ldots, |\langle \mathbf{u}_1, \mathbf{v}_d\rangle|^2, |\langle \mathbf{u}_2, \mathbf{v}_1\rangle|^2, \ldots, |\langle \mathbf{u}_2, \mathbf{v}_d\rangle|^2, \ldots, |\langle \mathbf{u}_d, \mathbf{v}_d\rangle|^2)^T \in \mathbb{R}^{d^2},$$

$$D = (0, 0, \ldots, d)^T \in \mathbb{R}^{d^2}.$$

Since $AA^* = d^2\mathbb{I}_{d^2}$ then $X = \dfrac{1}{d^2}A^*D$ is unique solution for (2.10). Since entries in the last column of A^* are all 1,

$$|\langle \mathbf{u}_k, \mathbf{v}_l\rangle|^2 = \frac{1}{d}, \qquad 1 \leq k, l \leq d.$$

So, $\mathcal{B}_1$ and $\mathcal{B}_2$ are mutually unbiased bases in $\mathbb{C}^d$.

Now we show the converse implication. Let $\mathcal{B}_1 = \{\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_d\}$ and $\mathcal{B}_2 = \{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d\}$ be MUBs. Define

$$U_i = \sum_{k=1}^{d} \omega^{ik}\mathbf{u}_k^*\mathbf{u}_k, \quad V_j = \sum_{l=1}^{d} \omega^{jl}\mathbf{v}_l^*\mathbf{v}_l, \quad 1 \leq i, j \leq d, \tag{2.11}$$

where $\omega = e^{2\pi i/d}$. We show $\mathcal{C}_1 = \{U_1, U_2, \ldots, U_d\}$ and $\mathcal{C}_2 = \{V_1, V_2, \ldots, V_d\}$ are the required sets in the hypothesis of the lemma. Since $\mathcal{B}_1$ and $\mathcal{B}_2$ are MUBs in $\mathbb{C}^d$, it is easy check that matrices in $\mathcal{C}_1$ and $\mathcal{C}_2$ are unitary and commuting and $\mathcal{C}_1 \cap \mathcal{C}_2 = \{\mathbb{I}_d\}$. It remains to show that matrices in $\mathcal{C}_1 \bigcup \mathcal{C}_2$ are pairwise orthogonal with respect to trace inner product. First we show this for two matrices $U_i \in \mathcal{C}_1$ and $V_j \in \mathcal{C}_2$, $1 \leq i, j \leq d$, $(i, j) \neq (d, d)$ as follows

$$\begin{aligned}\operatorname{Tr}(U_iV_j^*) &= \operatorname{Tr}\left(\sum_{k=1}^{d} \omega^{ik}\mathbf{u}_k^*\mathbf{u}_k \sum_{l=1}^{d} \omega^{-jl}\mathbf{v}_l^*\mathbf{v}_l\right) \\ &= \sum_{k=1}^{d}\sum_{l=1}^{d} \omega^{ik-jl} \operatorname{Tr}\left((\mathbf{u}_k^*\mathbf{u}_k)(\mathbf{v}_l^*\mathbf{v}_l)\right)\end{aligned}$$

$$= \sum_{k=1}^{d}\sum_{l=1}^{d} \omega^{ik-jl} |\langle \mathbf{u}_k, \mathbf{v}_l \rangle|^2$$
$$= \sum_{k=1}^{d}\sum_{l=1}^{d} \omega^{ik-jl} \frac{1}{d}$$
$$= \frac{1}{d} \left(\sum_{k=1}^{d} \omega^{ik} \right) \left(\sum_{l=1}^{d} \omega^{jl} \right)^{*}. \tag{2.12}$$

So, by (2.7), (2.12) is equal to zero. By the same argument, for $1 \leq i, j < d$, $i \neq j$

$$\mathrm{Tr}(U_i U_j^*) = \mathrm{Tr}\left(\sum_{k=1}^{d} \omega^{ik} \mathbf{u}_k^* \mathbf{u}_k \sum_{l=1}^{d} \omega^{-jl} \mathbf{u}_l^* \mathbf{u}_l \right) = 0,$$
$$\mathrm{Tr}(V_i V_j^*) = \mathrm{Tr}\left(\sum_{k=1}^{d} \omega^{ik} \mathbf{v}_k^* \mathbf{v}_k \sum_{l=1}^{d} \omega^{-jl} \mathbf{v}_l^* \mathbf{v}_l \right) = 0.$$

Thus $\mathcal{C}_1$ and $\mathcal{C}_2$ are as required. □

By the same argument as Lemma 2.8, we may extend the result of Lemma 2.8 as follows.

Theorem 2.9 ([1]). *There exist m MUBs in $\mathbb{C}^d$ if and only if there exist m sets $\mathcal{C}_1, \ldots, \mathcal{C}_m$, each consisting of d commuting unitary matrices in $M_d(\mathbb{C}^d)$ such that $\mathcal{C}_i \bigcap \mathcal{C}_j = \{\mathbb{I}_d\}$ for all $i \neq j$ and matrices in $\bigcup_{i=1}^{m} \mathcal{C}_i$ are mutually orthogonal.*

Example 2.10. *Define $\mathcal{C}_1 = \{U, \mathbb{I}_2\}, \mathcal{C}_2 = \{V, \mathbb{I}_2\}$, $\mathcal{C}_3 = \{W, \mathbb{I}_2\}$, where*

$$U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad V = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad W = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

$\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ *satisfy hypothesis of Theorem* 2.9. *Thus eigenvectors related to each set give us 3 MUBs*

$$\mathcal{B}_1 = \{(1,0),(0,1)\}, \quad \mathcal{B}_2 = \left\{\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(1,-1)\right\}, \quad \mathcal{B}_3 = \left\{\frac{1}{\sqrt{2}}(1,i), \frac{1}{\sqrt{2}}(1,-i)\right\}.$$

The following corollary uses Theorem 2.9 to give an upper bound on the number of MUBs in any given dimension.

Corollary 2.11. *There are at most* $d+1$ *MUBs in* $\mathbb{C}^d$.

Proof. Suppose there is a set of m MUBs in $\mathbb{C}^d$. By Theorem 2.8 there are m classes $\mathcal{C}_1, \ldots, \mathcal{C}_m$, containing $1+m(d-1)$ pairwise orthogonal matrices in the d^2 dimensional space of complex $d \times d$ matrices. Therefore $1 + m(d-1) \leq d^2$, so $m \leq d+1$. □

2.3 Generalized Spin matrices

Theorem 2.9 gives a way of constructing m MUBs from certain sets of unitary matrices. In other words, the existence of m sets of orthogonal $d \times d$ unitary matrices $\mathcal{C}_1, \ldots, \mathcal{C}_m$, each consisting of d matrices satisfying certain relations, provides m mutually unbiased bases in dimensions d. In this section we describe a construction of these sets of unitary matrices for prime dimensions p. The main results are due to A. O. Pittenger and M. H. Rubin (see [30]). Henceforth we assume that p is a prime number.

Definition 2.12 (Spin Matrix)**.** *Let* $\{\mathbf{v}_0, \mathbf{v}_1, \ldots, \mathbf{v}_{p-1}\}$ *be a fixed orthonormal basis of* $\mathbb{C}^p$ *and* $\omega = e^{(2\pi i/p)}$*. Define*

$$S_{0,1} = \sum_{m=0}^{p-1} \mathbf{v}_m^* \mathbf{v}_{m+1}, \quad S_{1,0} = \sum_{m=0}^{p-1} \omega^m \mathbf{v}_m^* \mathbf{v}_m, \tag{2.13}$$

where $\mathbf{v}_p = \mathbf{v}_0$*. For* $j, k \in \mathbb{Z}_p$*, we define the corresponding* ***Spin matrices*** *by*

$$S_{j,k} = (S_{1,0})^j (S_{0,1})^k. \tag{2.14}$$

To illustrate these matrices, here are the Spin matrices for $p = 3$. Using the standard basis $\{\mathbf{e}_0, \mathbf{e}_1, \mathbf{e}_2\}$ of $\mathbb{C}^3$ and $\omega = e^{(2\pi i/3)}$, the corresponding Spin matrices are

$$S_{0,0} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad S_{0,1} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad S_{0,2} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix},$$

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

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

Lemma 2.13 ([30])**.** *Let* $\omega = e^{(2\pi i/p)}$*. Spin matrices have the following properties:*

(1) $S_{0,1}S_{1,0} = \omega S_{1,0}S_{0,1} = \omega S_{1,1}$*;*

(2) $\mathrm{Tr}(S_{j,k}) = 0$ *unless* $(j,k) = (0,0)$*;*

(3) $S_{j,k}^* = \omega^{jk} S_{-j,-k}$*;*

(4) $S_{j,k} S_{a,b} = \omega^{ka} S_{j+a,k+b}$*;*

(5) *The set of Spin matrices are mutually orthogonal;*

(6) $(S_{j,k})^m = \omega^{jk\binom{m}{2}} S_{mj,mk}$*, where* $\binom{m}{2} = 0$ *for* $m = 0$ *or 1.*

Proof. Property (1): Let $\mathcal{B} = \{\mathbf{v}_0, \ldots, \mathbf{v}_{p-1}\}$ be the orthonormal basis in $\mathbb{C}^p$ from which the Spin matrices are built. Then

$$\begin{aligned} S_{0,1} S_{1,0} &= \sum_{m=0}^{p-1} (\mathbf{v}_m^* \mathbf{v}_{m+1}) \sum_{n=0}^{p-1} \omega^n (\mathbf{v}_n^* \mathbf{v}_n) \\ &= \sum_{m=0}^{p-1} \sum_{n=0}^{p-1} \omega^n \langle \mathbf{v}_{m+1}, \mathbf{v}_n \rangle \mathbf{v}_m^* \mathbf{v}_n. \end{aligned} \tag{2.15}$$

Since $\langle \mathbf{v}_{m+1}, \mathbf{v}_n \rangle \neq 0$ only for $n \equiv m+1 \pmod{p}$, then from (2.15) we have

$$\begin{aligned} S_{0,1} S_{1,0} &= \sum_{m=0}^{p-1} \omega^{m+1} \mathbf{v}_m^* \mathbf{v}_{m+1} \\ &= \omega \sum_{m=0}^{p-1} \omega^m \mathbf{v}_m^* \mathbf{v}_{m+1}. \end{aligned}$$

By the same calculation, it is easy to check that

$$S_{1,0} S_{0,1} = \sum_{m=0}^{p-1} \omega^m \mathbf{v}_m^* \mathbf{v}_{m+1}.$$

Thus $S_{0,1} S_{1,0} = \omega S_{1,0} S_{0,1}$.

Property (2): By (2.14), since $S_{j,0} = (S_{1,0})^j$ and $S_{0,k} = (S_{0,1})^k$, it is easy to check

that

$$S_{j,k} = \sum_{m=0}^{p-1} \omega^{mj} \mathbf{v}_m^* \mathbf{v}_{m+k}. \tag{2.16}$$

Since $\mathrm{Tr}(\mathbf{v}_m^* \mathbf{v}_{m+k}) = \langle \mathbf{v}_m, \mathbf{v}_{m+k} \rangle = \delta_{k,0}$, using (2.16) we have

$$\begin{aligned}
\mathrm{Tr}(S_{j,k}) &= \sum_{m=0}^{p-1} \omega^{mj} \mathrm{Tr}(\mathbf{v}_m^* \mathbf{v}_{m+k}) \\
&= \sum_{m=0}^{p-1} \omega^{mj} \langle \mathbf{v}_m, \mathbf{v}_{m+k} \rangle \\
&= \sum_{m=0}^{p-1} \omega^{mj} \delta_{k,0} \\
&= \delta_{j,0} \delta_{k,0}.
\end{aligned}$$

Property (3): Using (2.16) we have

$$S_{i,j}^* = \sum_{m=0}^{d-1} \omega^{-mj} \mathbf{v}_{m+k}^* \mathbf{v}_m = \omega^{jk} \sum_{n=k}^{d+k-1} \omega^{-nj} \mathbf{v}_n^* \mathbf{v}_{n-k} = \omega^{jk} S_{-j,-k}.$$

Properties (4), (5) and (6) are direct consequence of properties (1),(2) and (3). □

From Lemma 2.13 the set of Spin matrices of order p, $\{S_{j,k} : (j,k) \in \mathbb{Z}_p^2\}$, contains p^2 unitary matrices which are orthogonal. By Theorem 2.9, to obtain $p+1$ MUBs, we just need to partition the set of Spin matrices to $p+1$ subsets, each consisting of p commuting matrices. The rest of this section is devoted to finding such subsets.

By Lemma 2.13 part (4)

$$S_{j,k} S_{a,b} = \omega^{ka} S_{j+a,k+b}, \quad S_{a,b} S_{j,k} = \omega^{jb} S_{j+a,k+b}. \tag{2.17}$$

Thus, $S_{j,k}$ and $S_{a,b}$ commute if and only if $ka = jb$. Define the set of indices as follows

$$\mathbb{Z}_p^2 = \{(j,k) : j,k \in \mathbb{Z}_p\},$$

and the **symplectic product** $\circ : \mathbb{Z}_p^2 \times \mathbb{Z}_p^2 \to \mathbb{Z}_p$ by

$$u \circ v = ka - jb, \tag{2.18}$$

where $u = (j,k)$, $v = (a,b) \in \mathbb{Z}_p^2$. From (2.17), S_u and S_v commute if and only if the symplectic product of indices u and v equals zero. The following lemma shows how to find subsets of $\mathbb{Z}_p^2$ for which the corresponding Spin matrices associated to each subset commute.

Lemma 2.14 ([30])**.** *The $p+1$ index subsets defined by*

$$C_a = \{b(1,a) : b \in \mathbb{Z}_p\}, \quad a \in \mathbb{Z}_p,$$

$$C_\infty = \{b(0,1) : b \in \mathbb{Z}_p\},$$

partition the index set $\mathbb{Z}_p^2$ such that Spin matrices associated to each subset are commuting and have the identity matrix in common.

Proof. We need to show the symplectic product in each class is zero and $C_a \cap C_{a'} = \{(0,0)\}$ for all $a \neq a' \in \{0,1,\ldots,p-1,\infty\}$. Let $u = b(1,a)$ and $v = b'(1,a)$ be in C_a, then it is obvious that $u \circ v = 0$. If $b(1,a) = b'(1,a') \in C_a \cap C_{a'}$, then $b = b'$ and if $b \neq 0$, $a = a'$ thus $C_a \cap C_{a'} = \{(0,0)\}$. □

For example, for $p = 3$ the index sets defined in Proposition 2.14 are

$$C_0 = \{(0,0),(1,0),(2,0)\}, \qquad C_1 = \{(0,0),(1,1),(2,2)\},$$

$$C_2 = \{(0,0),(1,2),(2,1)\}, \qquad C_\infty = \{(0,0),(0,1),(0,2)\}.$$

Commuting subsets of $\{S_{j,k}; (j,k) \in \mathbb{Z}_3^2\}$ associated to each index set are

$$\mathcal{C}_0 = \{S_{0,0}, S_{1,0}, S_{2,0}\}, \qquad \mathcal{C}_1 = \{S_{0,0}, S_{1,1}, S_{2,2}\},$$

$$\mathcal{C}_2 = \{S_{0,0}, S_{1,2}, S_{2,1}\}, \qquad \mathcal{C}_\infty = \{S_{0,0}, S_{0,1}, S_{0,2}\}.$$

Thus, eigenvectors related to each set give 4 MUBs in $\mathbb{C}^3$. In the next section, we will find eigenvectors of Spin matrices for prime dimensions.

2.3.1 Eigenvectors of Spin matrices

By Lemma 2.13 and Lemma 2.14 the set of Spin matrices can be partitioned into $p+1$ commuting orthogonal unitary matrices. So, by Theorem 2.9 the orthonormal eigenvectors of Spin matrices corresponding to each set defined in Proposition 2.14 give $p+1$ MUBs. In this section we describe a way to obtain the eigenvectors of Spin matrices.

Definition 2.15. *Let p be an odd prime number. For each $u = (j,k) \in \mathbb{Z}_p^2 \backslash \{(0,0)\}$ and $r \in \mathbb{Z}_p$, define*

$$P_u(r) = \frac{1}{p} \sum_{m=0}^{p-1} (\omega^r S_u)^m, \tag{2.19}$$

where $(\omega^r S_u)^0 = \mathbb{I}_p$.

For $p = 2$, the $P_u(r)$s are defined as follows

$$P_{(0,1)}(0) = \frac{1}{2}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}, \quad P_{(0,1)}(1) = \frac{1}{2}\begin{pmatrix} 1 & -1 \\ -1 & 1 \end{pmatrix}, \quad P_{(1,1)}(0) = \frac{1}{2}\begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix},$$

$$P_{(1,1)}(1) = \frac{1}{2}\begin{pmatrix} 1 & -i \\ i & 1 \end{pmatrix}, \quad P_{(1,0)}(0) = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \quad P_{(1,0)}(1) = \frac{1}{2}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}.$$

A square matrix P is a **projection** if $P^2 = P$. If P is a Hermitian projection of rank one, then by Theorem 2.6, there exists a vector $\mathbf{v}$ such that

$$P = \mathbf{v}^*\mathbf{v}.$$

The following theorem characterizes the eigenvectors of Spin matrices in terms of one dimensional projections.

Theorem 2.16 ([30]). *For each $u = (1, a)$, $a \in \mathbb{Z}_p$, and $u = (0, 1)$, there exists a vector $\mathbf{v}_u(r) \in \mathbb{C}^p$, for some $r \in \mathbb{Z}_p$, such that $P_u(r) = \mathbf{v}_u(r)^*\mathbf{v}_u(r)$. Moreover, $\mathcal{B}_u = \{\mathbf{v}_u(r), r \in \mathbb{Z}_p\}$ is the set of eigenvectors of the set $\{S_{bu} : b \in \mathbb{Z}_p\}$. Thus $\mathcal{B}_u$s are $p + 1$ MUBs in $\mathbb{C}^p$.*

Indices of the form $u = (1, a)$, $a \in \mathbb{Z}_p$, and $u = (0, 1)$ are called **generator** of the index sets C_a and C_∞ defined in Lemma 2.14 respectively. The following lemma provides properties of $P_u(r)$s needed for proving Theorem 2.16.

Lemma 2.17 ([30],[29]). (1) *For each $u = (j, k) \in \mathbb{Z}_p^2 \backslash \{(0, 0)\}$, $\{P_u(r) : r \in \mathbb{Z}_p\}$ is a set of p mutually orthogonal Hermitian projections;*

(2) $(\omega^r S_u)^t = \sum_{m=0}^{p-1} \omega^{-mt} P_u(m+r)$, *for* $t \in \mathbb{Z}_p$ *and* $u \neq (0,0)$;

(3) *if* $p > 2$ *and* $u = (1,a)$, $a \in \mathbb{Z}_p$, *or* $u = (0,1)$ *is a generator, then for any* $b \in \mathbb{Z}_p$ *there exists* $s \in \mathbb{Z}_d$ *such that* $P_{bu}(r) = P_u(s)$;

(4) $\mathrm{Tr}(P_u(r)P_{u'}(s)) = \frac{1}{p}$ *for generators* u *and* u' *in different classes;*

(5) $\mathrm{Tr}(P_u) = 1$ *for* $u \neq (0,0)$.

Proof. Property (1): For $p = 2$, it is easy to check that $P_u(r)P_u(s) = \delta_{r,s}P_u(r)$. Let $p > 2$ be prime. Since for any r and $s \in \mathbb{Z}_p$, there exists $i \in \mathbb{Z}_p$ such that $s = r + i$, then

$$\begin{aligned} P_u(r)P_u(s) &= P_u(r)P_u(r+i) \\ &= \frac{1}{p^2}\sum_{m=0}^{p-1}(\omega^r S_u)^m \sum_{n=0}^{p-1}(\omega^{(r+i)} S_u)^n \\ &= \frac{1}{p^2}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}(\omega^r S_u)^{m+n}\omega^{in}. \end{aligned} \tag{2.20}$$

Let $l = m + n$. Then from (2.20)

$$\begin{aligned} P_u(r)P_u(r+i) &= \frac{1}{p^2}\sum_{m=0}^{d-1}\sum_{l=m}^{p-1+m}(\omega^r S_u)^l \omega^{i(l-m)} \\ &= \frac{1}{d^2}\sum_{m=0}^{p-1}\omega^{-im}\sum_{l=m}^{p-1+m}(\omega^r S_u)^l \omega^{il}. \end{aligned} \tag{2.21}$$

We have two cases for i in (2.21) as follows:

(a) if $i \neq 0$ then $\sum_{m=0}^{p-1}\omega^{-im} = 0$, so from (2.21) $P_u(r)P_u(r+i) = 0$;

(b) if $i = 0$ then (2.21) is equal to

$$\begin{aligned} P_u(r)^2 &= \frac{1}{p^2} \sum_{m=0}^{p-1} \sum_{l=m}^{p-1+m} (\omega^r S_u)^l \\ &= \frac{p}{p^2} \sum_{l=0}^{p-1} (\omega^r S_u)^l \\ &= P_u(r). \end{aligned}$$

Thus, $P_u(r)P_u(s) = \delta_{r,s} P_u(r)$.

