Combinatorial & Algebraic Approaches in Analyzing Mutually Unbiased Bases (MUBs) and Their Approximations

A THESIS

submitted in partial fulfillment of the requirements
for the award of the degree of

Doctor of Philosophy

in

Computer Science

by

Rakesh Kumar

under the supervision of

Prof. Subhamoy Maitra

APPLIED STATISTICS UNIT
INDIAN STATISTICAL INSTITUTE, KOLKATA

JULY 2025

To all the great teachers of humanity, whose enduring wisdom and guidance bear the weight of the universe.

Acknowledgments

After spending a few enriching years as a teacher, I embarked on a new journey as a Ph.D. student at the Indian Statistical Institute (ISI), Kolkata. As time passed, I found myself battling a quiet but persistent doubt about whether I was meant for research. I never felt competent in this space and often moved forward not with confidence, but with a kind of reluctant curiosity that refused to quit. What sustained me through those moments was the presence of a few remarkable individuals who never lost faith in me and continued to support me. My sincere gratitude goes to my supervisor, Prof. Subhamoy Maitra, and to my senior, Dr. Ajeet Kumar, who has been like a mentor to me. It is difficult to find the right words to capture my gratitude and respect for them.

I am grateful to the few professors at ISI, whose classes I attended during my Ph.D. coursework, Prof. Sourav Chakraborty, Prof. Ansuman Banerjee, Prof. Debrup Chakraborty, and Prof. Sasthi Charan Ghosh. I also want to express my gratitude to two teachers who played a significant role in shaping my mathematical journey. Mr. Jitendra Sharma, my high school teacher, introduced me to the beauty of mathematics at an early stage with great care and encouragement. Prof. Swadheen Pattanayak, who was both my professor and the Director of the Institute of Mathematics and Applications (IMA) in Bhubaneswar, taught me five courses during my undergraduate years at IMA. His teaching had a profound influence on my overall approach to learning.

I want to thank my research collaborators, Dr. Ajeet Kumar (IRS, Goverment of India), Dr. Arindam Banerjee (Assistant Professor at IIT Kharagpur), Dr. Saswat Sarangi (postdoctoral researcher at OIST, Japan), Dr. Konoy Kumar Das (postdoctoral researcher at CMI, Chennai), and Mr. Uddipto Mandal (B.Tech student at IIT Kharagpur) for their contributions to my thesis work.

Additionally, I am thankful to Dr. Arpita Maitra (Associate Professor at TCG - CREST, Kolkata), Mr. Suman Dutta (Researcher at ISI, Kolkata), and Mr. Uddipto Mandal for their invaluable support during the final phase of my thesis writing.

I would like to extend my sincere thanks to Avisek da, Umakant da, Arkabrata, Saswati, Priyanka, Shashi Shekhar, Sumit bhai, and Tattwamasi bhai. Each of them had made a meaningful contribution to my PhD Journey and beyond.

I truly cherished my life on the ISI campus, where I felt a strong sense of belonging in every corner. The serene atmosphere and the support from the staff and workers made my time memorable.

I am indebted to my family for their love and support. My heartfelt thanks to my younger brother, Rasu, whose unspoken care kept me steady during the final years of my Ph.D.

Abstract

Mutually Unbiased Bases (MUBs) are an important concept in quantum information theory. Two orthonormal bases in a d-dimensional complex Hilbert space $\mathbb{C}^d$ are said to be mutually unbiased if the absolute value of the inner product between any pair of vectors, one from each basis, is $1/\sqrt{d}$. A set of r orthonormal bases is called mutually unbiased if every pair of bases in the set is unbiased. It is known that at most $d+1$ mutually unbiased bases can exist in $\mathbb{C}^d$, and a set achieving this bound is termed a *complete sets of MUBs* in $\mathbb{C}^d$. We can construct $d+1$ MUBs if d is a power of a prime. However, the existence of a complete sets of MUBs in composite dimensions that are not a power of a prime remains a longstanding open problem. In such cases, the (naive) known general lower bound for the number of MUBs is p^r+1, where p^r is the smallest prime power dividing d. Consequently, we do not have more than seven MUBs and fewer than three MUBs in dimension six. However, Zauner (in 1999) conjectured that there are no more than three MUBs in $\mathbb{C}^6$.

This thesis is mainly structured into two parts. The first part focuses on the existence and extendibility of MUBs. We study this part from the perspective of combinatorics and Algebraic geometry. We study the extensibility of MUB triplets in $\mathbb{C}^6$, which are product bases. We provide a combinatorial proof for the form of a unitary matrix under specific conditions. Subsequently, we demonstrate that the unitary matrix, which can be viewed as the fourth MUB of triplets of MUBs in $\mathbb{C}^6$, is not possible. Additionally, we have studied the extendibility of a given set of MUBs from the point of view of algebraic geometry and commutative algebra. We investigated the ideals of the affine algebraic variety derived from a given set of k MUBs in any generic dimension d, $(k \leq d)$. We established a few notable results related to the complete intersection of ideals. Also, we prove that there is a one-to-one correspondence between the MUBs and the maximal commuting classes (bases) of orthogonal normal matrices in $\mathbb{C}^d$. It means that for m MUBs in $\mathbb{C}^d$, there are m commuting classes, each consisting of d commuting orthogonal normal matrices. The existence of maximal commuting basis for $\mathcal{M}_d(\mathbb{C})$ ensures the complete sets of MUBs in $\mathcal{M}_d(\mathbb{C})$.

The second part addresses the combinatorial construction of MUBs and approximate real MUBs (ARMUBs) in certain specific dimensions. In particular, we focus on the construction of Approximate Real Mutually Unbiased Bases (ARMUBs) for dimensions that are not

divisible by four. We show that it is possible to construct $\geq \lceil \sqrt{d} \rceil$ many ARMUBs for certain odd dimensions d of the form $d = (4n-t)s$, $t = 1, 2, 3$, where n is a natural number and s is an odd prime power. Also, we consider the parametrisation of MUBs to understand the degrees of freedom, and this can help explore various choices of MUBs so that one can explore several classes of them for multiple applications in quantum information. For dimension $d = s^2$, we present the construction of affine-parametric classes with $MOLS(s) + 2$ many MUBs, where $MOLS(s)$ is the number of Mutually Orthogonal Latin Squares of dimension s. If s is a power of a prime, then $MOLS(s) = s - 1$, and the number of MUBs will be $s + 1$. Considering the first one to be the identity matrix, in our construction, each of the rest $MOLS(s) + 1$ MUBs will have at least $s(s - 1)$ free parameters, so that a global unitary operation cannot absorb.

List of Publications

Conference publications included in the thesis:

- A. Kumar, **R. Kumar** and S. Maitra. *A Parametric Class of Mutually Unbiased Bases Using Resolvable Block Designs*. Progress in Cryptology – INDOCRYPT 2024, Springer LNCS, vol. 15495, pp. 356-373, 2024.
  https://doi.org/10.1007/978-3-031-80308-6_16

- A. Kumar, **R. Kumar**, S. Maitra and S. Sarangi. *Exploring the presence of* 4*-th MUB as a product basis in* $\mathbb{C}^6$. 8th Workshop on Design Theory, Hadamard Matrices and Applications (Hadamard 2025), 26-30 May, 2025, Sevilla.
  https://gestioneventos.us.es/hadamard2025

Journal publication included in this thesis:

- A. Banerjee, K. K. Das, A. Kumar, **R. Kumar** and S. Maitra. *On Obtaining New MUBs by Finding Points on Complete Intersection Varieties over* $\mathbb{R}$.
  International Journal of Theoretical Physics, 64 (227), 2025.
  https://doi.org/10.1007/s10773-025-06094-3

Submitted to Journal (Preprints uploaded in arXiv):

- A. Kumar, **R. Kumar**, S. Maitra and U. Mandal. *On Construction of Approximate Real Mutually Unbiased Bases for an infinite class of dimensions* $d \not\equiv 0 \bmod 4$.
  https://arxiv.org/abs/2507.07028

Contents

1 Introduction **5**

1.1 Preliminaries on MUBs 7

1.2 Thesis Plan 8

1.2.1 Contribution 1: Inextendibility of the set of three MUBs which are product bases in $\mathbb{C}^6$ 9

1.2.2 Contribution 2: On Obtaining New MUBs by Finding Points on Complete Intersection Varieties over $\mathbb{R}$ 9

1.2.3 Contribution 3: A parametric Class of Mutually Unbiased Bases Using Resolvable Block Designs 10

1.2.4 Contribution 4: Construction of Approximate Real MUBs for dimension which are not a multiple of four 11

1.3 Prerequisites 12

1.4 Conclusion 12

2 Background **14**

2.1 Basis definitions 14

2.2 Hadamard Matrix 17

2.2.1 Affine Parametrisation of Complex Hadamard Matrices 18

2.3 Mutually Unbiased Bases 19

2.3.1 Connection between MUBs and Hadamard matrices 19

2.3.2 Equivalent Sets of MUBs 20
2.3.3 Challenges in Composite (Not a power of a prime) Dimensions 22
2.3.4 Construction of a complete sets of MUBs in prime dimensions 23
2.4 Product state and Product basis 24
2.5 Combinatorial Designs and Mutually Unbiased Bases (MUBs) 26
2.5.1 Constructing MUBs in $\mathbb{C}^d$ Using Resolvable Block Designs (RBD) . . 28
2.6 Approximate Mutually Unbiased Bases 30
2.7 Algebraic Tools for Analyzing Systems of MUBs 32
2.8 Conclusion 36

3 Exploring the presence of 4-th MUB as a product basis in $\mathbb{C}^6$ 37
3.1 Introduction 37
3.1.1 Organization and contribution 38
3.2 Unitary matrix as product basis in dimension 6 38
3.3 Conclusion 46

4 On Obtaining MUBs by Finding Points on Complete Intersection Varieties over $\mathbb{R}$ 47
4.1 Introduction 48
4.1.1 Organization and Contribution 48
4.2 Studying Real Points on Intersection Varieties 49
4.2.1 Defining ideals of MUB 49
4.2.2 Ideals of the MUBs in dimension two 54
4.2.3 Results On Complete Intersection 57
4.3 Maximal Commuting Bases and MUBs 59
4.4 Conclusion 66

5 A parametric Class of Mutually Unbiased Bases Using Resolvable Block Designs **68**

5.1 Introduction 69

5.1.1 Organization & Contribution 69

5.2 Construction of Affine parametric form of MUBs for square dimension, $d = s^2$ 73

5.2.1 Introducing the parameters 75

5.2.2 Parametric Class of Hadamard Matrices 78

5.2.3 Comparison with Goyeneche et. al.'s work (2015) 81

5.2.4 Towards generalising the idea towards construction of an affine parametric class of Hadamard matrices for $d = k \times s$ 82

5.3 Conclusion 84

6 On Construction of Approximate Real Mutually Unbiased Bases for an infinite class of dimensions $d \not\equiv 0 \bmod 4$ **85**

6.1 Introduction 86

6.1.1 Organization & Contribution 86

6.1.2 Some basic examples related to MUBs 88

6.1.3 Example of ARMUBs in dimension two 90

6.2 Our Construction 91

6.2.1 Modifying real Hadamard matrices 91

6.2.2 Explaining the cases with $t = 1, 2, 3$ 96

6.2.3 Construction of ARMUBs 100

6.3 Conclusion 102

7 Conclusion **103**

7.1 Summary of the Thesis 103

7.2 Future Directions 106

7.3 Final Comments 107

Chapter 1

Introduction

Mutually Unbiased Bases (MUBs) have been widely investigated in quantum information theory, as well as in several areas of mathematics and computer science. Researchers from diverse backgrounds have shown a sustained interest in these highly symmetric bases in finite-dimensional Hilbert spaces.

Let $u_1, u_2, \ldots, u_d$ denote an orthonormal basis of a d-dimensional Hilbert space H. A unit vector $v \in H$ is said to be *complementary* to this basis if $|\langle u_i|v\rangle| = \frac{1}{\sqrt{d}}$ for all $1 \leq i \leq d$. Two orthonormal bases are said to be complementary or *mutually unbiased* if every vector from one basis is complementary to each vector in the other. Such pairs of bases are referred to as *Mutually Unbiased Bases*.

The concept of MUBs was initially introduced by Julian Schwinger, an American physicist, in 1960 [72], motivated by the study of unitary operator bases and their connection to maximal measurement incompatibility. An important property of mutually unbiased bases is that if a quantum state is prepared in one basis and measured using the other, the outcome probabilities are uniformly distributed. It implies that a measurement outcome reveals no information about the original state, provided the state was from a mutually unbiased basis. This inherent unpredictability makes MUBs particularly valuable in quantum information processing and quantum cryptography [21].

A natural question arises: how many Mutually Unbiased Bases can exist in a given dimension d? It was established in [85] that the number of MUBs in dimension d cannot exceed $d + 1$. A collection of $d + 1$ such bases is called a *complete sets of MUBs*. This

upper bound is known to be tight when d is a power of a prime [85]. A simplified proof of this result, employing bounds on exponential sums, was provided in [49]. Another significant approach, based on constructing MUBs via maximally commuting sets of orthogonal unitary matrices, was proposed in [5].

The existence problem of complete sets of MUBs has earned a place among "The new ten most annoying questions in quantum computing" [1]. It also appears on a widely recognised list of open problems in quantum information [53], and also finds a place in one of the hardest ones in "Five open problems in quantum information theory" [41].

A comprehensive review by McNulty and Weigert [66] presents various mathematically equivalent formulations of the existence problem of a complete sets of MUBs in composite dimensions that are not a power of a prime. These formulations span a broad spectrum of mathematical disciplines, including operator algebras, Galois rings, group theory, combinatorics, finite fields, and projective geometry [8, 17, 25, 46, 52, 69, 70, 71, 81].

Naturally, one may ask why there is a serious effort to search for complete sets of MUBs in composite dimensions that are not a power of a prime. The answer lies in their wide-ranging applications in quantum information theory. Complete sets of MUBs play a crucial role in tasks such as quantum state reconstruction [85], quantum state tomography [25, 68], quantum key distribution [11, 24], secret sharing [38, 79], the Mean King problem [32, 47], entanglement detection [74, 82], and quantum random access codes [3, 80]. These applications provide strong motivation to explore the existence of complete sets in such composite dimensions.

MUBs also play an important role in quantum physics. Many fundamental concepts, like quantum correlations [78, 42], quantum coherence[76, 48, 7], quantum degree of freedom [18], quantum state-space geometry [10, 31], complementarity [22, 51], incompatibility [28], Entropic uncertainty relations [4], quantum channels[67], SIC-POVM and frames [35, 37], and others.

There is much more to say about Mutually Unbiased Bases in composite dimensions beyond merely highlighting our inability to construct the complete sets. While these insights do not resolve the central question about whether a complete sets of MUBs exists in such composite dimensions, they still offer valuable understanding. Many aspects of mutually unbiased bases are reviewed in references [30, 66].

With this context, let us now present the outline of the thesis. This thesis has two main parts. One focuses on the extensibility of the set of MUBs in dimension d. Other studies construction of MUBs and Approximate Mutually Unbiased Bases (AMUBs) by exploiting the combinatorial structures like RBDs and MOLSs. Further, we consider the parameterisation of MUBs. The first two contributory Chapters 3 and 4 focus on whether the set of MUBs in dimension d can be extendible or not, and the last two contributory Chapters 5 and 6 focus on the construction of MUBs and AMUBs in specific dimensions.

In this regard, before briefing the contributions of this thesis, we begin by presenting the underlying problems that form the basis of our study.

1.1 Preliminaries on MUBs

For every quantum system, there is an association of complex finite-dimensional Hilbert space with that system. Initially, we adopt this formalism for convenience, as to study quantum states and operators. To proceed further in this direction, we need to define a few basic terms, notations, and concepts.

The inner product of the vectors $|a\rangle$ and $|b\rangle$ is often denoted as $\langle a|b\rangle$, and we will use this notation here.

Definition 1.1.1. *Two orthonormal bases in the in* $\mathbb{C}^d$, $\{|u_1\rangle, \ldots, |u_d\rangle\}$ *and* $\{|v_1\rangle, \ldots, |v_d\rangle\}$ *are called Mutually Unbiased if*

$$|\langle u_i|v_j\rangle| = \frac{1}{\sqrt{d}}, \ \forall i, j \in \{1, 2, \ldots, d\}.$$

Similarly, some r *orthonormal bases are called Mutually Unbiased Bases if they are pairwise Mutually Unbiased.*

Consider an example here for $d = 2$. The following are three MUBs in $\mathbb{C}^2$:

$$\begin{aligned} M_0 &= \{|0\rangle, |1\rangle\}, \\ M_1 &= \left\{\frac{|0\rangle + |1\rangle}{\sqrt{2}}, \frac{|0\rangle - |1\rangle}{\sqrt{2}}\right\}, \\ M_2 &= \left\{\frac{|0\rangle + i|1\rangle}{\sqrt{2}}, \frac{|0\rangle - i|1\rangle}{\sqrt{2}}\right\} \end{aligned}$$

if one considers two vectors $|u\rangle, |v\rangle$ from a any basis M_i, then by definition $|\langle u|v\rangle| = 0$. On the other hand, if $|u\rangle$ is from M_i, and $|v\rangle$ is from M_j, with $i \neq j$, then $|\langle u|v\rangle| = \frac{1}{\sqrt{2}}$.

The only (naive) known generic lower bound on the number of MUBs is $p^r + 1$, where p^r is the smallest prime power in the prime decomposition of the dimension d. Even after significant efforts in this direction for more than half a century, there is no evidence of beating the lower bound for composites that are not a power of a prime. Thus, this problem remains quite interesting. As we have pointed out earlier, one may refer to [53, Problem 13], where this question takes a place among the essential open problems in quantum information theory. Even, we do not know the exact number of MUBs in the smallest composite dimension, six which is not a power of a prime. However, the number of MUBs in $\mathbb{C}^6$ is known to be no more than seven and no less than three. We can get at least three MUBs for any d in $\mathbb{C}^d$ by the known lower bound. However, which of the numbers in between is the exact number of MUBs in dimension six is unknown (apart from the fact that it cannot be six, following from a general result by Weiner [81]). Zauner first conjectured that there are no more than three MUBs in dimension six [87], and this conjecture has not been resolved to date, despite substantial efforts.

We like to clarify here that, there are cases where this known lower bound has been improved [84] by exploiting the combinatorial structure, such as Mutually Orthogonal Latin Squares (MOLS) and Hadamard matrices. For example, we have at least six MUBs in $d = (26)^2$; however, the lower bound gives only five MUBs.

From the above discussion, it is evident that constructing an increasing number of mutually unbiased bases is immensely challenging, if not altogether elusive.

Next, let us present our thesis plan.

1.2 Thesis Plan

Next in Chapter 2, we provide a detailed explanation of the background materials. Let us now refer to the contributory chapters.

1.2.1 Contribution 1: Inextendibility of the set of three MUBs which are product bases in $\mathbb{C}^6$

In our first contributory chapter (Chapter 3), we have given a combinatorial proof that it's impossible to extend the set of three mutually unbiased product bases in $\mathbb{C}^6$ with certain constraints. We need to consider the following definition in this regard.

Definition 1.2.1. *A unit vector $|\psi\rangle \in \mathbb{C}^d$ with dimension $d = d_1 d_2$ can be written as a product state if $|\psi\rangle = |a\rangle \otimes |b\rangle$ where $|a\rangle \in \mathbb{C}^{d_1}$ and $|b\rangle \in \mathbb{C}^{d_2}$.*

Definition 1.2.2. *An orthonormal basis B of the space $\mathbb{C}^d$ with dimension $d = d_1 d_2$ is a product basis if each basis vector can be written in the form of $|a\rangle \otimes |b\rangle \in \mathbb{C}^d$, with states $|a\rangle \in \mathbb{C}^{d_1}$, and $|b\rangle \in \mathbb{C}^{d_2}$.*

Applying the above definitions and considering U as a unitary matrix (of order six) whose columns are vectors of the product basis B, we have provided an explicit form of U in certain instances. This can be formally stated as follows:

A unitary matrix U as a product basis can be represented as,

$$U = A_1 \otimes B_1 + A_2 \otimes B_2$$

where, $A_1 = \begin{bmatrix} |a_1\rangle & \mathbf{0} \end{bmatrix}, A_2 = \begin{bmatrix} \mathbf{0} & |a_2\rangle \end{bmatrix}$, such that $|a_1\rangle, |a_2\rangle \in \mathbb{C}^2$ and B_1, B_2 are unitary matrices of order three.

In the final part of this work, we prove that if U can be represented as above, i.e; $U = A_1 \otimes B_1 + A_2 \otimes B_2$, then it can't be a fourth MUB as an extension of three mutually unbiased bases in $\mathbb{C}^6$.

This chapter is based on the research work available at [55].

1.2.2 Contribution 2: On Obtaining New MUBs by Finding Points on Complete Intersection Varieties over $\mathbb{R}$

Chapter 4 presents the second contributory work of this thesis. In this chapter, we have studied the extendibility of a given set of MUBs from the point of view of algebraic geometry and commutative algebra. We investigated the ideals of the affine algebraic variety derived

from a given set of k MUBs in any generic dimension d, ($k \leq d$) and established a few notable results which are related to the complete intersection of ideals.

The system of polynomial equations derived from the MUB extension problem defines an affine algebraic variety in $\mathbb{R}^{2d^2}$. Thus, one can apply the classical Hilbert's Nullstellensatz to verify the existance of points in this variety, and hence the solution to the MUB extension problem. The structure of this variety, its dimension, degree, and number of irreducible components encodes crucial information about the existence and uniqueness of possible extensions. When the ideal generated by these polynomials forms a complete intersection, the variety has codimension equal to the number of generators, suggesting a well-constrained geometric object with a finite number of isolated points as solutions. This corresponds to a finite and potentially classifiable set of extensions. As an application of this method, we recover the solution to this problem when $d = 2$, as it is not possible to have four MUBs in $\mathbb{C}^2$.

Additionally, in this work, we consider extending the result of [5, Theorems 3.2 and 3.4] under the hypothesis related to existence of normal matrices. We prove that there is an one-to-one correspondence between the MUBs and the maximal commuting classes (bases) of orthogonal normal matrices in $\mathbb{C}^d$. It means that for m MUBs in $\mathbb{C}^d$, there are m commuting classes each consisting of d commuting orthogonal normal matrices. The existence of maximal commuting basis for $\mathcal{M}_d(\mathbb{C})$ ensures the complete sets of MUBs in $\mathcal{M}_d(\mathbb{C})$.

This chapter is based on our research work available at [6].

1.2.3 Contribution 3: A parametric Class of Mutually Unbiased Bases Using Resolvable Block Designs

Chapter 5 presents the third contributory work of this thesis. In this chapter, we have parametrised a set of MUBs for a square dimension $d = s^2$, which was constructed in [57]. Let us outline the constructions for MUBs. We take the dimension $d = s^2$, and consider the RBD having s^2 entities. To construct RBD, we start with MOLS of order s. For each MOLS of order s, we have $MOLS(s) + 2$ parallel classes in the RBD of order s^2. We convert each of the parallel classes into orthonormal bases (MUBs) using the Hadamard matrix of order s. If there exists a real Hadamard matrix of order s, then we will get only real MUBs. So, we have $MOLS(s) + 2$ real MUBs in dimension $d = s^2$, in which the first one is an identity

matrix.

We introduce affine parameters (phases) through diagonal and permutation unitary transformations and then pull out the redundant parameters only from columns (not rows) into each of the rest of the $MOLS(s)+1$ so that MUB structures remain preserved. In this way, we have introduced at least $s(s-1)$ many free parameters in each of the $MOLS(s)+1$ many MUBs that a global unitary operation cannot absorb. Further, we also present directions to generalize this for dimensions of the form $d = k \times s$.

This chapter is based on the research publication [54].

1.2.4 Contribution 4: Construction of Approximate Real MUBs for dimension which are not a multiple of four

Chapter 6 presents the final contributory work of this thesis. In this chapter, we have constructed Approximate Real Mutually Unbiased Bases (ARMUBs) in some specific dimensions d which are not mutiples of four. Let's first define the AMUBs in this regard.

Definition 1.2.3. *A set of r orthonormal bases $B_i, 1 \leq i \leq r$ of $\mathbb{C}^d$ are defined as β-AMUBs (Approximate MUBs) if for two vectors $v_1 \in B_{i_1}$ and $v_2 \in B_{i_2}$ ($i_1 \neq i_2$),*

$$|\langle v_1|v_2\rangle| \leq \frac{\beta}{\sqrt{d}}.$$

As it's not possible to get a pair of real MUB in odd dimensions. We have at least a pair of real MUB in only those dimensions that are multiples of four. In this work, we construct at least $\lceil\sqrt{d}\rceil$ many ARMUBs for specific odd dimensions d of the form $d = (4n-t)s$, $t = 1, 2, 3$, where n is a natural number and s is an odd prime power. Our method exploits any available $4n \times 4n$ real Hadamard matrix H_{4n} (conjectured to be true). It uses this to construct an orthogonal matrix Y_{4n-t} of size $(4n-t) \times (4n-t)$, such that the absolute value of each entry varies a little from $\frac{1}{\sqrt{4n-t}}$. In our construction, the absolute value of the inner product between any pair of basis vectors from two different ARMUBs will be $\leq \frac{1}{\sqrt{d}}(1 + O(d^{-\frac{1}{2}})) < 2$, for proper choices of parameters, the class of dimensions d being infinitely large, so $\beta = \frac{1}{\sqrt{d}}(1 + O(d^{-\frac{1}{4}}))$.

This chapter is based on our research work available at [56].

Chapter 7 concludes the thesis with a summary of the results and several directions towards the open questions that might be interesting for future research efforts.

1.3 Prerequisites

The reader is expected to have the mathematical background to learn or recall basic concepts up to the level of undergraduate mathematics, if necessary. In this regard, it is assumed that the reader is familiar with abstract as well as linear algebra, and has a basic understanding of combinatorial designs. However, we will provide more detailed explanations of the more involved algebraic and combinatorial structures in Chapter 2. The necessary background will be developed progressively in the following sections, with concepts introduced as and when required.

1.4 Conclusion

This thesis revolves around studying Mutually Unbiased Bases from perspectives of algebraic techniques and combinatorial designs. This is mainly structured in two parts. The first part focuses on the existence and extendibility of MUBs. We have explored a novel combinatorial proof towards the in-extendibility of the set of three MUBs which are product bases in dimension six with certain constraints. Additionally, we investigated the ideals of the affine algebraic variety derived from a given set of r MUBs in any generic dimension d, $(r \leq d)$ and established few results which are related to complete intersection of ideals. Moreover, we pointed out in [5] that there is a one-to-one correspondence between MUBs and the maximal commuting classes (bases) of orthogonal normal matrices in $\mathcal{M}_n(\mathbb{C})$.

The second part has two contributions. In the first one we parameterize set of MUBs for dimension $d = s^2$, which has been constructed using RBDs and Hadamard matrices. The prime idea was to introduce parameters (phases) through diagonal, to permute unitary transformations and then to pull out the redundant parameters only from columns (not rows) in such a way so that MUB structures remain preserved. In this way, we have introduced at least $s(s-1)$ many free parameters in each of the $MOLS(s)+1$ many MUBs from the set of $MOLS(s)+2$ many MUBs as one of them is Identity matrix. Then we consider the

construction of Approximate Real MUBs (ARMUBs) in certain dimensions $d = k \times s$, which is not a multiple of four and it can be expressed as the product of relatively two close factors k and s. Finally we conclude the thesis with a summary and future directions of research.

Chapter 2

Background

In this chapter, we briefly review existing research results related to Mutually Unbiased Bases and position our contributions in the broader context. As we have already discussed, the Mutually Unbiased Bases can be understood as an essential concept in quantum information theory. The mathematical framework for quantum information is a finite complex Hilbert space of dimension d. For every quantum system, there is an association of a complex finite-dimensional Hilbert space with that system. Initially, we adopt this formalism for convenience, as to study quantum states and operators. In this regard, let us present certain basic technical materials.

2.1 Basis definitions

In quantum information theory, a basis of a vector space $\mathbb{C}^d$ can be described by a unitary matrix of order d whose rows are orthonormal vectors in $\mathbb{C}^d$. Each row corresponds to a quantum state, and the entries of these vectors are complex numbers. We have followed standatd text [88].

We present the basic mathematical definitions that will be used throughout this thesis.

Definition 2.1.1 (**Vector Space:**). *A* vector space V *over the field of complex numbers* $\mathbb{C}$ *is a set of vectors that is closed under two operations: vector addition and scalar multiplication. Vector addition is associative and commutative, and there exists an identity element (called*

the zero vector*, denoted* 0*) as well as additive inverses for every vector in* V*. The set* V *is also closed under scalar multiplication by elements of* $\mathbb{C}$*, satisfying the following properties for all* $p, q \in \mathbb{C}$ *and all* $u, v \in V$ *as* $p(u+v) = pu + pv$, $(p+q)u = pu + qu$, $p(qu) = (pq)u$, *and* $1u = u$*, where* 1 *is the multiplicative identity in* $\mathbb{C}$*.*

Example 2.1.1. *The set* $\mathbb{C}^d = \{(z_1, z_2, \ldots, z_d) \mid z_i \in \mathbb{C} \text{ for all } i = 1, 2, \ldots, d\}$ *is a vector space over the complex number* $\mathbb{C}$*.*

This space satisfies all vector space axioms with scalars from $\mathbb{C}$*.*

Definition 2.1.2 (**Linearly Independent Vectors**:)**.** *A set of vectors* $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ *in a complex vector space* V *is said to be* linearly independent *if the only solution to the equation*

$$c_1\mathbf{v}_1 + c_2\mathbf{v}_2 + \cdots + c_k\mathbf{v}_r = \mathbf{0}$$

is $c_1 = c_2 = \cdots = c_r = 0$*, where each* $c_i \in \mathbb{C}$*.*

If there exists a nontrivial solution (i.e., some $c_i \neq 0$*), the vectors are said to be* linearly dependent*.*

Definition 2.1.3 (**Basis of a Vector Space**:)**.** *A set of vectors* $\{\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_r\}$ *in a complex vector space* V *is called a* basis *of* V *if:*

1. *The set is linearly independent.*
2. *The set spans* V*, i.e., every vector in* V *can be written as a linear combination of* $\mathbf{v}_1, \ldots, \mathbf{v}_r$*.*

Example 2.1.2. *If* $V = \mathbb{C}^d$*, the standard basis is the set* $\{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_d\}$*, where* $\mathbf{e}_i$ *is the vector with* 1 *in the* i*-th position and* 0 *elsewhere.*

Example 2.1.3. *Let* $V = M_d(\mathbb{C})$ *be the set of all complex* $d \times d$ *matrices. Then* V *is a vector space over* $\mathbb{C}$*.*

A standard basis for V *is the set*

$$\mathcal{B} = \{E_{ij} \mid 1 \leq i, j \leq d\},$$

where E_{ij} *is the matrix with a* 1 *in the* (i, j)*-th position and zeros elsewhere.*

Since there are d^2 *such matrices, the dimension of* V *is*

$$\dim M_d(\mathbb{C}) = d^2.$$

Definition 2.1.4 (**Inner product:**). *If* $|a\rangle, |b\rangle \in \mathbb{C}^d$ *then inner product of the vectors* $|a\rangle$ *and* $|b\rangle$ *is often denoted as* $\langle a, b\rangle$ *or,* $\langle a|b\rangle$.

Let $|a\rangle = (a_1, a_2, \ldots, a_d)$ *and* $|b\rangle = (b_1, b_2, \ldots, b_d)$ *are row vectors in* $\mathbb{C}^d$. *The* inner product *of* $|a\rangle$ *and* $|b\rangle$, *is defined as*

$$\langle a, b\rangle = \langle a|b\rangle = \sum_{i=1}^{d} a_i \, \overline{b_i},$$

where $\overline{b_i}$ *denotes the complex conjugate of* b_i.

However, if $|a\rangle, |b\rangle \in \mathbb{C}^d$ *are column vectors. Then,*

$$\langle a, b\rangle = \langle a|b\rangle = \sum_{i=1}^{d} \overline{a_i} \, b_i,$$

where $\overline{a_i}$ *denotes the complex conjugate of* a_i.

Definition 2.1.5 (**Orthogonality**:). *Two vectors* $\mathbf{u}, \mathbf{v} \in V$ *are said to be* orthogonal *if*

$$\langle \mathbf{u}, \mathbf{v}\rangle = 0.$$

Definition 2.1.6 (**Unitary Matrix**). *A matrix* U *is an* $d \times d$ *matrix with complex entries such that*

$$U^\dagger U = U U^\dagger = I.$$

Here, $U^\dagger$ *denotes the conjugate transpose of* U.

Remark 2.1.1. *An* orthogonal matrix *is the real analogue of a* unitary matrix.

Remark 2.1.2. *A Permutation matrix, which we denote by* P, *is a special class of unitary matrix which has entries from set* $\{0, 1\}$, *such that every row and column contain exactly one non zero entry. Note that Identity matrix is a permutation matrix.*

Remark 2.1.3. *Two unitary matrices* U_1 *and* U_2 *of same order, are said to be equivalent* $(U_1 \approx U_2)$ *if there exist diagonal unitary matrices* D_1, D_2 *and permutation matrices* P_1, P_2 *such that* $U_1 = D_1 P_1 U_2 P_2 D_2$. *Note that this is an* equivalence relation.

2.2 Hadamard Matrix

We begin by formally defining Hadamard matrices and reviewing some fundamental results and properties that will be relevant in subsequent discussions. We have followed the standard text [88] for this.

Definition 2.2.1 (**Complex Hadamard matrix:**). *A complex Hadamard matrix of order d with complex entries of modulus one such that*

$$H^\dagger H = HH^\dagger = dI.$$

Definition 2.2.2 (**Real Hadamard matrix:**). *A* real Hadamard matrix *of order d with entries from $\{1, -1\}$ such that $H^\top H = dI$.*

Remark 2.2.1. *We will simply say Hadamard matrix if it's real Hadamard matrix.*

Lemma 2.2.1. *There always exists a complex Hadamard matrix $F_d = (f_{jk})$ as $f_{jk} = \omega^{(j-1)(k-1)}$ for $1 \leq j, k \leq d$ and $d \geq 1$.*

Remark 2.2.2. *In Chapters 5 and 6, we see Hadamard matrix as a special class of unitary matrix. We define that as below.*

Definition 2.2.3 (**Hadamard matrix as a special class of unitary matrix:**). *An d-dimensional unitary matrix $H = (h_{ij}) : 1 \leq i, j \leq d$ is called Hadamard if $|h_{ij}| = \frac{1}{\sqrt{d}}$ for all $i, j \in \{0, 1, \ldots, d\}$.*

Remark 2.2.3. *Multiplying all elements of a row or a column of a Hadamard matrix by an arbitrary phase factor (a complex number of unit modulus) does not affect the Hadamard property of the matrix. Hence, any Hadamard matrix is equivalent (under row and column multiplications by phase factors) to one in which all entries in the first row and first column are 1. Such a matrix is called a* dephased Hadamard matrix*.*

Definition 2.2.4 (**Kronecker product:**). *Let $A = \big(a_{ij}\big) : 1 \leq i \leq n_1, 1 \leq j \leq m_1$ and $B = \big(b_{ij}\big) : 1 \leq i \leq n_2, 1 \leq j \leq m_2$ be two matrices of orders $(n_1 \times m_1)$ and $(n_2 \times m_2)$, respectively. Then the tensor (Kronecker) product between A and B is defined by an $(n_1 n_2 \times m_1 m_2)$ dimensional matrix, as follows.*

$$A \otimes B = \begin{pmatrix} a_{11}B & a_{12}B & \ldots & a_{1m_1}B \\ a_{21}B & a_{22}B & \ldots & a_{2m_1}B \\ \vdots & \vdots & \ddots & \vdots \\ a_{n_1 1}B & a_{n_1 2}B & \ldots & a_{n_1 m_1}B \end{pmatrix}.$$

In this regard, we have the following lemmas.

Lemma 2.2.2. *If H_1, H_2 are two Hadamard matrices of dimensions p and q, respectively. Then, $H_1 \otimes H_2$ is also a Hadamard matrix of order 'pq'.*

Lemma 2.2.3. $(A \otimes B)^\dagger = A^\dagger \otimes B^\dagger$.

Lemma 2.2.4. $(A \otimes B)(C \otimes D) = AC \otimes BD$*; given A and C have same dimension, and B and D have same dimension (dimension compatibility is there for matrix multiplication.)*

Remark 2.2.4 (**Sylvester construction:**)**.** *Hadamard matrices H_{2^k}, of order $2k$ for all k, can be constructed recursively using lemma 2.2.2 as $H_{2^k} = H_2 \otimes H_{2^{k-1}}$.*

Conjecture 2.2.1 (**Hadamard conjecture**:)**.** *There exists a Hadamard matrix for every order d, if $4|d$.*

Remark 2.2.5. *As of now, the Hadamard conjecture holds for all orders up to* 664*.*

2.2.1 Affine Parametrisation of Complex Hadamard Matrices

The concept of parametrisation is a powerful method to obtain new Hadamard matrices. It has been well studied in the literature by Haagerup [36], Dita [29], and others. If a Hadamard matrix has independent parameters, then there exist continuous inequivalent Hadamard matrices. Since the absolute value of all the entries of the Hadamard matrix is one, the independent parameter occurs in the phase of the entries of the Hadamard matrix. All Hadamard matrices lying on this continuum are collectively referred to as the family of Hadamard matrices, stemming from a starting point, which is by convention taken as the dephased Hadamard matrix, i.e., all the entries of the first row and first column are 1. The family is Affine if there exist a set of $H(\mathcal{R})$, stemming from a dephased Hadamard matrix, associated with the subspace $\mathcal{R}$ of the real space of $d \times d$ matrix, with zero in the first row and column such that $H(\mathcal{R}) = \{H \circ \exp(\iota R) : R \in \mathcal{R})$. Here $\circ$ denotes Hadamard product and $R \in \mathbb{R}^{d^2}$. We say that a Hadamard matrix $H(\mathcal{R})$ is an m-parameter affine family if R contains m free parameters and generates an m-dimensional subspace of $\mathcal{R}$, i.e $dim(R) = m$. Thus, this implies that the phases are a linear combination of the variables. Moreover, if m is the dimension of the subspace of R generated by the linear combination of the variables,

then H is called an m-parameter affine family. Note that m is essentially the number of independent linear combinations of the variables occurring in the phases of the entries of H.

With this background, let us now move towards the basics of MUBs.

2.3 Mutually Unbiased Bases

Let us revisit the example from the previous chapter for dimension $d = 2$, where the following three mutually unbiased bases(which have been defined in the last chapter) were considered:

$$\begin{aligned} M_0 &= \{|0\rangle, |1\rangle\}, \\ M_1 &= \left\{ \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle) \right\}, \\ M_2 &= \left\{ \frac{1}{\sqrt{2}}(|0\rangle + i|1\rangle), \frac{1}{\sqrt{2}}(|0\rangle - i|1\rangle) \right\}. \end{aligned}$$

In standard notation, the computational basis states are expressed as column vectors:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}.$$

Using this representation, we can express the three MUBs in dimension 2 as:

$$M_0^{(2)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M_1^{(2)} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad M_2^{(2)} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}.$$

Here, $M_0^{(2)}$ is simply the identity matrix. The matrix $M_1^{(2)}$ is the normalised version of the Hadamard matrix H_2, which is frequently encountered in quantum computing.

2.3.1 Connection between MUBs and Hadamard matrices

Mutually unbiased bases are orthonormal bases of $\mathbb{C}^d$, which can be viewed as unitary matrices of order d. So, each vector of an orthonormal basis can be seen as a column vector of a unitary matrix. Therefore, set of r MUBs in $\mathbb{C}^d$, can be represented as set of r unitary matrices $\{M_1, M_2, \ldots, M_r\}$. If we do a unitary transformation from left (multiplying by a

unitary matrix from left) to this set of r MUBs, then the new set will also be an r set of MUBs. By left-multiplying each matrix in the set by M_1^{-1}, we obtain following a new set of MUBs,

$$\{I, M_1^{-1}M_2, M_1^{-1}M_3, \ldots, M_1^{-1}M_r\}.$$

Since $M_1^{-1}M_j = \frac{1}{\sqrt{d}}H_j$, where H_j is a Hadamard matrix of order d, the set becomes:

$$\{I, \tfrac{1}{\sqrt{d}}H_2, \ldots, \tfrac{1}{\sqrt{d}}H_r\},$$

which also form a set of r MUBs, also $\frac{1}{\sqrt{d}}H_i^\dagger H_j$ are complex Hadamard matrices for every $2 \leq i < j \leq r$.

Definition 2.3.1 (**Mutually Unbiased Hadamard Matrices:**). *A pair of Hadamard matrix (H_i, H_j) is called mutually unbiased if*

$$\frac{1}{\sqrt{d}}H_i^\dagger H_j = H_k$$

Where H_k is another Hadamard matrix. A set $\{H_1, H_2, \ldots H_r\}$ of r Hadamard matrices is Mutually Unbiased Hadamard Matrices (MUHM) if every pair is unbiased.

One can refer to [9, 19, 44] for MUBs and Hadamard connection.

in this regard, we have the following definition for equivalent sets of MUBs:

2.3.2 Equivalent Sets of MUBs

Two sets of Mutually Unbiased Bases (MUBs), $\{M_1, M_2, \ldots, M_r\}$ and $\{N_1, N_2, \ldots, N_r\}$, are said to be *equivalent*, denoted by

$$\{M_1, M_2, \ldots, M_r\} \sim \{N_1, N_2, \ldots, N_r\},$$

if one can be obtained from the other by a combination of the following unitary transformations:

(1) **Global Unitary Transformation:** Left multiplication by a unitary matrix U:

$$\{M_1, M_2, \ldots, M_r\} \mapsto \{UM_1, UM_2, \ldots, UM_r\}.$$

(2) **Column-wise Phase Changes:** Right multiplication of each basis matrix M_i by a diagonal unitary matrix D_i:

$$\{M_1, M_2, \ldots, M_r\} \mapsto \{M_1 D_1, M_2 D_2, \ldots, M_r D_r\}.$$

(3) **Column Permutations:** Right multiplication of each basis matrix M_i by a permutation matrix P_i:

$$\{M_1, M_2, \ldots, M_r\} \mapsto \{M_1 P_1, M_2 P_2, \ldots, M_r P_r\}.$$

These operations preserve the mutual unbiasedness property among the bases, and hence the resulting sets are considered equivalent.

Example 2.3.1. *We give an explicit example of two* inequivalent *pairs of mutually unbiased bases in dimension $d = 4$.*

Let I_4 denote the standard basis of $\mathbb{C}^4$. Recall that a pair (I_4, H) forms a pair of mutually unbiased bases if and only if H is a 4×4 complex Hadamard matrix.

Pair 1 *Define*

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

Then (I_4, H_S) is a pair of mutually unbiased bases.

Pair 2 *Define*

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

Then (I_4, H_F) is also a pair of mutually unbiased bases.

These two pairs are inequivalent*. Indeed, H_S is equivalent to a real Hadamard matrix, whereas H_F is not equivalent to any real Hadamard matrix, as it necessarily contains non-removable complex phases. Hence the pairs (I_4, H_S) and (I_4, H_F) are not related by unitary transformations, permutations, and phase multiplications, and therefore form inequivalent pairs of mutually unbiased bases.*

2.3.3 Challenges in Composite (Not a power of a prime) Dimensions

The existence of a complete sets of MUBs in composite dimensions d which are not a power of a prime is still a central problem in the theory of MUBs. So, the Construction of the complete sets remains open. There are a few constructions for a complete sets of MUBs in dimensions d, which are a prime power [5, 85]. However, the non prime power case remains elusive; nevertheless, it is easy to obtain a lower bound on the number of MUBs here as follows.

Lemma 2.3.1. *Let us Assume that there is r_1 and r_2 MUBs in $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, respectively. Then there is at least $min\{r_1, r_2\}$ MUBs in $\mathbb{C}^{d_1 d_2}$.*

Proof. Let $r = min\{r_1, r_2\}$ be such that there are r MUBs in both $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$. Let

$$\{I, \tfrac{1}{\sqrt{d_1}}H_2, \ldots, \tfrac{1}{\sqrt{d_1}}H_r\} \text{ and } \{I, \tfrac{1}{\sqrt{d_2}}K_2, \ldots, \tfrac{1}{\sqrt{d_2}}K_r\}$$

be MUBs in $\mathbb{C}^{d_1}$ and $\mathbb{C}^{d_2}$, respectively. Then the following set

$$\{I_{d_1} \otimes I_{d_2}, \frac{1}{\sqrt{d_1 d_2}}H_2 \otimes K_2, \cdots, \frac{1}{\sqrt{d_1 d_2}}H_r \otimes K_r\}$$

is collection of r MUBs in $\mathbb{C}^{d_1 d_2}$. □

We provide an example of three MUBs $\mathbb{C}^6$.

Example 2.3.2. *Let*

$$M_0^2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad M_1^2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad M_2^2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ i & -i \end{bmatrix}$$

be three mutually unbiased bases in $\mathbb{C}^2$, and

if $\omega = e^{2\pi i/3}$, then four MUBs in $\mathbb{C}^3$ as:

$$M_0^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad M_1^3 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix},$$

$$M_2^3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{bmatrix}, \quad M_3^3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{bmatrix}.$$

Now, we construct three MUBs, say (M_0^6, M_1^6, M_2^6) *in* $\mathbb{C}^6$ *by taking all three MUBs from* $\mathbb{C}^2$ *and any three MUBs (out of four) from* $\mathbb{C}^3$*, say* M_0^3, M_1^3, M_2^3*:*

$$M_0^6 = M_0^2 \otimes M_0^3, \quad M_1^6 = M_1^2 \otimes M_1^3, \quad M_2^6 = M_2^2 \otimes M_2^3.$$

Corollary 2.3.1. *There exists at least a triplet of mutually unbiased bases in* $\mathbb{C}^d$ *for all* $d \geq 3$*.*

Remark 2.3.1. *It is worth noting that the above construction is the simplest known method for constructing MUBs in composite dimensions that are not powers of a prime. However, there exist a few other constructions for certain specific dimensions as well [16]. For a detailed discussion on the equivalence of various MUB constructions, the reader is referred to [45].*

2.3.4 Construction of a complete sets of MUBs in prime dimensions

Several known methods in the literature exist for constructing a complete sets of mutually unbiased bases for dimensions that are a power of a prime. Ivanović [43] provided the first construction of a complete sets of MUBs in a prime dimension. Later, Wootters and Fields [85] extended this by presenting a construction for a complete sets of MUBs for dimensions that are a power of a prime. In this section, we present the construction due to Bandyopadhyay *et al.* [5], specifically for the case of only prime dimension.

The core of this construction is the following two theorems from [5].

Theorem 2.3.1. *Let* $B_1 = \{|u_1\rangle, |u_2\rangle, \cdots, |u_d\rangle\}$ *be an orthonormal basis in* $\mathbb{C}^d$*. Suppose that there is a unitary operator* U *such that* $U|u_j\rangle = \alpha_j |u_{j+1}\rangle$*, where* $|\alpha_j| = 1$ *and* $|u_{d+1}\rangle = |u_1\rangle$*. If* $B_2 = \{|v_1\rangle, |v_2\rangle, \cdots, |v_d\rangle\}$ *be an orthonormal basis which is eigenvectors of* U*, then* B_1 *and* B_2 *are pair of MUB.*

Theorem 2.3.2. *If d is any prime and the vectors $\{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$ is the standard basis of $\mathbb{C}^d$, then the set of eigenvectors of the following unitary matrices*

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

form a set of $d+1$ MUB; where X_d and Z_d over $\mathbb{C}^d$ are unitary matrices as given below:

$$X_d |j\rangle = |j+1\rangle \text{ and } Z_d |j\rangle = \omega^j |j\rangle \text{ such that } X_d (Z_d)^k |j\rangle = (\omega^k)^j |j+1\rangle .$$

where ω is a dth root of unity; i.e; $\omega = e^{\frac{2\pi i}{d}}$.

Example 2.3.3. *The set of eigenvectors of the following unitary matrices form a set of MUB for $\mathbb{C}^3$.*

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

2.4 Product state and Product basis

Definition 2.4.1 (**Unit vector as product state:**). *A unit vector (pure state) $|\psi\rangle \in \mathbb{C}^{d_1 d_2}$ is said to be in a product state if*

$$|\psi\rangle = |a\rangle \otimes |b\rangle ,$$

where $|a\rangle \in \mathbb{C}^{d_1}$ and $|b\rangle \in \mathbb{C}^{d_2}$.

Example 2.4.1. *Let*

$$|a\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad |b\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \in \mathbb{C}^2$$

Then the joint state is

$$|\psi\rangle = |a\rangle \otimes |b\rangle = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \in \mathbb{C}^4.$$

This unit vector is a product state.

Definition 2.4.2 (**Unitary matrix as product basis**:). *An orthonormal (unitary) basis B of the space $\mathbb{C}^d$ with dimension $d = d_1 d_2 \cdots d_n$ is a product basis if each basis vector can be written in the form of $|v^1\rangle \otimes |v^2\rangle \otimes \cdots \otimes |v^n\rangle \in \mathbb{C}^d$, with states $|v^r\rangle \in \mathbb{C}^{d_r}, r = 1, 2, \cdots, n$.*

Example 2.4.2. *Let*

$$U_2 = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}, \quad U_3 = \frac{1}{\sqrt{3}}\begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \quad \textit{where } \omega = e^{2\pi i/3}.$$

Then the unitary matrix of order six as a product basis is given by

$$U = U_2 \otimes U_3 = \frac{1}{\sqrt{6}}\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \omega & \omega^2 & 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega & 1 & \omega^2 & \omega \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \omega & \omega^2 & -1 & -\omega & -\omega^2 \\ 1 & \omega^2 & \omega & -1 & -\omega^2 & -\omega \end{bmatrix}.$$

Each column of this matrix U is a product state. But if we consider a unitary matrix (basis) as a product basis of $\mathbb{C}^{pq}$, then it's not always possible to write $U = A \otimes B$ such that $A \in \mathbb{C}^p, B \in \mathbb{C}^q$. For a detailed study, please look at chapter 3.

Now let us consider a unitary matrix, which is not a product basis.

Example 2.4.3. *Define the 6×6 matrix*

$$U = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 & -1 & 0 \\ 0 & 0 & 1 & 0 & 0 & -1 \end{pmatrix}.$$

The columns of U are orthonormal, and hence U is a unitary matrix. Each column vector is of the form

$$\frac{1}{\sqrt{2}}\big(|0\rangle \otimes |j\rangle \pm |1\rangle \otimes |j\rangle\big), \quad j = 0, 1, 2,$$

which is entangled with respect to the bipartition $\mathbb{C}^2 \otimes \mathbb{C}^3$. Therefore, the orthonormal basis defined by U is not a product basis.

2.5 Combinatorial Designs and Mutually Unbiased Bases (MUBs)

A *combinatorial design*, or a *design*, refers to an arrangement of elements from a given set into subsets that satisfy certain specified conditions. We begin by formally defining a design. We have followed the standard textbook [75] for this purpose.

Definition 2.5.1. *A design is a pair (X, A) satisfying the following:*

1. *X is a set of elements, referred to as* points*, and*
2. *A is a collection of non-empty subsets of X, called* blocks*.*

A design is termed *simple* if no block is repeated within the collection A. In this thesis, we confine our study to simple designs only.

There are several classes of designs, but we focus here on two particular types, the *Resolvable Block Design (RBD)* and the *Latin square*.

Definition 2.5.2 (**Resolvable Block Design**)**.** *Given a design (X, A), a* parallel class *is a subset of disjoint blocks in A whose union equals X. If the set A can be partitioned into $r \geq 1$ such parallel classes, then the design (X, A) is said to be a* Resolvable Block Design (RBD)*.*

Example 2.5.1. *Consider the combinatorial designs (X, A_1) and (X, A_2) defined as follows:*

- $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$,
- $A_1 = \{(1, 2), (2, 3, 4), (5, 6, 7), (1, 8, 6), (2, 5), (6, 7), (2, 6, 8)\}$, *and*
- $A_2 = \{(1, 2, 3), (2, 4, 6), (3, 5, 8), (6, 8), (1, 7), (4, 5, 7)\}$.

The design (X, A_2) qualifies as a resolvable design since A_2 can be partitioned into two parallel classes:

$$P_1 = \{(1, 2, 3), (6, 8), (4, 5, 7)\} \quad \textit{and} \quad P_2 = \{(1, 7), (2, 4, 6), (3, 5, 8)\},$$

each consisting of disjoint subsets whose union equals X. Thus, P_1 and P_2 constitute a resolution of A_2. In contrast, the design (X, A_1) is not resolvable as it lacks such a resolution.

Definition 2.5.3 (**Latin Squares and Mutually Orthogonal Latin Squares**). *A* Latin square *of order s is an $s \times s$ array filled with s distinct symbols (typically the integers $1, 2, \ldots, s$), such that each symbol appears exactly once in every row and every column.*

Two Latin squares L_1 and L_2 of the same order s are said to be mutually orthogonal *if, when superimposed to form ordered pairs $(L_1(i,j), L_2(i,j))$, all s^2 resulting pairs are distinct.*

Example 2.5.2. *Consider the following Latin squares of order 3:*

$$L_1 = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix} \quad L_2 = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

Each number from 1 to 3 appears exactly once in each row and column in both L_1 and L_2, confirming that they are Latin squares of order 3.

Example 2.5.3 (**Mutually Orthogonal Latin Squares of Order 3**). *Let us now superimpose the entries of L_1 and L_2 to obtain the ordered pairs:*

$$\begin{bmatrix} (1,1) & (2,3) & (3,2) \\ (2,2) & (3,1) & (1,3) \\ (3,3) & (1,2) & (2,1) \end{bmatrix}$$

Since all 9 ordered pairs are distinct, L_1 and L_2 are mutually orthogonal Latin squares.

If there exists a collection of w Latin squares of order s, denoted $\{L_1, L_2, \ldots, L_w\}$, such that each pair is mutually orthogonal, then the set is referred to as a *set of Mutually Orthogonal Latin Squares (MOLS)* of order s, or simply w-MOLS(s).

Let $N(s)$ denote the maximum number of mutually orthogonal Latin squares of order s. Determining $N(s)$ for arbitrary values of s remains an open problem. However, it is known that $N(s) \leq s - 1$ for all s. When equality holds, i.e., when $N(s) = s - 1$, we say there exists a *complete sets* of MOLS(s). Complete sets are known to exist when s is a power of a prime [75, Section 6.4], but for values of s that are not prime powers, the value of $N(s)$ is significantly smaller.

A comprehensive table listing the best-known values of $N(s)$ for $s < 10000$ is provided in [2]. It has been shown that there exists a constant n_0 such that for all $s \geq n_0$, we have:

$$N(s) \geq \frac{1}{3} s^{\frac{1}{91}} \text{ [26]},$$

which was later improved by Wilson [83] to:

$$N(s) \geq s^{\frac{1}{17}}.$$

A further refinement appears in [84, Section 4], where the lower bound exponent was improved to $\frac{1}{14.8}$.

Hence, while $N(s) \to \infty$ as $s \to \infty$, a complete sets (i.e., $N(s) = s - 1$) only exists when s is a power of a prime. Additionally, it is worth noting that the existence of an affine plane of order q is equivalent to the existence of $(q-1)$ MOLS(q) [75, Theorem 6.32]. A concise survey on constructions of MOLS can be found in [27]. For combinatorial designs, refer to [2, 12, 13, 14, 15].

In this context, we recall the following result from [60], which is derived from the results in [84].

Theorem 2.5.1. *Consider a resolvable block design (RBD) (X, A) where $|X| = s^2$. Then, it is possible to construct $MOLS(s) + 2$ parallel classes, each consisting of s blocks of size s, such that any two blocks from different parallel classes intersect in exactly one point.*

2.5.1 Constructing MUBs in $\mathbb{C}^d$ Using Resolvable Block Designs (RBD)

We now present a construction method for mutually unbiased bases in $\mathbb{C}^d$ based on resolvable block designs.

Construction 2.5.1. *1. Consider a design (X, A) where the elements of X correspond to orthonormal basis vectors in $\mathbb{C}^d$. These vectors will be interpreted as columns. That is, for $|X| = d$, we write*

$$X = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\}, \quad \textit{with} \quad \langle\psi_i|\psi_j\rangle = \delta_{ij}.$$

The collection A consists of subsets of X, called blocks.

2. *Let $P = \{b_1, b_2, \ldots, b_s\}$ be a parallel class of (X, A), where each block b_i is a disjoint subset of X. Suppose there are r such parallel classes, whose union forms the full set A.*

3. *For a block* $b_t = \{|\psi_{t_1}\rangle, |\psi_{t_2}\rangle, \ldots, |\psi_{t_{n_t}}\rangle\} \in P$ *with size* $|b_t| = n_t$*, choose a unitary matrix* $u^t = (u^t_{i,j})$ *of size* $n_t \times n_t$*. Preferably, this matrix should be Hadamard or Hadamard-like.*

4. *Construct* n_t *new vectors using the vectors in* b_t *and the matrix* u^t *as follows:*

$$|\phi^t_i\rangle = \sum_{k=1}^{n_t} u^t_{i,k} |\psi_{t_k}\rangle, \quad \text{for } i = 1, 2, \ldots, n_t.$$

5. *Repeat the above step for each block* $b_j \in P$*, using a suitable* $n_j \times n_j$ *unitary matrix. Since* $\sum_{j=1}^{s} n_j = d$*, this procedure will produce exactly* d *orthonormal vectors.*

To illustrate this construction concretely, we present an example of building real MUBs in $\mathbb{R}^4$ using a resolvable $(4, 2, 1)$-BIBD. Let the set $X = \{1, 2, 3, 4\}$ represent the standard basis vectors of $\mathbb{R}^4$, and let the set of parallel classes $A = \{P_1, P_2, P_3\}$ be defined as:

$$P_1 = \{(1, 2), (3, 4)\}, \quad P_2 = \{(1, 3), (2, 4)\}, \quad P_3 = \{(1, 4), (2, 3)\}.$$

We apply the Hadamard matrix of order 2:

$$H_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

to each block of every parallel class, following the above construction. This yields three orthonormal bases corresponding to the three parallel classes:

$$M_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}, \quad M_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix}, \quad M_3 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix}.$$

The columns of M_1, M_2, and M_3 form orthonormal bases in $\mathbb{R}^4$, and together these constitute a set of three mutually unbiased bases. It is known that the maximum number of real MUBs in dimension $d = 4^s$, for $s \in \mathbb{N}$, is $\frac{d}{2} + 1$ [16]. Hence, for $d = 4$, the above construction achieves the maximum number of real MUBs. However, such maximality does not hold for arbitrary dimensions.

As observed, constructing mutually unbiased bases is a challenging problem in quantum information theory, especially in dimensions that are not powers of primes. To address this, one may consider relaxed variants such as *Approximate Mutually Unbiased Bases*. These approximate constructions retain many desirable features of exact MUBs while being more adaptable. We explore AMUBs in the next section.

2.6 Approximate Mutually Unbiased Bases

We now formally introduce the concept of Approximate Mutually Unbiased Bases, which serve as relaxed analogues of exact MUBs.

Definition 2.6.1 (**AMUBs**). *Let $\mathbb{C}^d$ be a complex vector space of dimension d. Consider two orthonormal bases:*

$$M_l = \left\{|\psi_1^l\rangle, |\psi_2^l\rangle, \ldots, |\psi_d^l\rangle\right\} \quad \textit{and} \quad M_m = \left\{|\psi_1^m\rangle, |\psi_2^m\rangle, \ldots, |\psi_d^m\rangle\right\},$$

in $\mathbb{C}^d$. The bases M_l and M_m are said to be approximately mutually unbiased *if*

$$\left|\langle\psi_i^l|\psi_j^m\rangle\right| \approx \frac{1}{\sqrt{d}} \quad \textit{for all } i, j \in \{1, 2, \ldots, d\}.$$

A collection of orthonormal bases $\mathbb{M} = \{M_1, M_2, \ldots, M_r\}$ in $\mathbb{C}^d$ is called a set of *Approximate Mutually Unbiased Bases* of size r if every pair of distinct bases in $\mathbb{M}$ satisfies the approximate unbiasedness condition. This approximation is intended to be as close as possible to the ideal value of $\frac{1}{\sqrt{d}}$, with minimal deviation.

If the bases in the collection are real (i.e., vectors in $\mathbb{R}^d$), the collection is referred to as a set of *Approximate Real Mutually Unbiased Bases*.

We now define two further refinements of approximate MUBs.

Definition 2.6.2 (β-**ARMUBs**). *A collection of r orthonormal bases M_i $(0 \leq i \leq r-1)$ in $\mathbb{R}^d$ is said to be a set of* β-Approximate Real MUBs (β-ARMUBs) *if, for every pair of distinct bases M_l and M_m, the following holds:*

$$\left|\langle\psi_i^l|\psi_j^m\rangle\right| \leq \frac{\beta}{\sqrt{d}} \quad \textit{for all } i, j \in \{1, 2, \ldots, d\}.$$

Remark 2.6.1. *In Chapter 6, we consider the setting* $\beta = \frac{1}{\sqrt{d}}(1 + O(d^{-1/4})) < 2$*, assuming appropriate parameter choices and for infinitely many values of* d*.*

Definition 2.6.3 (**Almost Perfect MUBs** [60])**.** *A collection of orthonormal bases* $\mathbb{M} = \{M_1, M_2, \ldots, M_r\}$ *is called a set of* Almost Perfect Mutually Unbiased Bases (APMUBs) *if the set of inner product magnitudes between vectors from different bases is*

$$\Delta = \left\{0, \frac{\beta}{\sqrt{d}}\right\},$$

where $\beta = 1 + O(d^{-\lambda}) \leq 2$ *for some real* $\lambda > 0$*. If the bases are real, the collection is referred to as a set of* Almost Perfect Real MUBs (APRMUBs)*.*

Example 2.6.1 (Example of an APMUB)**.** *We illustrate Definition 2.6.3 in the simplest nontrivial dimension* $d = 2$*.*

Let

$$M_1 = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

be the standard orthonormal basis of $\mathbb{C}^2$*.*

For a small real parameter ε*, define*

$$M_2 = \left\{ \begin{pmatrix} \cos\theta \\ \sin\theta \end{pmatrix}, \begin{pmatrix} -\sin\theta \\ \cos\theta \end{pmatrix} \right\}, \qquad \theta = \frac{\pi}{4} + \varepsilon.$$

It is straightforward to verify that M_2 *is an orthonormal basis of* $\mathbb{C}^2$*.*

For any $\mathbf{u} \in M_1$ *and* $\mathbf{v} \in M_2$*, we have*

$$|\langle \mathbf{u}, \mathbf{v} \rangle| \in \{|\cos\theta|, |\sin\theta|\}.$$

Using the Taylor expansions

$$\cos\left(\tfrac{\pi}{4} + \varepsilon\right) = \tfrac{1}{\sqrt{2}}\left(1 - \varepsilon + O(\varepsilon^2)\right), \qquad \sin\left(\tfrac{\pi}{4} + \varepsilon\right) = \tfrac{1}{\sqrt{2}}\left(1 + \varepsilon + O(\varepsilon^2)\right),$$

we obtain

$$|\langle \mathbf{u}, \mathbf{v} \rangle| = \frac{\beta}{\sqrt{2}}, \qquad \beta = 1 + O(\varepsilon).$$

Therefore, the set of inner product magnitudes between vectors from different bases satisfies

$$\Delta = \left\{0, \frac{\beta}{\sqrt{2}}\right\}, \qquad \beta \leq 2.$$

Hence, $\mathbb{M} = \{M_1, M_2\}$ *forms an example of an Almost Perfect Mutually Unbiased Basis (APMUB) in dimension* $d = 2$*. Since both bases are real, this also provides an example of an Almost Perfect Real MUB (APRMUB).*

Several constructions of approximate MUBs over both $\mathbb{C}^d$ and $\mathbb{R}^d$ have been developed. For a more detailed account of these constructions, the reader is referred to [23, 50, 59, 73].

Now, we shift our focus toward the algebraic structures that underpin the analysis of systems of polynomial equations, which naturally emerge in the study of Mutually Unbiased Bases in our contributory chapter 4. Specifically, we introduce key concepts from algebraic geometry and commutative algebra, such as ideals, affine varieties, and Gröbner bases. These tools play a crucial role in analyzing the ideals that arise from the algebraic relations governing MUBs and in understanding the solution space of the associated polynomial systems.

2.7 Algebraic Tools for Analyzing Systems of MUBs

In this section, we introduce the essential definitions from commutative algebra and algebraic geometry needed to study the ideals associated with MUBs. Our treatment follows the standard text [62], and although the definitions are given in a general context, we will focus on the case where the ring R is a polynomial ring over a field $\mathbb{K}$.