Now we need to show for each generator of the form $u = (1, a)$ or $u = (0, 1)$ and each $r \in \mathbb{Z}_p$, $P_u(r)$ is Hermitian. For $p = 2$ it is easy to check that $P_u(r) = P_u(r)^*$. Let $p > 2$ and $u = (1, a)$ then

$$\begin{aligned} P_u(r)^* &= \frac{1}{p} \sum_{m=0}^{p-1} ((\omega^r S_u)^m)^* \\ &= \frac{1}{p} \sum_{m=0}^{p-1} \omega^{-rm} \left(\omega^{a\binom{m}{2}} S_{(m,ma)} \right)^* \\ &= \frac{1}{p} \sum_{m=0}^{p-1} \omega^{-rm} \omega^{-a\binom{m}{2}} S^*_{(m,ma)}. \end{aligned} \tag{2.22}$$

Using Lemma 2.13 part (3) for the index (m, ma), $S^*_{(m,ma)} = \omega^{m^2 a} S_{(-m,-ma)}$. So (2.22) is equal to

$$\begin{aligned} P_u(r)^* &= \frac{1}{p} \sum_{m=0}^{p-1} \omega^{-rm - a\binom{m}{2}} \omega^{m^2 a} S_{(-m,-ma)} \\ &= \frac{1}{p} \sum_{m=0}^{p-1} \omega^{-rm} \omega^{a\left(m^2 - \binom{m}{2}\right)} S_{(-m,-ma)} \\ &= \frac{1}{p} \sum_{m=0}^{p-1} \omega^{-rm} \omega^{a\binom{m+1}{2}} S_{(-m,-ma)}. \end{aligned}$$

Let $m = p - n$. Since $S_{(n-p,(n-p)a)} = S_{(n,na)}$ and $S_{(n,na)} = \omega^{-a\binom{n}{2}}(S_{(1,a)})^n$, then

$$\begin{aligned} P_u(r)^* &= \frac{1}{p}\sum_{n=0}^{p-1}\omega^{r(n-p)}\omega^{a\binom{p-n+1}{2}}S_{(n-p,(n-p)a)} \\ &= \frac{1}{p}\sum_{n=0}^{p-1}\omega^{rn}\omega^{a\binom{p-n+1}{2}}S_{(n,na)} \\ &= \frac{1}{p}\sum_{n=0}^{p-1}\omega^{rn}\omega^{a\binom{p-n+1}{2}}\omega^{-a\binom{n}{2}}(S_{(1,a)})^n \qquad (2.23) \\ &= \frac{1}{p}\sum_{n=0}^{p-1}\omega^{rn}(S_{(1,a)})^n \qquad (2.24) \\ &= P_u(r). \end{aligned}$$

It is easy to check that $\omega^{a\binom{p-n+1}{2}}\omega^{-a\binom{n}{2}} = 1$, which we have used it to get (2.24) from (2.23). So, for any $r \in \mathbb{Z}_p$ and any generator of the form $u = (1, a)$, $a \in \mathbb{Z}_p$, $P_u(r)$ is Hermitian. By the same argument we can show that $P_u(r)$ is Hermitian for generator $u = (0, 1)$ and $r \in \mathbb{Z}_p$.

Property (2): From Definition 2.19, $P_u(r+m) = \sum_{n=0}^{p-1}(\omega^{r+m})^n(S_u)^n$. So

$$\begin{aligned} \sum_{m=0}^{p-1}\omega^{-mt}P_u(m+r) &= \frac{1}{p}\sum_{m=0}^{p-1}\omega^{-mt}\sum_{n=0}^{p-1}(\omega^{r+m})^n(S_u)^n \\ &= \sum_{n=0}^{p-1}(\omega^r S_u)^n\sum_{m=0}^{p-1}(\omega^{n-t})^m \\ &= \sum_{n=0}^{p-1}(\omega^r S_u)^n\delta(n,t) \qquad (2.25) \\ &= (\omega^r S_u)^t. \end{aligned}$$

The equality in (2.25) holds because $\sum_{m=0}^{p-1}(\omega^{n-t})^m = 0$ for $t \neq n$.

Property (3): By Lemma 2.13 part (6), $(S_{(b,ba)})^m = \omega^{-ma\binom{b}{2}}(S_{(1,a)})^{bm}$. Hence

$$\begin{aligned} P_{b(1,a)}(r) &= \frac{1}{p}\sum_{m=0}^{p-1}(\omega^r S_{b(1,a)})^m \\ &= \frac{1}{p}\sum_{m=0}^{p-1}\omega^{mr}\omega^{-ma\binom{b}{2}}S_{(1,a)}^{bm} \\ &= \frac{1}{p}\sum_{m=0}^{p-1}\omega^{m\left(r-a\binom{b}{2}\right)}S_{(1,a)}^{bm} \\ &= \frac{1}{p}\sum_{l=0}^{p-1}\omega^{lb^{-1}\left(r-a\binom{b}{2}\right)}S_{(1,a)}^{l} \\ &= P_{(1,a)}(s), \end{aligned}$$

where the last equality comes from substituting $l = bm$ and $s = b^{-1}\left(r - a\binom{b}{2}\right) \in \mathbb{Z}_p$.

Property (4): For $p = 2$ it is easy to check that $\mathrm{Tr}(P_u(r)P_{u'}(s)) = \frac{1}{d}$. Let $p > 2$ and let $u = (1, a)$, $u' = (1, a')$ be generators in different classes. Since $(S_{(1,a)})^m = \omega^{a\binom{m}{2}}S_{(m,ma)}$ (see Lemma 2.13 part (6)), then

$$\begin{aligned} \mathrm{Tr}(P_u(r)P_{u'}(s)) &= \frac{1}{p^2}\,\mathrm{Tr}\left(\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}(\omega^r S_u)^m(\omega^s S_{u'})^n\right) \\ &= \frac{1}{p^2}\sum_{m=0}^{p-1}\sum_{n=0}^{p-1}\omega^{mr+a\binom{m}{2}}\omega^{ns+a'\binom{n}{2}}\,\mathrm{Tr}(S_{mu}S_{nu'}). \end{aligned} \tag{2.26}$$

From Lemma 2.13 parts (2) and (4), $\mathrm{Tr}\,(S_{mu}S_{nu'}) = \mathrm{Tr}(\omega^{mna}S_{mu+nu'}) = 0$ except for the identity matrix, in which case, the index is $mu + nu' = n(1, a) + m(1, a') = (0, 0)$. Since $a \neq a'$, the only solution is $m = n = 0$. Thus $\mathrm{Tr}(S_{mu}S_{nu'}) = 0$ except for $n = m = 0$. For the case $m = n = 0$, $\mathrm{Tr}(S_{(0,0)}S_{(0,0)}) = \mathrm{Tr}(\mathbb{I}_p) = p$. So by (2.26), $\mathrm{Tr}(P_u(r)P_{u'}(s)) = \frac{1}{p}$. By the same argument, the result is true for the generators

$u = (1, a)$ and $u' = (0, 1)$.

Property (5): By Lemma 2.13 part (2), $\mathrm{Tr}(S_u^r) = 0$ except for $u = (0, 0)$ or $r = 0$. So $\mathrm{Tr}(P_u(r)) = \frac{1}{p} \sum_{m=0}^{p-1} \omega^{rm} \mathrm{Tr}(S_u^m) = \frac{1}{p} \mathrm{Tr}(\mathbb{I}_p) = 1$.

□

By Lemma 2.17, $P_u(r)^2 = P_u(r)$, so the eigenvalues of $P_u(r)$ are 0 and 1. Since $\mathrm{Tr}(P_u(r)) = 1$, multiplicity of eigenvalue 1 is one, so $P_u(r)$ is of rank one for any non-zero index u and $r \in \mathbb{Z}_p$. Moreover the $P_u(r)$s are Hermitian (see Lemma 2.17 part (1)), thus by Theorem 2.6, for $u \neq (0, 0)$ and $r \in \mathbb{Z}_p$, there exists $\mathbf{v}_u(r) \in \mathbb{C}^p$ such that

$$P_u(r) = \mathbf{v}_u(r)^* \mathbf{v}_u(r). \tag{2.27}$$

By Lemma 2.17 parts (1) and (4), for generators of the form $u = (1, a), a \in \mathbb{Z}_p$ or $u = (0, 1)$, the sets defined by $\mathcal{B}_u = \{P_u(r) : r \in \mathbb{Z}_p\}$ are orthogonal and projections from different sets $\mathcal{B}_u$ and $\mathcal{B}_{u'}$, $u \neq u'$ have trace $\frac{1}{d}$. Thus if we consider vectors derived from the factorization (2.27), then sets defined by

$$\mathcal{B}'_u = \{\mathbf{v}_u(r) : r \in \mathbb{Z}_p\}, \tag{2.28}$$

are mutually unbiased bases.

From Lemma 2.17 part (2), for $t \in \mathbb{Z}_p$ and generators of the form $u = (1, a)$, $a \in \mathbb{Z}_p$ and $u = (0, 1)$, we have

$$(\omega^r S_u)^t = \sum_{m=0}^{d-1} \omega^{-mt} P_u(m + r)$$

$$= \sum_{m=0}^{d-1} \omega^{-mt} \mathbf{v}_u(m+r)^* \mathbf{v}_u(m+r). \tag{2.29}$$

(2.29) shows that for each generator u of index sets from Proposition 2.14 the set $\{\mathbf{v}_u(r) : r \in \mathbb{Z}_p\}$ contains eigenvectors of the set of Spin matrices $\{(S_u)^t : t \in \mathbb{Z}_p\}$. Thus Theorem 2.16 is proved.

The following example constructs MUBs in dimension 2 using Theorem 2.16.

Example 2.18. *The commuting classes of Spin matrices for $p = 2$ and generators $u = (1,0)$, $u = (1,1)$ and $u = (0,1)$ are $\{S_{0,0}, S_{1,0}\}$, $\{S_{0,0}, S_{1,1}\}$, and $\{S_{0,0}, S_{0,1}\}$, where*

$$S_{(1,0)} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad S_{(1,1)} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad S_{(0,1)} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The projectors are determined by $\mathcal{B}_{(1,0)} = \{P_{(1,0)}(0), P_{(1,0)}(1)\}$, $\mathcal{B}_{(1,1)} = \{P_{(1,1)}(0), P_{(1,1)}(1)\}$ and $\mathcal{B}_{(0,1)} = \{P_{(0,1)}(0), P_{(0,1)}(1)\}$ where $P_u(r)$s are defined on page 25. So if we decompose projections in each class of the form $P_u(r) = \mathbf{v}_u(r)\mathbf{v}_u(r)^*$, then we get the following 3 sets of MUBs of the form (2.28)

$$\mathcal{B}'_{(1,0)} = \left\{ \mathbf{v}_{(1,0)}(0) = \frac{1}{\sqrt{2}}(1,1), \mathbf{v}_{(1,0)}(1) = \frac{1}{\sqrt{2}}(1,-1) \right\},$$
$$\mathcal{B}'_{(1,1)} = \left\{ \mathbf{v}_{(1,1)}(0) = \frac{1}{\sqrt{2}}(1,i), \mathbf{v}_{(1,1)}(1) = \frac{1}{\sqrt{2}}(1,-i) \right\},$$
$$\mathcal{B}'_{(0,1)} = \left\{ \mathbf{v}_{(0,1)}(0) = (1,0), \mathbf{v}_{(0,1)}(1) = (0,1) \right\}.$$

2.4 Construction of MUBs using Spin matrices in dimension $d = p^2$, p an odd prime

In Section 2.3 we built a set of unitary matrices (Spin matrices) and we partitioned this set into sets of commuting and orthogonal matrices. Indices in each class were of the form defined in Lemma 2.14. Then using Theorem 2.9, the eigenvectors of each commuting class of Spin matrices gives us MUBs. In this section we use a similar idea to construct MUBs in $\mathbb{C}^{p^2}$ using Spin matrices.

In this section we assume p is an odd prime number. For indices $u = (j, k)$ and $v = (a, b)$ in $\mathbb{Z}_p^2$, denote the tensor product of two Spin matrices S_u and S_v by $S_u \otimes S_v$, where S_u is same as defined in Definition 2.12. Then

$$\begin{aligned}(S_{u_1} \otimes S_{v_1})(S_{u_2} \otimes S_{v_2}) &= S_{u_1} S_{u_2} \otimes S_{v_1} S_{v_2} \\ &= \omega^{k_1 j_2 + b_1 a_2} S_{u_2} S_{u_1} \otimes S_{v_2} S_{v_1} \\ &= \omega^{k_1 j_2 + b_1 a_2} (S_{u_2} \otimes S_{v_2})(S_{u_1} \otimes S_{v_1})\end{aligned} \tag{2.30}$$

where $u_1 = (j_1, k_1), v_1 = (a_1, b_1), u_2 = (j_2, k_2)$ and $v_2 = (a_2, b_2)$ are in $\mathbb{Z}_p^2$. We have used (2.17) in (2.30). So, $S_{u_1} \otimes S_{v_1}$ and $S_{u_2} \otimes S_{v_2}$ commute if and only if

$$(k_1 j_2 - k_2 j_1) + (b_1 a_2 - b_2 a_1) = 0,$$

or

$$u_1 \circ u_2 + v_1 \circ v_2 = 0, \tag{2.31}$$

where $\circ$ is the symplectic product defined in (2.18). Let

$$V_4(\mathbb{Z}_p) = \{w = (j, k, a, b) = (u, v) : a, b, j, k \in \mathbb{Z}_p\}, \tag{2.32}$$

and define the **symplectic product** of $w_1 = (u_1, v_1)$ and $w_2 = (u_2, v_2)$ on the four dimensional space $V_4(\mathbb{Z}_p)$ as

$$w_1 \circ w_2 = u_1 \circ u_2 + v_1 \circ v_2. \tag{2.33}$$

The problem of finding commuting classes of Spin matrices is equivalent to partitioning $V_4(\mathbb{Z}_p)$ such that indices in each class satisfy $w_1 \circ w_2 = 0$. Next we demonstrate the procedure to find such classes.

Define the polynomial $f(x) = x^2 - D$ over $\mathbb{Z}_p$, where D is is not a quadratic residues modulo p. In other words the equation $x^2 = D$ has no solution in $\mathbb{Z}_p$. There exist at least $(p-1)/2$ such values of D (see [3]). For $p = 2$, there is no such D.

For any positive integer n, there exists a finite field with p^n elements; this is an extension field of the finite field $\mathbb{Z}_p$. In Algebra a finite field of order p^n is called a **Galois field** and is denoted by $GF(p^n)$. For details on Galois fields see [28, 36]. In this context, we denote a finite field of order p^n by $\mathbb{F}_{p^n}$. Let λ be a root of $f(x) = x^2 - D$ in $\mathbb{F}_{p^2}$. The Galois field of order p^2 is representable in the form

$$\mathbb{F}_{p^2} = \{j + k\lambda : j, k \in \mathbb{Z}_p\},$$

with operations as follows

$$(j + k\lambda) + (a + b\lambda) = (j + a) + (k + b)\lambda,$$

$$(j + k\lambda)(a + b\lambda) = ja + Dkb + \lambda(jb + ka).$$

Let $\mathbb{F}_{p^2}^2 = \{u = (\alpha, \beta) : \alpha, \beta \in \mathbb{F}_{p^2}\}$ and define the symplectic product for $u = (\alpha, \beta), u' = (\alpha', \beta') \in \mathbb{F}_{p^2}^2$ by

$$u \circ u' = \beta\alpha' - \alpha\beta'. \tag{2.34}$$

Let us define subsets of $\mathbb{F}_{p^2}^2$ for each $\alpha \in \mathbb{F}_{p^2}$ as follows

$$C_\alpha = \{\beta(1, 0) + \beta\alpha(0, 1) = \beta(1, \alpha) : \beta \in \mathbb{F}_{p^2}\} \tag{2.35}$$

$$C_\infty = \{\beta(0, 1) : \beta \in \mathbb{F}_{p^2}\}.$$

These are $p^2 + 1$ sets, each consisting of p^2 vectors and only $(0, 0)$ is in common between any two sets. If u and v are in the same set, $u \circ v = 0$. The proof is same as in Lemma 2.14.

Let $\alpha = j_1 + j_2\lambda$ and $\beta = k_1 + k_2\lambda$, $j_i, k_i \in \mathbb{Z}_p$, then $u = (\alpha, \beta) = \alpha(1, 0) + \beta(0, 1)$ can be written as

$$\begin{aligned} u &= (j_1 + j_2\lambda)(1, 0) + (k_1 + k_2\lambda)(0, 1) \\ &= j_1(1, 0) + j_2(\lambda, 0) + k_1(0, 1) + k_2(0, \lambda). \end{aligned} \tag{2.36}$$

(2.36) shows that $\mathbb{F}_{p^2}^2$ is a four-dimensional vector space over $\mathbb{Z}_p$. Our goal is to relate the symplectic product in $\mathbb{F}_{p^2}^2$ to the symplectic product in $V_4(\mathbb{Z}_4)$ defined in (2.34) and (2.33) respectively. We do this by defining an isomorphism from $\mathbb{F}_{p^2}^2$ to $V_4(\mathbb{Z}_p)$.

It suffices to define this isomorphism on the bases of each vector space. Let us define a basis for $\mathbb{F}_{p^2}^2$ over $\mathbb{Z}_p$ as follows

$$\mathcal{A} = \{e_0 = 2^{-1}(1,0), e_1 = (2D)^{-1}\lambda(1,0), f_0 = (0,1), f_1 = \lambda(0,1)\}. \tag{2.37}$$

It is easy to check that any element $(\alpha, \beta) = (j_1 + j_2\lambda, k_1 + k_2\lambda) \in {\mathbb{F}_{p^2}}^2$ is a linear combination of the elements in $\mathcal{A}$ as follows

$$(j_1 + j_2\lambda, k_1 + k_2\lambda) = 2j_1e_0 + 2Dj_2e_1 + k_1f_0 + k_2f_1, \tag{2.38}$$

where $j_1, j_2, k_1, k_2 \in \mathbb{Z}_p$. Let M be the linear mapping from $\mathbb{F}_{p^2}^2$ to $V_4(\mathbb{Z}_p)$ defined by its action on e_r and f_r for $r = 0, 1$ so that

$$\begin{aligned} M(e_0) &= (1,0,0,0), \quad M(e_1) = (0,0,1,0), \\ M(f_0) &= (0,1,0,0), \quad M(f_1) = (0,0,0,1). \end{aligned} \tag{2.39}$$

M is a $\mathbb{Z}_p$-isomorphism—a one-to-one, onto mapping that preserves the linear structure. By using (2.38), (2.39) and above notations, we have

$$M((\alpha, \beta)) = (2j_1, k_1, 2Dj_2, k_2). \tag{2.40}$$

It remains to relate the symplectic structure of $\mathbb{F}_{p^2}^2$ and $V_4(\mathbb{Z}_p)$. First we need the idea of the *trace* of a field extension.

Definition 2.19. *Let λ be a solution of the equation $x^2 = D$ in $\mathbb{F}_{p^2}\backslash\mathbb{Z}_p$. For each $\alpha = j + k\lambda \in \mathbb{F}_{p^2}$ define the* ***trace*** *of α by*

$$\mathrm{Tr}(\alpha) = 2j.$$

It is easy to check that for any $i, j \in \{1, 2\}$

$$\mathrm{Tr}(f_i \circ e_j) = \delta(i, j), \quad \mathrm{Tr}(e_i \circ e_j) = \mathrm{Tr}(f_i \circ f_j) = 0. \tag{2.41}$$

Theorem 2.20 ([30]). *Let $z_1 = (\alpha_1, \beta_1)$ and $z_2 = (\alpha_2, \beta_2) \in V_2(\mathbb{F}_{p^2})$ and let M be the linear mapping defined in* (2.39). *Then*

$$M(z_1) \circ M(z_2) = \mathrm{Tr}(z_1 \circ z_2). \tag{2.42}$$

Proof. In the notation of (2.38), let

$$z_1 = 2j_1e_0 + 2Dj_2e_1 + k_1f_0 + k_2f_1, \quad z_2 = 2r_1e_0 + 2Dr_2e_1 + s_1f_0 + s_2f_1.$$

Since $\mathcal{A}$ defined in (2.37) is a basis for $V_2(\mathbb{F}_{p^2})$ over $\mathbb{Z}_p$, we can write $z_1 \circ z_2$ in terms of basis elements. Using (2.41), we have

$$\begin{aligned}
\mathrm{Tr}(z_1 \circ z_2) &= (k_1 2r_1 - 2j_1 s_1) + (k_2 2Dr_2 - 2Dj_2 s_2) \\
&= (2j_1, k_1) \circ (2r_1, s_1) + (2Dj_2, k_2) \circ (2Dr_2, s_2) \\
&= (2j_1, k_1, 2Dj_2, k_2) \circ (2r_1, s_1, 2Dr_2, s_2) \\
&= M(z_1) \circ M(z_2).
\end{aligned}$$

□

For any $z_1, z_2 \in C_\alpha$, $z_1 \circ z_2 = 0$. So $\mathrm{Tr}(z_1 \circ z_2) = 0$. Using Equation (2.42) in Theorem 2.20, we have $M(z_1) \circ M(z_2) = 0$. Therefore, the symplectic product of

elements of $M(C_\alpha) \subset V_4(\mathbb{Z}_p)$ is equal to zero. It is well known [30] that if we want to have the property stated in Equation (2.42), we need a basis of the form $\mathcal{A}$ defined in (2.37).