Definition 2.7.1. *Let* R *be a ring and let* $a \in R$*, with* $a \neq 0$*. The element* a *is called a* non-zero divisor *if for any* $b \in R$*, the equation* $ab = 0$ *implies that* $b = 0$*. If there exists some nonzero* $a \in R$ *for which* $ab = 0$ *for some nonzero* $b \in R$*, then* a *is a* zero divisor*. A ring* R *that does not contain any nonzero zero divisors is referred to as an* integral domain*.*

Definition 2.7.2. *Let* R *be a ring. An ideal* $I \subseteq R$ *is said to be a* prime ideal *if one of the following equivalent conditions holds:*

1. *The quotient ring* R/I *is an integral domain.*
2. *For any* $a, b \in R$*, if* $ab \in I$*, then at least one of* $a \in I$ *or* $b \in I$ *holds.*

We denote by Spec(R) the set of all prime ideals of R.

Given a ring R, consider a chain of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n.$$

The number n is called the *length* of this chain. The *Krull dimension* of R is defined as the supremum of all such lengths of chains in R.

For a prime ideal $P \subseteq R$, the *height* of P, denoted by $ht(P)$, is the maximum length of a chain of prime ideals ending at P, i.e.,

$$P_0 \subsetneq P_1 \subsetneq \cdots \subsetneq P_n = P.$$

One common way to quantify the complexity of an ideal is through its height.

Definition 2.7.3. *Let $I \subseteq R$ be an ideal. Its* height*, denoted by $ht(I)$, is defined as*

$$ht(I) = \min\{ht(P) \mid I \subseteq P \text{ and } P \in Spec(R)\}.$$

Definition 2.7.4. *A sequence of elements $\mathbf{x} = x_1, \ldots, x_n$ in R is called an R-*regular sequence *(or simply a* regular sequence*) if:*

1. *For each $1 \leq i \leq n$, the element x_i is a non-zero divisor in the quotient $R/(x_1, \ldots, x_{i-1})$.*
2. *The quotient $R/\mathbf{x}R$ is nonzero.*

The concept of a complete intersection originates in algebraic geometry. Informally, an ideal defining an affine variety is a complete intersection if it can be generated by the smallest possible number of elements relative to the variety's co-dimension—that is, the variety is the intersection of hypersurfaces corresponding to the generators of the ideal.

Definition 2.7.5. *Let $I \subseteq R$ be an ideal. We say that I is a* complete intersection *if it can be generated by a regular sequence.*

Complete intersection ideals have many desirable properties. For example, the following result shows that, under suitable conditions, complete intersections lead to Cohen–Macaulay rings.

Proposition 2.7.1. *Let $(R, \mathbf{m})$ be a Cohen–Macaulay local ring and let $I \subseteq R$ be an ideal. If I is a complete intersection, then the quotient ring R/I is Cohen–Macaulay.*

A cornerstone of commutative algebra and algebraic geometry is Hilbert's Nullstellensatz. We will use this theorem to translate the problem of extending a system of MUBs into one of analyzing an affine algebraic variety. Let $\mathbb{K}$ be a field and $\overline{\mathbb{K}}$ its algebraic closure. For a subset $\Phi \subseteq \mathbb{K}[x_1, \ldots, x_n]$, an n-tuple $\alpha = (a_1, \ldots, a_n)$ with $a_i \in \overline{\mathbb{K}}$ is called an *algebraic zero* of Φ if $f(\alpha) = 0$ for every $f \in \Phi$. We denote by $Z(\Phi)$ the set of all such algebraic zeros.

Theorem 2.7.1. *[62, Theorem 5.4]*

1. *If $\Phi \subseteq \mathbb{K}[x_1, \ldots, x_n]$ has no algebraic zeros, then the ideal generated by Φ contains 1.*
2. *For any $\Phi \subseteq \mathbb{K}[x_1, \ldots, x_n]$ and any $f \in \mathbb{K}[x_1, \ldots, x_n]$ that vanishes on every algebraic zero of Φ, there exist an integer $t \geq 1$, polynomials $g_i \in \mathbb{K}[x_1, \ldots, x_n]$, and $h_i \in \Phi$ such that*
$$f^t = \sum_i g_i h_i.$$

We now review the notion of Gröbner bases, a fundamental tool for many results in commutative algebra. The reader is referred to standard texts [39, 40] for more details. For the remainder of this chapter, let S denote a polynomial ring over the field $\mathbb{R}$ and let $Mon(S)$ be the set of all monomials in S. Recall that a *total order* on a set P is a partial order $\leq$ such that for any two elements $x, y \in P$, either $x \leq y$ or $y \leq x$. A *monomial order* on S is a total order $<$ on $Mon(S)$ satisfying:

1. For any monomial $u \in Mon(S)$ with $u \neq 1$, we have $1 < u$.
2. For any monomials $u, v \in Mon(S)$ with $u < v$, and any $w \in Mon(S)$, we have $uw < vw$.

Common examples of monomial orders are the lexicographical order and the reverse lexicographical order. In what follows, we fix a monomial order $<$ on S and use it in all subsequent definitions and results.

For a nonzero polynomial

$$f = \sum_{v \in Mon(S)} a_v v \quad (a_v \in \mathbb{R}),$$

the *support* of f, denoted by $Supp(f)$, is defined as the collection of monomials v for which $a_v \neq 0$. The *initial monomial* of f with respect to $<$, denoted by $in_<(f)$, is the largest monomial in $Supp(f)$ under the order $<$.

Definition 2.7.6. *Let $I \neq 0$ be an ideal of S. The* initial ideal *of I with respect to $<$ is defined as*

$$in_<(I) := \big(\{\, in_<(f) \mid f \in I \,\}\big).$$

Note that $in_<(I)$ is an ideal generated entirely by monomials.

Definition 2.7.7. *Let $I \neq 0$ be an ideal of S. A finite set of nonzero polynomials $\{f_1, f_2, \ldots, f_s\} \subseteq I$ is called a* Gröbner basis *of I with respect to $<$ if*

$$in_<(I) = (in_<(f_1), in_<(f_2), \ldots, in_<(f_s)).$$

While a Gröbner basis for I with respect to a given order always exists, it is not unique. The division algorithm for polynomials (with respect to a fixed set) provides a method for checking whether a given set forms a Gröbner basis; see, for example, [39, Thm 2.2.1].

A central theorem in the theory of Gröbner bases is Buchberger's Criterion, which provides a necessary and sufficient condition for a generating set to be a Gröbner basis. Before stating this, we recall the following definition. For any two monomials $u, v \in S$, let $lcm(u, v)$ denote their least common multiple.

Definition 2.7.8. *For nonzero polynomials $f, g \in S$, let c_f and c_g be the coefficients of $in_<(f)$ and $in_<(g)$ in f and g, respectively. The* S-polynomial *of f and g is defined by*

$$S(f, g) = \frac{lcm(in_<(f), in_<(g))}{c_f\, in_<(f)}\, f - \frac{lcm(in_<(f), in_<(g))}{c_g\, in_<(g)}\, g.$$

A polynomial f is said to *reduce to* 0 with respect to a set $\{f_1, \ldots, f_m\}$ if, under the division algorithm, the remainder after division by these polynomials is 0. The following lemma is essential in several later proofs.

Lemma 2.7.1. *[39, Lemma 2.3.1] Let $f, g \neq 0$ be polynomials and suppose that $in_<(f)$ and $in_<(g)$ are relatively prime; that is,*

$$lcm(in_<(f), in_<(g)) = in_<(f)in_<(g).$$

Then the S-polynomial $S(f, g)$ reduces to 0 with respect to $\{f, g\}$.

We now state Buchberger's Criterion, a fundamental result that characterizes Gröbner bases.

Theorem 2.7.2. *[39, Buchberger's Criterion] Let $I \neq 0$ be an ideal of S and let $G = \{f_1, f_2, \ldots, f_m\}$ be a generating set for I. Then G is a Gröbner basis for I with respect to $<$ if and only if for every pair $i \neq j$, the S-polynomial $S(f_i, f_j)$ reduces to 0 with respect to G.*

2.8 Conclusion

In this chapter, we have assembled the mathematical preliminaries needed for the remainder of the thesis. The background on combinatorial designs—such as Resolvable Block Designs (RBDs), Mutually Orthogonal Latin Squares (MOLS), and Hadamard matrices—combined with core concepts from algebraic geometry and commutative algebra, underpins our exploration of MUBs. We now proceed to the first main contribution in Chapter 3.

Chapter 3

Exploring the presence of 4-th MUB as a product basis in $\mathbb{C}^6$

As discussed in the previous chapters, the existence of a complete sets of mutually unbiased bases in $\mathbb{C}^d$, when d is not a power of a prime, remains one of the central open problems in the theory of MUBs. It is known that there can be at most $d+1$ MUBs in $\mathbb{C}^d$; hence, in dimension six, the maximum number of MUBs is seven. However, despite considerable effort, only three mutually unbiased bases have been explicitly constructed in $\mathbb{C}^6$.

Numerous attempts have been made to extend such MUB triplets to larger sets in dimension six, but the question of whether these triples can be extended remains unresolved. In this direction, we approached the problem from another perspective and analytically proved the inextendibility of triples of mutually unbiased *product* bases in $\mathbb{C}^6$ under specific assumptions. Although this problem has been previously studied, our method of analysis and proof technique is both simple and novel.

3.1 Introduction

For a brief overview, refer to Definition 1.1.1 in Chapter 1. In a given dimension d, it is well established that the maximum number of mutually unbiased bases is $d+1$ [85]. When this upper bound is achieved, the set is termed a *complete sets of MUBs*. For dimensions where d is a power of a prime, such complete sets of $d+1$ MUBs can always be constructed.

In the case of $\mathbb{C}^6$, it is known that at most seven and at least three MUBs can exist, but the exact number remains unknown. To date, only three mutually unbiased bases have been explicitly constructed in this space. Zauner conjectured that no more than three MUBs exist in dimension six [87], and this conjecture remains unproven despite extensive investigation.

The simplest construction demonstrating the existence of a lower bound on the number of MUBs can be found in Lemma 2.3.1 of Chapter 2. Beyond this, several alternative constructions have been proposed in the literature [44, 45]. The concept of a *product basis* is formally introduced in Definition 2.4.2 of Chapter 2.

Furthermore, it has been shown that if a complete sets of seven MUBs were to exist in $\mathbb{C}^6$, it could not include a triple consisting solely of product bases [64, 65]. This leads to a natural question: can any pair of MUBs in $\mathbb{C}^6$ always be extended to a triplet? The answer is negative. Brierley and Weigert [20] demonstrated that the MUB pair $(\mathbb{I}, S_6)$—where S_6 denotes a *spectral matrix* and is also an isolated Hadamard matrix—cannot be extended to form a triplet of MUBs.

3.1.1 Organization and contribution

In Section 3.2, we provide a form of a unitary matrix, as a product basis whose columns constitute a product state in dimension six. The formal definition of a product state and product basis can be found in Definitions 2.4.1 and 2.4.2 of Chapter 2. Building upon this assumption, we provide a form of unitary matrix in dimension six under certain constraints. Using this framework, we then analytically prove that such a unitary matrix cannot serve as a new member to extend a given triplet of mutually unbiased product bases.

Section 3.3 provides the concluding remarks for this chapter.

3.2 Unitary matrix as product basis in dimension 6

In this section, we have studied the form of a unitary matrix U of order six as a product basis.

Consider an orthonormal basis in $\mathbb{C}^6$, S as given by

$$S = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_6\rangle\},$$

Let us also assume that all vectors in this basis can be decomposed into the tensor product of a two-dimensional and a three-dimensional vector. So we have

$$|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle \;\; \forall i \in \{1, 2, \ldots, 6\}.$$

We can always represent such a basis as the column vectors of a unitary matrix. Let U be the unitary matrix whose column vectors are the vectors of this matrix. So we have

$$U = \begin{bmatrix} |\psi_1\rangle & |\psi_2\rangle & \ldots & |\psi_6\rangle \end{bmatrix}.$$

Let $A = \{|a_1\rangle, |a_2\rangle, \ldots, |a_6\rangle\}$ and $B = \{|b_1\rangle, |b_2\rangle, \ldots, |b_6\rangle\}$. Notice that here all $|a_i\rangle$s and all $|b_i\rangle$s need not be distinct. However, the orthonormality of the vectors $|\psi_i\rangle$ imposes a condition on vectors $|a_i\rangle \in \mathbb{C}^2$ and vectors $|b_i\rangle \in \mathbb{C}^3$, which is

$$\langle\psi_i|\psi_j\rangle = \langle a_i|a_j\rangle \langle b_i|b_j\rangle = \delta_{ij}, \tag{3.1}$$

which may limit the number of distinct vectors in A and B. So, we want to count how many distinct vectors are really required to construct such a basis S. Let there be n distinct elements in A and let $\bar{A} \subseteq A$ which contains all distinct elements of set A; $\bar{A} = \{|\bar{a}_1\rangle, |\bar{a}_2\rangle, \ldots, |\bar{a}_n\rangle\}$. We denote the cardinality of a set X by $|X|$, so $|\bar{A}| = n$. Notice that if there are two vectors in A, $|a_i\rangle$ and $|a_j\rangle$, such that $|a_i\rangle = c\,|a_j\rangle$ for some non-zero complex number c, then we can simply transform $|a_i\rangle \to |a_j\rangle$ and $|b_i\rangle \to c\,|b_i\rangle$ so that final vector $|\psi_i\rangle$ remains unaffected. Hence, we will NOT consider vectors of the form $|a_i\rangle$ and $|a_j\rangle$ to be distinct.

Since we construct the set $\bar{A}$ by taking all distinct elements of the set A, hence $n \leq 6$. Also notice that different $|\psi_i\rangle$ vectors can be constructed from same $|\bar{a}_i\rangle$ and different $|b_i\rangle$. For example, consider $|\psi_1\rangle = |\bar{a}_1\rangle \otimes |b_1\rangle$ and $|\psi_2\rangle = |\bar{a}_1\rangle \otimes |b_2\rangle$. Here, we have two different $|\psi_1\rangle$ and $|\psi_2\rangle$ with the same $|\bar{a}_1\rangle$ iff $|b_1\rangle$ and $|b_2\rangle$ are different. We use the word *association* to talk about tensor products in the following sense. We say a vector in $\mathbb{C}^2$, say $|a\rangle$, is *associated* with a vector in $\mathbb{C}^3$, say $|b\rangle$ iff $|a\rangle \otimes |b\rangle = |\psi\rangle$ for some $|\psi\rangle \in S$. For the above example, we say $|\bar{a}_1\rangle$ is *associated* with two vectors different vectors in $\mathbb{C}^3$, say ($|b_1\rangle$ and $|b_2\rangle$) to give two different vectors $|\psi_1\rangle$ and $|\psi_2\rangle$ in $\mathbb{C}^6$.

Let a vector $|\bar{a}_i\rangle$ in $\bar{A}$ be *associated* with N_i vectors from B. *Associating* all of the $|\bar{a}_i\rangle$ with corresponding vectors in B should give us all the vectors in S, this implies that

$$\sum_{i=1}^{n} N_i = 6. \tag{3.2}$$

Now, for each i, let us relabel the set of all N_i vectors in B which are associated with $|\bar{a}_i\rangle$ as $\{\ |b_i^1\rangle,\ |b_i^2\rangle, \ldots,\ |b_i^{N_i}\rangle\ \}$. Eq. (3.1) ensures that $\langle b_i^j|b_i^k\rangle = 0\ \forall j,k \in \{\ 1,2,\ldots,N_i\ \}\ \ \forall i \in \{\ 1,2,\ldots,n\ \}$. In other words, all N_i vectors in the set $\{\ |b_i^1\rangle,\ |b_i^2\rangle, \ldots,\ |b_i^{N_i}\rangle\ \}$ must be mutually orthonormal. However, each vector $|b_i^j\rangle$ comes from a three-dimensional vector space $\mathbb{C}^3$, which means there cannot be more than three such mutually orthogonal vectors. Hence, we have the following inequality:

$$N_i \leq 3\ \ \forall i \in \{\ 1,2,\ldots,n\ \}. \tag{3.3}$$

Using Eq. (3.1), Eq. (3.2), Ineq. (3.3), we will prove a few lemmas below, and then we will write the form of U 3.2.4. For this specific form of U, we prove in 3.2.1 that it's impossible to extend the MUBs triplets which are product bases in $\mathbb{C}^6$.

Lemma 3.2.1. $|\bar{A}| \geq 2$. *That is A has at least* 2 *distinct vectors.*

Proof. Let $|A| = n$. Taking sum over all N_i in Ineq. (3.3), we have $\sum_{i=1}^{n} N_i \leq 3n$. But from Eq. (3.2), we know that $\sum_{i=1}^{n} N_i = 6$. This implies $6 \leq 3n$. Hence, we have $n \geq 2$. □

Notice that Eq. (3.1) demands $\langle b_i|b_j\rangle = 0$ if $\langle a_i|a_j\rangle \neq 0$. This means if $\langle \bar{a}_i|\bar{a}_j\rangle \neq 0$, then the all the $|b\rangle$ vectors *associated* with either $|\bar{a}_i\rangle$ or $|\bar{a}_j\rangle$ must be all mutually orthogonal. Number of such vectors which are either *associated* with $|\bar{a}_i\rangle$ or $|\bar{a}_j\rangle$ is $N_i + N_j$. Now $N_i + N_j$ cannot exceed three as there can be a maximum of three mutually orthonormal vectors in a three dimensional vector space $\mathbb{C}^3$. This can be generalised as follows.

Lemma 3.2.2. *Let the set,* $\{\ |\bar{a}_{i_1}\rangle,\ |\bar{a}_{i_2}\rangle, \ldots,\ |\bar{a}_{i_k}\rangle\ \} \subseteq \{\bar{A}\}$*, be such that no two pairs in the set are mutually orthogonal. Then*

$$\sum_{i \in \{\ i_1,\ldots,i_k\ \}} N_i \leq 3$$

Proof. Let B_u be the set of all q-dimensional vectors *associated* with the set $\{\ |\bar{a}_{i_1}\rangle,\ |\bar{a}_{i_2}\rangle, \ldots,\ |\bar{a}_{i_k}\rangle\}$. Clearly, $|B_u| = \sum_{i\in\{i_1,\ldots,i_k\}} N_i$, where $|B_u|$ denoted as the number of distinct elements in set B_u . Given that no two pairs in the set $\{\ |\bar{a}_{i_1}\rangle,\ |\bar{a}_{i_2}\rangle, \ldots,\ |\bar{a}_{i_k}\rangle\}$ are orthogonal, from Eq. (3.1), it implies that any pair of vectors from B_u must be orthogonal, and hence all vectors in B_u must be mutually orthogonal. As the number of mutually orthogonal vectors cannot exceed the dimensionality of the vector space, this implies that $\sum_{i\in\{i1,\ldots,i_k\}} N_i \leq 3$. □

Lemma 3.2.3. *There cannot be a common element between any two pairs of orthogonal vectors in $\bar{A}$.*

Proof. Let there be two such pairs of orthogonal vectors in $\bar{A}$ such that one vector is common in both pairs. Without the loss of generality, lets say $\langle\bar{a}_i|\bar{a}_j\rangle = 0$ and $\langle\bar{a}_i|\bar{a}_k\rangle = 0$. So we have two pairs of orthogonal vectors, $\{\ |\bar{a}_i\rangle,\ |\bar{a}_j\rangle\}$ and $\{\ |\bar{a}_i\rangle,\ |\bar{a}_k\rangle\}$ such that $|\bar{a}_i\rangle$ is the common vector in both. This implies that each of the pair form a basis of $\mathbb{C}^2$. So we have the following:

$$|\bar{a}_k\rangle = x\,|\bar{a}_i\rangle + y\,|\bar{a}_j\rangle$$

for some complex numbers x, y. Now, $\langle\bar{a}_i|\bar{a}_k\rangle = 0$ ensures that $x = 0$, which implies $|\bar{a}_k\rangle = y\,|\bar{a}_j\rangle$. As both of them are unit vectors, hence y can only be a complex number with unit magnitude. Hence $|\bar{a}_j\rangle$ and $|\bar{a}_k\rangle$ are not considered distinct as explained earlier while defining $\bar{A}$. But by definition, $\bar{A}$ only contains distinct elements. Hence such a case is not possible. □

Let us break the possible cases in this regards:

Case 1: If $\langle\bar{a}_i|\bar{a}_j\rangle \neq 0; \forall i, j \in \{1, 2, \cdots, n\}$.
Using lemma (3.2.2), we have $\sum_{i=1}^{n} N_i \leq 3$; i.e; $6 \leq 3$. Not possible!

Case 2: If *exactly one pair* of $\bar{A}$ is orthogonal, say $\langle\bar{a}_1|\bar{a}_2\rangle = 0$ and $\langle\bar{a}_i|\bar{a}_j\rangle \neq 0; \forall i, j \neq \{1, 2\}$.
Using lemma (3.2.2), we have the following inequalities:

$$N_1 + (N_3 + N_4 + \cdots + N_n) \leq 3, \tag{3.4a}$$

$$N_2 + (N_3 + N_4 + \cdots + N_n) \leq 3. \tag{3.4b}$$

Adding N_2 and N_1 on both sides in inequalities (3.4a) and (3.4b) respectively and using Eq. (3.2), we have:

$$6 \leq 3 + N_1 \leq 6, \tag{3.5a}$$

$$6 \leq 3 + N_2 \leq 6. \tag{3.5b}$$

Which gives result as $N_1 = N_2 = 3$. Since $N_i \geq 0 \ \forall i \in \{\, 1, 2, \ldots n \,\}$, it implies that $N_i = 0 \ \forall i \in \{\, 3, 4, \ldots, n \,\}$. This means there are only two distinct elements in the set $\bar{A}$.

Case 3: If *exactly two pairs* of $\bar{A}$ are orthogonal, say either $\langle \bar{a}_1 | \bar{a}_2 \rangle = 0$ and $\langle \bar{a}_3 | \bar{a}_4 \rangle = 0$ or, $\langle \bar{a}_1 | \bar{a}_2 \rangle = 0$ and $\langle \bar{a}_1 | \bar{a}_3 \rangle = 0$.
Let us first consider the subcase where $\langle \bar{a}_1 | \bar{a}_2 \rangle = 0$ and $\langle \bar{a}_3 | \bar{a}_4 \rangle = 0$. Notice that this case inherently assumes the existence of at least four distinct elements in A. Using lemma (3.2.2), we have the following inequalities:

$$N_1 + N_3 + (N_5 + \cdots + N_n) \leq 3 \tag{3.6a}$$

$$N_2 + N_4 + (N_5 + \cdots + N_n) \leq 3 \tag{3.6b}$$

$$N_3 + N_2 + (N_5 + \cdots + N_n) \leq 3 \tag{3.6c}$$

$$N_4 + N_1 + (N_5 + \cdots + N_n) \leq 3. \tag{3.6d}$$

We add the respective terms on both sides of Ineq. (3.6a)-(3.6d) to make the left hand side equal to $\sum_{i=1}^{n} N_i$ in each of the inequalities. Using Eq. (3.2) and Ineq. (3.3), we have the following inequalities:

$$6 \leq 3 + N_2 + N_4 \leq 6 \tag{3.7a}$$

$$6 \leq 3 + N_3 + N_1 \leq 6 \tag{3.7b}$$

$$6 \leq 3 + N_1 + N_4 \leq 6 \tag{3.7c}$$

$$6 \leq 3 + N_2 + N_3 \leq 6. \tag{3.7d}$$

Hence, we have the following equations from the above inequalities (3.7a), (3.7b), (3.7c), and (3.7d):

$$N_1 + N_2 + N_3 + N_4 = 6, \quad N_1 = N_2, \quad N_3 = N_4, \text{ and } N_i = 0 \ \forall i \in \{\, 5, 6, \ldots, n \,\}.$$

This implies that we have exactly four distinct vectors $|\bar{a}_1\rangle$, $|\bar{a}_2\rangle$, $|\bar{a}_3\rangle$, and $|\bar{a}_4\rangle$ in the set $\bar{A}$ such that $\langle \bar{a}_1, \bar{a}_2\rangle = 0$ and $\langle \bar{a}_3, \bar{a}_4\rangle = 0$; i.e; $|\bar{A}| = 4$.

Now, let us consider the another subcase where $\langle \bar{a}_1|\bar{a}_2\rangle = 0$ and $\langle \bar{a}_1|\bar{a}_3\rangle = 0$. But this case is not possible from lemma 3.2.3 as there is a common element $\bar{a_1}$ in both pairs.

Case 4: If *exactly three pairs* of $\bar{A}$ are orthogonal and only possibility is $\langle \bar{a}_1|\bar{a}_2\rangle = 0$, $\langle \bar{a}_3|\bar{a}_4\rangle = 0$, and $\langle \bar{a}_5|\bar{a}_6\rangle = 0$.
Using lemma (3.2.2), we have the following inequalities:

$$N_1 + N_3 + N_5 + (N_7 + \cdots + N_n) \leq 3 \tag{3.8a}$$
$$N_2 + N_4 + N_6 + (N_7 + \cdots + N_n) \leq 3 \tag{3.8b}$$
$$N_3 + N_2 + N_5 + (N_7 + \cdots + N_n) \leq 3 \tag{3.8c}$$
$$N_4 + N_1 + N_6 + (N_7 + \cdots + N_n) \leq 3 \tag{3.8d}$$
$$N_5 + N_1 + N_4 + (N_7 + \cdots + N_n) \leq 3 \tag{3.8e}$$
$$N_6 + N_2 + N_3 + (N_7 + \cdots + N_n) \leq 3 \tag{3.8f}$$
$$\tag{3.8g}$$

Adding Ineq. (3.8a) and Ineq. (3.8b), we have $\sum_{i=1}^{n} N_i + (N_7 + \cdots + N_n) \leq 2q \implies N_i = 0\ \forall i \in \{\, 7, 8, \ldots, n \,\} \implies \sum_{i=1}^{7} N_i \leq 6$.
So, we have the following equations that need to be satisfied simultaneously :

$$N_1 + N_2 + N_3 + N_4 + N_5 + N_6 = 6, \text{ and } N_i = 0\ \forall i \in \{\, 7, 8, \ldots, n \,\}.$$

In this scenario, we have $\{|\bar{a}_1\rangle, |\bar{a}_2\rangle, \cdots, |\bar{a}_6\rangle\} \in \mathbb{C}^2$ such that we have *exactly three* orthogonal pairs, $\langle \bar{a}_1, \bar{a}_2\rangle = 0$, $\langle \bar{a}_3, \bar{a}_4\rangle = 0$, and $\langle \bar{a}_5, \bar{a}_6\rangle = 0$.

Case 5: If *exactly four pairs* of $\bar{A}$ are orthogonal.
This case is not possible from lemma 3.2.3 as this case consider eight distinct elements in $\bar{A}$. But we need atmost six distinct elements i.e; $|\bar{A}| \leq 6$.

Lemma 3.2.4. *If* exactly one pair *of $\bar{A}$ are orthogonal, then U has the following form*

$$U = A_1 \otimes B_1 + A_2 \otimes B_2, \tag{3.9}$$

where B_1 and B_2 are 3×3 unitary matrices and $A_1 = \begin{bmatrix} |\bar{a}_1\rangle & \mathbf{0} \end{bmatrix}$, and $A_2 = \begin{bmatrix} \mathbf{0} & |\bar{a}_2\rangle \end{bmatrix}$, is a 2×2 matrices.

Proof. As in the case 2, we have shown that if exactly one pair of $\bar{A}$ is orthogonal, say $\langle \bar{a}_1 | \bar{a}_2 \rangle = 0$, then we get $N_1 = N_2 = 3$ and $N_i = 0 \ \forall i \in \{ 3, 4, \ldots, n \}$. So, $\bar{A} = \{ |\bar{a_1}\rangle, |\bar{a_2}\rangle \}$. Since $|\bar{a_1}\rangle$ is associated with three different vectors, say $B_1 = \{ |b_1\rangle, |b_2\rangle, |b_3\rangle \}$ and $|\bar{a_2}\rangle$ is associated with three different vectors, say $B_2 = \{ |b_4\rangle, |b_5\rangle, |b_6\rangle \}$. Note that B_1 and B_2 are orthonormal bases in $\mathbb{C}^3$. Let us represent the each element of the set

$$S = \{ |\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_6\rangle \}, \quad \text{where}$$

$$|\psi_i\rangle = |\bar{a}_1\rangle \otimes |b_i\rangle, \quad \text{and} \quad |\psi_{i+3}\rangle = |\bar{a}_2\rangle \otimes |b_{i+3}\rangle, \quad \forall i \in \{1, 2, 3\}.$$

Let U be the unitary matrix whose column vectors are the vectors of this matrix. So we have

$$U = \begin{bmatrix} |\psi_1\rangle & |\psi_2\rangle & \ldots & |\psi_6\rangle \end{bmatrix} = A_1 \otimes B_1 + A_2 \otimes B_2$$

such that B_1 and B_2 are unitary matrices and $A_1 = \begin{bmatrix} |\bar{a}_1\rangle & \mathbf{0} \end{bmatrix}$, and $A_2 = \begin{bmatrix} \mathbf{0} & |\bar{a}_2\rangle \end{bmatrix}$, is a 2×2 matrices. □

Lemma 3.2.5. *Let $d = pq$ and let A and B be unitary matrices of dimensions p and q respectively, such that*

$$A \otimes B = \frac{1}{\sqrt{pq}} H_d,$$

where H_d is a Hadamard matrix of order pq. Then A and B must be Hadamard matrices.

Proof. Let

$$A = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1p} \\ a_{21} & a_{22} & \cdots & a_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ a_{p1} & a_{p2} & \cdots & a_{pp} \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1q} \\ b_{21} & b_{22} & \cdots & b_{2q} \\ \vdots & \vdots & \ddots & \vdots \\ b_{q1} & b_{q2} & \cdots & b_{qq} \end{bmatrix}$$

be unitary matrices of orders p and q respectively.

It is given that

$$A \otimes B = \frac{1}{\sqrt{pq}} H_d \quad \Longrightarrow \quad |a_{ij}| \cdot |b_{kl}| = \frac{1}{\sqrt{pq}} \quad \Longrightarrow \quad |b_{kl}| = \frac{1}{\sqrt{pq}\,|a_{ij}|}.$$

Since $|b_{kl}|$ is independent of the indices k, l, it must be constant, say t. The same argument applies to $|a_{ij}|$, which must also be constant.

Now, since B is unitary, it follows that

$$\sum_{k=1}^{q} |b_{kl}|^2 = 1 \quad \text{for all } l \in \{1, 2, \ldots, q\}.$$

So,

$$\sum_{k=1}^{q} t^2 = 1 \quad \Rightarrow \quad qt^2 = 1 \quad \Rightarrow \quad t = \frac{1}{\sqrt{q}}.$$

Hence, $|b_{kl}| = \frac{1}{\sqrt{q}}$, and therefore $B = \frac{1}{\sqrt{q}} H_q$ for some Hadamard matrix H_q of order q.

Similarly,

$$|a_{ij}| = \frac{1}{\sqrt{pq} \cdot t} = \frac{1}{\sqrt{pq} \cdot \frac{1}{\sqrt{q}}} = \frac{1}{\sqrt{p}}.$$

Thus, $A = \frac{1}{\sqrt{p}} H_p$ for some Hadamard matrix H_p of order p.

This shows that if the tensor product of two unitary matrices is a Hadamard matrix, then both A and B must be Hadamard matrices. □

Theorem 3.2.1. *There doesn't exist unitary matrix U of order six, as product basis in the above form 3.2.4 such that*

$$\{M_1 \otimes N_1, M_2 \otimes N_2, ..., M_3 \otimes N_3, U\}$$

are MUBs in $\mathbb{C}^6$, where $M_i \in U_2, N_i \in U_3; \forall i = \{1, 2, 3\}$. Note that U_2 and U_3 are unitary matrices of order two and three, respectively.

Proof. Since $(M_i \otimes N_i, M_j \otimes N_j)$ is a pair of MUBs in $\mathbb{C}^6$ for $i \neq j$ and $\forall i, j = \{1, 2, 3\}$. So, from lemmas 2.2.3 and 2.2.4, we have $(M_i \otimes N_i)^\dagger (M_j \otimes N_j) = \frac{1}{\sqrt{6}} H = (M_i^\dagger \otimes M_j)(N_i^\dagger \otimes N_j)$. As both $(M_i^\dagger \otimes M_j)$ and $(N_i^\dagger \otimes N_j)$ are unitary matrices, so above lemma 3.2.5 implies that $(M_i^\dagger \otimes M_j)$ and $(N_i^\dagger \otimes N_j)$ are Hadamard matrices of order two and order three, respectively. This implies $M_i^\dagger$ and M_j are MUBs in $\mathbb{C}^2$ and also $N_i^\dagger$ and N_j are MUBs in $\mathbb{C}^3$. This eventually implies that (M_i, M_j) and (N_i, N_j) are MUB in $\mathbb{C}^2$ and $\mathbb{C}^3$ respectively.

Let $U = \begin{bmatrix} |\psi_1\rangle & |\psi_2\rangle & \cdots & |\psi_6\rangle \end{bmatrix}$ be a unitary matrix such that $|\psi_i\rangle = |a_i\rangle \otimes |b_i\rangle$. From 3.2.4,

$$U = A_1 \otimes B_1 + A_2 \otimes B_2,$$

where B_1 and B_2 are 3×3 unitary matrices and $A_1 = \begin{bmatrix} |\bar{a}_1\rangle & \mathbf{0} \end{bmatrix}$, $A_2 = \begin{bmatrix} \mathbf{0} & |\bar{a}_2\rangle \end{bmatrix}$, and $A = \begin{bmatrix} |\bar{a}_1\rangle & |\bar{a}_2\rangle \end{bmatrix}$ are 2×2 matrices. Suppose that $(U, M_i \otimes N_i)$ is a pair of MUBs, $\forall i = \{1, 2, 3\}$. Then, $U^\dagger (M_i \otimes N_i) = \frac{1}{\sqrt{6}} H_i$, where H_i is a Hadamard matrices. Also,

$$U^\dagger(M_i \otimes N_i) = \left(\begin{bmatrix} |a_1\rangle & \mathbf{0} \end{bmatrix}^\dagger \otimes B_1^\dagger + \begin{bmatrix} \mathbf{0} & |a_2\rangle \end{bmatrix}^\dagger \otimes B_2^\dagger \right) (M_i \otimes N_i) =$$
$$\begin{bmatrix} |a_1\rangle & \mathbf{0} \end{bmatrix}^\dagger M_i \otimes B_1^\dagger N_i + \begin{bmatrix} \mathbf{0} & |a_2\rangle \end{bmatrix}^\dagger M_i \otimes B_2^\dagger N_i$$

Let, $B_1^\dagger N_i = V_1^i$ and $B_2^\dagger N_i = V_2^i$. Note that $V_1^i, V_2^i \in U_3$. As we know if X and Y be unitary matrices such that $X = \begin{bmatrix} |x_1\rangle & |x_2\rangle & \cdots & |x_d\rangle \end{bmatrix}$,
$Y = \begin{bmatrix} |y_1\rangle & |y_2\rangle & \cdots & |y_d\rangle \end{bmatrix}$ then, $(X^\dagger Y)_{ij} = \langle x_i | y_j \rangle$. So,

$$U^\dagger(M_i \otimes N_i) = \begin{bmatrix} \langle a_1|m_1^i\rangle & \langle a_1|m_2^i\rangle \\ 0 & 0 \end{bmatrix} \otimes V_1^i + \begin{bmatrix} 0 & 0 \\ \langle a_2|m_1^i\rangle & \langle a_2|m_2^i\rangle \end{bmatrix} \otimes V_2^i$$

$$= \begin{bmatrix} \langle a_1|m_1^i\rangle\, V_1^i & \langle a_1|m_2^i\rangle\, V_1^i \\ \langle a_2|m_1^i\rangle\, V_2^i & \langle a_2|m_2^i\rangle\, V_2^i \end{bmatrix} = \frac{1}{\sqrt{6}} H_i.$$

This implies,

$$A^\dagger M_i = \begin{bmatrix} \langle a_1|m_1^i\rangle & \langle a_1|m_2^i\rangle \\ \langle a_2|m_1^i\rangle & \langle a_2|m_2^i\rangle \end{bmatrix} \text{ is } \frac{1}{\sqrt{2}} \text{ times a Hadamard matrix in } d = 2,$$

which means A and M_i must be MUBs for all $i = \{1, 2, 3\}$. This is a contradiction as we can't have more than three MUBs in $d = 2$. □

3.3 Conclusion

In this chapter, we studied a form of unitary matrix U, as a product basis in $\mathbb{C}^6$, under certain conditions. We analytically proved that such a matrix U cannot serve as an extension to a triplet of mutually unbiased product bases, ie, it cannot act as a fourth MUB when the first three bases are also product bases.

Our contribution lies in introducing a novel combinatorial perspective to approach this problem. While a better result has been established by McNulty and Weigert [65], who proved that extending mutually unbiased product bases in dimension six is impossible, our method offers an alternative viewpoint and proof technique.

Chapter 4

On Obtaining MUBs by Finding Points on Complete Intersection Varieties over $\mathbb{R}$

As discussed in Chapter 3, it is not possible to extend a set of three mutually unbiased bases that are product bases in $\mathbb{C}^6$. This chapter can be viewed as a natural extension of the previous one, where we continue our investigation into the extensibility of MUBs, now in a more general setting for arbitrary dimension d. We provide equivalent criteria for extending a set of MUBs for $\mathbb{C}^d$ by studying real points of a certain affine algebraic variety. This variety comes from the relations that determine the extendability of a system of MUBs. Finally, we show that some part of this variety gives rise to complete intersection domains. Further, we show that there is a one-to-one correspondence between MUBs and the maximal commuting classes (bases) of orthogonal normal matrices in $\mathcal{M}_d(\mathbb{C})$. It means that for m MUBs in $\mathbb{C}^d$, there are m commuting classes each consisting d commuting orthogonal normal matrices and the existence of maximal commuting basis for $\mathcal{M}_d(\mathbb{C})$ ensures the complete sets of MUBs in $\mathcal{M}_d(\mathbb{C})$.

4.1 Introduction

In this chapter, we study various problems related to Mutually Unbiased Bases through certain results of algebraic geometry. We approach the problem in the following way. Once we have k given MUBs in some given dimension d, the problem of finding the $(k+1)$-th MUB is essentially the problem of finding solutions to a system of polynomial equations in $2d^2$ real variables and having degree at most two.

We encounter polynomial systems $F = \{f_1, f_2, \ldots, f_t\}$, where $t = (k+1)d^2$, in $2d^2$ real variables over $\mathbb{R}$. Our goal is to find all common solutions—i.e., all tuples $x = (x_1, x_2, \ldots, x_{2d^2})$ for which $f_1(x) = f_2(x) = \cdots = f_t(x) = 0$.

To approach this, we compute a Gröbner basis for the ideal generated by F. This yields a new system $G = \{g_1, g_2, \ldots, g_r\}$ such that the ideals generated by F and G are the same (i.e., $\langle F \rangle = \langle G \rangle$), but G has desirable algebraic properties that facilitate solving the system.

The structure and complexity of the resulting Gröbner basis G depend heavily on the choice of monomial ordering, which plays a crucial role in computations and simplification.

4.1.1 Organization and Contribution

All kinds of mathematical preliminaries has been given in section 2.7 of chapter 2.

In Section 4.2, we set up the problem of finding a new MUB as a problem of solving polynomial systems in $2d^2$ variables. The ideals for dimension two are explained in Section 4.2.2. We analyse the case through an example to recover the complete sets of MUBs for dimension two and recover some known results. We then demonstrate that, starting with the identity matrix, the system of equations for generating the next MUB comprises a part consisting of equations of spheres and some homogeneous equations. The result explains that the ideal generated by the sphere part is a complete intersection prime ideal. This is presented in Section 4.2.3.

Our following results are essential in this direction.

Theorem [Theorem 4.2.1]. Let $A_1, A_2, \ldots, A_k$ be a system of k mutually unbiased bases in $\mathbb{C}^d$. Then this system can be extended to a system of $k+1$ MUBs if and only if the algebraic

variety $Z(M_{k+1}^{\{d\}})$ of the ideal $M_{k+1}^{\{d\}} = I^{\{d\}} + \sum_{i=1}^{k} J_{l,k+1}^{\{d\}} \subseteq \mathbb{R}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]$ has at least one point in $\mathbb{R}^{2d^2}$.

Theorem [Theorem 4.2.2]. Let $A_1, A_2, \ldots, A_{m-1}$ be a system of MUBs in $\mathbb{C}^d$, and assume that $A_1 = I_d$, the identity matrix. Then $J_{1,m}^{\{d\}}$, the ideal generated by the sphere equations, is a complete intersection prime ideal.

The significance of this result is that if we pass to the quotient ring obtained by modding out the polynomial ring by these equations the dimension reduction is maximum, i.e., same as the number of equations. The rings of this type are very much similar to polynomial rings. This allows us potentially to bring down the MUB finding problem to the study of a ring of potentially much lower dimension that inherits many nice properties of the larger polynomial ring.

Finally, in section 4.3, we show a connection between MUBs and the maximal commuting classes (bases) of orthogonal normal matrices in C^d instead of commuting bases containing orthogonal unitary matrices [5]. This observation of considering normal matrices over unitary matrices provides more flexibility. This connection reveals the necessary condition for the existence of MUB in any dimension. Also, we present an example for dimension four, where there are five commuting classes, and each consists of four orthogonal normal matrices.

4.2 Studying Real Points on Intersection Varieties

In this section, we will formally establish the problem of extending a system of MUB using the tools of algebraic geometry. Additionally, we will explore specific cases for the dimension 2. Subsequently, we will demonstrate how a particular ideal, arising from the investigation of this problem, exhibits some desirable properties in this regard.

4.2.1 Defining ideals of MUB

In this subsection, we establish a connection between the problem of extending a system of mutually unbiased bases and the problem of finding points on an affine algebraic variety. For the sake of clarity and completeness, we begin by recalling the definition of MUBs, which will serve as a foundation for the further discussions:

Definition 4.2.1. *Two orthonormal bases* $A \equiv \{|a_1\rangle, |a_2\rangle, \ldots, |a_d\rangle\}$ *and* $B \equiv \{|b_1\rangle, |b_2\rangle, \ldots, |b_d\rangle\}$ *in an* d *dimensional Hilbert spaces are mutually unbiased if*

$$|\langle a_i|b_j\rangle| = \frac{1}{\sqrt{d}}, \ \forall i, j = 1, 2, \ldots, d.$$

If we consider the vector space $\mathbb{C}^d$, the condition given in the above definition becomes $\|\mathbf{a}_i \cdot \overline{\mathbf{b}_j}\| = \frac{1}{\sqrt{d}}$ for any two orthonormal bases $\{\mathbf{a}_i : 1 \leq i \leq d\}$, and $\{\mathbf{b}_i : 1 \leq i \leq d\}$ of $\mathbb{C}^d$, where for a vector $\mathbf{v} = (v_1, \ldots, v_d) \in \mathbb{C}^d$, we denote $\overline{\mathbf{v}} := (\overline{v_1}, \ldots, \overline{v_d})^t$, the vector consisting of the complex conjugates transpose of the row vector $\mathbf{v}$.

Let $A = \{\mathbf{a_j} = (a_{1j}, a_{2j}, \ldots, a_{dj}) : 1 \leq j \leq d\}$ be a set of vectors in the vector space $\mathbb{C}^d$. For A to be a part of a MUB, A need to be orthonormal. More precisely, we must have $\mathbf{a_j} \cdot \overline{\mathbf{a_k}} = 0$ for any $1 \leq j \neq k \leq d$. We formulate this criterion in terms of algebraic equations as follows.

Let $z_{ij}, 1 \leq i, j \leq d$ be a set of complex variables. We write $\mathbf{z_j} = (z_{1j}, z_{2j}, \ldots, z_{dj})$, where $1 \leq j \leq d$. Any orthogonal set of d-vectors of $\mathbb{C}^d$ is a non-zero complex solution of the system of equations $\mathbf{z_j} \cdot \overline{\mathbf{z_k}} = 0, 1 \leq j \neq k \leq d$. Note that the equations $\mathbf{z_j} \cdot \overline{\mathbf{z_k}} = 0$ are not necessarily polynomial equations.

To overcome this problem, we reduce this system of complex equations to a system of real equations by making the substitution $z_{ij} = x_{ij} + iy_{ij}$, where x_{ij}, y_{ij} are real variables for all $1 \leq i, j \leq d$. Then the above orthogonality relations become

$$\begin{aligned}
\mathbf{z_j} \cdot \overline{\mathbf{z_k}} = \sum_{i=1}^{d} z_{ij} \cdot \overline{z_{ik}} &= \sum_{i=1}^{d} (x_{ij} + iy_{ij})(x_{ik} - iy_{ik}) \\
&= \sum_{i=1}^{d} \{(x_{ij}x_{ik} + y_{ij}y_{ik}) + i(x_{ik}y_{ij} - x_{ij}y_{ik})\} \\
&= \sum_{i=1}^{d} (x_{ij}x_{ik} + y_{ij}y_{ik}) + i \sum_{i=1}^{d} (x_{ik}y_{ij} - x_{ij}y_{ik}).
\end{aligned}$$

Now, separating the real and the imaginary parts, we obtain

$$\begin{cases}
\displaystyle\sum_{i=1}^{d} (x_{ij}x_{ik} + y_{ij}y_{ik}) = 0, 1 \leq j \neq k \leq d, \\
\displaystyle\sum_{i=1}^{d} (x_{ik}y_{ij} - x_{ij}y_{ik}) = 0, 1 \leq j \neq k \leq d.
\end{cases} \tag{4.1}$$

Note that the above equations are quadratic homogeneous polynomial equations. Then we can work over the polynomial ring $S = \mathbb{R}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]$. Therefore, any real solution of the above equation in $\mathbb{R}^{2d^2}$ corresponds to an orthogonal set of vectors in $\mathbb{C}^d$. In the language of algebraic varieties, we can say that any orthonormal set of d vectors of $\mathbb{C}^d$ correspond to the real points of the variety $Z(I^{\{d\}})$, where $I^{\{d\}}$ is the ideal of the polynomial ring S given by

$I^{\{d\}} = (\{\sum_{i=1}^{d}(x_{ij}x_{ik} + y_{ij}y_{ik}), \sum_{i=1}^{d}(x_{ik}y_{ij} - x_{ij}y_{ik}) | 1 \leq j \neq k \leq d\})$.

Thus, the study of these ideals may be helpful while studying MUB, as any MUB has to satisfy the above equations and hence, must come from a point of the variety $Z(I^{\{d\}})$.

Suppose that, for a given dimension d, there is a set of k MUBs, and we want to check whether this set of k MUBs can be extended to a set of $k+1$ MUBs. This problem can also be interpreted in terms of the existence of solutions to a set of algebraic equations. Let us fix the following notations: Let $A_1, A_2, \ldots, A_k$ be a set of k MUBs in dimension d. Let $A_l = \{\mathbf{a}_j^{(l)} : 1 \leq j \leq d\}$, where $\mathbf{a}_j^{(l)} \in \mathbb{C}^d$, and $\mathbf{a}_j^{(l)} = (a_{1j}^{(l)}, a_{2j}^{(l)}, \ldots, a_{dj}^{(l)})^t, 1 \leq j \leq d, 1 \leq l \leq k$, where $a_{ij}^{(l)} \in \mathbb{C}$ are complex numbers. Now, we want to check whether there is a set of orthonormal vectors $A_{k+1} = \{\mathbf{a}_j^{(k+1)} : 1 \leq j \leq d\}$, such that $A_1, A_2, \ldots, A_{k+1}$ is a system of $k+1$ MUBs. We now require to find out the algebraic relations that the vectors of the new MUB A_{k+1} need to satisfy to be a part of the above system of MUBs. First, note that the vectors in A_{k+1} have to be orthogonal, that is, they must come from the algebraic variety $Z(I^{\{d\}})$. More precisely, if we write $a_{ij}^{(k+1)} = b_{ij}^{(k+1)} + ic_{ij}^{(k+1)}$, then $x_{ij} = b_{ij}^{(k+1)}, y_{ij} = c_{ij}^{(k+1)}$ must be a solution of the system given in (4.1). Moreover, they also need to satisfy the condition given in the definition of the MUB (Definition 4.2.1). In other words, the vectors $\mathbf{a}_j^{(k+1)}, 1 \leq j \leq d$ must satisfy the following relations $|\langle \mathbf{a}_j^{(k+1)} \cdot \mathbf{a}_q^{(l)} \rangle|^2 = \frac{1}{d}$ for all $1 \leq j, q \leq d$,

and $1 \leq l \leq k$. This gives rise to the following relations:

$$\begin{aligned}
|\langle \mathbf{a}_j^{(k+1)} \cdot \mathbf{a}_q^{(l)} \rangle|^2 - \frac{1}{d} &= |\sum_{i=1}^{d} a_{ij}^{(k+1)} \cdot \overline{a_{iq}^{(l)}}|^2 - \frac{1}{d} \\
&= |\sum_{i=1}^{d} (b_{ij}^{(k+1)} + ic_{ij}^{(k+1)})(b_{iq}^{(l)} - ic_{iq}^{(l)})|^2 - \frac{1}{d} \\
&= |\sum_{i=1}^{d} \{(b_{ij}^{(k+1)} b_{iq}^{(l)} + c_{ij}^{(l)} c_{iq}^{(l)}) + i(b_{iq}^{(l)} c_{ij}^{(k+1)} - b_{ij}^{(k+1)} c_{iq}^{(l)})\}|^2 - \frac{1}{d} \\
&= |\sum_{i=1}^{d} (b_{ij}^{(k+1)} b_{iq}^{(l)} + c_{ij}^{(k+1)} c_{iq}^{(l)}) + i \sum_{i=1}^{d} (b_{iq}^{(l)} c_{ij}^{(k+1)} - b_{ij}^{(k+1)} c_{iq}^{(l)})|^2 - \frac{1}{d} \\
&= \{\sum_{i=1}^{d} (b_{ij}^{(k+1)} b_{iq}^{(l)} + c_{ij}^{(k+1)} c_{iq}^{(l)})\}^2 + \{\sum_{i=1}^{d} (b_{iq}^{(l)} c_{ij}^{(k+1)} - b_{ij}^{(k+1)} c_{iq}^{(l)})\}^2 - \frac{1}{d}.
\end{aligned}$$

In other words, the vectors in the new MUB A_{k+1} is a solution of the following system of algebraic equations in the variables $\mathbf{z_j} = (z_{1j}, z_{2j}, \ldots, z_{dj}), 1 \leq j \leq d$, with $z_{ij} = x_{ij} + iy_{ij}$, where x_{ij}, y_{ij} are real variables.

$$\begin{cases}
\sum_{i=1}^{d} (x_{ij}x_{ik} + y_{ij}y_{ik}) = 0, 1 \leq j \neq k \leq d, \\
\sum_{i=1}^{d} (x_{ik}y_{ij} - x_{ij}y_{ik}) = 0, 1 \leq j \neq k \leq d, \\
\sum_{i=1}^{d} (x_{ij}^2 + y_{ij}^2) = 1, \quad 1 \leq j \leq d, \\
\Big\{ \sum_{i=1}^{d} (x_{ij} b_{iq}^{(l)} + y_{ij} c_{iq}^{(l)}) \Big\}^2 + \Big\{ \sum_{i=1}^{d} (b_{iq}^{(l)} y_{ij} - x_{ij} c_{iq}^{(l)}) \Big\}^2 - \frac{1}{d} = 0, \\
\quad 1 \leq j, q \leq d, \ 1 \leq l \leq k.
\end{cases} \tag{4.2}$$

Now, we consider the following ideals in the polynomial ring $S = \mathbb{R}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]$ for $1 \leq l \leq k$:

$$J_{l,k+1}^{\{d\}} = (\{\sum_{i=1}^{d} (x_{ij} b_{iq}^{(l)} + y_{ij} c_{iq}^{(l)})\}^2 + \{\sum_{i=1}^{d} (b_{iq}^{(l)} y_{ij} - x_{ij} c_{iq}^{(l)})\}^2 - \frac{1}{d} : 1 \leq j, q \leq d).$$

Note that the ideal $J_{l,k+1}^{\{d\}}$ is generated by the polynomial relations coming from the MUB

conditions between the pair of orthonormal bases A_l and A_{k+1} for all $1 \leq l \leq k$. Now, we can give the following equivalent condition of whether a system of MUB of length k in the vector space $\mathbb{C}^d$ can be extended to a system of MUB of length $k+1$.

Theorem 4.2.1. *Let $A_1, A_2, \ldots, A_k$ be a system of k mutually unbiased bases. Then this system can be extended to a system of $k+1$ MUBs if and only if the algebraic variety $Z(M_{k+1}^{\{d\}})$ of the ideal $M_{k+1}^{\{d\}} = I^{\{d\}} + \sum_{i=1}^{k} J_{l,k+1}^{\{d\}} \subseteq \mathbb{R}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]$ has at least one point in $\mathbb{R}^{2d^2}$.*

Proof. Suppose that the variety $Z(M_{k+1}^{\{d\}})$ has a point $\alpha \in \mathbb{R}^{2d^2}$. Then, the point α corresponds to a real solution of the system (4.2) given above. Hence, by identifying this solution using $z_{ij} = x_{ij} + iy_{ij}$, we get a new set of MUB $A_{k+1} = [z_{ij}]_{d\times d}$, which extends the given system of MUBs. Conversely, suppose that the given system can be extended to a system of $k+1$ MUBs. Then by the similar arguments given above, we can say that the algebraic variety $Z(M_{k+1}^{\{d\}})$ has at least one point in $\mathbb{R}^{2d^2}$. □

As an immediate consequence, we have the following:

Corollary 4.2.1. *Let $A_1, A_2, \ldots, A_k$ be a system of k MUBs. If $M_{k+1}^{\{d\}} = (1)$, then this system of MUB cannot be extended to a system of $k+1$ MUBs.*

Let us also present the following technical result.

Proposition 4.2.1. *Let $A_1, A_2, \ldots, A_k$ be a system of k MUBs in $\mathbb{C}^d$. Then for any unitary matrix P, the system $PA_1, PA_2, \ldots, PA_k$ is again a system of k MUBs in $\mathbb{C}^d$.*

Proof. Note that for all $1 \leq i \leq k$, the matrix PA_i is again an unitary matrix, as

$$(PA_i)(PA_i)^* = PA_iA_i^*P^* = PP^* = I_d.$$

Since unitary matrices preserve inner products, it follows that the system
PA_1, PA_2, $\ldots$, PA_k satisfies the inner product condition given in the definition of the MUBs. □

Example 4.2.1. *Let $\omega = e^{2\pi i/3}$. Consider the MUB pair in $\mathbb{C}^3$:*

$$A_1 = I_3, \qquad A_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}.$$

Let $P = \mathrm{diag}(1, i, -1)$*, which is unitary. Then*

$$PA_1 = P, \qquad PA_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ i & i\omega & i\omega^2 \\ -1 & -\omega^2 & -\omega \end{pmatrix}.$$

Moreover,

$$(PA_1)^\dagger (PA_2) = A_1^\dagger P^\dagger P A_2 = A_1^\dagger A_2 = A_2,$$

whose entries all have modulus $1/\sqrt{3}$*. Hence* $\{PA_1, PA_2\}$ *is again a system of MUBs in* $\mathbb{C}^3$*.*

Let us now consider the real MUBs, that is, only allowing real entries in Definition 4.2.1. In this case, the defining ideals of a system of MUB become much simpler, and can be obtained by putting $y_{ij} = 0$ in the system of equations given in 4.2. Let $A_1, A_2, \ldots, A_k$ be a system of k MUBs with real entries. Then the defining ideal of the condition that this system can be extended to a system of $k+1$ MUBs with real entries is given by

$$M_{k+1}^{\{d\}} = I^{\{d\}} + \sum_{i=1}^{k} J_{l,k+1}^{\{d\}} \subseteq \mathbb{R}[x_{ij} : 1 \leq i, j \leq d],$$

where

$$I^{\{d\}} = (\sum_{i=1}^{d} x_{ij} x_{ik} : 1 \leq j \neq k \leq d),$$

and

$$J_{l,k+1}^{\{d\}} = (\sum_{i=1}^{d} x_{ij} b_{iq}^{(l)} - \frac{1}{\sqrt{d}} : 1 \leq j, q \leq d).$$

We shall denote the defining ideals of a system of MUBs with real entries in the same way as of the complex case, and mention it explicitly whenever we use it.

4.2.2 Ideals of the MUBs in dimension two

In this subsection, we study ideals defining the MUBs in dimension 2 from the point of view of polynomial algebra. Although MUBs in dimension 2 are all known in terms of complex Hadamard matrices, we want to frame the problem of finding a new MUB in dimension 2 in terms of finding points in certain real algebraic varieties. In view of Proposition 4.2.1, we

may start with the identity matrix I_2, and first try to extend it to a MUB of length 2. We now continue our discussion in the following steps.

Step 1: Let E be the system of vectors coming from the identity matrix I_2. Then $A_1 = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$. and we want to determine an orthonormal basis A_2 which makes the set $\{A_1, A_2\}$ a system of MUB of length 2.

Proposition 4.2.2. *Let E be the set of standard basis vectors of $\mathbb{C}^2$. Then any basis B_1 of $\mathbb{C}^2$, which makes the system $\{E, B_1\}$ a system of MUB, comes from a point on the real variety $Z(M_2^{\{2\}})$, where*

$$M_2^{\{2\}} = I^{\{2\}} + J_{1,4}^{\{2\}},$$

$$I^{\{2\}} = (x_{11}x_{12} + y_{11}y_{12} + x_{21}x_{22} + y_{21}y_{22}, x_{11}y_{12} - x_{12}y_{11} + x_{21}y_{22} - x_{22}y_{21}),$$

$$J_{1,4}^{\{2\}} = (x_{11}^2 + y_{11}^2 - \frac{1}{2}, x_{12}^2 + y_{12}^2 - \frac{1}{2}, x_{21}^2 + y_{21}^2 - \frac{1}{2}, x_{22}^2 + y_{22}^2 - \frac{1}{2}).$$

It is easy to check that $\{\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}\}$ is a point on the variety $Z(M_2^{\{2\}})$ given above.

Step 2: Let $B_1 = \{\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}\}$. then we have a system of MUB given by $\{E, B_1\}$, and we want to extend this to a system of MUB of length 3.

Proposition 4.2.3. *Let $\{E, B_1\}$ be a system of MUB. Then any basis B_2 of $\mathbb{C}^2$, which makes the system $\{E, B_1, B_2\}$ a system of MUB, comes from a point on the real variety $Z(M_3^{\{2\}})$, where*

$$M_3^{\{2\}} = M_2^{\{2\}} + J_{2,4}^{\{2\}},$$

$$J_{2,4}^{\{2\}} = ((x_{11} + x_{21})^2 + (y_{11} + y_{21})^2 - 1, (x_{11} - x_{21})^2 + (y_{11} - y_{21})^2 - 1,$$
$$(x_{12} + x_{22})^2 + (y_{12} + y_{22})^2 - 1, (x_{12} - x_{22})^2 + (y_{12} - y_{22})^2 - 1)$$

One can check that $\{\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}\}$ is a point on the variety $Z(M_3^{\{2\}})$ given above. Therefore, the collection $\{E, B_1, B_2\}$ is a system of MUBs for the vector space $\mathbb{C}^2$, where $B_2 = \{\frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ i \end{pmatrix}, \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -i \end{pmatrix}\}$.

It is known that one cannot extend the above system of MUB to a system of MUB of length 4. The discussions given below shows that our treatment of a system of MUB can detect this with simple algebraic manipulations.

Proposition 4.2.4. *Let $\{E, B_1, B_2\}$ be a system of MUB in dimension 2 given by*

$$E = \{\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}\},$$
$$B_1 = \{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-1\end{pmatrix}\},$$
$$B_2 = \{\frac{1}{\sqrt{2}}\begin{pmatrix}1\\i\end{pmatrix}, \frac{1}{\sqrt{2}}\begin{pmatrix}1\\-i\end{pmatrix}\}.$$

Then this system cannot be extended to a system of MUB in dimension 2 of length greater than or equal to 4.

Proof. Let us assume there exists another MUB, say $B_3 = \{\begin{pmatrix}b_{12}+ic_{12}\\b_{21}+ic_{21}\end{pmatrix}, \begin{pmatrix}b_{12}+ic_{12}\\b_{22}+ic_{22}\end{pmatrix}\}$. Then it follows from Theorem 4.2.1 that $x_{ij} = b_{ij}, y_{ij} = c_{ij}, 1 \leq i, j \leq 2$ is a point in the variety $Z(M_4^{\{2\}})$, where

$$M_4^{\{2\}} = I^{\{2\}} + J_{1,4}^{\{2\}} + J_{2,4}^{\{2\}} + J_{3,4}^{\{2\}}.$$

Now we claim that $M_4^{\{2\}} = (1)$ in $R = \mathbb{K}[x_{ij}, y_{ij}, 1 \leq i, j \leq 2]$. Note that

$$\begin{aligned}
I^{\{2\}} &= (x_{11}x_{12} + y_{11}y_{12} + x_{21}x_{22} + y_{21}y_{22}, x_{11}y_{12} - x_{12}y_{11} + x_{21}y_{22} - x_{22}y_{21})\\
J_{1,4}^{\{2\}} &= (x_{11}^2 + y_{11}^2 - \frac{1}{2}, x_{12}^2 + y_{12}^2 - \frac{1}{2}, x_{21}^2 + y_{21}^2 - \frac{1}{2}, x_{22}^2 + y_{22}^2 - \frac{1}{2})\\
J_{2,4}^{\{2\}} &= ((x_{11}+x_{21})^2 + (y_{11}+y_{21})^2 - 1, (x_{11}-x_{21})^2 + (y_{11}-y_{21})^2 - 1,\\
&\qquad (x_{12}+x_{22})^2 + (y_{12}+y_{22})^2 - 1, (x_{12}-x_{22})^2 + (y_{12}-y_{22})^2 - 1)\\
J_{3,4}^{\{2\}} &= ((x_{11}+y_{21})^2 + (y_{11}-x_{21})^2 - 1, (x_{11}-y_{21})^2 + (y_{11}+x_{21})^2 - 1,\\
&\qquad (x_{12}+y_{22})^2 + (y_{12}-x_{22})^2 - 1, (x_{12}-y_{22})^2 + (y_{12}+x_{22})^2 - 1)
\end{aligned}$$

Now, we do the following simplifications in the quotient ring $R/M_4^{\{2\}}$. For our convenience, we shall write f instead of $\overline{f}$ to denote the residue class of an element $f \in R$ in the quotient

ring $R/M_4^{\{2\}}$.

$$\begin{aligned}(x_{11}+x_{21})^2+(y_{11}+y_{21})^2-1 &= x_{11}^2+x_{21}^2+y_{11}^2+y_{21}^2+2(x_{11}x_{21}+y_{11}y_{21})-1\\ &= \frac{1}{2}+\frac{1}{2}+2(x_{11}x_{21}+y_{11}y_{21})-1\\ &= 2(x_{11}x_{21}+y_{11}y_{21})\end{aligned}$$

Similarly, we get

$$(x_{11}+y_{21})^2+(y_{11}-x_{21})^2-1 = 2(x_{11}y_{21}-y_{11}x_{21})$$

Using the above two relations, and the relations given in the ideal $J_{1,4}^{\{2\}}$, we obtain

$$\begin{aligned}&(x_{11}x_{12}+y_{11}y_{12}+x_{21}x_{22}+y_{21}y_{22})^2+(x_{11}y_{12}-x_{12}y_{11}+x_{21}y_{22}-x_{22}y_{21})^2\\ &= x_{11}^2x_{12}^2+y_{11}^2y_{12}^2+x_{21}^2x_{22}^2+y_{21}^2y_{22}^2+2(x_{11}x_{12}y_{11}y_{12}+x_{11}x_{12}x_{21}x_{22}\\ &\quad+x_{11}x_{12}y_{21}y_{22}+y_{11}y_{12}x_{21}x_{22}+y_{11}y_{12}y_{21}y_{22}+x_{21}x_{22}y_{21}y_{22})+x_{11}^2y_{12}^2+x_{12}^2y_{11}^2\\ &\quad+x_{21}^2y_{22}^2+x_{22}^2y_{21}^2+2(-x_{11}y_{12}x_{12}y_{11}+x_{11}y_{12}x_{21}y_{22}-x_{11}y_{12}x_{22}y_{21}\\ &\quad-x_{12}y_{11}x_{21}y_{22}+x_{12}y_{11}x_{22}y_{21}-x_{21}y_{22}x_{22}y_{21})\\ &= x_{11}^2(x_{12}^2+y_{12}^2)+y_{11}^2(y_{12}^2+x_{12}^2)+x_{21}^2(x_{22}^2+y_{22}^2)+y_{21}^2(y_{22}^2+x_{22}^2)+\\ &\quad2(x_{11}x_{12}x_{21}x_{22}+x_{11}x_{12}y_{21}y_{22}+y_{11}y_{12}x_{21}x_{22}+y_{11}y_{12}y_{21}y_{22}+x_{11}y_{12}x_{21}y_{22}\\ &\quad-x_{11}y_{12}x_{22}y_{21}-x_{12}y_{11}x_{21}y_{22}+x_{12}y_{11}x_{22}y_{21})\\ &= \frac{1}{2}x_{11}^2+\frac{1}{2}y_{11}^2+\frac{1}{2}x_{21}^2+\frac{1}{2}y_{21}^2+2\{x_{11}x_{21}(x_{12}x_{22}+y_{12}y_{22})+x_{11}y_{21}(x_{12}y_{22}-y_{12}x_{22})\\ &\quad+y_{11}x_{21}(y_{12}x_{22}-x_{12}y_{22})+y_{11}y_{21}(y_{12}y_{22}+x_{12}x_{22})\}\\ &= \frac{1}{2}\cdot\frac{1}{2}+\frac{1}{2}\cdot\frac{1}{2}+2\{(x_{11}x_{21}+y_{11}y_{21})(x_{12}x_{22}+y_{12}y_{22})\\ &\qquad+(x_{11}y_{21}-y_{11}x_{21})(x_{12}y_{22}-y_{12}x_{22})\}=\frac{1}{2}.\end{aligned}$$

This shows that $\frac{1}{2}\in M_4^{\{2\}}$, and hence $M_4^{\{2\}}=(1)$ in R. Therefore, the given system of MUB cannot be extended to a system of MUB of length 4. □

4.2.3 Results On Complete Intersection

In this subsection, we study the ideals arising from the MUBs from a view of commutative algebra. In the following theorem, we show that the ideal $J_{1,d}^{\{m\}}$ is a prime ideal generated by a regular sequence.