From (2.36) for any $\alpha = j_1 + j_2\lambda$, $\beta = k_1 + k_2\lambda \in \mathbb{F}_{p^2}$, $\lambda^2 = D$, each element $(\beta, \beta\alpha)$ in the class C_α is of the form

$$\begin{aligned}(\beta, \beta\alpha) &= (j_k + j_k\lambda, (k_1 + k_2\lambda)(j_1 + j_2\lambda)) \\ &= k_1(1,0) + k_2\lambda(1,0) + (k_1j_1 + k_2j_2D)(0,1) + \lambda(k_1j_2 + k_2j_1)(0,1) \\ &= 2k_1e_0 + 2Dk_2e_1 + (k_1j_1 + k_2j_2D)f_0 + (k_1j_2 + k_2j_1)f_1.\end{aligned}$$

Thus

$$\begin{aligned}M((\beta, \beta\alpha)) &= M(2k_1e_0 + 2Dk_2e_1 + (k_1j_1 + k_2j_2D)f_0 + (k_1j_2 + k_2j_1)f_1) \\ &= 2k_1M(e_0) + 2Dk_2M(e_1) + (k_1j_1 + k_2j_2D)M(f_0) + (k_1j_2 + k_2j_1)M(f_1) \\ &= (2k_1, k_1j_1 + k_2j_2D, 2Dk_2, k_1j_2 + k_2j_1). \qquad (2.43)\end{aligned}$$

Thus classes in $\mathbb{F}_{p^2}^2$ can be expressed by classes with elements of the form (2.43). So, each element of C_α is mapped to an element of C_{j_1,j_2}.

Lemma 2.21 ([30])**.** *Let p be an odd prime. The classes given by C_α and C_∞ defined in* (2.35) *are mapped to the following classes in $V_4(\mathbb{Z}_p)$*

$$\begin{aligned}C_{j_1,j_2} &= \{(2k_1, k_1j_1 + k_2j_2D, 2Dk_2, k_1j_2 + k_2j_1) : k_1, k_2 \in \mathbb{Z}_p\}, \\ C_\infty &= \{(0, k_1, 0, k_2) : k_1, k_2 \in \mathbb{Z}_p\}, \qquad (2.44)\end{aligned}$$

where $j_1,\ j_2 \in \mathbb{Z}_p$. *Moreover* $V_4(\mathbb{Z}_p) = \bigcup_{j_1,j_2} C_{j_1,j_2} \bigcup C_\infty$ *and the intersection of any two classes is* $\{(0,0,0,0)\}$. *Therefore the set of Spin matrices indexed by each class is commuting.*

Proof. First we show that in each class, the symplectic product defined in (2.33) is zero. Let $w_1 = (2k_1, k_1j_1 + k_2j_2D, 2Dk_2, k_1j_2 + k_2j_1) = (u_1, v_1)$ and $w_2 = (2k_1', k_1'j_1 + k_2'j_2D, 2Dk_2', k_1'j_2 + k_2'j_1) = (u_2, v_2)$ be two elements in C_{j_1,j_2}. Then

$$\begin{aligned} w_1 \circ w_2 &= (2k_1, k_1j_1 + k_2j_2D) \circ (2k_1', k_1'j_1 + k_2'j_2D) + \\ &\quad (2Dk_2, k_1j_2 + k_2j_1) \circ (2Dk_2', k_1'j_2 + k_2'j_1) \\ &= 0. \end{aligned}$$

It remains to show that $C_{j_1,j_2} \bigcap C_{j_1',j_2'} = (0,0,0,0)$ for $(j_1, j_2) \neq (j_1', j_2')$. Assume the contrary. Let $w = (2k_1, k_1j_1 + k_2j_2D, 2Dk_2, k_1j_2 + k_2j_1) \in C_{j_1,j_2} \bigcap C_{j_1',j_2'}$. Then we have the following equations

$$j_1k_1 + j_2k_2D = j_1'k_1 + j_2'k_2D, \quad j_1k_2 + j_2k_1 = j_1'k_2 + j_2'k_1.$$

We can rewrite the above system as

$$k_1(j_1 - j_1') + k_2D(j_2 - j_2') = 0, \quad k_2(j_1 - j_1') + k_1(j_2 - j_2') = 0.$$

Above system is homogeneous and has non-trivial solution if and only if $k_2^2D = k_1^2$. But D is not a quadratic residues modulo p. So, the system has only trivial solution

$j_1 - j_1' = 0$ and $j_2 - j_2' = 0$. So $(j_1, j_2) = (j_1', j_2')$. Contradiction. By the same argument we can show $C_\infty \bigcap C_{j_1,j_2} = (0,0,0,0)$. □

$V_4(\mathbb{Z}_p)$ has p^4 elements, partitioned by p^2+1 subsets of the form defined in Lemma 2.21. Spin matrices associated to each subset are commuting. Thus we have partitioned the Spin matrices of order p^2 into p^2+1 subsets of unitary matrices such that Spin matrices in each subset are commuting and orthogonal. Thus by Theorem 2.9 we have p^2+1 MUBs.

For example, for $p = 3$, $D = 2$ is not quadratic residues modulo 3. The sets of Spin matrices corresponding to C_{j_1,j_2}, $j_1, j_2 \in \mathbb{Z}_3$ and C_∞ defined in Lemma 2.21 are

$$\mathcal{C}_{j_1,j_2} = \left\{ S_{(2k_1, k_1 j_1 + 2k_2 j_2)} \otimes S_{(k_2, k_1 j_2 + k_2 j_1)} : k_1, k_2 \in \mathbb{Z}_3 \right\},$$

$$\mathcal{C}_\infty = \left\{ S_{(0,k_1)} \otimes S_{(0,k_2)} : k_1, k_2 \in \mathbb{Z}_3 \right\}.$$

2.5 Spin matrices of dimension $d = p^n$, p prime

In Section 2.4 we described how we can partition the set of Spin matrices of dimension $d = p^2$ into the commuting subsets. By the same methodology, A. O. Pittenger and M. H. Rubin (see [30]) partitioned the set of Spin matrices of dimension $d = p^n$, $n \in \mathbb{Z}$, into the commuting subsets.

Consider the n-fold tensor product of the Spin matrices

$$U_1 = S_{u_1} \otimes S_{u_2} \otimes \cdots \otimes S_{u_n},$$

$$U_2 = S_{v_1} \otimes S_{v_2} \otimes \cdots \otimes S_{v_n},$$

where $u_i = (j_i, k_i)$, $v_i = (a_i, b_i) \in \mathbb{Z}_p^2$ for $i = 1, \ldots n$. Then

$$\begin{aligned} U_1U_2 =& (S_{u_1} \otimes S_{u_2} \otimes \cdots \otimes S_{u_n})(S_{v_1} \otimes S_{v_2} \otimes \cdots \otimes S_{v_n}) \\ &= S_{u_1}S_{v_1} \otimes S_{u_2}S_{v_2} \otimes \cdots \otimes S_{u_n}S_{v_n} \\ &= \omega^{k_1a_1+k_2a_2+\cdots+k_na_n} S_{v_1}S_{u_1} \otimes S_{v_2}S_{u_2} \otimes \cdots \otimes S_{u_n}S_{v_n} \\ &= \omega^{k_1a_1+k_2a_2+\cdots+k_na_n} (S_{v_1} \otimes S_{v_2} \otimes \cdots \otimes S_{v_n})(S_{u_1} \otimes S_{u_2} \otimes \cdots \otimes S_{u_n}) \\ &= \omega^{k_1a_1+k_2a_2+\cdots+k_na_n} U_2U_1. \end{aligned}$$

By the same argument we see that

$$U_2U_1 = \omega^{b_1j_1+b_2j_2+\cdots+b_nj_n} U_1U_2.$$

Thus U_1 and U_2 commute if and only if

$$k_1a_1 + k_2a_2 + \cdots + k_na_n = b_1j_1 + b_2j_2 + \cdots + b_nj_n,$$

or equivalently

$$(k_1a_1 - b_1j_1) + (k_2a_2 - b_2j_2) + \cdots + (k_na_n - b_nj_n) = 0.$$

We may rewrite above equation in terms of the symplectic product as follows

$$u_1 \circ v_1 + u_2 \circ v_2 + \cdots + u_n \circ v_n = 0. \tag{2.45}$$

Define $V_{2n}(\mathbb{Z}_p)$ as follows

$$V_{2n}(\mathbb{Z}_p) = \{(j_1, k_1, j_2, k_2, \ldots, j_n, k_n) = (u_1, u_2, \ldots, u_n) : j_i, k_i \in \mathbb{Z}_p\}.$$

$V_{2n}(\mathbb{Z}_p)$ has p^{2n} elements. Our desire is to partition $V_{2n}(\mathbb{Z}_p)$ into $p^n + 1$ classes, each consisting of p^n elements such that elements in each class satisfy (2.45). This is doable by defining a structure on $\mathbb{F}_{p^n}$ analogously to the case $d = p^2$ in Section 2.4.

Let us now briefly explain the process of partitioning $V_{2n}(\mathbb{Z}_p)$.

A polynomial is said to be **irreducible** in $\mathbb{Z}_p$ if it cannot be factored into the product of two or more non-trivial polynomials whose coefficients are in $\mathbb{Z}_p$. For any p, there exists an irreducible polynomial of degree n over $\mathbb{Z}_p$ [3].

Let $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ be a an irreducible polynomial of degree n over $\mathbb{Z}_p$ and λ a root of f in $\mathbb{F}_{p^n}$, then f can be uniquely written in the form

$$f(x) = (x - \lambda)(d_{n-1}x^{n-1} + d_{n-2}x^{n-2} + \cdots + d_0), \quad d_i \in \mathbb{F}_{p^n}. \tag{2.46}$$

Any $\alpha \in \mathbb{F}_{p^n}$ can be written as follows

$$\alpha = a_{n-1}\lambda^{n-1} + a_{n-2}\lambda^{n-2} + \cdots + a_0, \qquad a_i \in \mathbb{Z}_p.$$

Define $\mathbb{F}_{p^n}^2$ by

$$\mathbb{F}_{p^n}^2 = \{u = (\alpha, \beta) : \alpha, \beta \in \mathbb{F}_{p^n}\}, \tag{2.47}$$

and the symplectic product of two elements $u = (\alpha, \beta)$, $u = (\alpha', \beta') \in \mathbb{F}_{p^n}^2$ by

$$u \circ u' = \beta\alpha' - \alpha\beta'.$$

Consider subsets of $\mathbb{F}_{p^n}^2$ as follows

$$C_\alpha = \{\beta(1, \alpha) : \beta \in \mathbb{F}_{p^n}\}, \ \ \alpha \in \mathbb{F}_{p^n}, \tag{2.48}$$

$$C_\infty = \{\beta(0,1) : \beta \in \mathbb{F}_{p^n}\}. \tag{2.49}$$

These give $p^n + 1$ subsets of $\mathbb{F}_{p^n}^2$, each consisting of p^n vectors, only $(0,0)$ common to any two sets. If u and v are in the same set, then it is easy check that $u \circ v = 0$. As with the case $d = p^2$, it is convenient to express the index sets in (2.48) and (2.49) in term of elements in $\mathbb{Z}_p$. So we need to relate each subset of $\mathbb{F}_{p^n}^2$ defined in (2.48) and (2.49) to a subset in $V_{2n}(\mathbb{Z}_p)$. First we need a $\mathbb{Z}_p$-isomorphism map M from $\mathbb{F}_{p^n}^2$ to $V_{2n}(\mathbb{Z}_p)$ like the map defined in (2.39). We just need to define M on bases of each spaces. $\mathbb{F}_{p^n}^2$ is a two-dimensional vector space over $\mathbb{F}_{p^n}$ and $\mathbb{F}_{p^n}$ is a n-dimensional space over $\mathbb{Z}_p$. Thus $\mathbb{F}_{p^n}^2$ is a $2n$-dimensional space over $\mathbb{Z}_p$. Define a basis for $\mathbb{F}_{p^n}^2$ as follows

$$\mathcal{A} = \{e_j = \frac{d_j}{f'(\lambda)}(1,0), f_k = \lambda^k(0,1) : 0 \le j,k \le n-1\} \tag{2.50}$$

where the d_js are defined in (2.46) and f' is derivative of f.

Definition 2.22. *Let λ be a root of the irreducible polynomial $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ over $\mathbb{Z}_p$. For each $\alpha = \alpha(\lambda) = a_{n-1}\lambda^{n-1} + \cdots + a_1\lambda + a_0 \in \mathbb{F}_{p^n}$, define $\mathrm{Tr}(\alpha)$ by*

$$\mathrm{Tr}(\alpha) = \textstyle\sum_{r=1}^{n} \alpha(\lambda_r),$$

where the λ_r for $r = 1, \ldots, n$ are the n distinct roots of $f(x)$ in $\mathbb{F}_{p^n}$.

Observe that $f_k \circ e_j$ is an element of $\mathbb{F}_{p^n}$. It is proved [30] that elements e_j and f_k defined in (2.50) satisfy

$$\mathrm{Tr}(f_k \circ e_j) = \delta(k, j). \tag{2.51}$$

The reason for defining coefficients $d_j/f'(\lambda)$ for e_js and λ^k for f_k is that the equation (2.51) holds only for these coefficients.

Using indexing beginning at 0, let M denote the linear mapping that maps $\mathcal{A}$ to the standard basis in $V_{2n}(\mathbb{Z}_p)$ as follows

$$M(e_j) = \mathbf{e}_{2j}, \quad M(f_j) = \mathbf{e}_{2j+1}, \quad 0 \leq j, \leq n-1, \tag{2.52}$$

where $\{\mathbf{e}_0, \ldots, \mathbf{e}_{2n-1}\}$ is the standard basis in $V_{2n}(\mathbb{Z}_p)$. When $n = 2$, M is as defined in (2.39). For every vector $u \in \mathbb{F}_{p^n}^2$, $M(u) \in V_{2n}(\mathbb{Z}_p)$.

By the same argument as in Theorem 2.20 and using (2.51), the symplectic products in $\mathbb{F}_{p^n}^2$ and $V_{2n}(\mathbb{Z}_p)$ are related by

$$M(z_1) \circ M(z_2) = \mathrm{Tr}(z_1 \circ z_2), \tag{2.53}$$

where $z_1, z_2 \in V\mathbb{F}_{p^n}^2$ and $M(z_1), M(z_2) \in V_{2n}(\mathbb{Z}_p)$ [30]. Now we may map each class in $\mathbb{F}_{p^n}^2$ defined in (2.48) to a class in $V_{2n}(\mathbb{Z}_p)$ by the following algorithm.

Keep all notations as defined in this section.

Let $\alpha = a_{n-1}\lambda^{n-1} + a_{n-2}\lambda^{n-2} + \cdots + a_0 \in \mathbb{F}_{p^n}$. Since $\{e_j, f_j : 0 \leq j \leq n-1\}$ is a basis for $\mathbb{F}_{p^n}^2$, then any element $(\beta, \beta\alpha) \in C_\alpha \subset \mathbb{F}_{p^n}^2$ can be written as follows

$$(\beta, \beta\alpha) = \sum_{j=0}^{n-1} x_j e_j + y_j f_j, \quad x_j, y_j \in \mathbb{Z}_p. \tag{2.54}$$

M acts on $(\beta, \beta\alpha)$ as follows

$$\begin{aligned} M((\beta, \beta\alpha)) &= \sum_{j=0}^{n-1} M(x_j e_j) + M(y_j f_j) \\ &= \sum_{j=0}^{n-1} x_j \mathbf{e}_{2j} + y_j \mathbf{e}_{2j+1}. \end{aligned} \tag{2.55}$$

On the other hand, for $z_1 = (\beta, \beta\alpha)$, $z_2 = (\beta', \beta'\alpha) \in C_\alpha$, $z_1 \circ z_2 = 0$. By using (2.51) we have

$$\mathrm{Tr}(z_1 \circ z_2) = M(z_1) \circ M_(z_2) = 0. \tag{2.56}$$

Thus by (2.55) and (2.56), if $\alpha \in \mathbb{F}_{p^n}$, then $M(C_\alpha) \subset V_{2n}(\mathbb{Z}_p)$ and the symplectic product of two elements of $M(C_\alpha)$ is zero. So, for each $\alpha = a_{n-1}\lambda^{n-1} + a_{n-2}\lambda^{n-2} + \cdots + a_0 \in \mathbb{F}_{p^n}$, we associate a class $M(C_\alpha) = C_{a_{n-1},\ldots,a_0}$ as follows

$$C_{a_{n-1},\ldots,a_0} = \left\{ (x_0, y_0, \ldots, x_{n-1}, y_{n-1}) : (\beta, \beta\alpha) = \sum_{j=0}^{n-1} x_j e_j + y_j f_j, \beta \in \mathbb{F}_{p^n}, x_j, y_j \in \mathbb{Z}_p \right\}. \tag{2.57}$$

Similarly, $M(C_\infty) = C'_\infty$ can be defined as follows

$$C'_\infty = \left\{ (0, y_0, \ldots, 0, y_{n-1}) : (0, \beta) = \sum_{j=0}^{n-1} y_j f_j : \beta \in \mathbb{F}_{p^n}, y_j \in \mathbb{Z}_p \right\}. \tag{2.58}$$

Thus the classes defined in (2.57) and (2.58) partition $V_{2n}(\mathbb{Z}_p)$ so that the symplectic product of two elements in each class is zero. Spin matrices derived from each class commute and are of the forms

$$\mathcal{C}_{a_{n-1},\ldots,a_0} = \left\{ S_{x_0,y_0} \otimes \cdots \otimes S_{x_{n-1},y_{n-1}} : (x_0, y_0, \ldots, x_{n-1}, y_{n-1}) \in C_{a_{n-1},\ldots,a_0} \right\},$$

and

$$\mathcal{C}_\infty = \left\{ S_{0,y_0} \otimes \cdots \otimes S_{0,y_{n-1}} : (0, y_0, \ldots, 0, y_{n-1}) \in C_\infty \right\}.$$

Thus we have a partition for a set of unitary matrices (Spin matrices) such that the Spin matrices from each class commute. Now we may use Theorem 2.9 to derive $p^n + 1$ MUBs in $\mathbb{C}^{p^n}$ from eigenvectors of the Spin matrices from each class.

Example 2.23. *For $p = n = 2$, an appropriate polynomial is $f(x) = x^2 + x + 1$. Then $f'(x) = 1$. If $f(\lambda) = 0$, then $\lambda^2 = \lambda + 1$ is the second root, given $d_1 = 1$ and $d_0 = \lambda^2$, since $x^2 + x + 1 = (x - \lambda)(x - \lambda - 1)$. Then*

$$e_0 = \lambda^2(1,0), \quad e_1 = (1,0), \quad f_0 = (0,1), \quad f_1 = \lambda(0,1).$$

The five classes of vectors in $\mathbb{F}_{2^2}^2$ indexed by $\alpha = j_0 + j_1\lambda$, $j_0, j_1 \in \mathbb{Z}_p$, are

$$C_0 = \{(0,0),(1,0),(\lambda,0),(\lambda^2,0)\} = \{0, e_1, e_0+e_1, e_0\},$$

$$C_1 = \{0,0),(1,1),(\lambda,\lambda),(\lambda^2,\lambda^2)\} = \{0, e_1+f_0, e_0+e_1+f_1, e_0+f_0+f_1\},$$

$$C_\lambda = \{0,0),(1,\lambda),(\lambda,\lambda^2),(\lambda^2,1)\} = \{0, e_1+f_1, e_0+e_1+f_0+f_1, e_0+f_0\},$$

$$C_{\lambda^2} = \{0,0),(1,\lambda^2),(\lambda,1),(\lambda^2,\lambda)\} = \{0, e_1+f_0+f_1, e_0+e_1+f_0, e_0+f_1\},$$

$$C_\infty = \{0,0),(0,1),(0,\lambda),(0,\lambda^2)\} = \{0, f_1, f_0+f_1, f_0\}.$$

Under the mapping M defined in (2.52) *for the case $d = 2^2$, the classes in $V_2(\mathbb{F}_{2^2})$ are mapped to classes in $V_4(\mathbb{Z}_2)$ as follows*

$$C_0 \to C_{0,0} = \{(0000),(0010),(1010),(1000)\},$$

$$C_1 \to C_{1,0} = \{(0000), (0110), (1011), (1101)\},$$

$$C_\lambda \to C_{0,1} = \{(0000), (0011), (1111), (1100)\},$$

$$C_{\lambda^2} \to C_{1,1} = \{(0000), (0111), (1110), (1001)\},$$

$$C_\infty \to C'_\infty = \{(0000), (0100), (0001), (0101)\}.$$

The Spin matrices corresponding to the above classes are

$$\mathcal{C}_{0,0} = \{S_{00} \otimes S_{00}, S_{00} \otimes S_{10}, S_{10} \otimes S_{10}, S_{10} \otimes S_{00}\},$$

$$\mathcal{C}_{1,0} = \{S_{00} \otimes S_{00}, S_{01} \otimes S_{10}, S_{10} \otimes S_{11}, S_{11} \otimes S_{01}\},$$

$$\mathcal{C}_{0,1} = \{S_{00} \otimes S_{00}, S_{00} \otimes S_{11}, S_{11} \otimes S_{11}, S_{11} \otimes S_{00}\},$$

$$\mathcal{C}_{1,1} = \{S_{00} \otimes S_{00}, S_{01} \otimes S_{11}, S_{11} \otimes S_{10}, S_{10} \otimes S_{01}\},$$

$$\mathcal{C}_\infty = \{S_{00} \otimes S_{00}, S_{01} \otimes S_{00}, S_{00} \otimes S_{01}, S_{01} \otimes S_{01}\},$$

where $S_{j,k}$ for $j, k \in \{0, 1\}$ are defined in Example 2.18. *5 MUBs are determined by eigenvectors of the Spin matrices in the 5 classes.*

2.6 Algebraic construction of MUBs for odd prime powers

In this section we present a construction based on Weil sums. First, some basic definitions.