Theorem 4.2.2. *Let $A_1, A_2, \ldots, A_{m-1}$ be a system of MUBs, and assume that $A_1 = I_d$, the identity matrix. Then $J_{1,m}^{\{d\}}$ is a complete intersection prime ideal.*

Proof. Let $J_{1,m}^{\{d\}} = (f_1, \ldots, f_{d^2})$. Note that $lcm(in(f_i), in(f_j)) = in(f_i)in(f_j)$ for all $i \neq j$, and hence by Lemma 2.7.1 the S-polynomials $S(f_i, f_j)$ reduces to 0 with respect to $f_1, \ldots, f_{m^2}$. Therefore, by Theorem 2.7.2, $\{f_1, \ldots, f_{d^2}\}$ is a Gröbner basis of $J_{1,m}^{\{d\}}$. Note that $(in(f_1), \ldots, in(f_{d^2}))$ is complete intersection ideal, as $\{in(f_i), 1 \leq i \leq d^2\}$ are monomials with $Supp(f_i) \cap Supp(f_j) = \phi$ for all $i \neq j$. Therefore, $J_{1,m}^{\{d\}}$ is also a complete intersection ideal.

To show that $R/J_{1,m}^{\{d\}}$ is a domain, we consider the following embedding of rings:

$$S/J_{1,m}^{\{d\}} = \frac{\mathbb{R}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]}{J_{1,m}^{\{d\}}} \hookrightarrow \frac{\mathbb{C}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]}{J_{1,m}^{\{d\}}},$$

where the embedding is defined by sending any $r \in \mathbb{R}$ to $r \in \mathbb{C}$, and $\overline{x_{ij}}, \overline{y_{ij}} \in S/J_{1,m}^{\{d\}}$ to $\overline{x_{ij}}, \overline{y_{ij}} \in \frac{\mathbb{C}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]}{J_{1,m}^{\{d\}}}$ respectively. If we can show that the ring $\frac{\mathbb{C}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]}{J_{1,m}^{\{d\}}}$ is a domain, then we are through. As $J_{1,m}^{\{d\}} = (x_{ij}^2 + y_{ij}^2 - \frac{1}{d} : 1 \leq i, j \leq d)$, we can write

$$\frac{\mathbb{C}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]}{J_{1,m}^{\{d\}}} = \bigotimes_{1 \leq i,j \leq d} \frac{\mathbb{C}[x_{ij}, y_{ij}]}{(x_{ij}^2 + y_{ij}^2 - \frac{1}{d})}.$$

Now, we shall show that $\frac{\mathbb{C}[x_{ij}, y_{ij}]}{(x_{ij}^2 + y_{ij}^2 - \frac{1}{d})}$ is an integral domain for all $1 \leq i, j \leq d$. Note that there is an isomorphism

$$\frac{\mathbb{C}[U_{ij}, V_{ij}]}{(U_{ij}V_{ij} - 1)} \cong \frac{\mathbb{C}[x_{ij}, y_{ij}]}{(x_{ij}^2 + y_{ij}^2 - \frac{1}{d})}$$

by identifying $U_{ij} \mapsto x_{ij} + iy_{ij}$ and $V_{ij} \mapsto x_{ij} - iy_{ij}$. But the ring $\frac{\mathbb{C}[U_{ij}, V_{ij}]}{(U_{ij}V_{ij} - 1)}$ is a localization of the polynomial ring $\mathbb{C}[U_{ij}]$ at the multiplicatively closed set $\{1, U_{ij}, U_{ij}^2, \ldots\}$. Therefore the ring $\frac{\mathbb{C}[U_{ij}, V_{ij}]}{(U_{ij}V_{ij} - 1)}$, being localization of an integral domain, is also an integral domain. As tensor product of integral domains is again an integral domain, we conclude that $\bigotimes_{1 \leq i,j \leq d} \frac{\mathbb{C}[x_{ij}, y_{ij}]}{(x_{ij}^2 + y_{ij}^2 - \frac{1}{d})}$ is an integral domain. Therefore, the ring $\frac{\mathbb{C}[x_{ij}, y_{ij} : 1 \leq i, j \leq d]}{J_{1,m}^{\{d\}}}$ is an integral domain, and hence the ideal $J_{1,m}^{\{d\}}$ is a prime ideal generated by a regular sequence. □

As an immediate consequence, we have the following

Corollary 4.2.2. *For any $m, d \in \mathbb{N}$, $ht(J_{1,m}^{\{d\}}) = d^2$.*

Proof. Since $J_{1,m}^{\{d\}}$ is generated by a regular sequence in a polynomial ring, by [62, Theorem 17.4.] we have $ht(J_{1,m}^{\{d\}}) = d^2$. □

The next result shows that the ideal $J_{1,m}^{\{d\}}$ coming from the system of MUBs with real entries is a prime ideal generated by a regular sequence.

Theorem 4.2.3. *Let $A_1, A_2, \ldots, A_{m-1}$ be a system of MUB, and assume that $A_1 = I_d$, the identity matrix. Then $J_{1,m}^{\{d\}}$ is a maximal ideal generated by a regular sequence, where $J_{1,m}^{\{d\}}$ is the ideal coming from the system of MUBs with real entries, given by*

$$J_{1,m}^{\{d\}} = (x_{ij} - \frac{1}{\sqrt{d}} : 1 \leq i, j \leq d)$$

Proof. Observe that $\frac{\mathbb{R}[x_{ij}:1\leq i,j\leq d]}{(x_{ij}-\frac{1}{\sqrt{d}}:1\leq i,j\leq d)} \cong \mathbb{R}$, and hence the assertion holds. □

We conclude this section with an open-ended question as conjecture that came out of our study of the defining ideals of a system of MUBs.

Conjecture 4.2.1. *Let $A_1, A_2, \ldots, A_{m-1}$ be a system of MUB, and assume that $A_1 = I_d$, the identity matrix. Then the ideal $I^{\{d\}} + J_{1,m}^{\{d\}}$ is a prime ideal generated by a regular sequence. Moreover, $ht(I^{\{d\}} + J_{1,m}^{\{d\}}) = 2d^2 - d$.*

4.3 Maximal Commuting Bases and MUBs

The question that we are discussing in this initiative is related to examine algebraic results related to MUBs. In this regard, we consider extending the result of [5, Theorems 3.2 and 3.4] under the hypothesis related to existence of normal matrices. We prove that there is an one-to-one correspondence between the MUBs and the maximal commuting classes (bases) of orthogonal normal matrices in $\mathbb{C}^d$. It means that for m MUBs in $\mathbb{C}^d$, there are m commuting classes each consisting of d commuting orthogonal normal matrices. The existence of maximal commuting basis for $\mathcal{M}_d(\mathbb{C})$ ensures the complete sets of MUBs in $\mathcal{M}_d(\mathbb{C})$.

Let $\mathcal{M}_d(\mathbb{C})$ denote the set of all $d \times d$ complex matrices. For any matrix $A \in \mathcal{M}_d(\mathbb{C})$, we use the standard notation $A^\dagger$ to denote the transpose of the conjugate matrix A. Two matrices $A, B \in \mathcal{M}_d(\mathbb{C})$ are orthogonal iff their trace inner product $< A, B >= tr(A^\dagger B) = 0$.

An $d \times d$ complex matrix $A \in \mathcal{M}_d(\mathbb{C})$ is called *unitarily diagonalizable* if $U^\dagger AU$ is diagonal for some unitary matrix U. Let us now present a few technical results.

Lemma 4.3.1. *An $d \times d$ complex matrix A is unitarily diagonalizable if and only if A is normal.*

Proof. Suppose A is unitarily diagonalizable. Then there exists a unitary matrix U and a diagonal matrix D such that

$$A = UDU^*.$$

Taking conjugate transpose gives

$$A^* = UD^*U^*.$$

Hence

$$AA^* = (UDU^*)(UD^*U^*) = UDD^*U^*, \qquad A^*A = (UD^*U^*)(UDU^*) = UD^*DU^*.$$

Since D is diagonal, hence $DD^* = D^*D$. Therefore,

$$AA^* = UDD^*U^* = UD^*DU^* = A^*A,$$

so A is normal.

Now suppose A is normal, i.e., $AA^* = A^*A$. By the Complex Spectral Theorem (also called the Spectral Theorem for normal matrices), a normal matrix on $\mathbb{C}^d$ admits an orthonormal basis of eigenvectors. Equivalently, there exists a unitary matrix U whose columns are orthonormal eigenvectors of A such that

$$U^*AU = D$$

is diagonal (with the eigenvalues of A on the diagonal). Thus

$$A = UDU^*,$$

showing that A is unitarily diagonalizable. □

Lemma 4.3.2. *There are at most d pairwise orthogonal commuting normal matrices in $\mathcal{M}_d(\mathbb{C})$.*

Proof. Let $A_1, \ldots, A_m$ be pairwise orthogonal commuting normal matrices in $\mathcal{M}_d(\mathbb{C})$. From lemma 4.3.1, there exists a unitary matrix, say $U \in \mathcal{M}_d(\mathbb{C})$, such that they are simultaneously diagonalizable. Then, the matrices $U^*A_1U, \ldots, U^*A_mU$ are a collection of diagonal orthogonal matrices. In this way, we get m orthogonal vectors which are basically the diagonal of $U^\dagger A_i U$ for $i = 1, 2, \ldots, m$. Therefore, $m \leq d$. □

Let $\mathcal{B} = \{U_1, \ldots, U_{d^2}\}$ be a basis of normal matrices of $\mathcal{M}_d(\mathbb{C})$ such that U_1 is the identity matrix $I_d \in \mathcal{M}_d(\mathbb{C})$. We say that the basis $\mathcal{B}$ is a *maximal commuting basis* for $\mathcal{M}_d(\mathbb{C})$ if B can be partitioned as

$$\mathcal{B} = \{I_d\} \cup \mathcal{C}_1 \cup \cdots \mathcal{C}_{d+1}$$

where each contains exactly $d-1$ commuting matrix from $\mathcal{B}$. In the next two theorems, we extend the result of [5, Theorems 3.2 and 3.4] under the hypothesis of existence of normal matrices.

Theorem 4.3.1. *If there is a maximal commuting basis of orthogonal normal matrices in $\mathcal{M}_d(\mathbb{C})$, then there is a set of $d+1$ mutually unbiased bases.*

Proof. Let $\mathcal{B}$ be a maximal commuting basis of orthogonal normal matrices in $\mathcal{M}_d(\mathbb{C})$. Consider the decomposition of $\mathcal{B}$ as follows:

$$\mathcal{B} = \{I_d\} \cup \mathcal{C}_1 \cup \cdots \cup \mathcal{C}_{d+1}.$$

For $1 \leq i \leq d+1$, we set

$$\mathcal{C}_i' = \{I_d\} \cup \mathcal{C}_i = \{U_{i,0}, U_{i,1}, \ldots, U_{i,d-1}\}.$$

Then by Lemma 4.3.2, each $\mathcal{C}_i'$ is a maximal set of pairwise orthogonal commuting normal matrices in $\mathcal{M}_d(\mathbb{C})$. Then for each $1 \leq i \leq d+1$, there is a unitary matrix V_i such that $V_i^* U_{i,t} V_i$ are diagonal matrices for each $0 \leq t \leq d-1$. Let $V_i = \{|v_1^i\rangle, |v_2^i\rangle, ..., |v_d^i\rangle\}$, where $|v_k^i\rangle$ are the column vectors of V_i. Then for all $0 \leq t \leq d-1$,

$$U_{i,t} = \sum_{k=1}^{d} \lambda_{i,t,k} |v_k^i\rangle \langle v_k^i|$$

We claim that, the matrices $V_1, \ldots, V_{d+1}$ form a system of MUBs. It suffices to show that $|\langle v_k^i \mid v_l^j \rangle|^2 = \frac{1}{d}$ for all $1 \leq i, j \leq d+1$ and $1 \leq k, l \leq d$. Now, due to the orthogonality of

the collection $\mathcal{B}$, it follows that

$$\mathrm{Tr}(U_{i,p}^* U_{j,q}) = \begin{cases} d & \text{if } p = q = 0, \\ 0 & \text{otherwise.} \end{cases}$$

On the other hand,

$$\begin{aligned} \mathrm{Tr}(U_{i,p}^* U_{j,q}) &= \mathrm{Tr}((\sum_{k=1}^{d} \lambda_{i,p,k} \left|v_k^i\right\rangle \left\langle v_k^i\right|)^* \sum_{l=1}^{d} \lambda_{j,q,l} \left|v_l^j\right\rangle \left\langle v_l^j\right|) \\ &= \sum_{k=1}^{d} \sum_{l=1}^{d} \lambda_{i,p,k}^* \lambda_{j,q,l} \mathrm{Tr}((\left|v_k^i\right\rangle \left\langle v_k^i\right|)^* (\left|v_l^j\right\rangle \left\langle v_l^j\right|)) \\ &= \sum_{k=1}^{d} \sum_{l=1}^{d} \lambda_{i,p,k}^* \lambda_{j,q,l} |\left\langle v_k^i \mid v_l^j\right\rangle|^2. \end{aligned}$$

Therefore, comparing the above, we obtain for all $1 \leq i, j \leq d+1$ and $0 \leq p, q \leq d-1$,

$$\sum_{k=1}^{d} \sum_{l=1}^{d} \lambda_{i,p,k}^* \lambda_{j,q,l} |\left\langle v_k^i \mid v_l^j\right\rangle|^2 = \begin{cases} d & \text{if } p = q = 0, \\ 0 & \text{otherwise.} \end{cases}$$

For each $1 \leq i \leq d+1$, consider the matrices M_i whose k^{th} row is the diagonal entries of the matrix $V_i U_{i,k} V_i^*$. Then M_i is a unitary matrix for all $1 \leq i \leq d+1$. Note that the above equality can be written as $AP = \lambda$, where

$$\begin{aligned} A &= M_i^* \otimes M_j \\ P &= (|\left\langle v_1^i \mid v_1^j\right\rangle|^2, |\left\langle v_2^i \mid v_2^j\right\rangle|^2, \ldots, |\left\langle v_d^i \mid v_d^j\right\rangle|^2)^T \\ \lambda &= (d, 0, 0, \ldots, 0)^T \end{aligned}$$

Since A is again an unitary matrix whose first row is the vector $(1, 1, \ldots, 1)$, it follows that $|\left\langle v_k^i \mid v_l^j\right\rangle|^2 = \frac{1}{d}$ for $1 \leq k, l \leq d$. □

Now we require a technical result.

Lemma 4.3.3. *Consider $\mathbb{C}^d$, let $\{1 = v_1, v_2, \ldots, v_d\}$ be the orthonormal basis vector of $\mathbb{C}^d$ where $1 = \frac{1}{\sqrt{d}} \begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \end{bmatrix}^t = v_1$. If $v_j = \{v_{j1}, v_{j2}, ..., v_{jd}\}$ then $< v_1, v_j >= 0$, that means $\sum_i v_{ji} = 0$; $\forall j = 2, 3, \ldots, d$.*

Using the above lemma, we prove the following result.

Theorem 4.3.2. *Let $B_1, B_2, \ldots, B_m$ be a set of MUBs in $\mathbb{C}^d$. Then there are m classes $C_1, C_2, \ldots, C_m$ each consisting of d commuting normal matrices, such that matrices in $C_1 \cup C_2 \cup \ldots \cup C_m$ are pairwise orthogonal.*

Proof. Let $B_j = \{|\psi_1^j\rangle, |\psi_2^j\rangle, \ldots, |\psi_d^j\rangle\}$. Then

$$\langle \psi_s^j | \psi_t^j \rangle = \delta_{s,t}; 1 \leq s, t \leq d.$$
$$|\langle \psi_s^j | \psi_t^j \rangle|^2 = \frac{1}{d}, 1 \leq j < k \leq m; 1 \leq s, t \leq d.$$

We label the matrices in the class C_j as $C_j = \{U_{j1}, U_{j2}, \ldots, U_{jd}\}$ where

$$U_{jt} = \sum_{i=1}^{d} v_{ti} |\psi_i^j\rangle \langle \psi_i^j| ; t = 1, 2, \ldots, d.$$

Note that $U_{j1} = I_d$ for $j = 1, 2, \ldots, m$ and U_{js}, U_{jt} are commuting, because both are diagonal relative to basis B_j. Finally U_{js} are normal matrices as

$$U_{js} U_{js}^\dagger = \left(\sum_{k=1}^{d} v_{sk} |\psi_k^j\rangle \langle \psi_k^j| \right) \left(\sum_{i=1}^{d} v_{si} |\psi_i^j\rangle \langle \psi_i^j| \right)^\dagger$$

$$= \sum_{k,i=1}^{d} v_{sk} \overline{v_{si}} \, |\psi_k^j\rangle \langle \psi_k^j | \psi_i^j \rangle \langle \psi_i^j| = \sum_{k=1}^{d} |v_{sk}|^2 |\psi_k^j\rangle \langle \psi_k^j| = U_{js}^\dagger U_{js}$$

Now we show that any pair of matrices U_{js}, U_{kj} are orthogonal if $s = j \neq 1$ in [consider $(js) \neq (kt)$].

$$\begin{aligned}
\langle U_{js}, U_{kt} \rangle &= \mathrm{Tr}(U_{js}^\dagger U_{kt}) \\
&= \mathrm{Tr} \left(\left(\sum_{m=1}^{d} v_{sm} |\psi_m^j\rangle \langle \psi_m^j| \right)^\dagger \left(\sum_{i=1}^{d} v_{ti} |\psi_i^k\rangle \langle \psi_i^k| \right) \right) \\
&= \mathrm{Tr} \left(\sum_{m=1}^{d} \sum_{i=1}^{d} v_{ti} v_{sm}^\dagger |\psi_m^j\rangle \langle \psi_m^j | \psi_i^k \rangle \langle \psi_i^k| \right)
\end{aligned}$$

Now,

$$\langle \psi_m^j | \psi_i^k \rangle = \begin{cases} \delta_{mi}, & \text{if } j = k, \\ \frac{1}{\sqrt{d}}, & \text{if } j \neq k \end{cases}$$

Thus,

$$\begin{aligned} \langle U_{js}, U_{kt} \rangle &= \mathrm{Tr} \left(\sum_{m,i} v_{sm}^\dagger v_{ti} \, |\psi_m^j\rangle \langle \psi_m^j | \psi_i^k \rangle \langle \psi_i^k | \right) \\ &= \sum_{m,i} v_{sm}^\dagger v_{ti} \, \mathrm{Tr} \left(|\psi_m^j\rangle \langle \psi_m^j | \psi_i^k \rangle \langle \psi_i^k | \right) \\ &= \sum_{m,i} v_{sm}^\dagger v_{ti} \left| \langle \psi_m^j | \psi_i^k \rangle \right|^2 \end{aligned}$$

If $j = k$, then $\langle v_{js}, v_{kt} \rangle = \sum_m v_{sm}^\dagger v_{tm} = \langle v_s, v_t \rangle = 0$.

If $j \neq k$, then $\langle v_{js}, v_{kt} \rangle = \sum_{m,i} v_{sm}^\dagger v_{ti} \cdot \frac{1}{d} = \frac{1}{d} \sum_{m,i} v_{sm}^\dagger v_{ti} = \frac{1}{d} \left(\sum_m v_{sm}^\dagger \right) \left(\sum_i v_{ti} \right) = \frac{1}{d} \times 0 \times 0 = 0$.

□

We now present an example for $d = 4$. There are five mutually unbiased bases, denoted by (I, B_2, B_3, B_4, B_5), in dimension $d = 4$. Hence, we have five commuting classes $(C_1, C_2, C_3, C_4, C_5)$, each containing four orthogonal normal matrices. Let $B = \{1 = v_1, v_2, v_3, v_4\}$ be an orthonormal basis of $\mathbb{C}^4$, where each basis vector $v_j = \{v_{j1}, v_{j2}, v_{j3}, v_{j4}\}$. Here,

$$\begin{aligned} 1 = v_1 &= \frac{1}{2}(1, 1, 1, 1)^\dagger, \\ v_2 &= \frac{1}{2}(1, 0, -1, 0)^\dagger, \\ v_3 &= \frac{1}{2}(0, 1, 0, -1)^\dagger, \\ v_4 &= \frac{1}{2}(1, -1, 1, -1)^\dagger. \end{aligned}$$

These are five MUBs for $d = 4$ as follows.

$$B_1 = I_4 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \quad B_2 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \\ 1 & -1 & 1 & -1 \end{bmatrix}, \quad B_3 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ -1 & -1 & 1 & 1 \\ -i & i & i & -i \\ -i & i & -i & i \end{bmatrix},$$

$$B_4 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ -i & -i & i & i \\ -i & i & i & -i \\ -1 & 1 & -1 & 1 \end{bmatrix}, \quad B_5 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ -i & -i & i & i \\ -1 & 1 & -1 & 1 \\ -i & i & i & -i \end{bmatrix}.$$

Following Theorem 4.3.2, we obtain the following five (maximal) commuting basis $(C_1, C_2, C_3, C_4, C_5)$, each containing four orthogonal normal commuting matrices and the

first one is identity.

$$C_1 = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} \right\}$$

$$C_2 = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & 2 & 2 & 0 \\ 2 & 0 & 0 & 2 \\ 2 & 0 & 0 & 2 \\ 0 & 2 & 2 & 0 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & 2 & -2 & 0 \\ 2 & 0 & 0 & -2 \\ -2 & 0 & 0 & 2 \\ 0 & -2 & 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \right\}$$

$$C_3 = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & 2 & 2i & 0 \\ -2 & 0 & 0 & -2i \\ -2i & 0 & 0 & 2 \\ 0 & 2i & 2 & 0 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & -2 & -2i & 0 \\ -2 & 0 & 0 & 2i \\ 2i & 0 & 0 & 2 \\ 0 & -2i & 2 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & i \\ 0 & 0 & -i & 0 \\ 0 & i & 0 & 0 \\ -i & 0 & 0 & 0 \end{bmatrix} \right\}$$

$$C_4 = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & 2i & 2i & 0 \\ -2i & 0 & 0 & 2i \\ -2i & 0 & 0 & 2i \\ 0 & -2i & -2i & 0 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & 2i & -2i & 0 \\ -2i & 0 & 0 & -2i \\ 2i & 0 & 0 & 2i \\ 0 & 2i & -2i & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \end{bmatrix} \right\}$$

$$C_5 = \left\{ \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & 2i & 0 & 2i \\ -2i & 0 & 2i & 0 \\ 0 & -2i & 0 & -2i \\ -2i & 0 & 2i & 0 \end{bmatrix}, \frac{1}{4}\begin{bmatrix} 0 & 2i & 0 & -2i \\ -2i & 0 & -2i & 0 \\ 0 & 2i & 0 & -2i \\ 2i & 0 & 2i & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ -1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix} \right\}.$$

This concludes the example.

4.4 Conclusion

As it is well known, the problem of extending a system of MUBs is in general a difficult problem. Our approach to solving this essentially boils down to finding real solutions to some specific system of polynomial equations over $\mathbb{R}$. Our work presents relevant theoretical study in this direction for further insight. In general, the main difficulty is the complexity of the Gröbner basis algorithm, which is very high in general. However, our result regarding

complete intersection demonstrated that it is possible to reduce the number of equations using techniques from commutative algebra. We have also shown that there is a one-to-one correspondence between MUBs and the maximal commuting classes (bases) of orthogonal normal matrices.

Chapter 5

A parametric Class of Mutually Unbiased Bases Using Resolvable Block Designs

In the preceding two chapters, we focused on the *extensibility* problem for a given set of Mutually Unbiased Bases, exploring whether an additional MUB can be added to a given collection in various dimensions. In this chapter, we consider the parameterisation of MUBs, allowing for the exploration of several classes for different applications. For dimension $d = s^2$, we present the construction of affine-parametric classes with $MOLS(s) + 2$ many MUBs, where $MOLS(s)$ is the number of Mutually Orthogonal Latin Squares of dimension s. If s is a power of a prime, then $MOLS(s) = s - 1$, and the number of MUBs will be $s + 1$. Considering the first one to be the identity matrix, in our construction, each of the rest $MOLS(s) + 1$ MUBs will have at least $s(s - 1)$ free parameters, so that a global unitary operation cannot absorb. Our result produces a larger number of MUBs, as well as more free parameters, in most cases. This can help in exploring various choices of MUBs in the protocols for higher-dimensional QKDs and other applications of MUBs related to quantum information.

5.1 Introduction

Let us now explain the problem that we are considering here.

In this chapter, we consider the introduction of free parameters in the sets of MUBs in the dimension d, with $d = s^2$. Thus, written in this manner, the contribution of [34] tells that any set of m real MUBs existing in dimension $d > 2$ can admit the introduction of $\frac{(m-1)d}{2} = \frac{(m-1)s^2}{2}$ free parameters that a global unitary operation cannot absorb. In our construction, we obtain $MOLS(s)+2$ MUBs, which is independent of the existence of m real MUBs. We consider the first MUB in our construction as the identity matrix. Each of the rest $MOLS(s)+1$ MUBs has $s(s-1)$, i.e., in total $(MOLS(s)+1)s(s-1)$ free parameters. In case, when $MOLS(s) = s-1$, the total number of free parameters is $s^2(s-1)$. Our construction produces a larger number of MUBs, as well as more free parameters, in most cases, though not universally.

5.1.1 Organization & Contribution

First, we provide the outline for the construction of real MUBs in dimension $d = s^2$. We take the dimension $d = s^2$, and consider the Resolvable Block Design (RBD) having s^2 entities. To construct RBD, we start with Mutually Orthogonal Latin Square (MOLS) of order s. For each MOLS of order s, we have $MOLS(s) + 2$ parallel classes in the RBD of order s^2. We convert each of the parallel classes into orthonormal bases using the Hadamard matrix of order s. If there exists a real Hadamard matrix of order s, then we will get only real MUBs. However, if we do not have the real ones, then we need to consider a complex Hadamard matrix of order s, which is guaranteed in every dimension. Using complex Hadamard matrices of order s, we will obtain complex MUBs. The general idea described above is adapted from [57], and a formal presentation of the construction is given in Subsection 5.1.1.

Our contributory results considering parametrization in the set of MUBs for dimension $d = s^2$, are presented in Section 5.2. A detailed comparison with existing works, particularly with the results of [34], is provided in Subsection 5.2.3. Finally, Section 5.3 concludes this chapter.

The basic idea from [57]

Our construction follows the method provided in [57] using *Resolvable Block Designs* (RBD). For more details about RBD, see [57] and the references therein. To proceed, we need to refer [57, Construction 1] first. We follow the same notation as in [57] and present the necessary background. In this direction, the construction of an orthonormal basis using a parallel class from an RBD (X, A), is as follows.

Construction 5.1.1.

1. *In a design (X, A), choose the elements of X as any set of orthonormal basis vectors of $\mathbb{C}^d$. That is, if $|X| = d$, then $X = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\}$, such that $\langle\psi_i|\psi_j\rangle = \delta_{ij}$. Hence, A, which contains blocks made out of the elements from X, would now consist of blocks with the elements from the set of chosen orthonormal basis vectors.*

2. *Let $B = \{b_1, b_2, \ldots, b_s\}$ be one of the parallel class of the design (X, A), where b_i's are disjoint blocks containing elements from X. Since B is a parallel class, this implies $X = b_1 \cup b_2 \cup \ldots \cup b_s$, and $b_i \cap b_j = \phi$ for all $1 \leq i \neq j \leq s$.*

3. *Consider one of the blocks $b_r = \{|\psi_{r_1}\rangle, |\psi_{r_2}\rangle, \ldots, |\psi_{r_{n_r}}\rangle\} \in B$ and let $|b_r| = n_r$. Corresponding to this block, choose any $n_r \times n_r$ unitary matrix whose elements are say u^r_{ij}, $i, j = 1, 2, \ldots, n_r$.*

4. *Next construct n_r many vectors in the following manner, using b_r and u^r_{ij}.*

$$|\phi^r_i\rangle = u^r_{i1}|\psi_{r_1}\rangle + u^r_{i2}|\psi_{r_2}\rangle + \ldots + u^r_{in_r}|\psi_{r_{n_r}}\rangle = \sum_{k=1}^{n_r} u^r_{ik}|\psi_{r_k}\rangle : i = 1, 2, \ldots, n_r.$$

5. *In a similar manner, corresponding to each block $b_j \in B$, construct n_j many vectors where $|b_j| = n_j$, using any $n_j \times n_j$ unitary matrix. Since $\sum_{j=1}^{s} n_j = d$, we will get exactly d many vectors.*

Let us construct the matrix M_B of size $d \times d$ having column vectors as $|\phi^r_i\rangle$. Therefore, $M_B = \left(|\phi^1_1\rangle, \ldots, |\phi^1_{n_1}\rangle, |\phi^2_1\rangle, \ldots, |\phi^2_{n_2}\rangle, \ldots, |\phi^s_1\rangle, \ldots, |\phi^s_{n_s}\rangle\right)$. From [57, Lemma 1], the $|\phi^r_i\rangle$'s corresponding to a parallel class B of X form an orthonormal set of basis vectors. Hence, M_B is a unitary matrix. In this regard, we have the following lemma as per Construction 5.1.1. Later Example 5.2.1 provides a more detailed view on this.

Lemma 5.1.1. *Refer to Construction 5.1.1 and the unitary matrix M_B above. If X consists of the computational basis vectors, then $M_B = P_B H$, where P_B is a permutation matrix of size $d \times d$ and H is a block diagonal matrix consisting of unitary matrices of size $n_j \times n_j$ $(j = 1, 2, \ldots, s)$ as block matrices.*

Proof. Using Construction 5.1.1, we obtain the set of orthonormal basis vectors $|\phi_i^l\rangle$'s over $d-$ dimensional vector space, by choosing elements of X as computational basis vectors. That is, $X = \{|i\rangle : i = 1, 2, \ldots, d\}$, where $|i\rangle$ is a column vector of size $d \times 1$ which has all the entries as zero except the i^{th} one, which is 1.

Let us refer to [57, Construction 1]. From each block B_l of size n_l, one gets n_l many basis vectors. These basis vectors can be arranged as columns of $d \times n_l$ size matrix i.e., $\left[|\phi_1^l\rangle \ \ldots \ |\phi_{n_1}^l\rangle\right]$. From construction, this matrix can be written as

$$\left[|\phi_1^l\rangle \ \ldots \ |\phi_{n_1}^l\rangle\right] = \left[|\psi_{l_1}\rangle \ |\psi_{l_2}\rangle \ldots |\psi_{l_{n_l}}\rangle\right] H^{l^\dagger},$$

where $H^{l^\dagger}$ is the Hadamard matrix of size $n_l \times n_l$ and $|\psi_{l_i}\rangle \in X$. Now, concatenating all the column vectors constructed from different blocks, which are s in numbers, we have the unitary matrix M_B, where

$$M_B = \left[|\phi_1^1\rangle \ldots |\phi_{n_1}^1\rangle \ |\phi_1^2\rangle \ldots |\phi_{n_2}^2\rangle \ \ldots |\phi_1^s\rangle \ \ldots |\phi_{n_s}^s\rangle\right] =$$

$$\left[|\psi_{1_1}\rangle \ \ldots |\psi_{1_{n_1}}\rangle \ |\psi_{2_1}\rangle \ldots |\psi_{2_{n_2}}\rangle \ldots \ |\psi_{s_1}\rangle \ldots \ |\psi_{s_{n_s}}\rangle\right] \begin{pmatrix} H^{1^\dagger} & 0 & \ldots & 0 & 0 \\ 0 & H^{2^\dagger} & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & H^{(s-1)^\dagger} & 0 \\ 0 & 0 & \ldots & 0 & H^{s^\dagger} \end{pmatrix}.$$

Given that $|\phi_i\rangle$'s are the orthonormal basis vectors, we have the unitary matrix $M_B = \left[|\phi_1^1\rangle \ldots |\phi_{n_1}^1\rangle \ |\phi_1^2\rangle \ldots |\phi_{n_s}^s\rangle\right]$. This is also evident from above, as it is a product of two unitary matrices. Note that $|\psi_{l_i}\rangle \in X$, which are the columns of computational basis vectors. Since the blocks of the parallel class form the partition of X, each computational basis vector appears exactly once in any one of the blocks.
Thus $\left[|\psi_{1_1}\rangle \ldots |\psi_{1_{n_1}}\rangle |\psi_{1_1}\rangle \ldots |\psi_{1_{n_1}}\rangle \ldots |\psi_{1_1}\rangle \ldots |\psi_{1_{n_1}}\rangle\right]$ is a permutation matrix and let us name it as P_B, which is decided by the parallel class $\mathcal{P}$. Since $H^{j^\dagger}$ are unitary matrix, we have $M_B = P_B H$, where H is a block diagonal Hadamard matrix, where each block consists

of a Hadamard matrix whose size is equal to the size of the blocks of the parallel class, and P is a permutation matrix, which is decided by the elements in the blocks of the parallel class. □

Thus, we see that the number of unitary matrices constructed using the RBDs is dependent on the number of parallel classes. In this regard, we have the existing theorem from [60], which in turn follows from the result of [84], which we present here.

Theorem 5.1.1. *Consider an RBD (X, A) such that $|X| = s^2$, then one can construct $MOLS(s) + 2$ many parallel classes, each having s many blocks of size s and any two blocks from different parallel classes will have exactly one point in common.*

We also need the following technical results.

Lemma 5.1.2. *Let M_1 and M_2 be a pair of MUBs in d-dimensional vector space. Then $M_1^\dagger M_2$ is a Hadamard matrix.*

Proof. Let $M_1 = [v_1\, v_2\, \dots v_d]$ and $M_2 = [w_1\, w_2\, \dots w_d]$. Then, from Definition 1.1.1, $(M_1^\dagger M_2)_{i,j} = \overline{v_i}.w_j = \frac{\exp(\iota\phi_{ij})}{\sqrt{d}}$ for some ϕ_{ij} called phase factor. Further, since M_1 and M_2 are unitary matrices, $M_1^\dagger M_2$ is also a unitary matrix. Hence, $M_1^\dagger M_2$ is a Hadamard matrix. □

Note that, if H is a Hadamard matrix, then it is also an MUB with respect to the Identity matrix. Since we can generate a pair of MUBs in parametric form using Construction 5.1.1, one can use this idea to construct a Hadamard matrix in parametric form for any composite dimension. We now state the following technical results that will be used later for parameterisation.

Lemma 5.1.3. *If D_1 is a diagonal matrix and P_1 is a permutation matrix, then $D_1P_1 = P_1D_2$ for some diagonal matrix D_2, having the same diagonal entries as those of D_1.*

Proof. For a permutation matrix, we have $P_1^{-1} = P_1^T$. Hence $D_2 = P_1^T D_1 P_1$. Thus, if P_1 is modified by changing the l^{th} column to the k^{th} column, then P_1^T will also be modified by the movement of the l^{th} row to the k^{th} row. Thus $(D_2)_{kk} = (D_1)_{ll}$, and hence D_2 will be a diagonal matrix having the same diagonal entries as in D_1. In fact, if P_1 is represented by σ, then $(D_2)_{\sigma(l)\sigma(l)} = (D_1)_{ll}$. □

Lemma 5.1.4. *For any square matrix M if $MD_1 = D_2M$, where D_1 and D_2 are diagonal matrices, then $D_1 = D_2 = \alpha \mathrm{I}$, where α is some constant.*

Proof. Since D_1 and D_2 are diagonal matrices, they can be expressed as

$$D_1 = \mathrm{diag}(d_{11}, d_{12}, \ldots, d_{1n}), \quad D_2 = \mathrm{diag}(d_{21}, d_{22}, \ldots, d_{2n}),$$

Since we have, $MD_1 = D_2M$, consider the $(ij)^{th}$ elements for both sides. We will have,

$$(MD_1)_{ij} = M_{ij}d_{1j} = d_{2i}M_{ij} = (D_2M)_{ij}.$$

This equation implies that either $M_{ij} = 0$ or $d_{1j} = d_{2i}$. Since M is any square matrix, so we have $d_{1j} = d_{2i}$ for all ij's. Hence all the diagonal elements are constant, say α. So, $D_1 = D_2 = \alpha I$. □

From the above, we immediately have the following result.

Corollary 5.1.1. *For a general block diagonal matrix M_B if $M_BD_1 = D_2M_B$, where D_1 and D_2 is a diagonal matrix then $D_1 = D_2 = D_I$ where D_I is a block diagonal matrix, such that non zero block matrices are, of the form $\alpha_r \mathrm{I}_r$. The size of the blocks is equal to the size of the blocks in the matrix M_B and α_r is a constant for each block.*

5.2 Construction of Affine parametric form of MUBs for square dimension, $d = s^2$

If $|X| = d = s^2$, then we can construct RBD (X, A) such that it has $MOLS(s) + 2$ many parallel classes, each having s many blocks of size s such that blocks from different parallel classes will have exactly one point in common. Suppose, the $MOLS(s) + 2$ many parallel classes are denoted by $C_1, C_2, \ldots, C_w$.

Then, the above construction method would produce $MOLS(s) + 2$ number of MUBs. Moreover, when $s = p$, a prime number, $MOLS(p) = p - 1$ and in such a scenario, one can construct $(p + 1)$ many MUBs of dimension $p^2 = d$. Toward the end of this Section, we estimate the maximum permissible free parameters in the newly constructed set of MUBs. Let us now describe the following construction in line with Theorem 5.1.1 (see [60] for more details).

Construction 5.2.1. *Let (X, A) be an RBD such that $|X| = d = s^2$ for some $s \in \mathbb{N}$. Suppose, the set X is represented as $X = \{1, 2, \ldots, s^2\}$ and the $MOLS(s) + 2$ many parallel classes are denoted by $A = \{C_0, C_1, \ldots, C_w\}$, where each C_i represents a partition of X. Assuming each element $k \in X$ as a d-dimensional vector, having only a non-zero entry as 1 at the k^{th} position, each block of a parallel class turns out to be a $d \times s$ dimensional matrix. Concatenation of s many such matrices corresponding to a parallel class provides a $d \times d$ dimensional matrix for the same parallel class C_i. Following the construction method, discussed before, we can construct the set of $w+1$ many sparse MUBs [57]. Denoting the set as $\{M_0, M_1, \ldots, M_w\}$, where $M_i = P_i \mathbb{H}_i$. Here, P_i is the d dimensional permutation matrix having 1's at the $(m, n)^{th}$ position if and only if m is the n^{th} entry in the parallel class C_i, with $1 \leq n \leq s^2$.*

Here $w =$ MOLS$(s) + 1$. The orthonormal bases are constructed from MUBs, because any pair of blocks from two different parallel classes has exactly one element in common, which is called the intersection number (μ). The intersection number plays a critical role in the construction of the approximate MUBs using RBDs [57, 58]. Note that P_i is determined by the parallel classes C_i. Since the first entry of the first block of every parallel class is 1, we have $(P_i)_{11} = 1, \forall i$. Further, $\mathbb{H}_i$ is a block diagonal matrix, where each block matrix consists of a Hadamard matrix of order s.

Now using the set of $w + 1$ MUBs, we obtain a set of w many Mutually Unbiased Hadamard matrices $\{H_1, \ldots, H_w\}$ where $H_i = M_0^\dagger M_i = \mathbb{H}_0^\dagger P_0^T P_i \mathbb{H}_i$, where $P_0^\dagger = P_0^T$. This follows from Lemma 5.1.2. Note that starting with I_0, the identity matrix, it forms a set of $w + 1$ MUBs.

Note that when all the Hadamard matrices in $\mathbb{H}$ are identical, say H, then $\mathbb{H} = \mathbb{I}_s \otimes H$ and hence we have

$$M_i = P_i \left(\mathbb{I}_s \otimes H \right),$$

where $\mathbb{I}_s$ denotes the identity matrix of order s. In this situation
we have $H_i = \left(\mathbb{I}_s \otimes H^\dagger \right) P_0^T P_i \left(\mathbb{I}_s \otimes H \right)$.

Example 5.2.1. *Let $|X| = 2^2$ such that $X = \{1, 2, 3, 4\}$. The underlying parallel classes can be represented as follows.*

$$C_0 : \{1, 2\}, \{3, 4\}, C_1 : \{1, 3\}, \{2, 4)\}, C_2 : \{1, 4\}, \{2, 3)\}.$$

Consider the two dimensional Hadamard matrix as $H = \frac{1}{\sqrt{2}}\left(\begin{smallmatrix} 1 & 1 \\ 1 & -1 \end{smallmatrix}\right)$. *Therefore, the sparse MUBs are denoted by*

$$M_0 = P_0 \cdot M_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} = P_0 \left(\mathbb{I} \otimes H\right),$$

$$M_1 = P_1 \cdot M_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix} = P_1 \left(\mathbb{I} \otimes H\right),$$

$$M_2 = P_2 \cdot M_0 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix} = P_2 \left(\mathbb{I} \otimes H\right).$$

Using the above matrices, we obtain the following set of two Mutually Unbiased Hadamard matrices:

$$H_1 = M_0^\dagger \cdot M_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}^\dagger \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix},$$

$$H_2 = M_0^\dagger \cdot M_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}^\dagger \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{pmatrix} = \frac{1}{2} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{pmatrix}.$$

Along with Identity Matrix I_4, we obtain a set of 3 MUBs.

5.2.1 Introducing the parameters

Next, we show that using the above method we can introduce affine parameters in a set of w many mutually unbiased Hadamard matrices, so constructed thereby demonstrating the

existence of a parametric form of mutually unbiased bases, in every dimension of the form $d = s^2$. We do this by exploiting the fact that $\mathbb{H}$ is block diagonal matrix where each block is a Hadamard matrix of order s and noting that $D_i(\theta)\mathbb{H}$ is also blocked Hadamard matrix, where $D_i(\theta)$ is a diagonal unitary matrix, with diagonal entries of the form $\exp(\iota\theta_i)$, where θ_i is a independent parameter.

Thus using above we have $\mathbb{M}_i = P_i D_i(\theta)\mathbb{H}$. Therefore,

$$\mathbb{M}_i^\dagger \mathbb{M}_j = \mathbb{H}_0^\dagger D_i^\dagger(\theta) P_i^T P_j D_j(\theta)\mathbb{H}.$$

Note that $P^\dagger = P^T$ for any permutation matrix P. Note that the product of two permutations is another permutation, and the product of two diagonal matrices is again a diagonal matrix. Thus using the Lemma 5.1.3 above, the term $D_i(\theta)P_i^T P_j D_j(\theta)$ can be written as $\tilde{P}_j\tilde{D}_j(\theta)$, where $\tilde{D}_j(\theta)$ is a unitary diagonal matrix having diagonal entries of the form $\exp(\iota\theta_i)$, for some θ_i where θ_i's are independent parameters and $\tilde{P}_j$ is some permutation matrix. Hence, the total independent parameters are equal to the dimension of the matrix, which is s^2. Thus, the set of Mutually Unbiased Hadamard matrices are

$$\{H_1 = \mathbb{M}_0^\dagger\mathbb{M}_1, H_2 = \mathbb{M}_0^\dagger\mathbb{M}_2, \ldots, H_w = \mathbb{M}_0^\dagger\mathbb{M}_w\},$$

where

$$H_i = \mathbb{M}_0^\dagger\mathbb{M}_i = \mathbb{H}^\dagger\tilde{P}_j\tilde{D}_j(\theta)\mathbb{H}.$$

Now referring to Corollary 5.1.1, if D is a block diagonal matrix, such that each block matrix is $\alpha_r I_s$, where I_s is the identity matrix of order s then D commutes with block diagonal matrix H, which contain block matrix of size s. Hence

$$\tilde{D}_j(\theta) = \tilde{D}_{j1}(\theta)\tilde{D}_{j2}(\theta),$$

where, $\tilde{D}_{j2}(\theta)$ is a block diagonal matrix where each block is of form $\exp(\iota\theta_j)I_s$ and $\tilde{D}_{j1}(\theta)$ is block diagonal matrix having diagonal entries of the form $\exp(\iota\theta_j)$. Hence from Corollary 5.1.1, $\tilde{D}_{j2}(\theta)$ will commute with $\mathbb{H}$. Thus

$$H_i = \mathbb{H}^\dagger\tilde{P}_j\tilde{D}_j(\theta)\mathbb{H} = \mathbb{H}^\dagger\tilde{P}_j\tilde{D}_{j1}(\theta)\tilde{D}_{j2}(\theta)\mathbb{H} = \mathbb{H}^\dagger\tilde{P}_j\tilde{D}_{j1}(\theta)\mathbb{H}\tilde{D}_{j2}(\theta).$$

Since all the θ_j's are free parameters, we can absorb s many of them in $\tilde{D}_{j2}(\theta)$. Further, multiplying the Unitary Diagonal Matrix from left to an MUB matrix does not affect the

equivalence of the MUBs, as it corresponds to multiplying an MUB vector with some arbitrary phase. Thus

$$H_i \equiv \mathbb{H}^\dagger \tilde{P}_j \tilde{D}_{j1}(\theta)\mathbb{H},$$

where the number of independent parameters become

$$s^2 - s = s(s-1).$$

Furthermore, note that such set $\{I_0, H_1, \ldots, H_w\}$ also forms a class of MUBs for $\mathbb{C}^d$. Thus, in this process, we also construct a class of $MOLS(s)+2$ many affine-parametric MUBs for dimension $d = s^2$ (We say affine parameters because all the parameters (variables) are linear). One should note that, when determining the number of free parameters, we can remove redundant parameters only from columns, not from rows; otherwise, the MUB-structures will be destroyed. Therefore, each such basis matrix, except Identity (I_0), contains at least $s(s-1)$ many free parameters.

Further note that while constructing block diagonal Hadamard matrices $\mathbb{H}$ in Construction 5.2.1, we had the liberty to choose s many Hadamard matrices of size s. Now if each of these Hadamard matrices contains r_i^k many free parameters, $i = 1, 2, \ldots, s$, then the total number of free parameters in each of these bases, $\mathbf{H}_k$ would further be increased by $\left(\sum_{i=1}^{s} r_i^k\right)$. Moreover, the $\mathbf{H}_k \equiv \mathbb{H}_0^\dagger \widetilde{P}_k \widetilde{D}_{k1}(\theta)\mathbb{H}_k$. The free parameter in $\mathbb{H}_0^\dagger$, by virtue of the construction, would be common to all the $\mathbf{H}_k$'s. Thus each $\mathbf{H}_k$ would have the number of independent parameters given by

$$\left(\sum_{i=1}^{s} r_i^0 + \sum_{i=1}^{s} r_i^k\right) + s(s-1),$$

where the $\sum_{i=1}^{s} r_i^0$ many parameters would be common to all the MUHM. Thus our main contribution in this regard can be summarized in the following theorem.

Theorem 5.2.1. *For dimension $d = s^2$ let $w = MOLS(s) + 1$, there exists a set of MUBs $\{\mathrm{I}, H_1, H_2, \ldots, H_w\}$ consisting of the identity matrix and the MUHMs, such that each Hadamard matrix H_i have at least $s(s-1)$ many independent affine parameters, that cannot be absorbed by a global unitary operation.*

Proof. The proof follows from discussion above, The fact that the parameters cannot be absorbed by any global unitary operation is clear when one note that each of the affine

parameters in H_l is independent from any other affine parameters of say H_k, coupled with the fact that I Identity matrix is also present in the set, hence these parameters cannot be absorbed by any global unitary operations. □

Now let us illustrate this with an example for $d = 4$. The matrices $\mathbb{M}_0^\dagger\mathbb{M}_1$ and $\mathbb{M}_0^\dagger\mathbb{M}_2$ can be made affine parametric MUBs, each having $2(2-1) = 2$ free parameters, by pulling out parameters only from the columns and not from the rows, in the following way.

$$\mathbb{M}_0^\dagger\mathbb{M}_1 = \frac{1}{2}\begin{pmatrix} e^{i\theta_1} & e^{i\theta_1} & e^{i\theta_2} & e^{i\theta_2} \\ e^{i\theta_1} & e^{i\theta_1} & -e^{i\theta_2} & -e^{i\theta_2} \\ e^{i\theta_3} & -e^{i\theta_3} & e^{i\theta_4} & -e^{i\theta_4} \\ e^{i\theta_3} & -e^{i\theta_3} & -e^{i\theta_4} & e^{i\theta_4} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ e^{i\alpha} & -e^{i\alpha} & e^{i\beta} & -e^{i\beta} \\ e^{i\alpha} & -e^{i\alpha} & -e^{i\beta} & e^{i\beta} \end{pmatrix},$$

$$\mathbb{M}_0^\dagger\mathbb{M}_2 = \frac{1}{2}\begin{pmatrix} e^{i\phi_1} & e^{i\phi_1} & e^{i\phi_2} & e^{i\phi_2} \\ e^{i\phi_1} & e^{i\phi_1} & -e^{i\phi_2} & -e^{i\phi_2} \\ e^{i\phi_4} & -e^{i\phi_4} & e^{i\phi_3} & -e^{i\phi_3} \\ -e^{i\phi_4} & e^{i\phi_4} & e^{i\phi_3} & -e^{i\phi_3} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ e^{i\gamma} & -e^{i\gamma} & e^{i\delta} & -e^{i\delta} \\ -e^{i\gamma} & e^{i\gamma} & e^{i\delta} & -e^{i\delta} \end{pmatrix}.$$

The matrices $\{\mathrm{I}_d, \mathbb{M}_0^\dagger\mathbb{M}_1(\alpha,\beta), \mathbb{M}_0^\dagger\mathbb{M}_2(\gamma,\delta)\}$ form a class of three affine parametric MUBs for dimension 4. Other than the identity matrix, there are two free parameters in each of them. Note that here $4 = 2^2$, for which we have $2 + 1 = 3$ affine parametric MUBs. Thus, when s is some prime power, we have the following corollary.

Corollary 5.2.1. *Consider $d = q^2$, where q is some prime power. Then there exists a set of q many MUHMs, each having at least $q(q-1)$ independent affine parameters that a global unitary operation cannot absorb.*

5.2.2 Parametric Class of Hadamard Matrices

As noted above, the set $\{H_1 = \mathbb{M}_0^\dagger\mathbb{M}_1, H_2 = \mathbb{M}_0^\dagger\mathbb{M}_2, \ldots, H_w = \mathbb{M}_0^\dagger\mathbb{M}_w\}$ forms Mutually Unbiased Hadamard matrices, i.e., each H_i is a Hadamard matrix. Each of these matrices has $s(s-1)$ many free parameters. Since the Hadamard property of a matrix remains unaffected even when the rows are multiplied by some arbitrary phase, it can be used to further reduce the free parameter by multiplying a suitable diagonal unitary matrix from the left. Consider any H_i as given above, i.e., $H_i \equiv \mathbb{H}^\dagger\tilde{P}_j\tilde{D}_{j1}(\theta)\mathbb{H}$. Now $\tilde{P}_j\tilde{D}_{j1}(\theta) = \bar{D}_{j1}(\theta)\tilde{P}_j$,

where $\bar{D}_{j1}(\theta)$ is a diagonal unitary matrix having same entries as $\tilde{D}_{j1}(\theta)$. However, the first entry of $\bar{D}_{j1}(\theta)\tilde{P}_j$ is also 1. This is because the $\tilde{P}_j$ is a permutation matrix with the first entry as 1. Now as done in the case of MUB, for further reducing the parameters, we expressed the $\tilde{D}_j$ and product of two diagonal matrix viz $\tilde{D_{j1}}\tilde{D_{j2}}$ such that $\tilde{D_{j2}}$ commute with $\mathbb{H}$. Hence we again express $\tilde{D_{j1}} = \tilde{D_{j3}}\tilde{D_{j4}}$ such that $\tilde{D_{j3}}$ commutes with $\mathbb{H}_0^\dagger$. Thus, by choosing suitable $\tilde{D_{j3}}$, we can reduce the number of affine parameters remaining in $\tilde{D_{j4}}$. However, the first entry of $\tilde{D_{j3}}\widetilde{P}_j$ is also 1. This is because the $\widetilde{P}_j$ is a permutation matrix with the first entry $(\widetilde{P}_j)_{11} = 1$. Hence only $s-1$ independent parameters can be chosen, using which one can further reduce $s-1$ parameters in $\tilde{D_{j4}}$. Hence, the number of independent affine parameters is $s(s-1) - (s-1) = (s-1)^2$.

Continuing with our example of $|X| = 2^2$, we have the following matrices:

$$\mathbb{M}_0^\dagger \mathbb{M}_0 = M_0^\dagger D(\theta) P_0 M_0 = M_0^\dagger D(\theta) M_0 = \mathbb{I}_d,$$

$$\mathbb{M}_0^\dagger \mathbb{M}_1 = M_0^\dagger D(\theta) P_1 M_0 = M_0^\dagger D(\theta) M_1.$$

Assuming the parameters in $D(\theta)$ as $\theta_1, \theta_2, \theta_3$ and θ_4, we obtain

$$\mathbb{M}_0^\dagger \mathbb{M}_1 = \frac{1}{2}\begin{pmatrix} e^{i\theta_1} & e^{i\theta_1} & e^{i\theta_2} & e^{i\theta_2} \\ e^{i\theta_1} & e^{i\theta_1} & -e^{i\theta_2} & -e^{i\theta_2} \\ e^{i\theta_3} & -e^{i\theta_3} & e^{i\theta_4} & -e^{i\theta_4} \\ e^{i\theta_3} & -e^{i\theta_3} & -e^{i\theta_4} & e^{i\theta_4} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & e^{i\theta} & -e^{i\theta} \\ 1 & -1 & -e^{i\theta} & e^{i\theta} \end{pmatrix},$$

$$\text{and } \mathbb{M}_0^\dagger \mathbb{M}_2 = M_0^\dagger D(\phi) P_2 M_0 = M_0^\dagger D(\phi) M_2.$$

Again, assuming the parameters in $D(\phi)$ as ϕ_1, ϕ_2, ϕ_3 and ϕ_4, we obtain

$$\mathbb{M}_0^\dagger \mathbb{M}_2 = \frac{1}{2}\begin{pmatrix} e^{i\phi_1} & e^{i\phi_1} & e^{i\phi_2} & e^{i\phi_2} \\ e^{i\phi_1} & e^{i\phi_1} & -e^{i\phi_2} & -e^{i\phi_2} \\ e^{i\phi_4} & -e^{i\phi_4} & e^{i\phi_3} & -e^{i\phi_3} \\ -e^{i\phi_4} & e^{i\phi_4} & e^{i\phi_3} & -e^{i\phi_3} \end{pmatrix} = \frac{1}{2}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & e^{i\phi} & -e^{i\phi} \\ -1 & 1 & e^{i\phi} & -e^{i\phi} \end{pmatrix}.$$

One can now check that the matrices $\mathbb{M}_0^\dagger \mathbb{M}_1$ and $\mathbb{M}_0^\dagger \mathbb{M}_2$ form a class of affine parametric Hadamard matrices, each having $(2-1)(2-1) = 1$ free parameter. However, they might not be mutually unbiased, since the inner product between the i^{th} column of $\mathbb{M}_0^\dagger \mathbb{M}_1$ and the j^{th} column of $\mathbb{M}_0^\dagger \mathbb{M}_2$ may not be equal to $\frac{1}{2}$ in certain cases. Thus, here we need additional efforts.

It is to be noted that the method described in Construction 5.2.1 enables us to construct the following interesting class of MUBs in square dimension.

Corollary 5.2.2. *In square dimension $d = s^2$, we can have a set of $MOLS(s) + 2$ many affine-parametric MUBs having the same eigenvalues and components of eigen-vectors are permutations of one of the MUBs.*

Proof. Following Construction 5.2.1, we begin with an RBD (X, C) with $|X| = s^2$ and $C = \{C_0, C_1, \ldots, C_w\}$ representing the parallel classes. Corresponding to each parallel class, we can construct a class of sparse MUBs $\{M_0, M_1, \ldots, M_w\}$, such that $M_i = P_i (\mathbb{I}_s \otimes H)$, where P_i represents the permutation matrix and H is a Hadamard matrix as defined earlier. Observe that, if M_i, M_j are MUBs, so are $M_i P_i^T$ and $M_j P_j^T$, since

$$\left(M_i P_i^T\right)^\dagger M_j P_j^T = \left(P_i^T\right)^\dagger M_i^\dagger M_j P_j^T.$$

Now, consider the set of MUBs $\{M_0 P_0^T, M_1 P_1^T, \ldots, M_w P_w^T\}$. Note that the eigenvalues of $(\mathbb{I}_s \otimes H)$ are the same as the eigenvalues (each eigenvalue has multiplicity as order of H) of H and multiplication by a permutation matrix does not change the eigenvalues of the resultant matrix, it only changes the eigenvectors.

Suppose, λ denotes the eigenvalues of $(\mathbb{I}_s \otimes H)$ with an eigenvector $\mathbf{Y}$, i.e.

$$(\mathbb{I}_s \otimes H)\, \mathbf{Y} = \lambda \mathbf{Y}.$$

Now $M_i P_i^T = P_i (\mathbb{I}_s \otimes H) P_i^T$ will also have the same eigenvalues, irrespective of the choice of permutation matrices. Suppose the corresponding eigenvector is given by $\mathbf{Z}$, i.e.,

$$\begin{aligned} P_i (\mathbb{I}_s \otimes H) P_i^T \mathbf{Z} = \lambda \mathbf{Z} \Rightarrow & P_i^T \left[P_i (\mathbb{I}_s \otimes H) P_i^T \mathbf{Z}\right] = \lambda P_i^T \mathbf{Z} \\ & \Rightarrow (\mathbb{I}_s \otimes H) \left(P_i^T \mathbf{Z}\right) = \lambda \left(P_i^T \mathbf{Z}\right). \end{aligned}$$

Thus, $\mathbf{Y} = \left(P_i^T \mathbf{Z}\right) \Rightarrow \mathbf{Z} = P_i \mathbf{Y}$. Hence, the class of $MOLS(s) + 2$ MUBs $\{M_0 P_0^T, M_1 P_1^T, \ldots, M_w P_w^T\}$ have the same eigenvalues and the corresponding eigenvectors are given by $P_i \mathbf{Y}$, where $\mathbf{Y}$ is the eigenvector of M_0 corresponding to the same eigenvalue. □

Example 5.2.2. *Let us continue with the earlier example of $d = 2^2$. Here,*

$$M_0 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix}$$

and the set of eigenvalues of M_0 is given by ± 1. One of the eigen-vectors corresponding to the eigenvalue 1 is given by $\mathbf{Y} = \left(0, 0, 1+\sqrt{2}, 1\right)^T$. The matrix $M_1 P_1^T$ is given by

$$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & -1 & 0 \\ 0 & 1 & 0 & -1 \end{pmatrix}$$

and the eigen-vector of $M_1 P_1^T$ corresponding to the eigenvalue 1 is given by $\mathbf{Z} = \left(0, 1+\sqrt{2}, 0, 1\right)^T = P_1 \mathbf{Y}$. This follows from the previous corollary.

5.2.3 Comparison with Goyeneche et. al.'s work (2015)

In this initiative, we construct a class of $MOLS(s) + 2$ many affine-parametric MUBs for dimension $d = s^2$, each having $s(s-1)$ many free parameters other than the identity matrix. In the example above, corresponding to Construction 5.2.1 (the RBD construction), we presented three real MUBs in dimension 4. After applying the appropriate unitary transformation, we obtained one identity matrix and two real Hadamard matrices. Each Hadamard matrix contains at least two parameters, giving a total of 4, counting both matrices. We could also prepare examples with exactly four parameters in total. This is similar to the result of Goyeneche et. al. [34], which also introduced four free parameters in dimension 4.

For dimension 16, our approach introduces at least 48 parameters compared to 64 as in [34]. Here, the work of [34] has an advantage, because there are nine real MUBs (maximum possible real MUBs in dimension 16), and our RBD construction provides only 5. We could introduce at least 12 parameters in each MUB, whereas it is only 8 in each MUB of dimension 16 for [34]. In any dimension other than a power of four, i.e., 4^k, our method introduces higher number of parameters than [34], because our construction of introducing parameters is not based on the existence of real ones, and most dimensions generally admit at most two real MUBs [16].

In dimension 9, we have 4 MUBs through our RBD construction and we can introduce at least 6 parameters in each MUB making a total of at least 18 parameters in three, considering the first one as identity. So, we have introduced parameters in every dimension irrespective of whether we have real or complex MUBs through MOLS construction. In this dimension,

other than identity, no real MUB is available, and hence the construction of [34] cannot be applied at all. Thus, our result of Theorem 5.2.1 provides a broader class with more parameters in general and this is an improvement over [34].

5.2.4 Towards generalising the idea towards construction of an affine parametric class of Hadamard matrices for $d = k \times s$

The Resolvable Block Design (RBD) approach enables us to construct at least MOLS$(s)+2$ many MUBs in $d = s^2$, because for this situation we have RBD(X, A) which has MOLS$(s)+2$ parallel classes, where each parallel class consists of constant block size (s) and any pair of blocks from different parallel classes have exactly one point in common, i.e., $\mu = 1$. Further $\beta = 1$, which is the bound on the absolute value of the dot product between any pair of vectors from different bases. Such properties cannot be achieved when dimension is not square, i.e., $d = k \times s$ and $k \neq s$.

In such a situation, one can always construct RBD(X, A) which has at least two parallel classes having $\mu = 1$ and $\beta = 1$. For this we provide the following technique for constructing RBD(X, A) with $|X| = d = k \times s$, having two parallel class namely $\mathcal{P}_k$ and $\mathcal{P}_s$, where $\mathcal{P}_k$ consists of s blocks each of constant size k and $\mathcal{P}_s$ consists of k blocks each of constant size s such that any pair of block from different parallel classes, has exactly one element in common.

Construction 5.2.2. *Consider $d = k \times s$, where k and s are positive integers.*

1. *Let the elements of $X = \{1, 2, \ldots, s, s+1, \ldots, 2s, 2s+1 \ldots, ks\}$*

2. *Define $\mathcal{P}_s = \{\mathcal{B}_1^s = \{1, 2, \ldots, s\}, \mathcal{B}_2^s = \{s+1, s+2, \ldots, 2s\}, \ldots, \mathcal{B}_k^s = \{(k-1)s+1, (k-1)s+2, \ldots, ks\}$. Hence, $\mathcal{P}_s$ is a parallel class having k many blocks $\{\mathcal{B}_i^s\}_{i=1,2,\ldots,k}$, where each block has exactly s elements.*

3. *Now construct $\mathcal{P}_k$ having s many blocks $\{\mathcal{B}_i^k\}_{i=1,2,\ldots,s}$, such that every block has exactly one element from each $\mathcal{B}_i^s$, hence each $\{\mathcal{B}_i^k\}_{i=1,2\ldots s}$ is of size k. Hence $\mathcal{P}_k$ can be constructed in large number of ways. One simple way would be $\mathcal{P}_k = \{\mathcal{B}_1^k = \{1, s+1, \ldots, (k-1)s+1\}, \mathcal{B}_2^k = \{2, s+2, \ldots, (k-1)s+2\}, \ldots, \mathcal{B}_s^k = \{s, 2s, \ldots, ks\}\}$.*

Using these two parallel classes, we can obtain at least a pair of MUBs. Note that once P_s is fixed, there are $\sum_j^s j^k$ many different P_k's possible, which in turn may be exploited to get obtain an affine parametric Hadamard matrix. However, examining their equivalence appears to be a very challenging task. To characterize, the constructed affine parametric Hadamard matrix, using RBD$(X, \{\mathcal{P}_s, \mathcal{P}_k\})$, we prove following lemma, which essentially reproduces the results of [29], in terms of number of affine parameters. However, further analysis is required to see if Hadamard matrices are equivalent to the one provided in [29].