Definition 2.24. *For $\alpha \in F = \mathbb{F}_{p^n}$ and $K = \mathbb{Z}_p$, the trace $\mathrm{Tr}_{F/K}(\alpha)$ of α over $\mathbb{Z}_p$ is defined by*

$$\mathrm{Tr}_{F/K}(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{m-1}}.$$

Henceforth, we use Tr instead of $\mathrm{Tr}_{F/K}$ for convenience. If we consider $\mathbb{F}_{p^n}$ as n-dimensional vectors space over $\mathbb{Z}_p$, it is well know that Tr is a linear transformation from $\mathbb{F}_{p^n}$ onto $\mathbb{Z}_p$, i.e., $\mathrm{Tr}(c_1\alpha + c_2\beta) = c_1\,\mathrm{Tr}(\alpha) + c_2\,\mathrm{Tr}(\beta) \in \mathbb{Z}_p$ for $\alpha, \beta \in \mathbb{F}_{p^n}$ and $c_1, c_2 \in \mathbb{Z}_p$ [27].

For each non-zero element $x \in \mathbb{Z}_p$, define a non-trivial additive **character** $\chi_x : \mathbb{F}_{p^m} \mapsto \mathbb{C}\backslash\{0\}$ by

$$y \mapsto \omega^{\mathrm{Tr}(xy)}, \tag{2.59}$$

where $\omega = e^{(2\pi i/p)}$, a primitive pth root of unity. It is easy to check that for any $x \in \mathbb{F}\backslash\{0\}$

$$\sum_{y \in \mathbb{F}_{p^n}} \chi_x(y) = 0. \tag{2.60}$$

See [21] for the proof.

The next lemma plays a crucial role for this section. You may see a proof in [27].

Lemma 2.25 (**Weil sums**). *Let χ be the non-trivial additive character of $\mathbb{F}_{p^m}$ defined in* (2.59)*, where p is an odd prime number and let $f(X) \in \mathbb{F}_{p^n}[X]$ be a polynomial of degree* 2*. Then*

$$\left| \sum_{x \in \mathbb{F}_{p^n}} \chi(f(x)) \right| = \sqrt{d},$$

where $d = p^n$.

Ivanovic in 1981 [22] found the following construction for MUBs of prime power dimensions. A.Klappenecker and M.Rötteler gave an elementary proof of the construction in [24] by taking advantage of Weil sums.

Theorem 2.26 ([22],[24]). *Let $p > 2$ be a prime number. For each $a \in \mathbb{F}_{p^m}$, define a set of vectors by*

$$\mathcal{B}_a = \{\mathbf{v}_{a,b} | b \in \mathbb{F}_{p^n}\},$$

where $\mathbf{v}_{a,b}$ is a vector of length p^n defined as follows. Considering elements of $\mathbb{F}_{p^n}$ as an index set, the xth component of $\mathbf{v}_{a,b}$ is defined by

$$(\mathbf{v}_{a,b})_x = \frac{1}{\sqrt{d}} \omega^{\mathrm{Tr}(ax^2+bx)}, \quad x \in \mathbb{F}_{p^n}, \tag{2.61}$$

where $d = p^n$. Then the sets $\mathcal{B}_a$ and the standard basis, form $p^n + 1$ mutually unbiased bases in $\mathbb{C}^{p^n}$.

Proof. The inner product of two vectors defined in (2.61) is

$$|\langle \mathbf{v}_{a,b}, \mathbf{v}_{c,d} \rangle| = \left| \frac{1}{d} \sum_{x \in \mathbb{F}_{p^n}} \omega^{\mathrm{Tr}((a-c)x^2+(b-d)x)} \right|.$$

By considering possible cases for the values of a, b, c, d, if $a = c$ and $b \neq d$ the right hand side is equal 0 by (2.60). If $a = c$ and $b = d$ then the inner product is equal to 1. Thus $\mathcal{B}_a$ is an orthonormal basis for any $a \in \mathbb{F}_{p^n}$. On the other hand, if $a \neq c$, then the right hand side evaluates to $\dfrac{1}{\sqrt{d}}$ by Lemma 2.25, which proves that the bases $\mathcal{B}_a$ and $\mathcal{B}_c$ are mutually unbiased. Since for any $x \in \mathbb{F}_{p^n}$, $\left|(\mathbf{v}_{a,b})_x\right|^2 = \dfrac{1}{d}$, the standard basis is mutually unbiased to $\mathcal{B}_a$ for $a \in \mathbb{F}_{p^n}$. □

Example 2.27. *For $d = p = 3$, $\mathbb{F}_3 = \{0, 1, 2\}$. Using the construction given in Theorem 2.26, the bases are*

$$\mathcal{B}_0 = \{\mathbf{v}_{0,0}, \mathbf{v}_{0,1}, \mathbf{v}_{0,2}\} = \left\{ \frac{1}{\sqrt{3}}(1,1,1), \frac{1}{\sqrt{3}}(1,\omega,\omega^2), \frac{1}{\sqrt{3}}(1,\omega^2,\omega) \right\},$$
$$\mathcal{B}_1 = \{\mathbf{v}_{1,0}, \mathbf{v}_{1,1}, \mathbf{v}_{1,2}\} = \left\{ \frac{1}{\sqrt{3}}(1,\omega,\omega), \frac{1}{\sqrt{3}}(1,\omega^2,1), \frac{1}{\sqrt{3}}(1,1,\omega^2) \right\},$$
$$\mathcal{B}_2 = \{\mathbf{v}_{2,0}, \mathbf{v}_{2,1}, \mathbf{v}_{2,2}\} = \left\{ \frac{1}{\sqrt{3}}(1,\omega^2,\omega^2), \frac{1}{\sqrt{3}}(1,1,\omega), \frac{1}{\sqrt{3}}(1,\omega,1) \right\},$$

and the standard basis form 4 mutually unbiased bases. For instance $\mathbf{v}_{2,1} \in \mathcal{B}_2$ is calculated in the following manner

$$\begin{aligned}
\mathbf{v}_{2,1} &= \frac{1}{\sqrt{3}} \left((\mathbf{v}_{2,1})_0, (\mathbf{v}_{2,1})_1, (\mathbf{v}_{2,1})_2 \right) \\
&= \frac{1}{\sqrt{3}} \left(\omega^{\mathrm{Tr}(2(0)^2+0)}, \omega^{\mathrm{Tr}(2(1)^2+1)}, \omega^{\mathrm{Tr}(2(2)^2+2)} \right) \\
&= \frac{1}{\sqrt{3}} \left(1, 1, \omega \right).
\end{aligned}$$

2.6.1 Algebraic construction of MUBs for even prime powers

In Section 2.6, we stated a construction for MUBs in dimension equal to an odd prime power based on Weil sums. We cannot use Weil sums for the case $p = 2$ because Lemma 2.25 does not apply in even characteristic. In this section we consider the case $p = 2$. We use Galois rings for constructing MUBs for dimensions of the form $d = 2^n$.

A polynomial $F(x) \in \mathbb{Z}_2[x]$ is **primitive** if it has a root ξ in $\mathbb{F}_{2^n}$ and $\{0, 1, \xi, \ldots, \xi^{2^n-2}\}$ is the entire field $\mathbb{F}_{2^n}$, and moreover, $F(x)$ is the smallest degree polynomial having

ξ as root. It is well known that there exists a unique polynomial $h(x) \in \mathbb{Z}_4[x]$ such that $h(x) \equiv F(x) \pmod 2$ and $h(x)$ divides $x^{2^n-1} - 1$ as a polynomial in $\mathbb{Z}_4[x]$ [16]. For example, if $F(x) = x^3 + x + 1$ then $h(x) = x^3 + 2x^2 + x - 1$. See [16] for an algorithm showing how $h(x)$ can be found from a given primitive polynomial $F(x)$. Let α be a root of $h(x)$. In fact, α can be chosen such that it is a primitive $(2^n - 1)$th root of unity. The corresponding **Galois ring**, $GR(4^n)$, is defined by

$$GR(4^n) = \mathbb{Z}_4[\alpha]. \tag{2.62}$$

$GR(4^n)$ has 4^n elements. Define $\mathcal{T}_n$ by

$$\mathcal{T}_n = \{0, 1, \alpha, \ldots, \alpha^{2^n-2}\}. \tag{2.63}$$

$\mathcal{T}_n$ contains all the distinct $(2^n - 1)$th roots of unity. Every element $r \in GR(4^n)$ can be represented uniquely of the form

$$r = \alpha^j + 2\alpha^m,$$

for $j, m \in \{0, 1, \ldots, 2^n - 2\}$, see [39] for details. The map $\sigma : GR(4^n) \to GR(4^n)$ defined by $\sigma(r) = \sigma(\alpha^j + 2\alpha^m) = \alpha^{2j} + 2\alpha^{2m}$ is called the **Frobenius automorphism** [[39], p.86]. Using σ^t to denote t-fold composition of σ, define the **trace map** Tr : $GR(4^n) \to \mathbb{Z}_4$ by

$$\mathrm{Tr}(r) = \sum_{t=0}^{n-1} \sigma^t(r), \tag{2.64}$$

where σ^0 denotes the identity map. You may see a comprehensive discussion on Galois rings in [16] and [39].

Lemma 2.28 ([43]). *Using the same notations as above and let $i^2 = -1$. Define $\Gamma : GR(4^n) \to \mathbb{C}$ by*

$$\Gamma(r) = \sum_{k=0}^{2^n-2} i^{\mathrm{Tr}(r\alpha^k)}. \tag{2.65}$$

Then

$$|\Gamma(r)| = \begin{cases} 0 & \text{if } r \in 2\mathcal{T}_n, r \neq 0; \\ 2^n & \text{if } r = 0; \\ \sqrt{2^n} & \text{otherwise.} \end{cases}$$

Theorem 2.29. *Let $GR(4^n)$ and $\mathcal{T}_n$ be sets defined in* (2.62) *and* (2.63). *For $\alpha^j, \alpha^m \in \mathcal{T}_n$, $j, m \in \{0, 1, \ldots, 2^n - 2\}$, define 2^n dimensional vectors $\mathbf{v}_{\alpha^i,\alpha^j}$ with kth entry, $k \in \{0, 1, \ldots, 2^n - 2\}$, by*

$$\left(\mathbf{v}_{\alpha^j,\alpha^m}\right)_k = \frac{1}{\sqrt{2^n}} i^{\mathrm{Tr}\left((\alpha^j + 2\alpha^m)\alpha^k\right)}. \tag{2.66}$$

Then, for $j = 0, 1, \ldots, 2^n - 2$, the sets

$$\mathcal{B}_{\alpha^j} = \{\mathbf{v}_{\alpha^j,\alpha^m} | m = 0, 1, \ldots, 2^n - 2\}, \tag{2.67}$$

and the standard basis form $2^n + 1$ MUBs in $\mathbb{C}^{2^n}$.

Proof. The inner product of two vectors $\mathbf{v}_{\alpha^j,\alpha^m}$ and $\mathbf{v}_{\alpha^{j'},\alpha^{m'}}$ with entries defined in (2.66) is

$$\left|\langle \mathbf{v}_{\alpha^j,\alpha^m}, \mathbf{v}_{\alpha^{j'},\alpha^{m'}} \rangle\right| = \frac{1}{2^n} \left| \sum_{k=0}^{2^n-2} i^{\mathrm{Tr}\left((\alpha^j - \alpha^{j'} + 2(\alpha^m - \alpha^{m'}))\alpha^k\right)} \right|.$$

If $j = j'$ and $m \neq m'$, since $2(\alpha^m - \alpha^j) \in 2\mathcal{T}_n$ then the right hand side equals to 0 by *Lemma* 2.28. If $j = j'$ and $m = m'$ then right hand side is equal to 1. This shows that $\mathcal{B}_{\alpha^j}$ is an orthonormal basis.

When $j \neq j'$, i.e., the vectors belong to different bases, then $r = (\alpha^j - \alpha^{j'}) + 2(\alpha^m - \alpha^{m'}) \notin 2\mathcal{T}_n$. Thus by Lemma 2.28, $\left|\langle \mathbf{v}_{\alpha^j,\alpha^m}, \mathbf{v}_{\alpha^{j'},\alpha^{m'}} \rangle\right| = \frac{1}{\sqrt{2^n}}$, hence $\mathcal{B}_{\alpha^j}$ and $\mathcal{B}_{\alpha^{j'}}$ are mutually unbiased.

The entries of the vectors $\mathbf{v}_{\alpha^j,\alpha^m}$ have absolute value $\frac{1}{\sqrt{2^n}}$, so the standard basis and $\mathcal{B}_{\alpha^j}$ are mutually unbiased for all $\alpha^j \in \mathcal{T}_n$. □

Example 2.30. *For $n = 2$, $h(x) = x^2 + x + 1$ is an irreducible polynomial in $\mathbb{Z}_4[x]$ with root α, such that $\alpha^{2^2-1} = 1$. Let $\mathcal{T}_2 = \{0, 1, \alpha, \alpha^2\}$. Consider the Galois ring $GR(4^2) = \mathbb{Z}_4[\alpha]$ with 16 elements. Any $r \in GR(4^2)$ is of the form $r = \alpha^j + 2\alpha^m$, $j, m \in \{0, 1, 2\}$. For $\alpha^j, \alpha^m \in \mathcal{T}_2$, $\sigma(\alpha^j + 2\alpha^m) = \alpha^{2j} + 2\alpha^{2m}$, $\sigma^0(\alpha^j + 2\alpha^m) = \alpha^j + 2\alpha^m$. Using* (2.64), $\mathrm{Tr}(\alpha^j + 2\alpha^m) = \sigma^0(\alpha^j + 2\alpha^m) + \sigma(\alpha^j + 2\alpha^m) = \alpha^j + 2\alpha^m + \alpha^{2j} + 2\alpha^{2m} \in \mathbb{Z}_4$. *The 4 bases constructed in Theorem* 2.29 *are*

$$\mathcal{B}_0 = \{\mathbf{v}_{0,0}, \mathbf{v}_{0,1}, \mathbf{v}_{0,\alpha}, \mathbf{v}_{0,\alpha^2}\}, \qquad \mathcal{B}_1 = \{\mathbf{v}_{1,0}, \mathbf{v}_{1,1}, \mathbf{v}_{1,\alpha}, \mathbf{v}_{1,\alpha^2}\},$$

$$\mathcal{B}_\alpha = \{\mathbf{v}_{\alpha,0}, \mathbf{v}_{\alpha,1}, \mathbf{v}_{\alpha,\alpha}, \mathbf{v}_{\alpha,\alpha^2}\}, \qquad \mathcal{B}_{\alpha^2} = \{\mathbf{v}_{\alpha^2,0}, \mathbf{v}_{\alpha^2,1}, \mathbf{v}_{\alpha^2,\alpha}, \mathbf{v}_{\alpha^2,\alpha^2}\}.$$

Applying (2.66) *yields*

$$\mathcal{B}_0 = \left\{\frac{1}{2}(1,1,1,1), \frac{1}{2}(1,1,-1,-1), \frac{1}{2}(1,-1,-1,1), \frac{1}{2}(1,-1,1,-1)\right\},$$
$$\mathcal{B}_1 = \left\{\frac{1}{2}(1,-1,-i,-i), \frac{1}{2}(1,1,1,1), \frac{1}{2}(1,1,1,1), \frac{1}{2}(1,1,1,1)\right\},$$

$$\mathcal{B}_{\alpha} = \left\{ \frac{1}{2}(1,-i,-i,-1), \frac{1}{2}(1,-i,i,1), \frac{1}{2}(1,i,i,-1), \frac{1}{2}(1,i,-i,1) \right\},$$
$$\mathcal{B}_{\alpha^2} = \left\{ \frac{1}{2}(1,-i,-1,-i), \frac{1}{2}(1,-i,1,i), \frac{1}{2}(1,i,1,-i), \frac{1}{2}(1,i,-1,i) \right\}.$$

These four bases and the standard basis form an extremal set of five mutually unbiased bases of $\mathbb{C}^4$. *For instance,* $\mathbf{v}_{\alpha,1} \in \mathcal{B}_{\alpha}$ *is evaluated as follows*

$$\begin{aligned}
\mathbf{v}_{\alpha,1} &= \frac{1}{2}\left((\mathbf{v}_{\alpha,1})_0, (\mathbf{v}_{\alpha,1})_1, (\mathbf{v}_{\alpha,1})_{\alpha}, (\mathbf{v}_{\alpha,1})_{\alpha^2}\right) \\
&= \frac{1}{2}\left(i^{\mathrm{Tr}(0)}, i^{\mathrm{Tr}(\alpha+2)}, i^{\mathrm{Tr}((\alpha+2)\alpha)}, i^{\mathrm{Tr}\left((\alpha+2)\alpha^2\right)}\right) \\
&= \frac{1}{2}(1,-i,i,1).
\end{aligned}$$

2.7 Construction of MUBs in non-prime power dimensions

All constructions described so far in this chapter are for prime power dimensions. Assuming $N_{MUB}(d)$ represents the maximum number of MUBs of dimension d, we see that for prime power dimensions d, $N_{MUB}(d)$ attains the maximum, $N_{MUB}(d) = d+1$. So far there is no construction for non-prime power dimensions that gives a complete set of MUBs. Zauner's conjecture states for non-prime power dimensions $N_{MUB}(d) < d+1$ [44]. For example, $d = 6$ is the first non-prime power dimension, and only 3 MUBs are known. The following lemma gives a lower bound for the number of MUBs for any dimension d.

Lemma 2.31 ([24])**.** *Let* $d = p_1^{m_1} p_2^{m_2} \dots p_l^{m_l}$ *be a factorization of* d *in to distinct primes* p_i. *Then*

$$N_{MUB}(d) \geq \min_i p_i^{m_i} + 1.$$

Proof. We know that for any prime power dimension $p_i^{m_i}$ there exists $p_i^{m_i} + 1$ MUBs. Let $n = \min_i N_{MUB}(p_i^{m_i})$. For each $1 \leq i \leq l$, there exists n MUBs $\mathcal{B}_1^{(i)}, \ldots, \mathcal{B}_n^{(i)}$ in $\mathbb{C}^{p_i^{m_i}}$. For $1 \leq k \leq n$, let

$$\mathcal{B}_k^{(i)} = \{\mathbf{v}_k^{i,j} : j = 1, 2, \ldots p^i\}. \tag{2.68}$$

Defined basses in $\mathbb{C}^d$ as follows

$$\mathcal{B}'_k = \left\{\mathbf{v}_k^{1,j_1} \otimes \ \mathbf{v}_k^{2,j_2} \cdots \otimes \mathbf{v}_k^{l,j_l} : j_1 \in \{1, \ldots p_1^{m_1}\}, \ldots, j_l \in \{1, \ldots p_l^{m_l}\}\right\}.$$

It is easy to check that $\mathcal{B}'_1, \mathcal{B}'_2, \ldots, \mathcal{B}'_n$ are n MUBs in $\mathbb{C}^d$. □

Example 2.32. *Let $d = 6$. For $p_1 = 2$ we have 3 MUBs in $\mathbb{C}^2$ and for $p_2 = 3$ we have 4 MUBs in $\mathbb{C}^3$. So, we choose 3 MUBs in $\mathbb{C}^2$ and 3 MUBs in $\mathbb{C}^3$ as follows*

$$\begin{aligned}
\mathcal{B}_1^{(1)} &= \left\{\mathbf{v}_1^{1,1} = (1,0), \mathbf{v}_1^{1,2} = (0,1)\right\}, \\
\mathcal{B}_2^{(1)} &= \left\{\mathbf{v}_2^{1,1} = \frac{1}{\sqrt{2}}(1,1), \mathbf{v}_2^{1,2} = \frac{1}{\sqrt{2}}(1,-1)\right\}, \\
\mathcal{B}_3^{(1)} &= \left\{\mathbf{v}_3^{1,1} = \frac{1}{\sqrt{2}}(1,i), \mathbf{v}_3^{1,2} = \frac{1}{\sqrt{2}}(1,-i)\right\}.
\end{aligned}$$

$$\begin{aligned}
\mathcal{B}_1^{(2)} &= \left\{\mathbf{v}_1^{2,1} = (1,0,0), \mathbf{v}_1^{2,2} = (0,1,0), \mathbf{v}_1^{2,3} = (0,0,1)\right\}, \\
\mathcal{B}_2^{(2)} &= \left\{\mathbf{v}_2^{2,1} = \frac{1}{\sqrt{3}}(1,1,1), \mathbf{v}_2^{2,2} = \frac{1}{\sqrt{3}}(1,\omega^2,\omega), \mathbf{v}_2^{2,3} = \frac{1}{\sqrt{3}}(1,\omega,\omega^2)\right\}, \\
\mathcal{B}_3^{(2)} &= \left\{\mathbf{v}_3^{2,1} = \frac{1}{\sqrt{3}}(1,1,\omega), \mathbf{v}_3^{2,2} = \frac{1}{\sqrt{3}}(1,\omega^2,\omega^2), \mathbf{v}_3^{2,3} = \frac{1}{\sqrt{3}}(1,\omega,1)\right\}.
\end{aligned}$$

Using the construction given in Lemma 2.31*, we have* 3 *MUBs in* $\mathbb{C}^6$ *as follows*

$$\mathcal{B}'_1 = \{\mathbf{v}_1^{1,1} \otimes \mathbf{v}_1^{2,1}, \mathbf{v}_1^{1,1} \otimes \mathbf{v}_1^{2,2}, \mathbf{v}_1^{1,1} \otimes \mathbf{v}_1^{2,3}, \mathbf{v}_1^{1,2} \otimes \mathbf{v}_1^{2,1}, \mathbf{v}_1^{1,2} \otimes \mathbf{v}_1^{2,2}, \mathbf{v}_1^{1,2} \otimes \mathbf{v}_1^{2,3}\},$$

$$\mathcal{B}'_2 = \{\mathbf{v}_2^{1,1} \otimes \mathbf{v}_2^{2,1}, \mathbf{v}_2^{1,1} \otimes \mathbf{v}_2^{2,2}, \mathbf{v}_2^{1,1} \otimes \mathbf{v}_2^{2,3}, \mathbf{v}_2^{1,2} \otimes \mathbf{v}_2^{2,1}, \mathbf{v}_2^{1,2} \otimes \mathbf{v}_2^{2,2}, \mathbf{v}_1^{1,2} \otimes \mathbf{v}_2^{2,3}\},$$

$$\mathcal{B}'_3 = \{\mathbf{v}_3^{1,1} \otimes \mathbf{v}_3^{2,1}, \mathbf{v}_3^{1,1} \otimes \mathbf{v}_3^{2,2}, \mathbf{v}_3^{1,1} \otimes \mathbf{v}_3^{2,3}, \mathbf{v}_3^{1,2} \otimes \mathbf{v}_3^{2,1}, \mathbf{v}_3^{1,2} \otimes \mathbf{v}_3^{2,2}, \mathbf{v}_3^{1,2} \otimes \mathbf{v}_3^{2,3}\}.$$

The construction in Lemma 2.31 is known as the **reduced power** construction. From Lemma 2.31, we see for any dimension $d \geq 2$, $N_{MUB}(d) \geq 3$. But it remains to be seen whether for the case non-prime dimension d, $N_{MUB}(d) = d + 1$. There is numerical evidence that, if the dimension is not prime power, $N_{MUB}(d) < d + 1$ [44].

2.8 Difference sets and mutually unbiased bases

In this section we discuss the relationship between difference sets in a group and the MUB problem. This material is based on recent work by C. Godsil and A. Roy [14]. In first two subsections we will introduce difference sets and character groups and then we use these notions to construct MUBs.

2.8.1 Difference sets

Let D be a subset of group G. Define elements of group algebra $\mathbb{C}[G]$ as follows

$$\mathbf{D} = \sum_{d \in D} d, \;\; \mathbf{D}^{-1} = \sum_{d \in D} d^{-1}, \quad \mathbf{G} = \sum_{g \in G} g.$$

Definition 2.33. *Let G be a group of order n. A subset $D = \{d_1, d_2, \ldots, d_k\}$ of G with k elements is an (n, k, λ)-**difference set** if every non-identity element in G can be expressed as a quotient $d_i d_j^{-1}$ of elements of D in exactly λ ways.*

For example, $D = \{1, 2, 4\}$ is a $(7, 3, 1)$-difference set in $G = \mathbb{Z}_7$.

A simple counting of elements $d_i d_j^{-1}$ of a (n, k, λ)-difference set shows that $k^2 - k = \lambda(n-1)$. From the definition of difference sets, it is easy to see that if D is an (n, k, λ)-difference set then

$$\mathbf{D}\mathbf{D}^{-1} = k \cdot e_G + \lambda(\mathbf{G} - e_G), \tag{2.69}$$

where e_G is the identity element of G.

2.8.2 Characters of a finite abelian group

Let G be a finite abelian group. A function $\chi : G \longrightarrow \mathbb{C}\backslash\{0\}$ mapping the group to the non-zero complex numbers is called a **character** of G if it is a group homomorphism, that is, for all $g_1, g_2 \in G$, $\chi(g_1 g_2) = \chi(g_1)\chi(g_2)$. It is well-known [21] that if χ is a character of a finite abelian group G, then each function value $\chi(g)$ is a root of unity. For instance if $G = \mathbb{Z}_n$, n characters χ_j for $j = 0, 1, \ldots, n-1$ and $g \in \mathbb{Z}_n$ are defined by $\chi_j(g) = e^{2i\pi gj/n}$. In general, a finite abelian group of order n has exactly n distinct characters [21]. Let us denote the set of characters of G by $G^* = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$, where χ_0 is the trivial character, i.e., $\chi_0(g) = 1$ for every $g \in G$. G^* is a group under

multiplication $(\chi_j\chi_k)(g) = \chi_j(g)\chi_k(g)$, $\chi_j^{-1}(g) = \overline{\chi_j(g)}$.

Let D be a $(n, k, 1)$-difference set in G and let $\chi_j \in G^*$, define

$$\chi_j(\mathbf{D}) = \sum_{d\in D} \chi_j(d), \quad \chi_j(\mathbf{D}^{-1}) = \sum_{d\in D} \chi_j(d^{-1}), \quad \chi_j(\mathbf{G}) = \sum_{g\in G} \chi_j(g).$$

By applying χ_j on (2.69) for $\lambda = 1$ we have

$$\chi_j(\mathbf{D}\mathbf{D}^{-1}) = k + \chi_j(\mathbf{G} - e_G). \tag{2.70}$$

It is is easy to check that for a non-trivial $\chi_j \in G^*$, $\chi_j(\mathbf{G}) = \sum_{g\in G} \chi_j(g) = 0$ and $\chi_0(\mathbf{G} - e_G) = n - 1 = k^2 - k$. Since $\chi_j(\mathbf{D}\mathbf{D}^{-1}) = \chi_j(\mathbf{D})\overline{\chi_j(\mathbf{D})} = |\chi_j(\mathbf{D})|^2$, so from (2.70) we have

$$|\chi_j(\mathbf{D})|^2 = \begin{cases} k^2 & \text{if } \chi_j = \chi_0; \\ k - 1 & \text{otherwise.} \end{cases} \tag{2.71}$$

2.8.3 Equiangular lines

A set of m lines in $\mathbb{C}^d$ spanned by unit vectors $\mathbf{x}_1, \ldots, \mathbf{x}_m$ is **equiangular** if there is a constant c such that

$$|\langle \mathbf{x}_i, \mathbf{x}_j \rangle| = c.$$

Let $\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_m$ be m sets of MUBs. If for each $1 \le i \le m$, we choose a vector $\mathbf{v}_i \in \mathcal{B}_i$, set as representative, then these vectors span a set of equiangular lines with $c = \dfrac{1}{\sqrt{d}}$. So MUBs give a special case for equiangular lines. In this subsection we give a construction of equiangular lines based on difference sets and then we extend

it to MUBs in the next subsection.

Let $D = \{d_1, d_2, \ldots, d_k\}$ be a $(n, k, 1)$-difference set in abelian group G and $G^* = \{\chi_0, \chi_1, \ldots, \chi_{n-1}\}$ the set of characters of G. For $0 \leq j \leq n-1$ define vectors $\mathbf{v}_j \in \mathbb{C}^k$ whose ith component is $\chi_j(d_i)$ for $d_i \in D$. In other words,

$$\mathbf{v}_j = (\chi_j(d_1), \ldots, \chi_j(d_k)) \in \mathbb{C}^k. \tag{2.72}$$

Then

$$|\langle \mathbf{v}_j, \mathbf{v}_k \rangle|^2 = \left| \sum_{d_i \in D} \chi_j(d_i) \overline{\chi_k(d_i)} \right|^2 = \left| \sum_{d_i \in D} (\chi_j \chi_k^{-1})(d_i) \right|^2. \tag{2.73}$$

Since G^* is a group, $\chi_j \chi_k^{-1} = \chi_l$, for some $0 \leq l \leq n-1$. Thus from (4.13) and (2.73) we conclude

$$|\langle \mathbf{v}_j, \mathbf{v}_k \rangle|^2 = |\chi_l(\mathbf{D})|^2 = \begin{cases} k^2 & \text{if } \chi_l = \chi_0, \\ k - 1 & \text{otherwise.} \end{cases}$$

Thus $\{\mathbf{v}_j : 0 \leq j \leq n-1\}$ is a set of n equiangular lines in $\mathbb{C}^k$. So if there exists a $(n, k, 1)$-difference set, then there exists n equiangular lines in $\mathbb{C}^k$.

Example 2.34. *$D = \{1, 2, 4\}$ is a $(7, 3, 1)$-difference set in $G = \mathbb{Z}_7$. Define $\chi_j(k) = e^{2i\pi jk/7}$ for $j, k \in \mathbb{Z}_7$. Then vectors defined by*

$$\mathbf{v}_j = (\chi_j(1), \chi_j(2), \chi_j(4)), \qquad 0 \leq j \leq 6,$$

are seven equiangular lines in $\mathbb{C}^3$.

2.8.4 Relative difference sets and the MUB problem

Definition 2.35. *Let D be a k-subset of a finite abelian group G and N a subgroup of G such that $|G| = mn$ and $|N| = n$. D is a (m, n, k, λ)-* ***difference set relative to*** *N if*

$$\mathbf{D}\mathbf{D}^{-1} = k \cdot e_G + \lambda(\mathbf{G} \backslash \mathbf{N}).$$

If $k = m$, then it is called ***semi-regular****.*

Let $D = \{d_1, d_2, \ldots d_k\}$ be a semi-regular (k, n, k, λ)-difference set relative to N in an abelian group G. Denote the set of characters of $H = G/N$ by H^*. H^* is a subgroup of G^* with k elements [31]. Denote the ith coset of H^* by H_i^* for $1 \leq i \leq n$. For each character $\chi_j \in H_i^*$, $0 \leq j \leq k-1$ define a vector in $\mathbb{C}^k$ as follows

$$\mathbf{v}_j = \frac{1}{\sqrt{k}}(\chi_j(d_1), \ldots, \chi_j(d_k)) \in \mathbb{C}^k. \tag{2.74}$$

Define $\mathcal{B}_i = \{\mathbf{v}_j : \chi_j \in H_i^*, 0 \leq j \leq k-1\}$. Vectors defined in (2.74) satisfy

$$|\langle \mathbf{v}_j, \mathbf{v}_k \rangle| = \begin{cases} 1, & \chi_j = \chi_k; \\ 0, & \chi_j \neq \chi_k \ \text{ but } \chi_j \chi_k^{-1} \in H_i^*; \\ \dfrac{1}{\sqrt{k}}, & \text{otherwise.} \end{cases} \tag{2.75}$$

See [35] for the proof. Thus bases $\mathcal{B}_i$, $1 \leq i \leq n$, are orthogonal and mutually unbiased. Since every component of $\mathbf{v}_j$ has norm $1/\sqrt{k}$, the standard basis also is unbiased to each $\mathcal{B}_i$. So if there is a semi-regular (k, n, k, λ)-relative difference set in an abelian group of order nk, then there exists $n+1$ mutually unbiased bases in $\mathbb{C}^k$.

Example 2.36. *For $n = 2$ and $k = 4$, $D = \{1, a, b, a^3b\}$ is a semi-regular $(4, 2, 4, 2)$-difference set relative to $N = \{1, a^2\}$ in $G = \mathbb{Z}_4 \times \mathbb{Z}_2 =< a, b : a^4 = b^2 = 1, ab = ba >$. Let $G^* = \{\chi_0, \chi_1, \ldots, \chi_7\}$ be the set of characters of G. The character table of G is*

	1	a	a^2	a^3	ab	a^2b	a^3b	b
χ_0	1	1	1	1	1	1	1	1
χ_1	1	-1	1	-1	-1	1	-1	1
χ_2	1	-1	1	-1	1	-1	1	-1
χ_3	1	1	1	1	-1	-1	-1	-1
χ_4	1	i	-1	$-i$	i	-1	$-i$	1
χ_5	1	$-i$	-1	i	$-i$	-1	i	1
χ_6	1	i	-1	$-i$	$-i$	1	i	-1
χ_7	1	$-i$	-1	i	i	1	$-i$	-1

Consider the set $H = G/N = \{N, aN, bN, abN\}$ and its character set $H^* = \{\chi_0, \chi_1, \chi_2, \chi_3\}$. It is easy to check that H^* is a subgroup of G^* and it has two cosets $H_1^* = H^*$ and $H_2^* = \chi_4 H^* = \{\chi_4, \chi_5, \chi_6, \chi_7\}$ in G^*. For each coset, we define a vector of the form (2.72) in $\mathbb{C}^4$ as follows

$$\mathbf{v}_0 = \frac{1}{2}\left(\chi_0(1), \chi_0(a), \chi_0(b), \chi_0(a^3b)\right), \qquad \mathbf{v}_1 = \frac{1}{2}\left(\chi_1(1), \chi_1(a), \chi_1(b), \chi_1(a^3b)\right),$$
$$\mathbf{v}_2 = \frac{1}{2}\left(\chi_2(1), \chi_2(a), \chi_2(b), \chi_2(a^3b)\right), \qquad \mathbf{v}_3 = \frac{1}{2}\left(\chi_3(1), \chi_2(a), \chi_3(b), \chi_3(a^3b)\right),$$
$$\mathbf{v}_4 = \frac{1}{2}\left(\chi_4(1), \chi_4(a), \chi_2(b), \chi_4(a^3b)\right), \qquad \mathbf{v}_5 = \frac{1}{2}\left(\chi_5(1), \chi_5(a), \chi_5(b), \chi_5(a^3b)\right),$$

$$\mathbf{v}_6 = \frac{1}{2}\left(\chi_5(1), \chi_5(a), \chi_5(b), \chi_5(a^3b)\right), \qquad \mathbf{v}_7 = \frac{1}{2}\left(\chi_7(1), \chi_2(a), \chi_7(b), \chi_7(a^3b)\right),$$

where the values can be determined from the character table. Bases corresponding to cosets H_1^* *and* H_2^* *are* $\mathcal{B}_1 = \{\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3\}$ *and* $\mathcal{B}_2 = \{\mathbf{v}_4, \mathbf{v}_5, \mathbf{v}_6, \mathbf{v}_7\}$ *respectively.* $\mathcal{B}_1, \mathcal{B}_2$ *and the standard basis in* $\mathbb{C}^4$ *are 3 MUBs.*

It is well know that there exists a semi-regular relative $(p^i, p^i, p^i, 1)$-relative difference set in an abelian group of order p^{2i} for any positive integer i and prime number p [23]. Thus, for $p = 2$ we have a complete set of $2^i + 1$ MUBs in $\mathbb{C}^{2^i}$ and this can be considered as an alternative construction of MUBs for even prime powers that we discussed on Subsection 2.6.1. Relative difference sets are not easy to find. Chris Godsil and Aidan Roy in [14] found a construction for relative difference sets.

Let $k = p_1^{m_1} p_2^{m_2} \dots p_l^{m_l}$, and $m = \min_j p_j^{m_j}$. By the reduced power construction, we have $m + 1$ MUBs in $\mathbb{C}^k$. Moreover, if there exists a semi-regular (k, n, k, λ)- relative difference set, then we have $n + 1$ MUBs in $\mathbb{C}^k$. So, this construction of MUBs using relative difference sets give us more MUBs than reduced power construction if $n > m$. There are still efforts to find semi-regular relative difference sets in an abelian group that give more MUBs in comparison to the reduced power construction, but this problem is open still [11]. In other words, it is unknown whether there exists a semi-regular (k, n, k, λ)-relative difference set such that $n > m$.

Two sets of MUBs $M = \{\mathcal{B}_1, \mathcal{B}_2, \dots, \mathcal{B}_m\}$ and $M' = \{\mathcal{B}'_1, \mathcal{B}'_2, \dots, \mathcal{B}'_m\}$ in $\mathbb{C}^d$ are

equivalent if there exists an unitary operator U mapping M to M'. In other words

$$\{U(\mathcal{B}_1), U(\mathcal{B}_2), \ldots, U(\mathcal{B}_m)\} = \{\mathcal{B}'_1, \mathcal{B}'_2, \ldots, \mathcal{B}'_m\}. \tag{2.76}$$

Now, we may ask if the construction using relative difference sets is equivalent to other constructions that were discussed in this chapter. Still this question remains unanswered. For example, it is well known that there exists a semi-regular $(392, 8, 392, 49)$-difference set in $\mathbb{Z}_7^2 \times \mathbb{Z}_4^3$ relative to $\mathbb{Z}_2^3$ [8]. So, there exist 9 MUBs in $\mathbb{C}^{392}$. Since $392 = 2^3\, 7^2$, by reduced power construction, there exists 9 MUBs in $\mathbb{C}^{392}$. The question is: are these sets of MUBs constructed from different methods equivalent?

2.9 Conclusion

In this chapter we stated the problem of existence of sets of MUBs and the upper bound for the number of MUBs. We demonstrated that for prime power dimensions we can attain the maximum number of MUBs. We mentioned an interesting connection between existence of maximal commuting bases of orthogonal unitary matrices and set of MUBs by Theorem 2.9. Then we constructed commuting classes of unitary matrices (Spin matrices) that satisfy Theorem 2.9. We could not apply this method when the dimension d is a product of different primes instead of being a prime power (the simplest case that belongs to this category is when $d = 6$). We discussed a construction for MUBs in non-prime dimensions in Section 2.7. Finally in Subsection 2.8.4 we examined that existence of $(k, n, k, 1)$-relative-difference set in an abelian

group implies the existence of $n + 1$ MUBs.

Chapter 3

MUTUALLY UNBIASED BASES AND 2-DESIGNS

In this chapter, we explain the relationship between MUBs and 2-designs. First we introduce some notations and definitions related to this chapter.

3.1 Definitions and preliminaries

Let S^{d-1} be defined as follows

$$S^{d-1} = \{\mathbf{x} \in \mathbb{C}^d : \langle \mathbf{x}, \mathbf{x} \rangle = 1\}.$$

We say two vectors $\mathbf{u}$ and $\mathbf{v}$ in S^{d-1} are equivalent, $\mathbf{u} \sim \mathbf{v}$, if and only if $\mathbf{u} = e^{i\theta}\mathbf{v}$ for some $\theta \in \mathbb{R}$. It is easy to see that $\sim$ is an equivalence relation. The **equivalence class** for any $\mathbf{x} \in S^{d-1}$ is defined by

$$[\mathbf{x}] = \{\mathbf{y} \in S^{d-1} : \mathbf{x} \sim \mathbf{y}\}.$$

Denote the quotient space $S^{d-1}/\sim$ by

$$CS^{d-1} = \{[\mathbf{x}] : \mathbf{x} \in S^{d-1}\}.$$

Definition 3.1. *A **Borel set** is any subset in a topological space that can be formed from open sets (or, equivalently, from closed sets) through the operations of countable union, countable intersection, and relative complement.*

Definition 3.2 ([13]). *Let S be a topological space and Σ be the collection of all Borel subsets of S. A function σ from Σ to the extended real number line is called a* ***Borel measure*** *if it satisfies the following properties:*

(1) $\sigma(E) \geq 0$ *for all* $E \in \Sigma$,

(2) $\sigma(\emptyset) = 0$,

(3) *for all countable collections* $\{E_i\}_{i \in I}$ *of pairwise disjoint sets in* Σ

$$\sigma\left(\bigcup_{i \in I} E_i\right) = \sum_{i \in I} \sigma\left(E_i\right).$$

For $S = S^{d-1}$, a Borel measure σ is called $U(d)$-**invariant** if for any $d \times d$ unitary matrix U, and for any Borel set $E \subseteq S^{d-1}$, $\sigma(UE) = \sigma(E)$. For more details on topological properties of S^{d-1} see [33].

It is well known that there is, up to a positive multiplicative constant, a unique non-trivial $U(d)$-invariant measure σ on the σ-algebra of Borel subsets of S^{d-1}[33]. The following functional analysis theorem plays a crucial role in this chapter.

Theorem 3.3 ([33]). *Let $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_d)$ be an ordered d-tuple of non-negative integers α_i , $\mathbf{z} = (z_1, \ldots, z_d) \in \mathbb{C}^d$ and $\mathbf{z}^{\boldsymbol{\alpha}} = z_1^{\alpha_1} \cdots z_d^{\alpha_d}$. Let σ be the $U(d)$-invariant Borel measure on S^{d-1}, for which $\sigma(S^{d-1}) = 1$. Then*

$$\int_{S^{d-1}} |\mathbf{z}^{\boldsymbol{\alpha}}|^2 d\sigma(\mathbf{z}) = \frac{\boldsymbol{\alpha}!(d-1)!}{(d-1+|\boldsymbol{\alpha}|)!}, \tag{3.1}$$

where $\boldsymbol{\alpha}! = \alpha_1! \cdots \alpha_d!$ and $|\boldsymbol{\alpha}| = \alpha_1 + \cdots + \alpha_d$.