Lemma 5.2.1. *For dimension $d = k \times s$, there exists a Hadamard matrix H_i having at least $(k-1)(s-1)$ many affine parameters, such that the first row and first column consist of 1.*

Proof. Using Construction 5.2.1, with RBD having only two parallel classes, and applying the diagonal unitary matrix $D(\theta)$ as in Theorem 5.2.1, we obtain the set

$$\{\mathrm{I}, H_1 = \mathbb{M}_0^\dagger \mathbb{M}_1 \equiv \mathbb{H}_0^\dagger \widetilde{P}_j \widetilde{D}_{j1}(\theta) \mathbb{H}_1\}.$$

Here H_i is a Hadamard matrix with at least $d - k = k(s-1)$ many free parameters. Since the Hadamard property of a matrix remains unaffected even when the rows are multiplied by some arbitrary phase, we use this to further reduce the number of free parameters by multiplying a suitable diagonal unitary matrix from the left.

Consider H_1 as given above, i.e., $H_1 \equiv \mathbb{H}_0^\dagger \widetilde{P}_j \widetilde{D}_{j1}(\theta) \mathbb{H}_1$. Now $\widetilde{P}_j \widetilde{D}_{j1}(\theta) = \bar{D}_{j1}(\theta) \widetilde{P}_j$, where $\bar{D}_{j1}(\theta)$ is a diagonal unitary matrix having same entries as $\widetilde{D}_{j1}(\theta)$. Since we can also multiply the phase factor to the rows of the H_1, we use this to further reduce the number of affine parameters, which are introduced because of $\widetilde{D}_{j1}(\theta)$. Let us write $\bar{D}_{j1}(\theta) = \bar{D}^1_{j1}(\theta) \bar{D}^2_{j1}(\theta)$, such that $\bar{D}^1_{j1}(\theta)$ is a block diagonal unitary matrix, where block diagonals are of the form $\exp(\iota \alpha_r) I_k$, where $r = 1, 2, \ldots, s$. Hence the matrix $\bar{D}^1_{j1}(\theta)$ will commute with $\mathbb{H}_0^\dagger$. Thus, by choosing suitable α_r we can reduce the number of affine parameters remaining in $\bar{D}^2_{j1}(\theta)$. However, the first entry of $\bar{D}_{j1}(\theta) \widetilde{P}_j$ is also 1. This is because the $\widetilde{P}_j$ is a permutation matrix with the first entry $(\widetilde{P}_j)_{11} = 1$. Thus $\alpha_1 = 0$. Hence only $s-1$ independent α_r's can be chosen, using which one can further reduce $s-1$ parameters. Hence number of independent affine parameters are $k(s-1) - (s-1) = (k-1)(s-1)$. That the first row and the first column of $H_1 \equiv \mathbb{H}_0^\dagger \bar{D}^2_{j1}(\theta) \widetilde{P}_j \mathbb{H}_1$ follows from fact that each block of $\mathbb{H}_0$ and $\mathbb{H}_1$ have first row and first column having 1, along with the fact that $(\widetilde{P}_j)_{11} = 1$. □

As done previously, while choosing the Hadamard matrices for $\mathbb{H}_0$, if they have $\{k_i\}_{i=1,\ldots,s}$ many independent parameters, then the constructed Hadamard matrix of order d will have

extra parameters. Similarly for $\mathbb{H}_1$ if the Hadamard matrices have $\{r_i\}_{i=1,\ldots s}$ many independent parameters, then the maximum number of free parameters in each H_1 would be given by $\left(\sum_{i=1}^{k} k_i + \sum_{i=1}^{s} r_i\right) + (k-1)(s-1)$. One should also refer to [63, Section 2.2], [77, Section 4.5], [33] and [36, Proposition 2.9] in this direction.

For example, using two parallel classes for $d = 2 \times 3 = 6$, from the above analysis we get $(k-1)(s-1) = 2$ parameters corresponding to the Hadamard matrix. For the RBD having two parallel classes constructed for $d = 6$, we obtain the resultant parametric Hadamard matrix as

$$\mathbb{M}_0^{\dagger}\mathbb{M}_1(\alpha,\beta) = \frac{1}{\sqrt{6}} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \omega & \omega^2 & e^{i\alpha} & \omega e^{i\alpha} & \omega^2 e^{i\alpha} \\ 1 & \omega & \omega^2 & -e^{i\alpha} & -\omega e^{i\alpha} & -\omega^2 e^{i\alpha} \\ 1 & \omega^2 & \omega & e^{i\beta} & \omega^2 e^{i\beta} & \omega e^{i\beta} \\ 1 & \omega^2 & \omega & -e^{i\beta} & -\omega^2 e^{i\beta} & -\omega e^{i\beta} \end{pmatrix}.$$

Thus $\{\mathrm{I}, \mathbb{M}_0^{\dagger}\mathbb{M}_1(\alpha,\beta)\}$ form a pair of MUBs in $d = 6$ with 2 parameters.

5.3 Conclusion

In this chapter, we considered the introduction of parameters in MUBs. The MUBs have applications in several areas of quantum information and cryptography. Thus, such parameterisation may provide better flexibility in choosing from a larger class of options. Our results show improvements over the work of [34] in terms of the number of MUBs as well as parameters for most of the dimensions $d = s^2$. Furthermore, we also present directions for generalising this to dimensions of the form $d = k \times s$. As we are discussing about free parameters, that a global unitary operation cannot absorb, we need to analyse this more critically. In this regard, we require a closer look at the equivalence between the two sets of MUBs.

Chapter 6

On Construction of Approximate Real Mutually Unbiased Bases for an infinite class of dimensions $d \not\equiv 0 \bmod 4$

In the previous chapter, we considered the parametrisation of real MUBs in dimension s^2, where the general construction of those MUBs was inspired by the work in [57]. Building on that line of investigation, this chapter presents our first contribution toward the study of Approximate Mutually Unbiased Bases. In particular, we focus on the construction of Approximate Real Mutually Unbiased Bases for dimensions that are not divisible by four. In this setting, the existence of exact real MUBs remains challenging due to the unresolved status of the Hadamard conjecture. In this chapter, for the first time, we show that it is possible to construct $\geq \lceil \sqrt{d} \rceil$ many ARMUBs for certain odd dimensions d of the form $d = (4n - t)s$, $t = 1, 2, 3$, where n is a natural number and s is an odd prime power. Our method exploits any available $4n \times 4n$ real Hadamard matrix H_{4n} (conjectured to be true) and uses this to construct an orthogonal matrix Y_{4n-t} of size $(4n - t) \times (4n - t)$, such that the absolute value of each entry varies a little from $\frac{1}{\sqrt{4n-t}}$. In our construction, the absolute value of the inner product between any pair of basis vectors from two different ARMUBs will be $\leq \frac{1}{\sqrt{d}}(1 + O(d^{-\frac{1}{4}})) < \frac{2}{\sqrt{d}}$, for proper choices of parameters, the class of dimensions d being infinitely large.

6.1 Introduction

We refer to Section 2.6 of Chapter 2 for the necessary preliminaries on approximate mutually unbiased bases. As is well known, there exist nearly $d+1$ MUBs in $\mathbb{C}^d$ and approximately $\frac{d}{2}+1$ real MUBs in $\mathbb{R}^d$, respectively. However, a large number of real MUBs are non-existent for most dimensions [16]. In fact, it is only for dimensions of the form $d = 4^s$, $s > 1$, that one can construct the maximum number of $\frac{d}{2}+1$ real MUBs. For most other dimensions, particularly those that are not perfect squares, at best only two real MUBs are known to exist [16]. For a comprehensive overview, one may refer to [16, Table 1]. This scarcity provides strong motivation for the construction of Approximate Real MUBs, a direction increasingly explored in recent literature [57, 59, 86]. The number of real MUBs remains significantly limited [16] when the problem is considered over the real vector space $\mathbb{R}^d$. This observation is also summarized in [61, Theorem 3.2]. In this context, it is important to note that for dimensions $d > 2$ with $d \not\equiv 0 \pmod 4$, it is impossible to construct even a pair of real MUBs. This follows directly from the non-existence of real Hadamard matrices in such dimensions, since the existence of a pair of real MUBs would imply the existence of a real Hadamard matrix.

With this motivation, in this chapter, we focus on the construction of Approximate Real MUBs (ARMUBs) in dimensions $d > 2$ where $d \not\equiv 0 \pmod 4$.

6.1.1 Organization & Contribution

The organization of this chapter is as follows.

In Section 2.6 of Chapter 2, we define mutually unbiased bases and their approximate variants. Furthermore, in Subsection 2.5.1, we present a combinatorial method to construct MUBs in certain dimensions. We outline existing ideas, along with illustrative examples, that will be relevant to our contributions in later chapters.

In Section 6.2, we construct the orthogonal matrices of orders $4n-t$, $t = 1, 2, 3$, from real Hadamard matrix H_{4n} of order $4n$. We name these as ϵ-Hadamard matrices. Finally, using such matrices and suitable Resolvable Block Designs, we construct ARMUBs for dimensions $d = q(4n - t)$, for $t = 1, 2, 3$. We will show that when q is an odd prime power, and the order of $4n$ and q are the same, then we can have order of $\sqrt{d}$ many ARMUBs with

significantly low inner product values. We demonstrate that when q is an odd prime power and $\gcd(q, 4n) = 1$, then the number of such ARMUBs can reach up to $\sqrt{d}$, with significantly low inner product values between vectors—making them highly efficient approximations.

To compare with the earlier works, we will refer to [57, 59, 60].

- In [59], the ARMUBs are constructed for the dimensions $d = (4x)^2$, where x is a prime power. The number of such ARMUBs was $\frac{\sqrt{d}}{4} + 1$, and the value of the inner products was $\leq \frac{4}{\sqrt{d}}$.
- This has been improved in [57], where ARMUBs for dimensions $d = q(q + 1)$, when prime power $q \equiv 3 \bmod 4$ were considered. The inner products were improved to $< \frac{2}{\sqrt{d}}$, and $\lceil \sqrt{d} \rceil$ many such ARMUBs could be obtained. In certain cases results were available for $d = sq^2$, where q is a prime power and $sq \equiv 0 \bmod 4$.
- Later APMUBs (Almost Perfect) MUBs were studied in [60], and several constructions over complex numbers were considered. The constructions could be achieved for reals, but in those cases the dimensions are again divisible by 4, as they require existence of real Hadamard matrices.

In this chapter we modify (subsection 6.2.1) the real Hadamard matrices to have real unitary ones of dimensions $d = q(4n-t)$, for $t = 1, 2, 3$, which we refer as ϵ-Hadamard. These are used in conjunction with RBDs in line of the constructions in [57, 60] to obtain new constructions of β-ARMUBs for the dimensions $d > 2$ and $d \not\equiv 0 \bmod 4$, with $\beta < 2$. In algebraic terms, this bound on absolute value of the inner product is $\leq \frac{1}{\sqrt{d}}(1 + O(d^{-\frac{1}{4}}))$.

When s is an odd prime power, and the order of $4n - t$ and s are same, we obtain $O(\sqrt{d})$ many ARMUBs for such dimensions. Note that even a pair of real MUBs are not available for the dimensions $d > 2$ and $d \not\equiv 0 \bmod 4$ and thus the approximate versions are the only relevant solutions in this direction, which we first present in this chapter.

While exploring approximate MUBs over $\mathbb{C}^d$, several constructions were proposed in [23, 50, 73]. However, these techniques are not applicable when constructing real MUBs. In this context, a construction for Approximate Real MUBs (ARMUBs) was introduced in [59], utilising real Hadamard matrices. It was shown in [59] that for dimensions of the form $d = (4q)^2$, where q is a prime, one can construct $\frac{\sqrt{d}}{4} + 1$ ARMUBs, with the maximum inner product between vectors from different bases being $\frac{4}{\sqrt{d}}$.

This result was further generalized and improved in [57] using Resolvable Block Designs (RBDs). Specifically, the construction in [59] was extended to dimensions of the form $d = sq^2$, where q is a prime power. Moreover, the parameters were enhanced in [57], where it was shown that for $d = q(q+1)$, with q a prime power satisfying $q \equiv 3 \bmod 4$, it is possible to construct $\lceil \sqrt{d} \rceil = q+1$ ARMUBs. In this case, the maximum inner product between vectors from different bases is upper bounded by $\frac{2}{\sqrt{d}}$.

Thus, the improvements achieved in [57] are twofold: firstly, the number of available ARMUBs is increased, and secondly, the upper bound on the inner product between vectors from different bases is reduced compared to the result in [59]. Recent developments in this direction, particularly concerning Approximate Pairwise Real MUBs (APRMUBs), have also been reported in [60], although that work does not address odd-dimensional cases.

6.1.2 Some basic examples related to MUBs

Let us now proceed with a few examples with small dimensions. Let us consider, $i = \sqrt{-1}$ denotes the imaginary unit, and $\omega = e^{2\pi i/3}$ denotes a primitive third root of unity. For $d = 2$, where we have 3 MUBs, $M_0^{(2)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $M_1^{(2)} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $M_2^{(2)} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$, the first two being real. However, this is not possible for the dimension $d = 3$. There are indeed four MUBs, that can be represented as $M_0^{(3)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$, $M_1^{(3)} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ \omega^2 & 1 & \omega \\ \omega^2 & \omega & 1 \end{bmatrix}$,

$M_2^{(3)} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}$, $M_3^{(3)} = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ \omega & \omega^2 & 1 \\ \omega & 1 & \omega^2 \end{bmatrix}$, but except the identity, none of them are reals. Thus the a pair of real MUBs is not available in this scenario.

Let us now present a set of five MUBs for $d = 4$:

$$M_0^{(4)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, M_1^{(4)} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}, M_2^{(4)} = \frac{1}{2}\begin{bmatrix} 1 & -1 & -i & -i \\ 1 & -1 & i & i \\ 1 & 1 & i & -i \\ 1 & 1 & -i & i \end{bmatrix},$$

$$M_3^{(4)} = \frac{1}{2}\begin{bmatrix} 1 & -i & -i & -1 \\ 1 & -i & i & 1 \\ 1 & i & i & -1 \\ 1 & i & -i & 1 \end{bmatrix}, M_4^{(4)} = \frac{1}{2}\begin{bmatrix} 1 & -i & -1 & -i \\ 1 & -i & 1 & i \\ 1 & i & -1 & i \\ 1 & i & 1 & -i \end{bmatrix}.$$

There is only a pair of real MUBs in this case. Now the question is whether the number of real MUBs in dimension $d = 4$ can be extended beyond 2, and the answer is affirmative, as shown by the following example with three real MUBs.

$$M_1' = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}, M_2' = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix}, M_3' = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{bmatrix}.$$

Consider the multiplication by the inverse of M_1' from the left hand side. Here $M_1' = (M_1')^\dagger = (M_1')^{-1}$. Then we obtain, $(M_1'')^{-1} = (M_1')^{-1}M_1' = I$:

$$M_2'' = (M_1')^{-1}M_2' = (M_1')^\dagger M_2' = \frac{1}{2}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

and

$$M_3'' = (M_1')^{-1}M_3' = (M_1')^\dagger M_3' = \frac{1}{2}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \\ 1 & -1 & 0 & 0 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ -1 & 1 & 1 & -1 \end{bmatrix}$$

as Hadamard matrices. As the examples contain real values only, the notation † works as simple transpose here. The structures of M_1', M_2', M_3' can be achieved by the following method that has been used extensively in [57, 60] in design of Approximate MUBs.

6.1.3 Example of ARMUBs in dimension two

We illustrate the notion of Approximate Mutually Unbiased Bases (ARMUBs) through a simple example in dimension $d = 2$. Although exact real MUBs exist in this dimension, this example serves to demonstrate how small perturbations lead naturally to approximate unbiasedness.

Let

$$\mathcal{B}_0 = \left\{ |e_1\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ |e_2\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}$$

be the computational basis of $\mathbb{C}^2$.

For a small real parameter ε with $|\varepsilon| \ll 1$, define the perturbed real orthonormal basis

$$\mathcal{B}_1^{(\varepsilon)} = \left\{ |v_1\rangle = \frac{1}{\sqrt{2+\varepsilon^2}} \begin{pmatrix} 1 \\ 1+\varepsilon \end{pmatrix},\ |v_2\rangle = \frac{1}{\sqrt{2+\varepsilon^2}} \begin{pmatrix} 1+\varepsilon \\ -1 \end{pmatrix} \right\}.$$

The inner products between vectors from $\mathcal{B}_0$ and $\mathcal{B}_1^{(\varepsilon)}$ satisfy

$$|\langle e_1 \rangle\, v_1| = \frac{1}{\sqrt{2+\varepsilon^2}},$$
$$|\langle e_2 \rangle\, v_1| = \frac{1+\varepsilon}{\sqrt{2+\varepsilon^2}},$$

and similarly for $|v_2\rangle$. Consequently,

$$\max_{i,j} |\langle e_i \rangle\, v_j| = \frac{1+\varepsilon}{\sqrt{2+\varepsilon^2}} = \frac{1}{\sqrt{2}} \left(1 + O(\varepsilon)\right).$$

Thus, the pair of bases $\{\mathcal{B}_0, \mathcal{B}_1^{(\varepsilon)}\}$ forms a β-ARMUB in $\mathbb{C}^2$ with

$$\beta = \frac{1+\varepsilon}{\sqrt{2}},$$

in accordance with Definition 1.2.3. As $\varepsilon \to 0$, this construction recovers an exact pair of mutually unbiased bases.

6.2 Our Construction

In this section we present our technique to have ARMUBs, which were not presented earlier in literature. For construction of ARMUBs, similar to Construction 2.5.1 [57, 60], we make use of RBD(X, A), with $|X| = d = k \times s$, where $s > k$ and s, k are as close as possible, so that both s, k are of $O(\sqrt{d})$. Since $d > 2$ is not multiple of 4, thus k or s cannot be a multiple of 4. For constructing ARMUBs corresponding to each parallel class of an RBD, we exploit suitable orthogonal matrix Y, which we call (as in Definition 6.2.1 later) ϵ-Hadamard Matrix of order k, modifying a real Hadamard one of order $k + t$ (where $k + t$ is divisible by 4) such that $|(Y)_{ij}|$, the absolute value of each entry $(Y)_{ij}$ is very close to $\frac{1}{\sqrt{k}}$. The Hadamard conjecture tells that in such cases we have the existence, and thus we can consider $t = \{1, 2, 3\}$ for our purpose. Let us now consider how do we modify the Hadamard matrices.

6.2.1 Modifying real Hadamard matrices

As discussed, we will construct orthogonal matrix of order $k \in \{4n - 1, 4n - 2, 4n - 3\}$ from Hadamard matrix of order $4n$, using the method presented below. We will call such orthogonal matrices as ϵ-Hadamard Matrices. We define the notion of ϵ-Hadamard matrices of order k, which in some sense can be considered as close counterpart of Hadamard in such order, where no Hadamard matrix exists ($k \neq 4n$) and will be helpful in constructing β-ARMUBs with good properties. The basic property of Hadamard matrix which is helpful in such construction, is the same absolute value of all the entries, which is $\frac{1}{\sqrt{4n}}$. Taking cue from this, we intend to construct orthogonal matrix for order $k \neq 4n$, such that the absolute value of the entries of the matrix are very close to each other. In this regard, let us present the following definition for our purpose.

Definition 6.2.1. *For an orthogonal matrix $\mathbb{O}_{k\times k}$, if the absolute value of each entry of this matrix $|(\mathbb{O}_{k\times k})_{ij}| = \frac{1+\epsilon_{ij}}{\sqrt{k}}$, where $\epsilon_{ij} = \pm O(k^{-\lambda}) < 1$, such that $\lambda > 0$, then we call the orthogonal matrix $\mathbb{O}_{k\times k}$ an ϵ-Hadamard matrix, when $\epsilon = \max_{i,j} |\epsilon_{ij}|$.*

If there are choices of many such matrices, then we will consider the one with least ϵ available at hand. When k is a multiple of 4, assuming Hadamard conjecture, it is obvious that the minimal value of ϵ is zero, but when $k > 2$ is not a multiple of 4, finding the

global minima of ϵ appears to be a very challenging problem. However, we first show in Theorem 6.2.1 that such result with $\epsilon < 1$ can be achieved. Later, in Section 6.2.2, we will consider various U and correspondingly, we will obtain the orthogonal matrix with the least ϵ.

We now have the following technical result. Please note that with certain abuse of notations, we write $U_{t\times t}$ to express that it is a $t \times t$ matrix, but while explaining we only write U as we can refer the (i, j)-th element as subscript such as U_{ij} or $(U)_{ij}$. We let $\mathbb{I}_{t\times t}$ refer to the identity matrix of order $t \times t$.

Lemma 6.2.1. *Let* $N = \begin{bmatrix} U_{t\times t} & V_{t\times(m-t)} \\ W_{(m-t)\times t} & D_{(m-t)\times(m-t)} \end{bmatrix}_{m\times m}$ *be an* $m \times m$ *orthogonal matrix, containing block matrices* U, V, W, *and* D *of sizes as indicated. If either* $(\mathbb{I}+U)$ *or* $(\mathbb{I}-U)$ *is a nonsingular matrix, then* $Y_1 = D - W(\mathbb{I}+U)^{-1}V$ *and* $Y_2 = D + W(\mathbb{I}-U)^{-1}V$ *are both orthogonal matrices of order* $m - t$.

Proof. For a matrix A, the transpose is referred as A^T. Since $NN^T = \mathbb{I}_{m\times m}$, we have

$$\begin{aligned} UU^T + VV^T &= \mathbb{I}_{t\times t}, \\ UW^T + VD^T &= \mathbb{O}_{t\times(m-t)}, \\ WU^T + DV^T &= \mathbb{O}_{(m-t)\times t}, \\ WW^T + DD^T &= \mathbb{I}_{(m-t)\times(m-t)}. \end{aligned}$$

Suppose $(\mathbb{I}+U)^{-1}$ exists. Consider, the matrix $Y_1 = D - W(\mathbb{I}+U)^{-1}V$. Then,

$$\begin{aligned} Y_1Y_1^T &= \left(D - W(\mathbb{I}+U)^{-1}V\right)\left(D - W(\mathbb{I}+U)^{-1}V\right)^T \\ &= \left(D - W(\mathbb{I}+U)^{-1}V\right)\left(D^T - V^T(\mathbb{I}+U^T)^{-1}W^T\right) \\ &= DD^T - DV^T(\mathbb{I}+U^T)^{-1}W^T - W(\mathbb{I}+U)^{-1}VD^T \\ &\quad + W(\mathbb{I}+U)^{-1}VV^T(\mathbb{I}+U^T)^{-1}W^T \\ &= \mathbb{I} - WW^T + WU^T(\mathbb{I}+U^T)^{-1}W^T + W(\mathbb{I}+U)^{-1}UW^T \\ &\quad + W(\mathbb{I}+U)^{-1}VV^T(\mathbb{I}+U^T)^{-1}W^T \\ &= \mathbb{I} - W\left[\mathbb{I} - U^T(\mathbb{I}+U^T)^{-1} - (\mathbb{I}+U)^{-1}U - (\mathbb{I}+U)^{-1}VV^T(\mathbb{I}+U^T)^{-1}\right]W^T. \end{aligned}$$

Now consider the expression inside the brackets:

$$\begin{aligned}
&\mathbb{I} - U^T(\mathbb{I}+U^T)^{-1} - (\mathbb{I}+U)^{-1}U - (\mathbb{I}+U)^{-1}VV^T(\mathbb{I}+U^T)^{-1} \\
&= (\mathbb{I}+U)^{-1}(\mathbb{I}+U)(\mathbb{I}+U^T)(\mathbb{I}+U^T)^{-1} - (\mathbb{I}+U)^{-1}(\mathbb{I}+U)U^T(\mathbb{I}+U^T)^{-1} \\
&\quad - (\mathbb{I}+U)^{-1}U(\mathbb{I}+U^T)(\mathbb{I}+U^T)^{-1} - (\mathbb{I}+U)^{-1}VV^T(\mathbb{I}+U^T)^{-1} \\
&= (\mathbb{I}+U)^{-1}\left[(\mathbb{I}+U)(\mathbb{I}+U^T) - (\mathbb{I}+U)U^T - U(\mathbb{I}+U^T) - (\mathbb{I}-UU^T)\right](\mathbb{I}+U^T)^{-1}.
\end{aligned}$$

Since,

$$\begin{aligned}
&(\mathbb{I}+U)(\mathbb{I}+U^T) - (\mathbb{I}+U)U^T - U(\mathbb{I}+U^T) - (\mathbb{I}-UU^T) \\
&= \mathbb{I} + U^T + U + UU^T - U^T - UU^T - U - UU^T - \mathbb{I} + UU^T = \mathbb{O},
\end{aligned}$$

we obtain, $Y_1Y_1^T = \mathbb{I}$. Similarly in above line, one can also show that if $(\mathbb{I}-U)$ is invertible, then $Y_2 = D + W(\mathbb{I}-U)^{-1}V$ is an Orthogonal matrix of size $(m-t)\times(m-t)$. □

Note that the inverse of $(\mathbb{I}+U)$ will exist if eigen-value of U is not equal to -1 and similarly inverse of $(\mathbb{I}-U)$ will exist if eigen value of U is not equal to 1. In fact, U and $(\mathbb{I}\pm U)^{-1}$ commutes. Hence if ν is the eigen value of U then $\frac{1}{\nu\pm1}$ is the eigen vale of $(\mathbb{I}\pm U)^{-1}$. Hence, assuming the inverse of $(\mathbb{I}\pm U)$ exists, there is a simple form for the inverse of the matrix $(\mathbb{I}\pm U)$ in terms of power U, when $||U|| < 1$. This states that $(\mathbb{I}\pm U)^{-1} = \mathbb{I}\mp U + U^2 \mp U^3 + U^4 \ldots$

A particular form of matrix $(\mathbb{I}\pm U)$ is relevant for demonstrating specific constructions, when it is of the form $(\mathbb{I}+\frac{1}{\alpha}X)$, where X is a $t\times t$ matrix. Towards this we have following result.

Lemma 6.2.2. *Let $\kappa, \gamma, \alpha, \vartheta$ be real.*

1. *If $X^2 = \kappa\mathbb{I} + \gamma X$, then the inverse of the matrix $\left(\mathbb{I}+\frac{1}{\alpha}X\right)$ exists if $\alpha^2+\gamma\alpha-\kappa \neq 0$ and is given by $\frac{\alpha(\alpha+\gamma)}{\alpha^2+\gamma\alpha-\kappa}\left(\mathbb{I}-\frac{1}{\alpha+\gamma}X\right)$.*
2. *If $X^3 = \kappa\mathbb{I} + \gamma X + \vartheta X^2$, then the inverse of the matrix $\left(\mathbb{I}+\frac{1}{\alpha}X\right)$ exists if $\alpha^3+\vartheta\alpha^2-\gamma\alpha+\kappa \neq 0$ and is given by $\frac{\alpha(\alpha(\alpha+\vartheta)-\gamma)}{\alpha^3+\vartheta\alpha^2-\gamma\alpha+\kappa}\left(\mathbb{I}-\frac{\alpha+\vartheta}{\alpha(\alpha+\vartheta)-\gamma}X+\frac{1}{\alpha(\alpha+\vartheta)-\gamma}X^2\right)$.*

Proof. The proofs are as follows.

1. When $X^2 = \kappa\mathbb{I} + \gamma X$ consider $(\alpha\mathbb{I} + X)\left((\gamma + \alpha)\mathbb{I} - X\right) = \alpha(\alpha + \gamma)\mathbb{I} + \gamma X - X^2 = (\alpha^2 + \gamma\alpha - \kappa)\mathbb{I}$. Hence if $\alpha^2 + \gamma\alpha - \kappa \neq 0$, the first result follows.

2. When $X^3 = \kappa\mathbb{I} + \gamma X + \vartheta X^2$, consider $(\alpha\mathbb{I} + X)\left((\alpha(\alpha + \vartheta) - \gamma)\mathbb{I} - (\alpha + \vartheta)X + X^2\right) = (\alpha^3 + \vartheta\alpha^2 - \gamma\alpha)\mathbb{I} - \gamma X - \vartheta X^2 + X^3 = (\alpha^3 + \vartheta\alpha^2 - \gamma\alpha + \kappa)\mathbb{I}$. Hence if $\alpha^3 + \vartheta\alpha^2 - \gamma\alpha + \kappa \neq 0$, the second result follows.

□

In the above lemma, if X satisfies the item 1, then we should use that, and one may note that the solution from item 2 will be the same. In case, item 1 is not satisfied, then we should exploit item 2. This is because, the computation in the second case will be more involved.

Note that when X is 2×2 matrix, we will have $X^2 = \gamma X + \kappa\mathbb{I}$, where $\gamma = \mathrm{Tr}(X)$ and $\kappa = -\mathrm{Det}(X)$. When X is a 3×3 matrix, $X^3 = \vartheta X^2 + \gamma X + \kappa\mathbb{I}$ where $\vartheta = \mathrm{Tr}(X)$, $\gamma = \sum_{i>j}(X)_{ij}(X)_{ji} - (X)_{ii}(X)_{jj}$ and $\kappa = \mathrm{Det}(X)$.

Let us now concentrate on eigen value characterization. When $X^2 = \kappa\mathbb{I} + \gamma X$ then the eigen values of X are the roots of the equation $\lambda^2 - \gamma\lambda - \kappa = 0$, and hence has maximum two different values, say $\{\lambda_1, \lambda_2\}$. Thus, X is similar to diagonal matrix $\mathrm{Diag}(\lambda_1, \ldots, \lambda_1, \lambda_2, \ldots \lambda_2)$. Similarly when $X^3 = \kappa\mathbb{I} + \gamma X + \vartheta X^2$ then eigen values of X are the roots of the equation $\lambda^3 - \vartheta\lambda^2 - \gamma\lambda - \kappa = 0$ and in this case X has maximum three different e-values, say $\{\lambda_1, \lambda_2, \lambda_3\}$ and hence X is similar to diagonal matrix $\mathrm{Diag}(\lambda_1, \ldots \lambda_1, \lambda_2, \ldots \lambda_2, \lambda_3, \ldots \lambda_3)$.

We use this and apply the above Lemma 6.2.1 for the case when N is a real Hadamard matrix of order $m = 4n$, denoting it by H_{4n} and obtain the following result.

Note that, in Lemma 6.2.1, there is no $\frac{1}{\sqrt{4n}}$ before the matrix, that we start using from the following result. This is by abuse of notation. Lemma 6.2.1 is only used to prove the orthogonality and thus, we did not use the constant term outside as in the Hadamard matrix. Thus, the U, V, W, D as follows actually differ from those of Lemma 6.2.1 by a constant multiplier.

Theorem 6.2.1. *Let* $H_{4n} = \frac{1}{\sqrt{4n}} \begin{bmatrix} U_{t\times t} & V_{t\times(4n-t)} \\ W_{(4n-t)\times t} & D_{(4n-t)\times(4n-t)} \end{bmatrix}_{n\times n}$. *If* $t < \sqrt{n}$ *then* $Y_1 = D - W(\mathbb{I} + U)^{-1}$ *and* $Y_2 = D + W(\mathbb{I} - U)^{-1}V$ *are* ϵ*-Hadamard matrices of order* $(4n - t)$, *such that* $\frac{1}{\sqrt{4n}}\left(1 - \frac{t}{\sqrt{4n}-t}\right) \leq |(Y_{1,2})_{ij}| \leq \frac{1}{\sqrt{4n}}\left(1 + \frac{t}{\sqrt{4n}-t}\right)$ *with* $\epsilon = \frac{t}{\sqrt{k}} + \mathcal{O}(k^{-1}) \leq 1$.