Considering CS^{d-1} as a quotient space of S^{d-1}, define the quotient map $\pi : S^{d-1} \to CS^{d-1}$ by $\pi(\mathbf{x}) = [\mathbf{x}]$. For any Borel subset $A \subset CS^{d-1}$, $\pi^{-1}(A)$ is a Borel subset in S^{d-1} [32]. Define a Borel measure μ for a Borel subset $A \subset CS^{d-1}$ by $\mu(A) = \sigma(\pi^{-1}(A))$, where σ is the Borel measure on S^{d-1}.

Let f be a complex-valued function on S^{d-1}. The integration in Theorem 3.3 which is on the space S^{d-1}, may be expressed as an integration on CS^{d-1} with the following formula [5]

$$\int_{S^{d-1}} f(\mathbf{x}) d\sigma(\mathbf{x}) = \frac{1}{2\pi} \int_{CS^{d-1}} \left(\int_{-\pi}^{\pi} f(e^{i\theta}\mathbf{x}) d\theta \right) d\mu(\mathbf{x}). \tag{3.2}$$

Consider the special case $f(\mathbf{x}) = |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k}$, where k is a non-negative integer and $\mathbf{y} \in S^{d-1}$ is fixed. Since $f(e^{i\theta}\mathbf{x}) = f(\mathbf{x})$, by using (3.2) we have

$$\int_{S^{d-1}} f(\mathbf{x}) d\sigma(\mathbf{x}) = \int_{CS^{d-1}} f(\mathbf{x}) d\mu(\mathbf{x}). \tag{3.3}$$

In this chapter we assume $\langle \mathbf{x}, \mathbf{y} \rangle^0 = 1$ for any $\mathbf{x}, \mathbf{y} \in \mathbb{C}^d$. Moreover, $\binom{m}{0} = 1$ for any positive integer m.

Lemma 3.4 ([25])**.** *Let μ be the unique $U(d)$-invariant Borel measure on CS^{d-1} such that $\mu(CS^{d-1}) = 1$. Then for all $\mathbf{y} \in S^{d-1}$,*

$$\int_{CS^{d-1}} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} d\mu(\mathbf{x}) = \frac{1}{\binom{d+k-1}{k}}, \tag{3.4}$$

where k is any non-negative integer.

Proof. The group of $d \times d$ complex unitary matrices, $U(d)$, acts transitively on CS^{d-1}. I.e., for any $\mathbf{y} \in CS^{d-1}$ there exists a unitary matrix U such that $U\mathbf{y} = \mathbf{e}_1$, where $\mathbf{e}_1$

is the first vector in the standard basis of $\mathbb{C}^d$. Since $|\langle \mathbf{x}, \mathbf{y}\rangle|^{2k} = |\langle U\mathbf{x}, U\mathbf{y}\rangle|^{2k}$,

$$\begin{aligned}\int_{CS^{d-1}} |\langle \mathbf{x}, \mathbf{y}\rangle|^{2k} d\mu(\mathbf{x}) &= \int_{CS^{d-1}} |\langle U\mathbf{x}, U\mathbf{y}\rangle|^{2k} d\mu(\mathbf{x}) \\ &= \int_{CS^{d-1}} |\langle U\mathbf{x}, \mathbf{e}_1\rangle|^{2k} d\mu(\mathbf{x}) \\ &= \int_{CS^{d-1}} |\langle \mathbf{x}, \mathbf{e}_1\rangle|^{2k} d\mu(\mathbf{x}).\end{aligned}$$

Assuming $\mathbf{x} = (x_1, x_2, \ldots, x_d)$ and using Theorem 3.3 and (3.3), we obtain

$$\int_{CS^{d-1}} |\langle \mathbf{x}, \mathbf{e}_1\rangle|^{2k} d\mu(\mathbf{x}) = \int_{CS^{d-1}} |x_1^k|^2 d\mu(\mathbf{x}) = \frac{k!(d-1)!}{(d-1+k)!} = \frac{1}{\binom{d+k-1}{k}}.$$

□

3.2 Quantum t-designs

Here we discuss the concept of quantum t-designs introduced by H. Barnum [2]. Then in section 3.3, we will examine relationship between MUBs and 2-designs due to Andreas Klappenecker and Martin Rötteler [25].

Let $\mathrm{Hom}_d(k)$ denote the subset of $\mathbb{C}[x_1, \ldots, x_d, y_1, \ldots, y_d]$ that consists of all homogeneous polynomials of degree k in variables $x_1, \ldots, x_d$ and homogeneous of degree k in the variables $y_1, \ldots, y_d$. In other words, for every polynomial $p \in \mathrm{Hom}_d(k)$ we have

$$p(\alpha\mathbf{x}, \beta\mathbf{y}) = \alpha^k \beta^k p(\mathbf{x}, \mathbf{y}),$$

where $\mathbf{x} = (x_1, \ldots, x_d)$, $\mathbf{y} = (y_1, \ldots, y_d) \in \mathbb{C}^d$ and $\alpha, \beta \in \mathbb{C}$. We associate to each polynomial p in $\mathrm{Hom}_d(k)$ a function p_0, by defining $p_0(\mathbf{x}) = p(\mathbf{x}, \overline{\mathbf{x}})$. Define

$$\mathrm{Hom}_d(k)_0 = \{p_0 : p \in \mathrm{Hom}_d(k)\}.$$

Because of the homogeneity condition, $p_0(e^{i\theta}\mathbf{x}) = p_0(\mathbf{x})$, holds for every $\theta \in \mathbb{R}$ and $p_0 \in \mathrm{Hom}_d(k)_0$. So, every $p_0 \in \mathrm{Hom}_d(k)_0$ is well-defined on CS^{d-1}.

Let $\mathbf{x}^{\otimes k} = \mathbf{x} \otimes \cdots \otimes \mathbf{x} \in \mathbb{C}^{d^k}$ be the k-fold tensor product of $\mathbf{x} \in \mathbb{C}^d$. It is easy to check that any polynomial $p_0 \in \mathrm{Hom}_d(k)_0$ is of the form

$$p_0 = \sum_{j=1}^{d^{2k}} c_j \langle \mathbf{x}^{\otimes k} \otimes \overline{\mathbf{x}}^{\otimes k}, \mathbf{e}_j \rangle \tag{3.5}$$

where $\mathbf{e}_j$ is the jth standard basis vector in $\mathbb{C}^{d^{2k}}$, and $c_j \in \mathbb{C}$.

For example, if $p(\mathbf{x}, \mathbf{y}) = 3x_1^2 y_1 y_2 - 5x_1 x_2 y^2 \in \mathrm{Hom}_2(2)$, then $p_0(\mathbf{x}) = 3x_1^2\overline{x_1 x_2} - 5x_1 x_2 \overline{x_2}^2 \in \mathrm{Hom}_2(2)_0$ can be written as follows

$$p_0 = 3\langle \mathbf{x}^{\otimes 2} \otimes \overline{\mathbf{x}}^{\otimes 2}, \mathbf{e}_2 \rangle - 5\langle \mathbf{x}^{\otimes 2} \otimes \overline{\mathbf{x}}^{\otimes 2}, \mathbf{e}_8 \rangle, \tag{3.6}$$

where $\mathbf{e}_2$ and $\mathbf{e}_8$ are the second and eighth standard basis vectors in $\mathbb{C}^{16}$ respectively.

Definition 3.5. *Let X be a finite subset of CS^{d-1} and μ the normalized Borel measure on CS^{d-1}. For a positive integer t, we call X a **quantum t-design** in CS^{d-1} if and only if*

$$\frac{1}{|X|} \sum_{\mathbf{x} \in X} \left(\mathbf{x}^{\otimes t} \otimes \overline{\mathbf{x}}^{\otimes t}\right) = \int_{CS^d - 1} \left(\mathbf{x}^{\otimes t} \otimes \overline{\mathbf{x}}^{\otimes t}\right) d\mu(\mathbf{x}). \tag{3.7}$$

From now we just say t-designs instead of quantum t-designs and the case $t = 2$ shall be of greatest concern to us.

Applying the inner product with $\mathbf{e}_j$s on both sides of (3.7) and using (3.5) we conclude that a finite subset X of CS^{d-1} is t-design if and only if

$$\frac{1}{|X|}\sum_{\mathbf{x}\in X} p_0(\mathbf{x}) = \int_{CS^{d-1}} p_0(\mathbf{x})d\mu(\mathbf{x}), \tag{3.8}$$

holds for any $p_0 \in \mathrm{Hom}_d(t)_0$. That is, (3.7) and (3.8) are equivalent. The equation (3.8) says the average of any polynomial function in $\mathrm{Hom}_d(t)_0$ over the t-design is exactly the same as its average over the Borel measure.

Example 3.6. *Let* $X = \left\{(1,0),(0,1),\frac{1}{\sqrt{2}}(1,1),\frac{1}{\sqrt{2}}(1,-1),\frac{1}{\sqrt{2}}(1,i),\frac{1}{\sqrt{2}}(1,-i)\right\} \subset CS^1$, *and let* μ *be the Borel measure on* CS^1. *Define* $\mathbf{w} \in \mathbb{C}^{16}$ *as follows*

$$\mathbf{w} = \frac{1}{6}\sum_{\mathbf{x}\in X} \mathbf{x}^{\otimes 2}\otimes\overline{\mathbf{x}}^{\otimes 2} - \int_{CS^1} \mathbf{x}^{\otimes 2}\otimes\overline{\mathbf{x}}^{\otimes 2}d\mu(\mathbf{x}).$$

It is easy to check that $\langle \mathbf{x}^{\otimes 2}\otimes\overline{\mathbf{x}}^{\otimes 2}, \mathbf{y}^{\otimes 2}\otimes\overline{\mathbf{y}}^{\otimes 2}\rangle = |\langle \mathbf{x},\mathbf{y}\rangle|^4$. *Now,*

$$\langle \mathbf{w},\mathbf{w}\rangle = \frac{1}{36}\sum_{\mathbf{x},\mathbf{y}\in X} |\langle \mathbf{x},\mathbf{y}\rangle|^4 - \frac{2}{6}\sum_{\mathbf{y}\in X}\int_{CS^1} |\langle \mathbf{x},\mathbf{y}\rangle|^4 d\mu(\mathbf{x}) + \int_{CS^1}\int_{CS^1} |\langle \mathbf{x},\mathbf{y}\rangle|^4 d\mu(\mathbf{x})d\mu(\mathbf{y}).$$

Using Lemma 3.4 *for* $d = k = 2$, $\displaystyle\int_{CS^1} |\langle \mathbf{x},\mathbf{y}\rangle|^4 d\mu(\mathbf{x}) = \frac{1}{\binom{2+2-1}{2}} = \frac{1}{3}$ *for any* $\mathbf{y} \in S^1$. *Since* $\displaystyle\frac{1}{36}\sum_{\mathbf{x},\mathbf{y}\in X} |\langle \mathbf{x},\mathbf{y}\rangle|^4 = \frac{1}{3}$, *then*

$$\langle \mathbf{w},\mathbf{w}\rangle = \frac{1}{3} - \frac{2}{6}\cdot 6\left(\frac{1}{3}\right) + \frac{1}{3} = 0.$$

Thus $\mathbf{w} = \mathbf{0}$ *and we have*

$$\frac{1}{6}\sum_{\mathbf{x}\in X} \mathbf{x}^{\otimes 2}\otimes\overline{\mathbf{x}}^{\otimes 2} = \int_{CS^1} \mathbf{x}^{\otimes 2}\otimes\overline{\mathbf{x}}^{\otimes 2}d\mu(\mathbf{x}). \tag{3.9}$$

So X is a 2-design. For any $i \in \{1, 2, \ldots, 16\}$, the inner product of the left side of (3.9) *with each $\mathbf{e}_i$ (ith element of standard basis) is equal to the inner product of the right side of* (3.9) *with $\mathbf{e}_i$. So for any polynomial $p_0 \in Hom_2(2)_0$*

$$\frac{1}{6}\sum_{\mathbf{x}\in X} p_0(\mathbf{x}) = \int_{CS^1} p_0(\mathbf{x}) d\mu(\mathbf{x}).$$

For instance, if we consider the polynomial defined in (3.6) *and using* (3.9)*, then*

$$\begin{aligned}\left\langle \frac{1}{6}\sum_{\mathbf{x}\in X} \mathbf{x}^{\otimes 2} \otimes \overline{\mathbf{x}}^{\otimes 2}, 3\mathbf{e}_2 - 5\mathbf{e}_8 \right\rangle &= \frac{1}{6}\sum_{\mathbf{x}\in X} \left\langle \mathbf{x}^{\otimes 2} \otimes \overline{\mathbf{x}}^{\otimes 2}, 3\mathbf{e}_2 - 5\mathbf{e}_8 \right\rangle \\ &= \frac{1}{6}\sum_{\mathbf{x}\in X} p_0(\mathbf{x}).\end{aligned}$$

Similarly, if we calculate the inner product of $3\mathbf{e}_2 - 5\mathbf{e}_8$ with the right side of (3.9)*, we conclude*

$$\frac{1}{6}\sum_{\mathbf{x}\in X} p_0(\mathbf{x}) = \int_{CS^1} p_0(\mathbf{x}) d\mu(\mathbf{x}).$$

3.2.1 Welch's inequality

Suppose that X is a finite non-empty subset of S^{d-1}. Welch in [33] proved that vectors in X satisfy the inequality

$$\frac{1}{|X|^2}\sum_{\mathbf{x},\mathbf{y}\in X} |\langle \mathbf{x}, \mathbf{y}\rangle|^{2k} \geq \frac{1}{\binom{d+k-1}{k}}, \tag{3.10}$$

for all integers $k \geq 0$.

Theorem 3.7 ([25])**.** *Let X be a finite non-empty subset of CS^{d-1} and μ the Borel measure on CS^{d-1}. Then the following statements are equivalent:*

(1) *X is a t-design,*

(2) *for all $\mathbf{x} \in \mathbb{C}^d$, and all integers $0 \leq k \leq t$,*

$$\frac{1}{|X|} \sum_{\mathbf{y} \in X} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} = \frac{\langle \mathbf{x}, \mathbf{x} \rangle^k}{\binom{d+k-1}{k}}, \tag{3.11}$$

(3) *the set X attains the Welch's bound for all integers k in the range $0 \leq k \leq t$, that is*

$$\frac{1}{|X|^2} \sum_{\mathbf{x}, \mathbf{y} \in X} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} = \frac{1}{\binom{d+k-1}{k}}. \tag{3.12}$$

Proof. $1 \Rightarrow 2$. Let $p_0(\mathbf{y}) = |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k}$, for a fixed vector $\mathbf{x} \in \mathbb{C}^d$ and integer $0 \leq k \leq t$. $p_0(\mathbf{y})$ is a polynomial function in $\mathrm{Hom}_d(k)_0$. Since X is a t-design, using (3.8) we get

$$\begin{aligned} \frac{1}{|X|} \sum_{\mathbf{y} \in X} p_0(\mathbf{y}) &= \frac{1}{|X|} \sum_{\mathbf{y} \in X} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} \\ &= \langle \mathbf{x}, \mathbf{x} \rangle^k \int_{CS^d - 1} \left| \left\langle \frac{\mathbf{x}}{\langle \mathbf{x}, \mathbf{x} \rangle^{\frac{1}{2}}}, \mathbf{y} \right\rangle \right|^{2k} d\mu(\mathbf{y}). \end{aligned}$$

By Lemma 3.4 we have

$$\langle \mathbf{x}, \mathbf{x} \rangle^k \int_{CS^d - 1} \left| \left\langle \frac{\mathbf{x}}{\langle \mathbf{x}, \mathbf{x} \rangle^{\frac{1}{2}}}, \mathbf{y} \right\rangle \right|^{2k} d\mu(\mathbf{y}) = \frac{\langle \mathbf{x}, \mathbf{x} \rangle^k}{\binom{d+k-1}{k}}.$$

Thus

$$\frac{1}{|X|} \sum_{\mathbf{y} \in X} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} = \frac{\langle \mathbf{x}, \mathbf{x} \rangle^k}{\binom{d+k-1}{k}}.$$

$2 \Rightarrow 3$. X is a subset of CS^{d-1}, so summing over $\mathbf{x} \in X$ in equation (3.11) yields (3.12).

$3 \Rightarrow 1$. Let $\mathbf{x}^{\otimes k} = \mathbf{x} \otimes \cdots \otimes \mathbf{x} \in \mathbb{C}^{d^k}$. It is easy to check that $\langle \mathbf{x}^{\otimes k}, \mathbf{y}^{\otimes k} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle^k$. Define $\mathbf{w} \in \mathbb{C}^{d^{2k}}$ as follows

$$\mathbf{w} = \frac{1}{|X|} \sum_{\mathbf{x} \in X} \left(\mathbf{x}^{\otimes k} \otimes \overline{\mathbf{x}}^{\otimes k} \right) - \int_{CS^{d-1}} \left(\mathbf{x}^{\otimes k} \otimes \overline{\mathbf{x}}^{\otimes k} \right) d\mu(\mathbf{x}). \tag{3.13}$$

By using Lemma 3.4 and assuming X attains Welch's bound for all integers $0 \leq k \leq t$, we can evaluate the inner product $\langle \mathbf{w}, \mathbf{w} \rangle$ as follows

$$\begin{aligned} \langle \mathbf{w}, \mathbf{w} \rangle = & \frac{1}{|X|^2} \sum_{\mathbf{x}, \mathbf{y} \in X} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} - \frac{2}{|X|} \sum_{\mathbf{x} \in X} \int_{CS^{d-1}} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} d\mu(\mathbf{y}) + \\ & \int_{CS^{d-1}} \int_{CS^{d-1}} |\langle \mathbf{x}, \mathbf{y} \rangle|^{2k} d\mu(\mathbf{y}) d\mu(\mathbf{x}) \\ & = \frac{1}{\binom{d+k-1}{k}} - \frac{2|X|}{|X| \binom{d+k-1}{k}} + \frac{1}{\binom{d+k-1}{k}} \\ & = 0. \end{aligned} \tag{3.14}$$

The inner integral in (3.14) is equal to $\binom{d+k-1}{k}^{-1}$ by Lemma 3.4. Since $\langle \mathbf{w}, \mathbf{w} \rangle = 0$, we have $\mathbf{w} = 0$. Thus X is a t-design. □

3.3 Mutually unbiased bases are 2-designs

In this section we use information from previous sections to show that MUBs are 2-designs and that the converse of this statement is also true in special cases.

For a given subset X of CS^{d-1} let us define the **angle set** of X by

$$\Delta = \{ |\langle \mathbf{x}, \mathbf{y} \rangle|^2 : \mathbf{x}, \mathbf{y} \in X, \mathbf{x} \neq \mathbf{y} \}.$$

For example the angle set of a union of MUBs in CS^{d-1} is $\{0, 1/d\}$.

For an element $\mathbf{x} \in X$ and $\theta \in \Delta$, define

$$\delta_\theta(\mathbf{x}) = \{\mathbf{y} \in X : |\langle \mathbf{x}, \mathbf{y} \rangle|^2 = \theta\}.$$

If for any $\theta \in \Delta$, $|\delta_\theta(\mathbf{x})|$ is independent of $\mathbf{x}$ then X is called a **regular scheme**.

Our next lemma characterizes 2-designs in terms of regular schemes.

Lemma 3.8. *If X is a complex 2-design consisting of $d(d+1)$ elements in CS^{d-1} such that $\Delta = \{0, 1/d\}$, then X is a regular scheme and $|\delta_{\frac{1}{d}}(\mathbf{x})| = d^2$ for any $\mathbf{x} \in X$.*

You may find the proof in [18, 19].

Theorem 3.9 ([25])**.** *A set X with $d(d+1)$ elements in CS^{d-1} and angle set $\Delta = \{0, 1/d\}$ is a 2-design if and only if X is a union of $d+1$ mutually unbiased bases in $\mathbb{C}^d$.*

Proof. Let X be the union of $d+1$ MUBs in CS^{d-1}. By Theorem 3.7 it is enough to show X attains the upper bound in Welch's inequality for $0 \leq k \leq 2$. For $k = 0$ it is obvious since $|X| = d(d+1)$.

Since $|\langle \mathbf{x}, \mathbf{y} \rangle|^2 = 0$ or $\frac{1}{d}$ and for all $d(d+1)$ elements $\mathbf{x}$ in X there are exactly d^2 elements $\mathbf{y}$ such that $|\langle \mathbf{x}, \mathbf{y} \rangle|^2 = \frac{1}{d}$, thus for $k = 1$ we have

$$\frac{1}{|X|^2} \sum_{\mathbf{x},\mathbf{y} \in X} |\langle \mathbf{x}, \mathbf{y} \rangle|^2 = \frac{d(d+1)}{d^2(d+1)^2} \left(1 + d^2 \frac{1}{d} + (d-1)0\right) = \frac{1}{d} = \frac{1}{\binom{d+1-1}{1}}.$$

For $k = 2$, $|\langle \mathbf{x}, \mathbf{y} \rangle|^4 = 0$ or $\frac{1}{d^2}$ for $\mathbf{x}, \mathbf{y} \in X$. Thus

$$\frac{1}{d^2(d+1)^2}\sum_{\mathbf{x},\mathbf{y}\in X}|\langle \mathbf{x},\mathbf{y}\rangle|^4 = \frac{d(d+1)}{d^2(d+1)^2}\left(1+d^2\frac{1}{d^2}+(d-1)0\right) = \frac{1}{\binom{d+2-1}{2}}.$$

For proving the other direction, if X is a 2-design with angle set $\Delta = \{0, 1/d\}$ and $d(d+1)$ elements, by Lemma 3.8, $|\delta_{\frac{1}{d}}(\mathbf{x})| = d^2$ for all $\mathbf{x} \in X$. So, for any $\mathbf{x} \in X$ exist exactly d^2 elements, $\mathbf{y} \in X$ such that $|\langle \mathbf{x},\mathbf{y}\rangle|^2 = \frac{1}{d}$. Thus the sets $\mathcal{B}_{\mathbf{x}} = \{\mathbf{x}\}\bigcup \delta_0(\mathbf{x})$ are $d+1$ mutually unbiased bases. □

For example, the 2-design X in Example 3.6 is a union of 3 MUBs in $\mathbb{C}^2$.

3.4 Conclusion

In this chapter we discussed the relationship between MUBs and complex 2-designs. We have shown that any 2-design in dimension d which consists of $d(d+1)$ elements and has angle set $\{0, 1/d\}$ can be partitioned into $d+1$ MUBs. So any construction for 2-designs with the mentioned properties leads to a construction of MUBs (see [19]). We have also seen that MUBs attain Welch's inequality in (3.10) for $k = 0, 1, 2$. Shayne Waldron discovered the relationship shown in Theorem 3.9 in the case of real spaces [38]. Shortly afterwards, Andreas Klappennecker and Martin Rötteler [25] generalized the result over the complex spaces, which is the case we have discussed in this chapter.

Chapter 4

MUTUALLY UNBIASED BASES AND LATIN SQUARES

In this chapter we consider the relationship between the existence of MUBs and Latin Squares in square dimensions. A **Latin Square** is an $s \times s$ array filled with s different symbols, each occurring exactly once in each row and exactly once in each column. For example, here is a 4×4 Latin Square

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

We will discuss Latin Squares further in Section 4.3. For more information about Latin Squares see [7]. In Section 4.1 we begin by introducing some preliminary notions.

4.1 Preliminaries

A vector $\mathbf{m} = (m_1, \ldots, m_d) \in \{0, 1\}^d$ is called an **incidence vector**. The **Hamming weight** of $\mathbf{m}$ is the number of 1s in components of $\mathbf{m}$. Assuming that the Hamming

weight of an incidence vector $\mathbf{m} \in \{0,1\}^d$ is s, the **support** of $\mathbf{m}$ is

$$\text{supp}(\mathbf{m}) = \{j_1, \ldots, j_s : m_{j_1} = \cdots = m_{j_s} = 1\}, \tag{4.1}$$

and indices are sorted, i.e., $j_1 < \cdots < j_s$.

Definition 4.1 ([41]). *Let $Y = \{B_1, \ldots, B_k\}$ be a collection of k sets each consisting of s incidence vectors of length s^2, $\mathbf{m}_{ij} \in B_i$, $i = 1, \ldots, k$ and $j = 1, \ldots, s$, i.e., $\mathbf{m}_{ij}$ is jth incidence vector in B_i, with the following properties*

(1) $\langle \mathbf{m}_{ij}, \mathbf{m}_{il} \rangle = 0$, *for all* $1 \le i \le k$ *and* $1 \le j \ne l \le s$,

(2) $\langle \mathbf{m}_{ij}, \mathbf{m}_{cl} \rangle = 1$, *for all* $1 \le i \ne c \le k$ *and* $1 \le j, l \le s$.

Then we say that Y is a (k, s)-net.

Example 4.2. *For for $s = 2$, let*

$$B_1 = \{\mathbf{m}_{11} = (1,1,0,0), \mathbf{m}_{12} = (0,0,1,1)\},$$

$$B_2 = \{\mathbf{m}_{21} = (1,0,1,0), \mathbf{m}_{22} = (0,1,0,1)\},$$

$$B_3 = \{\mathbf{m}_{31} = (1,0,0,1), \mathbf{m}_{32} = (0,1,1,0)\}.$$

Then $Y = \{B_1, B_2, B_3\}$ is a $(3,2)$-net.

Definition 4.3 ([41]). *Let $\mathbf{m}$ be a vector in $\{0,1\}^d$ with supp$(\mathbf{m}) = \{j_1, j_2, \ldots, j_s\}$, and let $\mathbf{v} \in \mathbb{C}^s$ be an arbitrary vector. Define the **embedding** of $\mathbf{v}$ into $\mathbb{C}^d$ **controlled***

by $\mathbf{m}$*, denoted by* $\mathbf{v} \uparrow \mathbf{m}$*, to be the following vector in* $\mathbb{C}^d$

$$\mathbf{v} \uparrow \mathbf{m} = \sum_{r=1}^{s} v_r \mathbf{e}_{j_r}, \tag{4.2}$$

where v_r *is the* r*th entry of the vector* $\mathbf{v}$*, and* $\mathbf{e}_{j_r}$ *the* j_r*th standard basis vector of* $\mathbb{C}^d$*.*

Example 4.4. *For* $d = 6$ *and* $s = 3$*, let*

$$\mathbf{m} = (1, 0, 1, 0, 0, 1) \in \{0, 1\}^6, \quad \mathbf{v} = (1, -1, i) \in \mathbb{C}^3.$$

$supp(\mathbf{m}) = \{1, 3, 6\}$*. Using notations in Definition* 4.3 *we have*

$$\mathbf{v} \uparrow \mathbf{m} = (1, 0, -1, 0, 0, i) \in \mathbb{C}^6.$$

An $n \times n$ matrix $H = [h_{j,k}]_{j,k=1}^{n}$, $h_{j,k} \in \mathbb{C}$, $|h_{j,k}| = 1$, is a **generalized Hadamard** matrix if $HH^* = n\mathbb{I}$. Generalized Hadamard matrices exist for any positive integer n [17]. For example, taking $\omega = e^{2i\pi/n}$, $H = [\omega^{jk}]_{j,k=1}^{n}$ is an $n \times n$ generalized Hadamard matrix.

4.2 Construction of MUBs in square dimensions using nets

In this section, we examine a construction for MUBs using nets. This construction is due to P. Wocjan and T. Beth [41].

Let $Y = \{B_1, B_2, \ldots, B_k\}$ be a (k, s)-net with incidence vectors $\mathbf{m}_{rj} \in B_r$ for $r \in \{1, \ldots, k\}$, $j \in \{1, \ldots, s\}$, and let $H = [h_{l,l'}]_{l,l'=1}^{s} = (\mathbf{h}_1 | \cdots | \mathbf{h}_s)$ a generalized Hadamard matrix with columns $\mathbf{h}_1 \ldots \mathbf{h}_s$ of length s. Define sets $\mathcal{B}_r$ by

$$\mathcal{B}_r = \left\{ \mathbf{v}_{l,j}^r = \frac{1}{\sqrt{s}}(\mathbf{h}_l \uparrow \mathbf{m}_{rj}) \middle| \quad \mathbf{m}_{rj} \in B_r;\ j,l = 1,\ldots,s \right\}. \tag{4.3}$$

For $r, r' \in \{1,\ldots,k\}$ and $j, j', l, l' \in \{1,\ldots,s\}$, let

$$\mathbf{v}_{l,j}^r = \frac{1}{\sqrt{s}}\,(\mathbf{h}_l \uparrow \mathbf{m}_{rj}) \in \mathcal{B}_r, \quad \mathbf{v}_{l',j'}^{r'} = \frac{1}{\sqrt{s}}\,(\mathbf{h}_{l'} \uparrow \mathbf{m}_{rj'}) \in \mathcal{B}_{r'}.$$

We want to show that the sets defined in (4.3) are k MUBs. We consider the following cases.

(a) If $r = r'$ and $j \neq j'$. Since Y is a (k,s)-net, by properties (1) in Definition 4.1, $\langle \mathbf{m}_{rj}, \mathbf{m}_{rj'} \rangle = 0$. So

$$\left|\left\langle \mathbf{v}_{l,j}^r, \mathbf{v}_{l',j'}^r \right\rangle\right|^2 = 0.$$

(b) If $r = r'$ and $j = j'$. Since $HH^* = s\mathbb{I}_s$, $\langle \mathbf{h}_l, \mathbf{h}_{l'} \rangle = s\delta(l,l')$. So

$$\begin{aligned}\left|\left\langle \mathbf{v}_{l,j}^r, \mathbf{v}_{l',j}^r \right\rangle\right|^2 &= \frac{1}{s^2}\left|\langle \mathbf{h}_l, \mathbf{h}_{l'} \rangle\right|^2 \\ &= \delta(l,l').\end{aligned}$$

So, $\mathcal{B}_r$ is an orthonormal basis in $\mathbb{C}^{s^2}$.

(c) If $r \neq r'$ and $j, j' \in \{1,\ldots,s\}$. By properties (2) in Definition 4.1, $\langle \mathbf{m}_{rj}, \mathbf{m}_{r'j'} \rangle = 1$. Let $\mathbf{m}_{rj}$ and $\mathbf{m}_{r'j'}$ have 1 in common in tth position. Then

$$\begin{aligned}\left|\left\langle \mathbf{v}_{l,j}^r, \mathbf{v}_{l',j'}^{r'} \right\rangle\right|^2 &= \frac{1}{s^2}|h_{t,l}\overline{h_{t,l'}}|^2 \\ &= \frac{1}{s^2}.\end{aligned}$$

Consequently $\mathcal{B}_r$ and $\mathcal{B}_{r'}$ are mutually unbiased bases for $r \neq r'$. Thus, if there exists a (k, s)-net, then there exists k MUBs of the form (4.3) in $\mathbb{C}^{s^2}$.

Example 4.5. *By applying the above construction for $s = 2$, using the $(3, 2)$-net in Example 4.2 and the Hadamard matrix of order 2*

$$H = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix},$$

we obtain 3 MUBs in $\mathbb{C}^4$

$$\mathcal{B}_1 = \left\{ \frac{1}{\sqrt{2}}(1,1,0,0), \frac{1}{\sqrt{2}}(1,-1,0,0), \frac{1}{\sqrt{2}}(0,0,1,1), \frac{1}{\sqrt{2}}(0,0,1,-1) \right\},$$
$$\mathcal{B}_2 = \left\{ \frac{1}{\sqrt{2}}(1,0,1,0), \frac{1}{\sqrt{2}}(1,0,-1,0), \frac{1}{\sqrt{2}}(0,1,0,1), \frac{1}{\sqrt{2}}(0,1,0,-1) \right\},$$
$$\mathcal{B}_3 = \left\{ \frac{1}{\sqrt{2}}(1,0,0,1), \frac{1}{\sqrt{2}}(1,0,0,-1), \frac{1}{\sqrt{2}}(0,1,1,0), \frac{1}{\sqrt{2}}(0,1,-1,0) \right\}.$$

4.3 Nets and orthogonal Latin Squares

From the construction described in Section 4.2, we see that the existence of a (k, s)-net and a Hadamard matrix of size s leads to a construction of k MUBs in $\mathbb{C}^{s^2}$. The problem of finding a large collection of incidence vectors satisfying Definition 4.1 is related to finding orthogonal Latin Squares. A set of Latin Squares $\{L_1, \ldots, L_m\}$ is said to be **mutually orthogonal** (MOLS) if, for every two Latin Squares L_i and L_j, $i \neq j$, the symbol pairs formed by juxtaposing the two arrays are all distinct.

Example 4.6. *Following arrays are* 3 *mutually orthogonal Latin Squares*

1	2	3	4
4	3	2	1
2	1	4	3
3	4	1	2

1	2	3	4
3	4	1	2
4	3	2	1
2	1	4	3

1	2	3	4
2	1	4	3
3	4	1	2
4	3	2	1

Here we briefly discuss the relationship between orthogonal Latin Squares and nets.

Definition 4.7. *An* ***orthogonal array****, denoted by* $OA(k, s)$*, is a* $k \times s^2$ *array* $A = [a_{i,j}]$*, with entries from an* s*-set* S *having the property that in any two rows, each (ordered) pair of symbols from* S *occurs exactly once.*

Example 4.8. *Let* $S = \{1, 2, 3, 4\}$*. An* $OA(5, 4)$ *is*

$$\begin{pmatrix} 1111222233334444 \\ 1234123412341234 \\ 1234432121433412 \\ 1234341243212143 \\ 1234214334124321 \end{pmatrix}$$

.

Lemma 4.9 ([7])**.** *Let* $\{L_1, \ldots, L_k\}$ *be a set of* k *mutually orthogonal Latin Squares on symbols* $\{1, \ldots, s\}$*. Form a* $(k + 2) \times s^2$ *array* $A = [a_{i,j}]$ *whose columns are* $(i, j, L_1(i, j), L_2(i, j), \ldots, L_k(i, j))^T$ *for* $1 \leq i, j \leq s$*. Then* A *is an orthogonal array,*

$OA(k+2,s)$. This process can be reversed to recover k MOLS of size s from an $OA(k+2,s)$, by choosing any two rows of the OA to index the rows and columns of the k Latin Squares.

For instance, the $OA(5,4)$ in Example 4.8 is derived from the 3 MOLS in Example 4.6 by applying the construction in Lemma 4.9.

Definition 4.10. *A **transversal design** of **group size** s, **block size** k, denoted $TD(k,s)$, is a triple $(V,\mathcal{G},\mathcal{B})$, where*

(1) *V is a set of ks elements;*

(2) *$\mathcal{G}$ is a partition of V into k classes (**groups**), each of size s;*

(3) *$\mathcal{B}$ is a collection of k-subsets of V (**blocks**);*

(4) *every unordered pair of elements from V is contained either in exactly one group or in exactly one blocks, but not both.*

Lemma 4.11 ([7])**.** *Let $A=[a_{i,j}]$ be an $OA(k,s)$ on the s symbols in X and $V = X\times\{1,\ldots,k\}$ (a set of size ks). Define $\mathcal{B}$ to be the sets of blocks $B_j=\{(a_{i,j},i): 1\le i\le k\}$, for $1\le j\le s^2$. Let $\mathcal{G}$ be the partition of V whose classes are $G_i=\{X\times\{i\}\}$, $1\le i\le k$. Then $(V,\mathcal{G},\mathcal{B})$ is a $TD(k,s)$. This process can be reversed to recover an $OA(k,s)$ from a $TD(k,s)$.*

Example 4.12. *From the* 3 *Latin Squares in Example* 4.6*,* $OA(5,4)$ *in Example* 4.8 *and Lemma* 4.11 *we have a* $TD(5,4)$ *on* $V = \{1,2,3,4\} \times \{1,2,3,4,5\}$ *whose blocks are*

$$B_1 = \{11,12,13,14,15\}, \quad B_2 = \{11,22,23,24,25\}, \quad B_3 = \{11,32,33,34,35\},$$
$$B_4 = \{11,42,43,44,45\}, \quad B_5 = \{21,12,43,34,25\}, \quad B_6 = \{21,22,33,44,15\},$$
$$B_7 = \{21,32,23,14,45\}, \quad B_8 = \{21,42,13,24,35\}, \quad B_9 = \{31,12,23,44,35\},$$
$$B_{10} = \{31,22,13,34,45\}, \quad B_{11} = \{31,32,43,24,15\}, \quad B_{12} = \{31,42,33,14,25\},$$
$$B_{13} = \{41,12,33,24,45\}, \quad B_{14} = \{41,22,43,14,35\}, \quad B_{15} = \{41,32,13,44,25\},$$
$$B_{16} = \{41,42,23,34,15\}.$$

Now if, for every element of the $TD(k,s)$ constructed in Lemma 4.11, we consider a vector of length s^2 whose ith entry is 1 if it belongs to B_i, otherwise 0. Then we have ks vectors which can be partitioned such that the properties in Definition 4.1 for being a net are satisfied.

For example if we consider the set of blocks in Example 4.12, $\mathcal{B} = \{B_1, \ldots, B_{16}\}$, then for element $34 \in B_3, B_5, B_{10}, B_{16}$, the incidence vector is

$$\mathbf{m}_{34} = (0,0,1,0,1,0,\ldots,0,1,0,\ldots,0,1) \in \{0,1\}^{16},$$

where $\text{supp}(\mathbf{m}_{34}) = \{3,5,10,16\}$. So by the constructions in Lemma 4.9 and Lemma 4.11 we have the following theorem.

Theorem 4.13 ([7]). *Each of the following is equivalent to the existence of k MOLS of size s.*

(1) *An $OA(k+2, s)$.*

(2) *$TD(k+2, s)$.*

(3) *A $(k+2, s)$-net.*

Construction of MUBs using nets as in (4.3), which requires existence of orthogonal Latin Squares, is called the **Latin MUB construction**. This is because from Theorem 4.13, the existence of k orthogonal Latin Squares of size s is equivalent to a $(k+2, s)$-net. Thus from (4.3) we have $k+2$ MUBs in $\mathbb{C}^{s^2}$.

Let $N_{MOLS}(s)$ denote the maximum number of MOLS of order s. It is well-known that $N_{MOLS}(s) \leq s-1$. Further when s is a prime power, we have a complete set of orthogonal Latin Squares i.e., $N_{MOLS}(s) = s-1$ [17, 26]. No construction for a complete set of mutually orthogonal Latin Squares for non-prime power orders is known at the present. Beth [4] showed that there is a number s_0 such that for all $s \geq s_0$, $N_{MOLS}(s) \geq s^{\frac{1}{14.8}}$. Thus by the Latin MUB construction, $N_{MUB}(s^2) \geq s^{\frac{1}{14.8}} + 2$ for all positive integers except for finitely many. So, by the Latin MUB construction, we conclude

$$normalmatrixes \lim_{s \to \infty} N_{MUB}(s^2) = \infty. \tag{4.4}$$

4.3.1 Latin MUB construction in dimension 4

Although in some dimensions the Latin MUB construction gives a better lower bound for the number of MUBs compared with reduced power construction, in some dimensions it doesn't. In Section 4.4 we will discuss on dimensions for which the Latin MUB constructions gives better lower bound. In this section we shall see that there is no basis $\mathcal{B}_4$ in $\mathbb{C}^4$ that is mutually unbiased to the 3 MUBs of dimension $d = 2^2$ from the Latin MUB construction in Example 4.5. Whereas we know from Theorem 2.29 that in dimension 4 we have 5 MUBs.

Lemma 4.14 ([6])**.** *A $(s+1, s)$-net spans $\mathbb{R}^{s^2}$.*

Proof. Let $Y = \{B_1, B_2, \ldots, B_{s+1}\}$ be a $(s+1, s)$-net. Since a $(s+1, s)$-net has $s(s+1)$ incidence vectors of length s^2, and the inner product of each vector with any vector from a different set is equal to 1, thus for any $i \in \{1, \ldots, s^2\}$, there is exactly one vector in each block that has 1 in the ith position. By adding all these vectors from each of the $s+1$ blocks, we get the vector $\mathbf{v}_i = (1, \ldots, 1, (s+1)_i, 1, \ldots, 1)$. Let

$$\mathbf{w} = \sum_{j=1}^{s^2} \mathbf{v}_j = (s(s+1), s(s+1), \ldots, s(s+1)) .$$

Then

$$\mathbf{e}_i = \frac{1}{s^2(s+1)} ((s(s+1)\mathbf{v}_i - \mathbf{w}).$$

□

Lemma 4.15 ([6]). *Let $X = \{\mathcal{B}_1, \ldots, \mathcal{B}_{s+1}\}$ be a set of $s+1$ MUBs in $\mathbb{C}^{s^2}$ constructed from the Latin MUB construction. If there exists a an orthonormal basis $\mathcal{B}$ in $\mathbb{C}^{s^2}$ mutually unbiased to bases in X, then for any vector $\mathbf{w} = (w_1, w_2, \ldots, w_{s^2}) \in \mathcal{B}$, $|w_i| = \frac{1}{s}$, for $i = 1, \ldots, s^2$.*

Proof. $X = \{\mathcal{B}_1, \mathcal{B}_2, \ldots, \mathcal{B}_{s+1}\}$ is a set of $s+1$ MUBs in $\mathbb{C}^{s^2}$ derived from the Latin MUB construction. So, X is derived from an $(s+1, s)$-net, $Y = \{B_1, B_2, \ldots, B_{s+1}\}$. Let $H = (\mathbf{h}_1|\mathbf{h}_2|\cdots|\mathbf{h}_s)$ be a generalized Hadamard matrix of order s. Fix $r \in \{1, 2, \ldots, s+1\}$ and fix $i \in \{1, 2, \ldots, s^2\}$. From the Latin MUB construction in (4.3), for $j \in \{1, 2, \ldots, s\}$, $\mathbf{u}_j = \frac{1}{\sqrt{s}}(\mathbf{h}_j \uparrow \mathbf{m}_{ri}) \in \mathcal{B}_r$ where $\mathbf{m}_{ri}$ is an incidence vector of the block B_r such that $\text{supp}(\mathbf{m}_{ri}) = \{i_1, \ldots, i_s\}$. Let $\mathbf{w} = (w_1, \ldots, w_{s^2})$ be an arbitrary vector from a new basis $\mathcal{B}$ in $\mathbb{C}^{s^2}$, that is mutually unbiased to the $s+1$ MUBs in X. Let $\widetilde{\mathbf{w}}_i = (w_{i_1}, \ldots, w_{i_s})$ be a vector in $\mathbb{C}^s$, whose i_jth component is same as i_jth component of $\mathbf{w}$ for each $i_j \in \text{supp}(\mathbf{m}_{ri})$. Since $\mathbf{w}$ is unbiased to the vector $\mathbf{u} \in \mathcal{B}_r$, therefore

$$\begin{aligned} |\langle \mathbf{u}, \mathbf{w} \rangle| &= \left| \left\langle \frac{1}{\sqrt{s}} \mathbf{h}_j, \widetilde{\mathbf{w}} \right\rangle \right| \\ &= \frac{1}{s}. \end{aligned} \tag{4.5}$$

For $j = 1, \ldots, s$, the inner product of $\mathbf{w}$ and $\mathbf{u}_j = \frac{1}{\sqrt{s}}(\mathbf{h}_j \uparrow \mathbf{m}_{ri})$ can be written

$$\frac{1}{\sqrt{s}} H \widetilde{\mathbf{w}}_i^* = \mathbf{v}^T, \tag{4.6}$$

where $\mathbf{v} = (v_1, \ldots, v_s)$ is some vector in $\mathbb{C}^s$ with $|v_k| = \frac{1}{s}$, for $1 \leq k \leq s$. Since $\frac{1}{\sqrt{s}}H$ is a unitary matrix, then $\langle \widetilde{\mathbf{w}}_i, \widetilde{\mathbf{w}}_i \rangle = \langle \mathbf{v}, \mathbf{v} \rangle = \dfrac{1}{s}$. Since (4.6) is true regardless of choice of $\mathbf{m}_{ri}$, we get the system of equations for each $r \in \{1, \ldots, s+1\}$ and $i \in \{1, \ldots, s^2\}$ as follows

$$\begin{aligned} \langle \mathbf{m}_{ri}, (|w_1|^2, \ldots, |w_{s^2}|^2) \rangle &= \sum_{i_l \in \mathrm{supp}(\mathbf{m}_{ri})} |w_{i_l}|^2 \\ &= \langle \widetilde{\mathbf{w}}_i, \widetilde{\mathbf{w}}_i \rangle \\ &= \frac{1}{s}. \end{aligned} \tag{4.7}$$

The system of equations (4.7) has a solution $|w_{i_l}|^2 = \frac{1}{s^2}$. By Lemma 4.14, incidence vectors from a $(s+1, s)$-net span $\mathbb{R}^{s^2}$. So the system of equations corresponding to (4.7) is full rank and has unique solution $|w_i|^2 = \frac{1}{s^2}$. □

Now, Lemma 4.15 may be used to show that there is no new orthogonal basis $\mathcal{B}_4$ in $\mathbb{C}^4$ mutually unbiased to the 3 MUBs in Example 4.5. Assume the contrary. Assume $\mathbf{w}$ to be a vector from the new basis $\mathcal{B}_4$ unbiased to the 3 MUBs in Example 4.5. By Lemma 4.15, all entries of $\mathbf{w}$ have the same modulus. Thus without loss of generality assume $\mathbf{w} = \frac{1}{2}(1, w_1, w_2, w_3)$ is a vector from the new basis $\mathcal{B}$ such that $|w_1| = |w_2| = |w_3| = 1$. Consider the following vectors from Example 4.5

$$\mathbf{v}_1 = \frac{1}{\sqrt{2}}(1,1,0,0) \in \mathcal{B}_1, \quad \mathbf{v}_2 = \frac{1}{\sqrt{2}}(1,0,1,0) \in \mathcal{B}_2, \quad \mathbf{v}_3 = \frac{1}{\sqrt{2}}(0,1,1,0) \in \mathcal{B}_3.$$

Since $\mathbf{w}$ is mutually unbiased to $\mathbf{v}_1$, $\mathbf{v}_2$ and $\mathbf{v}_3$,

$$|\langle \mathbf{v}_1, \mathbf{w} \rangle|^2 = |\langle \mathbf{v}_2, \mathbf{w} \rangle|^2 = |\langle \mathbf{v}_3, \mathbf{w} \rangle|^2 = \frac{1}{4}, \tag{4.8}$$

or equivalently

$$|1 + w_1|^2 = |1 + w_2|^2 = |w_1 + w_2|^2 = 2. \tag{4.9}$$

It is easy to see that (4.9) has no solutions. So, $\mathcal{B}_4$ does not exist.

4.4 Discussion of Latin MUB construction

The construction for MUBs in this chapter was based on the existence of mutually orthogonal Latin Squares. The Latin MUB construction for prime power dimensions of the form $p^{2\alpha}$ gives $p^\alpha + 1$ MUBs whereas we we know that that there exists $p^{2\alpha} + 1$ MUBs in that dimension. But in some dimensions the Latin MUB construction gives us a better lower bound for the number of MUBs. For example it is well-known [7] that $N_{MOLS}(30) \geq 4$. Thus from Theorem 4.13 we have $N_{MUB}(30^2) \geq 6$. Whereas from reduced power construction in Theorem 2.31, $N_{MUB}(30^2) \geq 4$.

Wilson [40] showed $N_{MOLS}(s) \geq 6$ for all $s \geq 76$. Therefore by the Latin MUB construction, $N_{MUB}(s^2) \geq 8$ for $s \geq 76$. For the case $s \equiv 2 \pmod 4$, $s \geq 76$, the minimum prime power in s is 2. So by the reduced power construction $N_{MUB}(s^2) \geq 5$. Therefore, the Latin MUB construction gives us better lower bound for the number of MUBs in these dimensions.

Chapter 5

REAL MUTUALLY UNBIASED BASES

In this chapter we restrict the MUB problem to real space $\mathbb{R}^d$. We will give an upper bound for the number of real MUBs. We will we show that for some dimensions, real MUBs don't exist.

5.1 An upper bound for real MUBs

Theorem 2.9 applies to real MUBs. In other words, the existence of m classes $\mathcal{C}_1, \ldots, \mathcal{C}_m$, each having d commuting real symmetric $d \times d$ matrices such that for $i \neq j$, $C_i \bigcap C_j = \{\mathbb{I}_d\}$ and matrices in $\bigcup_{i=1}^{m} \mathcal{C}_i$ are mutually orthogonal, is equivalent to existence of m MUBs in $\mathbb{R}^d$.

Let $\mathcal{C}_1, \ldots \mathcal{C}_m$ be the classes as mentioned. The union of these classes has $m(d-1)+1$ real symmetric matrices and span of these $m(d-1)+1$ matrices is a subspace of the space of real symmetric matrices. Since the dimension of the space of real $d \times d$ symmetric matrices is $d(d+1)/2$, then

$$\begin{aligned} m(d-1)+1 \leq & \frac{d(d+1)}{2} \\ m \leq & \frac{d}{2}+1. \end{aligned}$$

So, the number of MUBs in $\mathbb{R}^d$ is less that or equal to $\frac{d}{2}+1$.

Example 5.1. *Define* $\mathcal{C}_1 = \{U, \mathbb{I}_2\}, \mathcal{C}_2 = \{V, \mathbb{I}_2\}$*, where*

$$U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

$\mathcal{C}_1, \mathcal{C}_2$ *satisfy hypothesis of Theorem* 2.9 *for the real case. The eigenvectors corresponding to* $\mathcal{C}_1$ *and* $\mathcal{C}_2$ *give us 2 real MUBs in* $\mathbb{R}^2$

$$\mathcal{B}_1 = \{(1,0),(0,1)\}, \quad \mathcal{B}_2 = \left\{\frac{1}{\sqrt{2}}(1,1), \frac{1}{\sqrt{2}}(1,-1)\right\}.$$

We may also find a lower bound for real MUBs depending on the existence of MOLS by using the Latin MUB construction introduced in Chapter 4. Let us denote the maximum number MUBs in $\mathbb{R}^d$ by $N_{MUB}(\mathbb{R}^d)$. If there exists a Hadamard matrix of order $\sqrt{d}$, then $N_{MUB}(\mathbb{R}^d) \geq N_{MOLS}(\sqrt{d}) + 2$ for any positive integer d.

5.1.1 Real MUBs and Hadamard matrices

A $d \times d$ matrix H with entries in $\{-1, +1\}$ is called a **Hadamard matrix** if $HH^T = d\mathbb{I}_d$. In this section, we find some restrictions on the existence of real MUBs in a given dimension d by using Hadamard matrices.

Theorem 5.2 ([15])**.** *If there exists a Hadamard matrix of order d, then d is 1, 2, or a multiple of 4.*

Proof. Let $d \geq 3$, and let H be a Hadamard matrix of order d. We may multiply rows and columns of H by -1 or permute two columns and H will still be a Hadamard matrix. Then first 3 rows of H can be arranged as follows

$$\left(\begin{array}{ccc|ccc|ccc|ccc} 1 & \cdots & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 & 1 & \cdots & 1 \\ 1 & \cdots & 1 & 1 & \cdots & 1 & -1 & \cdots & -1 & -1 & \cdots & -1 \\ 1 & \cdots & 1 & -1 & \cdots & -1 & 1 & \cdots & 1 & -1 & \cdots & -1 \end{array}\right).$$

Let j, k, l, m denote the number of columns in each sector shown. Then by the orthogonality condition we have

$$j + k + l + m = d, \quad j + k - l - m = 0, \quad j - k + l - m = 0, \quad j - k - l + m = 0.$$

The sum of the above equations is $4j = d$. Thus d is a multiple of 4 as claimed. □

Let $\mathcal{B}_1, \ldots, \mathcal{B}_m$ be m mutually unbiased bases in $\mathbb{R}^d$. Without loss of generality we may assume $\mathcal{B}_1$ is the standard basis. For $2 \leq i \leq m$, associate with every basis $\mathcal{B}_i$ a matrix H_i whose columns are vectors in $\mathcal{B}_i$. Since all the bases are unbiased to $H_1 = \mathbb{I}_d$, then H_is are Hadamard matrices scaled by $\frac{1}{\sqrt{d}}$. So, by Theorem 5.2, if there exists at least two real MUBs in $\mathbb{R}^d$, then $d = 2$ or $4|d$.

Proposition 5.3 ([6]). *If $d > 2$ and $4|d$, but d is not a square, then $N_{MUB}(\mathbb{R}^d) \leq 2$. Moreover, $N_{MUB}(\mathbb{R}^d) = 2$ if and only if a Hadamard matrix of order d exists.*

Proof. Assume $\mathcal{B}_1, \mathcal{B}_2$ and $\mathcal{B}_3$ are three bases for $\mathbb{R}^d$ that are mutually unbiased. Associate with every basis $\mathcal{B}_i$, for $i = 1, 2, 3$, a matrix H_i whose columns are vectors

in $\mathcal{B}_i$. Without loss of generality we may assume that $H_1 = \mathbb{I}_d$ and the first column of the matrix H_2 is $\mathbf{x} = \frac{1}{\sqrt{d}}(1, 1, \ldots, 1)^T$. We may do this by multiplying each rows or columns of H_is by -1 if it is necessary. This does not change the absolute values of the inner products between the column vectors of $\mathcal{B}_2$ and $\mathcal{B}_3$. Let $\mathbf{y} = \frac{1}{\sqrt{d}}(h_1, h_2, \ldots, h_d)^T$ (with $h_i = \pm 1$) be the first column of H_3. Applying the MUB condition to the first column of H_2 and H_3 implies that

$$|\langle \mathbf{x}, \mathbf{y} \rangle| = \frac{1}{d} \left| \sum_{i=1}^{d} h_i \right| = \frac{1}{\sqrt{d}}.$$

Since $h_i = \pm 1$, for $1 \leq i \leq d$, it is obvious that if d is not square the last equation cannot hold.

Therefore, $\mathcal{B}_3$ cannot exist.

If there exists a Hadamard matrix H of order d, then the columns of H scaled by $\frac{1}{\sqrt{d}}$ comprise vectors of a basis $\mathcal{B}$ which is mutually unbiased to the standard basis. □

Lemma 5.4 ([6]). *If $d = 4s^2$ for an odd positive integer s, then $N_{MUB}(\mathbb{R}^d) \leq 3$.*

Proof. Assume the contrary, that there are 4 MUBs in $\mathbb{R}^d$, $\mathcal{B}_0, \mathcal{B}_1$, $\mathcal{B}_2$ $\mathcal{B}_3$, where $\mathcal{B}_0$ is the standard basis. Let $\mathbf{v}_1 \in \mathcal{B}_1, \mathbf{v}_2 \in \mathcal{B}_2, \mathbf{v}_3 \in \mathcal{B}_3$. Without loss of generality we may assume $\mathbf{v}_1 = \frac{1}{2s}(1, 1, \ldots, 1)$. Consider a partition of $\mathbf{v}_2$ and $\mathbf{v}_3$ as was done in Theorem 5.2. Here we denote -1 by " $-$ ". Let

$$\mathbf{v}_2 = \frac{1}{2s}(1, 1, \ldots, 1|1, 1, \ldots, 1|-, -, \ldots, -|-, -, \ldots, -)$$
$$\mathbf{v}_3 = \frac{1}{2s}(1, 1, \ldots, 1|-, -, \ldots, -|1, 1, \ldots, 1|-, -, \ldots, -).$$

Denote by j, k, l and m the number of positions in blocks as shown in $\mathbf{v}_2$ and $\mathbf{v}_3$ respectively. By applying the MUB condition to the vectors $\mathbf{v}_1$, $\mathbf{v}_2$ and $\mathbf{v}_3$ we obtain the following equations

$$\langle \mathbf{v}_i, \mathbf{v}_i \rangle = j + k + l + m = 4s^2, \qquad \langle \mathbf{v}_1, \mathbf{v}_3 \rangle = j - k + l - m = \pm 2s,$$

$$\langle \mathbf{v}_1, \mathbf{v}_2 \rangle = j + k - l - m = \pm 2s, \qquad \langle \mathbf{v}_2, \mathbf{v}_3 \rangle = j - k - l + m = \pm 2s.$$

Adding all equations together gives

$$j = s^2 + \tfrac{s(\pm 1 \pm 1 \pm 1)}{2}.$$

The equation in the parenthesis can only have values ± 3 or ± 1. Since s is odd, it follows that j is not an integer−a contradiction. The result follows. □

For the case $d = 4^i s^2$, where $i > 1$ is an integer, if there exists $2^i s$ MOLS and a Hadamard matrix of order $2^i s$ then there exists at least $N_{MOLS}(2^i s) + 2$ real MUBs of dimension $4^i s^2$. For details see sections 4.2 and page 83.

5.2 Conclusion

In this chapter we discussed the dimensions in which real MUBs can exist and we saw that in comparison to complex MUBs, dimensions for which real MUBs exist are limited. We found $\frac{d}{2}+1$ as an upper bound for the number of real MUBs of dimension d.

One main question on real MUBs is the following: if $d = 4s^2$, s an odd positive integer, does $N_{MUB}(\mathbb{R}^d) = 3$ always hold, or only for certain values of s? In this chapter we also showed if for any $d \equiv 0 \pmod 4$ a Hadamard exists, then $N_{MUB}(\mathbb{R}^d) \geq 2$. Finding examples that exceed the lower bound still is a goal.

REFERENCES

[1] S. Bandyopadhyay, P. Boykin, V. Roychowdhury, and F. Vatan, *A new proof for the existence of mutually unbiased bases*, Algorithmica, 34 (2002), pp. 512–528.

[2] H. Barnum, *Information-disturbance tradeoff in quantum measurement on the uniform ensemble and on the mutually unbiased bases*. arXiv:quant-ph/0205155, 2002.

[3] J. Beachy and W. Blair, *Abstract algebra (Third edition)*, Waveland Press Inc, 2006.

[4] T. Beth, *Eine bemerkung zur abschäatzung der anzahl orthogonaler lateinischer quadrate mittels siebverfahren*, Abh. Math. Sem. Hamburg, 53 (1983), pp. 284–288.

[5] N. Bourbaki, *Integration II Chapter 7*, Springer, 2004.

[6] P. O. Boykin, M. Sitharam, M. Tarifi, and P. Wocjan, *Real mutually unbiased bases*. arXiv:quant-ph/0502024v2, 2005.

[7] C. J. Colbourn and J. H. Dinitz, *The CRC Handbook of Combinatorial Designs*, CRC Press, Boca Raton FL, 1996.

[8] J. A. Davis, J. Jedwab, and M. Mowbray, *New families of semi-regular relative difference sets*, Designs, Codes and Cryptography, 13 (1998), pp. 131–146.

[9] P. A. M. Dirac, *The Principles of Quantum Mechanics*, Oxford University Press, Oxford, 1958.

[10] U. Fano, *Description of states in quantum mechanics by density matrix and operator techniques*, Reviews of Modern Physics, 29 (1957), pp. 74–93.

[11] T. Feng and Q. Xiang, *Semi-regular relative difference sets with large forbidden subgroups*, Combinatorial Theory, 115 (2008), pp. 1456–1473.

[12] R. Feynman, R. Leighton, and M. Sands, *The Feynman Lectures on Physics, Quantum Mechanics*, Addison–Wesley Publishing, USA, 1965.

[13] M. H. Freedman and F. Quinn, *Topology of 4-Manifolds*, Princeton University Press, 1990.

[14] C. Godsil and A. Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics, 30 (2009), pp. 246–262.

[15] J. Hadamard, *Résolution d'une question relative aux déterminants*, Bull. des Sciences Math., 17 (1893), pp. 240–246.

[16] A. R. Hammons and P. V. Kumar, *The 24-linearity of Kerdock, Preparata, Goethals, and related codes*, IEEE Trans. Inform. Theory, 40 (1994), pp. 301–319.

[17] A. S. Hedayat, N. J. A. Sloane, and J. Stufken, *Orthogonal Arrays*, Springer Series in Statistics, 1999.

[18] S. G. Hoggar, *Parameters of t-designs in FP^{n-1}*, Europ. J. Combin., 5 (1984), pp. 29–36.

[19] ——, *t-designs with general angle set*, Europ. J. Combin., 13 (1992), pp. 257–271.

[20] R. A. Horn and C. R. Johnson, *Topics in Matrix Analysis*, Cambridge University Press, Cambridge, UK, 1991.

[21] I. M. Isaacs, *Character Theory of Finite Groups*, Dover Publications, 1994.

[22] I. D. Ivanovic, *Geometrical description of quantum state determination*, Journal of Physics A, 14 (1981), pp. 3241–3245.

[23] D. Junglickel, *On automorphism groups of divisible designs*, Canada. J . Math, 34 (1982), pp. 257–297.

[24] A. Klappenecker and M. Röetteler, *Constructions of mutually unbiased bases*. arXiv:quant-ph/0309120, 2003.

[25] A. Klappenecker and M. Rötteler, *Mutually unbiased bases are complex projective 2-designs*, Proc. IEEE International Symposium on Information Theory, (1965), pp. 1740–1744.

[26] C. F. Laywine and G. Mullen, *Discrete Mathematics using Latin Squares*, Wiley, 1998.

[27] R. Lidl and H. Niederreiter, *Introduction to finite fileds and their applications*, Cambrige University Press, Cambrig.

[28] R. J. McEliece, *Finite fields for computer science and eengineers*, Kluwer Academic Publishers, Boston, 1987.

[29] A. O. Pittenger and M. H. Rubin, *Separability and Fourier representations of density matrices*, Physics Review A, 62 (2000), pp. 32311–32313.

[30] ——, *Mutually unbiased bases, generalized spin matrices and separability*, Linear Algebra and its Applications, 390 (2004), pp. 255–278.

[31] A. Pott, P. V. Kumar, T. Helleseth, and D. Jungnickel, *Difference Sets, Sequences, and their Correlation Properties*, Springer, 1999.

[32] V. A. Rohlin, *On the fundamental ideas of measure theory*, American Mathematical Society, 25 (1952), pp. 107–150.

[33] W. Rudin, *Function Theory in the Unit Ball of* $\mathbb{C}^n$, Springer, New York, 1980.

[34] J. Schwinger, *Unitary operator bases*, Proc. Natl. Acad. Sci., 46 (1960), pp. 570–579.

[35] R. Turyn, *Character sums and difference sets*, Pacific J. Math, 15 (1965), pp. 319–346.

[36] B. L. van der Waerden, *Modern Algebra*, Ungar Publ. Co., New York, 1955.

[37] J. von Neumann, *Mathematical Foundations of Quantum Mechanics*, Princeton University Press, Princeton, 1996.

[38] S. Waldron, *Generalized Welch bound equality sequences are tight frames*, IEEE Trans. Inf. Thry., 49 (2003), pp. 2307–2309.

[39] Z. Wan, *Quaternary Codes*, World-Scientific, Singapore, 1997.

[40] R. M. Wilson, *Concerning the number of mutually orthogonal latin squares*, DISCRETE MATHEMATICS, 9 (1974), pp. 181–198.

[41] P. Wocjan and T.Beth, *New construction of mutually unbiased bases in square dimensions*, Quantum Information and Computation, 5 (2005), pp. 93–101.

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

[43] K. Yang, T. Helleseth, P. V. Kumar, and A. G. Shanbhag, *On the weight hierarchy of Kerdock codes over* $\mathbb{Z}_4$, IEEE Transaction on information Theory, 42 (1996), pp. 1587–1593.

[44] G. Zauner, *Quantendesigns, Grüundzuge einer nichtkommutativen Designtheorie (in German)*, PhD thesis, University of Vienna, 1999.