Proof. Here U, V, W and D sub sub matrix of a Hadamard matrix H_{4n} as explained in Lemma 6.2.1. We have $(U)_{ij} = \frac{\pm 1}{\sqrt{4n}}$. Hence, $(\mathbb{I} \pm U)$ would be diagonally dominant matrix if $t < \sqrt{4n}$ and thus would be non-singular. That is why $(\mathbb{I} \pm U)$ would be invertible.

When all the entries of U are identical i.e., $\frac{+1}{\sqrt{4n}}$ (or $\frac{-1}{\sqrt{4n}}$), then $(U^r)_{ij} = \frac{t^{r-1}}{(\sqrt{4n})^r}$ (or $\frac{(-t)^{r-1}}{(\sqrt{4n})^r}$) respectively, else we will have $|(U^r)_{ij}| \leq \frac{t^{r-1}}{(\sqrt{4n})^r}$. Now, for the convergence of the series for $(\mathbb{I} \pm U)^{-1} = \mathbb{I} \mp U + U^2 \mp U^3 + U^4 \ldots$, each entry of the series should converge. For this the sufficient condition is $\frac{t^{r-1}}{(\sqrt{4n})^r} < 1 \implies t < \sqrt{4n}$, which is also the condition for diagonal dominance. This diagonal dominance implies the invertibility of the matrix. Thus any square sub matrix U of size $t < \sqrt{4n}$ of Hadamard matrix of order $4n$, will have valid series expansion for $(\mathbb{I}-U)^{-1}$ or $(\mathbb{I}+U)^{-1}$ in terms of the powers of U. Hence using Lemma 6.2.1 above we have Y_1 and Y_2 as $Y_1 = D - W(\mathbb{I}+U)^{-1}V = \frac{1}{\sqrt{4n}}\left(\mathsf{D} - \frac{1}{\sqrt{4n}}WV + \frac{1}{4n}WUV - \frac{1}{(4n)^{\frac{3}{2}}}WU^2V \ldots\right)$ and $Y_2 = D + W(\mathbb{I}-U)^{-1}V = \frac{1}{\sqrt{4n}}\left(\mathsf{D} + \frac{1}{\sqrt{4n}}WV + \frac{1}{4n}WUV + \frac{1}{(4n)^{\frac{3}{2}}}WU^2V \ldots\right)$.

Now, in order to get the bound on $(Y_{1,2})_{ij}$, note that all the matrices U, V, W, D have the entries ± 1 only. Therefore, $|(WV)_{ij}| \leq t$, $|(WUV)_{ij}| \leq t^2$ and in general $|(WU^rV)_{ij}| \leq t^{r+1}$. Hence, the absolute value of the entries in the matrix would be bounded above, which implies $|(Y_{1,2})_{ij}| \leq \frac{1}{\sqrt{4n}}\left(1 + \frac{t}{\sqrt{4n}} + (\frac{t}{\sqrt{4n}})^2 + (\frac{t}{\sqrt{4n}})^3 \ldots\right) = \frac{1}{\sqrt{4n}}\left(1 + \frac{t}{\sqrt{4n}-t}\right)$ for $t < \sqrt{4n}$. Similarly the absolute values of the entries in the matrix Y_q is bounded below, which would be given by $|(Y_q)_{ij}| \geq \frac{1}{\sqrt{4n}}\left(1 - \frac{t}{\sqrt{4n}} - (\frac{t}{\sqrt{4n}})^2 - (\frac{t}{\sqrt{4n}})^3 \ldots\right) = \frac{1}{\sqrt{4n}}\left(1 - \frac{t}{\sqrt{4n}-t}\right)$. Now using $k = 4n-t$, we have $|(Y_{1,2})_{ij}| \leq \frac{1}{\sqrt{k+t}}\left(1 + \frac{t}{\sqrt{k+t}-t}\right) = \frac{1}{\sqrt{k+t}-t} = \frac{1+\epsilon}{\sqrt{k}}$ where $\epsilon = \frac{\sqrt{k}}{\sqrt{k+t}-t} - 1$. Hence in order to have $\epsilon \leq 1$ we get inequality $9k^2 + 24kt + 16t^2(t-1)^2 - 40kt^2 \geq 0$. Since $k, t > 0$, thus in this inequality only last term is negative. Hence in order to get a simple form, we may ignore the intermediate terms , then we get $9k^2 - 40kt^2 \geq 0 \Rightarrow t \leq \sqrt{\frac{9k}{40}} < \sqrt{\frac{k}{4}} < \sqrt{n}$. Thus when $t < \sqrt{n}$ the $Y_{1,2}$ are ϵ-Hadamard matrices, with $\epsilon < 1$. And in terms of the order (k) of the ϵ-Hadamard matrices , we have $|(Y_{1,2})_{ij}| \leq \frac{1}{\sqrt{k}}\left(1 + \frac{t}{\sqrt{k}} + \mathcal{O}\left(k^{-1}\right)\right)$. □

As there are various options for real Hadamard matrices, when they exist, for $t \geq 1$, there are various possibilities of U too and corresponding to each possibility, we will have different Y_1, Y_2. Thus, we should consider which one can be chosen for the best result among the various possibilities of U, we are considering.

6.2.2 Explaining the cases with $t = 1, 2, 3$

We present explicit constructions of orthogonal matrices $Y_{(4n-t)\times(4n-t)}$ (i.e., Y_1 or Y_2 as in Theorem 6.2.1) by considering the block matrix $U_{t\times t}$. The matrix U denotes a $t \times t$ matrix whose entries are all ± 1. For $t = 1$, we have $U = \pm 1$. Given one element, without loss of generality, fix $U_1 = 1$. For $t = 2$, as there are 4 elements, we have $2^4 = 16$ possible configurations of U. For $t = 3$, there are $2^9 = 512$ possible configurations.

We have examined several (not all) cases out of these and here we present the results for the ϵ-Hadamard matrix to have the least ϵ among the ones we considered below. As we have pointed out, H_{4n} be an orthogonal matrix of the form

$$H_{4n} = \frac{1}{\sqrt{4n}} \begin{bmatrix} U_{t\times t} & V_{t\times(4n-t)} \\ W_{(4n-t)\times t} & D_{(4n-t)\times(4n-t)} \end{bmatrix},$$

where $t < \sqrt{4n}$ and all submatrices are real. Then the following cases are to be discussed one by one.

The case $t = 1$

If $t = 1$, i.e., $U = [1]$, then we construct

$$Y_1 = \frac{1}{\sqrt{4n}} \left(D + \frac{1}{\sqrt{4n} - 1} WV \right), \quad Y_2 = \frac{1}{\sqrt{4n}} \left(D - \frac{1}{\sqrt{4n} + 1} WV \right).$$

Both Y_1 and Y_2 are orthonormal matrices of order $(4n - 1)$ with entries satisfying:

$$|(Y_1)_{ij}| \in \frac{1}{\sqrt{4n}} \left\{ 1 + \frac{1}{\sqrt{4n} - 1}, 1 - \frac{1}{\sqrt{4n} - 1} \right\}, \quad |(Y_2)_{ij}| \in \frac{1}{\sqrt{4n}} \left\{ 1 + \frac{1}{\sqrt{4n} + 1}, 1 - \frac{1}{\sqrt{4n} + 1} \right\}.$$

Y_2 is the $\epsilon-$Hadamard matrix closest to Hadamard matrix, as ϵ corresponding to Y_2 is lesser than that of Y_1.

Here our construction yields an ϵ-Hadamard matrix with

$$\epsilon = \frac{\sqrt{4n - 1}}{\sqrt{4n}} \left(\frac{\sqrt{4n} + 2}{\sqrt{4n} + 1} \right) - 1 < \frac{1}{2\sqrt{n}},$$

as the best one assuming D, W and V are any possible sub-matrices of a Hadamard matrix.

The case $t = 2$

If $t = 2$, there are a total of $2^4 = 16$ possible configurations for the matrix U. When

$$U \in \left\{ \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix} \right\},$$

we have $U^2 = 2U - 2\mathbb{I}$. This implies the following matrix inverses:

$$\left(\mathbb{I} + \frac{1}{\sqrt{4n}} U \right)^{-1} = \frac{4n + 2\sqrt{4n}}{4n + 2\sqrt{4n} + 2} \left(\mathbb{I} - \frac{1}{\sqrt{4n} + 2} U \right),$$
$$\left(\mathbb{I} - \frac{1}{\sqrt{4n}} U \right)^{-1} = \frac{4n - 2\sqrt{4n}}{4n - 2\sqrt{4n} + 2} \left(\mathbb{I} + \frac{1}{\sqrt{4n} - 2} U \right).$$

Hence, we define the matrices:

$$Y_1 = \frac{1}{\sqrt{4n}} \left(D - \frac{\sqrt{4n} + 2}{4n + 2\sqrt{4n} + 2} WV + \frac{1}{4n + 2\sqrt{4n} + 2} WUV \right),$$

$$Y_2 = \frac{1}{\sqrt{4n}} \left(D + \frac{\sqrt{4n} - 2}{4n - 2\sqrt{4n} + 2} WV + \frac{1}{4n - 2\sqrt{4n} + 2} WUV \right).$$

Both Y_1 and Y_2 are orthonormal matrices of order $(4n - 2)$. Here,Y_2 is the $\epsilon-$Hadamard matrix closest to Hadamard matrix, ϵ of Y_2 is lesser than that of Y_1. When

$$U \in \left\{ \begin{bmatrix} -1 & -1 \\ 1 & -1 \end{bmatrix}, \quad \begin{bmatrix} -1 & 1 \\ -1 & -1 \end{bmatrix} \right\},$$

we have $U^2 = -2U - 2\mathbb{I}$. This implies the following matrix inverses:

$$\left(\mathbb{I} + \frac{1}{\sqrt{4n}} U \right)^{-1} = \frac{4n - 2\sqrt{4n}}{4n - 2\sqrt{4n} + 2} \left(\mathbb{I} - \frac{1}{\sqrt{4n} - 2} U \right),$$
$$\left(\mathbb{I} - \frac{1}{\sqrt{4n}} U \right)^{-1} = \frac{4n + 2\sqrt{4n}}{4n + 2\sqrt{4n} + 2} \left(\mathbb{I} + \frac{1}{\sqrt{4n} + 2} U \right).$$

Hence, we define the matrices:

$$Y_1 = \frac{1}{\sqrt{4n}} \left(D - \frac{\sqrt{4n} - 2}{4n - 2\sqrt{4n} + 2} WV + \frac{1}{4n - 2\sqrt{4n} + 2} WUV \right),$$

$$Y_2 = \frac{1}{\sqrt{4n}}\left(D + \frac{\sqrt{4n}+2}{4n+2\sqrt{4n}+2}WV + \frac{1}{4n+2\sqrt{4n}+2}WUV\right).$$

Both Y_1 and Y_2 are orthonormal matrices of order $(4n-2)$. Y_1 is the $\epsilon-$Hadamard matrix closest to Hadamard matrix, ϵ of Y_1 is lesser than that of Y_2.

One may note that, Y_2 of the first case, i.e., for $U^2 = 2U - 2\mathbb{I}$ and Y_1 in the second case, i.e., for $U^2 = -2U - 2\mathbb{I}$, have the same ϵ hence are two matrices are equally close to a Hadamard matrix.

In this case, our construction yields an ϵ-Hadamard matrix with

$$\epsilon = \frac{\sqrt{4n-2}}{\sqrt{4n}}\left(\frac{4n+2}{4n-2\sqrt{4n}+2}\right) - 1 < \frac{2}{\sqrt{n}},$$

as the best result assuming D, W and V are any possible sub-matrices of a Hadamard matrix.

The case $t = 3$

If $t = 3$, there are a total of $2^9 = 512$ possible configurations for the matrix U, where each entry is either $+1$ or -1. When

$$U \in \left\{ \begin{array}{cccc} \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & -1 \end{bmatrix}, & \begin{bmatrix} -1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & -1 \end{bmatrix}, & \begin{bmatrix} -1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, & \begin{bmatrix} -1 & -1 & 1 \\ -1 & 1 & -1 \\ 1 & -1 & -1 \end{bmatrix}, \\ \begin{bmatrix} 1 & -1 & 1 \\ -1 & -1 & -1 \\ 1 & -1 & -1 \end{bmatrix}, & \begin{bmatrix} -1 & -1 & 1 \\ -1 & -1 & -1 \\ 1 & -1 & 1 \end{bmatrix}, & \begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & -1 \end{bmatrix}, & \begin{bmatrix} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & 1 \end{bmatrix}, \\ \begin{bmatrix} 1 & -1 & 1 \\ -1 & -1 & -1 \\ 1 & -1 & -1 \end{bmatrix}, & \begin{bmatrix} -1 & -1 & 1 \\ -1 & -1 & -1 \\ 1 & -1 & 1 \end{bmatrix}, & \begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & -1 \end{bmatrix}, & \begin{bmatrix} -1 & 1 & -1 \\ 1 & -1 & -1 \\ -1 & -1 & 1 \end{bmatrix} \end{array} \right\}.$$

we have $U^3 = -U^2 + 4U + 4\mathbb{I}$. This implies the following matrix inverses:

$$\left(\mathbb{I} + \frac{1}{\sqrt{4n}}U\right)^{-1} = \frac{4n\sqrt{4n} - 4n - 4\sqrt{4n}}{4n\sqrt{4n} - 4n - 4\sqrt{4n} + 4}\left(\mathbb{I} - \frac{\sqrt{4n}-1}{4n-\sqrt{4n}-4}U + \frac{1}{4n-\sqrt{4n}-4}U^2\right),$$

$$\left(\mathbb{I} - \frac{1}{\sqrt{4n}}U\right)^{-1} = \frac{4n\sqrt{4n} + 4n - 4\sqrt{4n}}{4n\sqrt{4n} + 4n - 4\sqrt{4n} - 4}\left(\mathbb{I} + \frac{\sqrt{4n}+1}{4n+\sqrt{4n}-4}U + \frac{1}{4n+\sqrt{4n}-4}U^2\right).$$

Hence, we define the matrices:

$$Y_1 = \frac{1}{\sqrt{4n}}\left(D - \frac{4n-\sqrt{4n}-4}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}WV + \frac{\sqrt{4n}-1}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}WUV \right.$$
$$\left. - \frac{1}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}WU^2V\right),$$
$$Y_2 = \frac{1}{\sqrt{4n}}\left(D + \frac{4n+\sqrt{4n}-4}{4n\sqrt{4n}+4n-4\sqrt{4n}-4}WV + \frac{\sqrt{4n}+1}{4n\sqrt{4n}+4n-4\sqrt{4n}-4}WUV \right.$$
$$\left. + \frac{1}{4n\sqrt{4n}+4n-4\sqrt{4n}-4}WU^2V\right).$$

Then Y_1 and Y_2 are orthonormal matrices of order $(4n-3)$. Y_1 is the $\epsilon-$Hadamard matrix closest to Hadamard matrix, ϵ of Y_1 is lesser than that of Y_2.
When

$$U \in \left\{ \begin{bmatrix} 1 & -1 & 1 \\ -1 & 1 & 1 \\ 1 & 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & -1 \\ 1 & -1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & -1 \\ 1 & 1 & 1 \\ -1 & 1 & -1 \end{bmatrix}, \begin{bmatrix} 1 & -1 & -1 \\ -1 & 1 & -1 \\ -1 & -1 & -1 \end{bmatrix}, \right.$$
$$\left. \begin{bmatrix} 1 & -1 & 1 \\ -1 & -1 & 1 \\ 1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 1 \\ 1 & -1 & -1 \\ 1 & -1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 & -1 \\ 1 & -1 & 1 \\ -1 & 1 & 1 \end{bmatrix}, \begin{bmatrix} 1 & -1 & -1 \\ -1 & -1 & -1 \\ -1 & -1 & 1 \end{bmatrix} \right\}.$$

we have $\mathsf{U}^3 = \mathsf{U}^2 + 4\mathsf{U} - 4\mathbb{I}$. This implies the following matrix inverses:

$$\left(\mathbb{I} + \frac{1}{\sqrt{4n}}U\right)^{-1} = \frac{4n\sqrt{4n}+4n-4\sqrt{4n}}{4n\sqrt{4n}+4n-4\sqrt{4n}-4}\left(\mathbb{I} - \frac{\sqrt{4n}+1}{4n+\sqrt{4n}-4}U + \frac{1}{4n+\sqrt{4n}-4}U^2\right),$$
$$\left(\mathbb{I} - \frac{1}{\sqrt{4n}}U\right)^{-1} = \frac{4n\sqrt{4n}-4n-4\sqrt{4n}}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}\left(\mathbb{I} + \frac{\sqrt{4n}-1}{4n-\sqrt{4n}-4}U + \frac{1}{4n-\sqrt{4n}-4}U^2\right).$$

Hence, we define the matrices:

$$Y_1 = \frac{1}{\sqrt{4n}}\left(D - \frac{4n+\sqrt{4n}-4}{4n\sqrt{4n}+4n-4\sqrt{4n}-4}WV + \frac{\sqrt{4n}+1}{4n\sqrt{4n}+4n-4\sqrt{4n}-4}WUV \right.$$
$$\left. - \frac{1}{4n\sqrt{4n}+4n-4\sqrt{4n}-4}WU^2V\right),$$
$$Y_2 = \frac{1}{\sqrt{4n}}\left(D + \frac{4n-\sqrt{4n}-4}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}WV + \frac{\sqrt{4n}-1}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}WUV \right.$$
$$\left. + \frac{1}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}WU^2V\right).$$

Then Y_1 and Y_2 are orthonormal matrices of order $(4n-3)$. Y_2 is the $\epsilon-$Hadamard matrix closest to Hadamard matrix, ϵ of Y_2 is lesser than that of Y_1.

One may note that, Y_1 of the first case and Y_2 of of the second case have the same ϵ. Hence the two matrices are equally close to a Hadamard matrix. In this case, our construction yields a ϵ-Hadamard matrix with

$$\epsilon = \frac{\sqrt{4n-3}}{\sqrt{4n}}\left(\frac{4n\sqrt{4n}+8n+2\sqrt{4n}+10}{4n\sqrt{4n}-4n-4\sqrt{4n}+4}\right) - 1 < \frac{4}{\sqrt{n}}, for\ n\ \geq 4,$$

as the best result assuming D, W and V are any possible submatrix of a Hadamard matrix.

We can summarise these in the following results.

Theorem 6.2.2. *For $t = 1, 2, 3$, it is possible to construct real ϵ-Hadamard matrices of dimension $4n - t$ with $\epsilon = \frac{\rho_t}{\sqrt{n}}$, where $\rho_t = \frac{1}{2}, 2$ and 4 respectively for $t = 1, 2, 3$.*

Programs in Python are implemented in this regard to experiment with such ϵ-Hadamard matrices, and the repository is available at [89]. We have noted that the actual values are even smaller than the expressions in Theorem 6.2.2, but the expressions will be more complicated.

6.2.3 Construction of ARMUBs

As we have already discussed, construction for Approximate MUBs using Hadamard and other unitary matrices in conjunction with Resolvable Block Designs have been presented in [57, 59, 60]. The basic concept is to utilize an RBD(X, A), with $|X| = d = k \times s$, having

constant block size k, such that it has as many parallel classes as possible, but any pair of block from different parallel classes, should have maximum 1 point in common ($\mu = 1$) (as we have discussed in subsection 2.5.1 of Chapter 2). Here we need to use the unitary matrix of the order of block size k, to convert each parallel class into an orthonormal basis.

Given this context, we present the main result as follows.

Theorem 6.2.3. *Let $d = k \times s$, such that $s > k$ and s is a power of odd prime. Let ϵ-Hadamard matrix Y of order k exist. Then one can obtain $s \geq \lceil \sqrt{d} \rceil$ many β-ARMUBs, with $\beta \leq 1 + O(d^{-\frac{1}{4}})$, which is < 2 for an infinite class of dimensions d.*

Proof. We broadly consider Construction 2.5.1, to obtain the orthonormal basis vectors in $\mathbb{R}^d$ corresponding to each parallel class in RBD(X, A) using ϵ-Hadamard matrix Y. Following [57, 60] the absolute value of the dot product of any pair of basis vectors u, v from different orthonormal basis $| \langle u, v \rangle | \leq \mu |(Y)_{ij}|^2_{\max} \leq (\frac{1+\epsilon}{\sqrt{k}})^2 = \frac{(1+\epsilon)^2}{k}$, where μ is the intersection number and in this case any pair of blocks from different parallel classes will have maximum one point in common, i.e., $\mu = 1$. When $s - k > 0$ and s a power of prime, then one can construct RBD(X, A) having s many parallel classes, each with s many blocks of constant block size k (refer to [60, Construction 3, Lemma 5] for exact details).

With proper manipulations of constants and noting the power of primes are at least as dense as the primes, we will obtain an odd prime power $s > \sqrt{d}$, in an expected distance $O(\log d)$ from $\sqrt{d}$. Thus, considering Theorem 6.2.2 for the values of ϵ, we obtain the inner product value between two vectors from two different ARMUBs $\leq \frac{(1+\epsilon)^2}{k} \leq \frac{1}{\sqrt{d}}(1 + O(d^{-\frac{1}{4}}))$. This gives $\beta \leq 1 + O(d^{-\frac{1}{4}})$. □

Example 6.2.1. *Let us now consider an example for $d = 79 \times 3^4$, where $k = 79, s = 3^4$. In this case there are $79 + 1 = 80$ complex MUBs, but no pair of real ones. The existing works in this regard [57, 59, 60] do not consider this case too. In this effort, we will obtain $3^4 = 81$ many ARMUBs, which is $\lceil \sqrt{d} \rceil + 1$. As $79 = 4 \times 20 - 1$, from Theorem 6.2.2, we have $\epsilon < \frac{1}{2\sqrt{n}} = \frac{1}{2\sqrt{20}}$. Now, $k = 4n - 1 = 79$, thus, the numeric expression will be $\beta < 1.252$.*

In case, we consider $k = 43$, instead of 79, we obtain $\beta \leq 1.697$. Naturally, we obtain the value of β closest to 1 (from above), when k, s are very close.

6.3 Conclusion

In this work, we presented constructions of β-ARMUBs for certain dimensions d that are not multiples of 4, when d is of the form $(4n-t)s$, where s is an odd prime power. Specifically, we obtain $\beta = 1 + O(d^{-\frac{1}{4}}) < 2$, which is the upper bound of the inner product between any two vectors from two different MUBs. The number of ARMUBs available for these cases are $\geq \lceil \sqrt{d} \rceil$. Such classes of ARMUBs, for dimensions not divisible by 4, had not be presented earier. However, our constructions do not yield real APMUBs (Almost Perfect Real MUBs or APRMUBs) since the set Δ in our case cannot guarantee $|\Delta| = 2$, which is mandatory for an APMUB construction, i.e., in our case, there may be more than 2 values of inner products. As no pair of real MUBs exists for dimensions $d \not\equiv 0 \bmod 4$, such constructions for APRMUBs would be an interesting research direction.

Chapter 7

Conclusion

In this chapter, we conclude the thesis by emphasising that several fundamental questions remain unresolved, particularly concerning the extensibility of given sets of Mutually Unbiased Bases and the explicit construction of exact MUBs in composite dimensions d that are not a power of a prime. Although this thesis has also explored approximate variants of MUBs, the core challenges surrounding exact constructions continue to persist, despite extensive research efforts spanning the past five decades. Readers interested in a more comprehensive discussion of these open problems are encouraged to consult [30, 53] and the references cited therein.

7.1 Summary of the Thesis

This thesis examines several aspects of the theory of MUBs, a fundamental concept in quantum information theory with connections to Algebraic geometry and combinatorics. Our goal has been to investigate the extensibility through algebra and combinatorics and to construct the MUBs and their approximation in specific dimensions, exploiting combinatorial structures like Resolvable Block Designs (RBD) and Mutually Orthogonal Latin Squares (MOLS).

The thesis is divided into two main parts. The first part focuses on the extendibility of known sets of MUBs. In particular, we have considered the existence problem of new MUBs by interpreting it through the lens of algebraic geometry and combinatorics, which is

elaborated upon in Chapters 3 and 4.

In chapter 3, we have studied the extensibility of MUB triplets in $\mathbb{C}^6$, which are product bases, i.e, whether the fourth MUB exists if we have a set of three mutually unbiased product bases in $\mathbb{C}^6$. We have another perspective to look at this problem through an elementary combinatorial approach. In this process, considering all possible cases, we provided an explicit form (in Lemma 3.2.4) of a unitary matrix U (as MUB) in a certain case. Finally, with this form of a unitary matrix U, we prove one can't extend triplets of mutually unbiased product bases in $\mathbb{C}^6$.

In chapter 4, we have explored possible extension of a given set of k MUBs in any dimension d through certain results of algebraic geometry. The basic idea is, if we have a set of k given MUBs for dimension d, then the problem of finding the $(k+1)$-th MUB, is essentially the problem of finding solutions to a system of polynomial equations in $2d^2$ real variables and having degree atmost two. Under this set up we show that the existence or non-existence of MUBs become problems of finding real points on some algebraic varieties. We next analyse the case through an example to recover the complete sets of MUBs for dimension two. Then we show that if we start with the identity matrix, then the system of equations to generate the next MUB contains a part consisting of equations of spheres and some homogeneous equations. The result explains that the ideal generated by the sphere part is a complete intersection prime ideal. This is presented in Section 4.2.3.

Finally, in Section 4.3, we show a connection between MUBs in $\mathbb{C}^d$ and maximal commuting classes (bases) of orthogonal normal matrices of order d instead of commuting bases containing orthogonal unitary matrices [5]. This observation of considering normal matrices over unitary matrices provides more flexibility. This connection reveals the necessary condition for the existence of MUBs in any dimension.

The second part of this thesis is devoted to the combinatorial construction of MUBs and Approximate Real MUBs (ARMUBs) in certain specific dimensions. Also, we consider parametrization of MUBs to understand the degrees of freedom and this can be helpful in exploring various choices of MUBs so that one can explore several classes of them for various applications in quantum information.

Our methodology exploits combinatorial structures like RBD, MOLS and real Hadamard matrices to achieve our goal which are elaborated in details in the last two contributory chapters 5 and 6.

In chapter 5, we consider the introduction of parameters in the set of MUBs for dimension $d = s^2$. In this regard, we have assumed the result from [60], which in turn follows from the result of [84] that given an RBD (X, A) such that $|X| = s^2$, then one can construct $MOLS(s) + 2$ many parallel classes, each having s many blocks of size s and any two blocks from different parallel classes will have exactly one point in common. Then, we convert each of the parallel classes into orthonormal bases (MUBs) using the Hadamard matrix of order s, as we assumed that real Hadamard matrix exist of order s.

We begin by introducing affine (phase) parameters using diagonal and permutation unitary operations. Then we pull out the redundant parameters only from columns (not rows) into each of the rest of the $MOLS(s)+1$ (as first one becomes *identity matrix*) so that MUB structures remain preserved. This construction ensures the presence of at least $s(s-1)$ free parameters in each basis that are invariant under global unitary transformations. Our result produces a larger number of real MUBs (as we work for square dimensions) as well as more free parameters in most cases. This can help in exploring various choices of MUBs in the protocols for higher-dimensional QKDs and other applications of MUBs related to quantum information. Furthermore, we provide a framework for extending this construction to composite dimensions of the form $d = k \times s$.

In our last contributory chapter 6, we talk about the approximate MUBs where we compromise with the unbiasedness property of MUBs, i.e, the inner product of two vectors drawn from two different bases is relaxed, instead of being fixed to a constant value.

In this chapter, we particularly talk about approximate real MUBs for such dimensions that are not multiples of four. This is interesting because we can't have a pair of real MUBs for such a dimension. On the other hand, we can construct at least $\lceil \sqrt{d} \rceil$ many ARMUBs for specific odd dimensions d of the form $d = (4n - t)s$, $t = 1, 2, 3$, where n is a natural number and s is an odd prime power. Our key idea is to construct an orthogonal matrix of order $(4n - t) \times (4n - t)$ by using a Hadamard matrix of order $4n$ (we assume that the Hadamard conjecture is true) such that each entry of the orthogonal matrix does not vary too much.

With this backdrop, let us now present a few problems that we find interesting for future research.

7.2 Future Directions

As we have already discussed, there are substantial number of open problems in the domain of MUBs. The research presented in this thesis also opens up afew avenues for future exploration. Below, we outline some promising directions that stem from the contributory works.

In chapter 3, we investigated the possibility of expressing a unitary matrix U of order six as a product basis in $\mathbb{C}^6$, but we were not successful in obtaining a general form. This motivates a broader line of inquiry in determining the structure of unitary matrix in $\mathbb{C}^6$, or more generally in $\mathbb{C}^d$, that can be realized as product bases. One could then explore whether sets of MUBs comprising such mutually unbiased product bases are extendible.

Furthermore, our approach suggests that one may look for unitary matrices in which almost five of the six columns are product states. It would then be worthwhile to investigate whether such a matrix U can be seen as a new MUB as the extension of in a triplet of mutually unbiased product bases. This line of study may offer new insights into the structure and limitations of MUBs in composite dimensions.

In chapter 4, we studied the problem of extending a set of MUBs from the perspective of algebraic geometry. Our approach reduces this problem to finding real points on a certain affine algebraic variety, which arises from the algebraic relations governing the extensibility of a system of MUBs. In general, the main difficulty is the complexity of the Gröbner basis algorithm, which is very high in general. For large dimensions, Gröbner basis computations become increasingly complex, making the systematic exploration of defining ideals of the MUB extension problem computationally challenging. To address this, one promising direction is the development or application of more efficient algorithms targeted to this specific problem, such as those from numerical algebraic geometry or homotopy continuation methods. Alongside this, a deeper investigation into the geometric structure of the associated affine variety, particularly its dimension, irreducible components, and whether the defining ideal is radical or prime, etc. could offer sharper criteria for the existence and uniqueness of extensions, thereby refining our understanding of when a system of MUBs can be extended or shown to be maximal.

In chapter 5, we consider the parameterisation of MUBs so that one can explore several classes for them. A deeper analysis of the free parameters introduced via affine transforma-

tions may help in classifying the in-equivalent MUBs.

Then, in chapter 6, we presented constructions of β-ARMUBs for certain dimensions d. However, our constructions do not yield real APMUBs (Almost Perfect Real MUBs or APRMUBs) since the set Δ in our case may not satisfy $|\Delta| = 2$, which is mandatory for an APMUB construction, i.e., in our case, there may be more than 2 values of inner products. As no pair of real MUBs exists for dimensions $d \not\equiv 0 \bmod 4$, such constructions for APRMUBs would be an interesting research direction.

7.3 Final Comments

In this thesis, we have undertaken a theoretical study of Mutually Unbiased Bases. Specifically, we study the extendibility of a given set of MUBs in arbitrary dimensions using algebraic and combinatorial approaches. In addition, we have constructed approximate real MUBs in dimensions that are not divisible by four, in cases where we don't have even a pair of real MUBs. Furthermore, we consider the parametrisation of real MUBs in dimension $d = s^2$, as we sometimes surpass the known (naive) lower bound of MUBs when the dimension is a perfect square. Our method leverages combinatorial structures, such as RBD, MOLS, and Hadamard matrices, to achieve these goals.

Bibliography

[1] S. Aaronson. *The new ten most annoying questions in quantum computing.* 2014. doi: https://scottaaronson.blog/?p=1792

[2] R. J. R. Abel, C. J. Colbourn, and J. H. Dinitz. *Mutually orthogonal Latin squares (MOLS).* Part III, Chapter 3, Handbook of Combinatorial Designs, Edited by C.J. Colbourn and J.H. Dinitz, CRC Press, pp. 111–142, 2006. doi: https://doi.org/10.1201/9781420010541

[3] E. A. Aguilar, J. J. Borkala, P. Mironowicz, and M. Pawlowski. *Connections Between Mutually Unbiased Bases and Quantum Random Access Codes.* Phys. Rev. Lett. 121, 050501, 2018. doi: https://doi.org/10.1103/PhysRevLett.121.050501, arXiv: https://arxiv.org/abs/1709.04898, 2018

[4] A. Azarchs. *Entropic uncertainty relations for incomplete sets of mutually unbiased observables.* arXiv preprint quant-ph/0412083, 2004. doi: https://doi.org/10.48550/arXiv.quant-ph/0412083

[5] S. Bandyopadhyay, P. O. Boykin, V. Roychowdhury, and F. Vatan. *A new proof for the existence of mutually unbiased bases.* Algorithmica, 34(4): 512–528, 2002. doi: https://doi.org/10.1007/s00453-002-0980-7, URL: https://arxiv.org/abs/quant-ph/0103162, 2001

[6] A. Banerjee, K. K. Das, A. Kumar, R. Kumar and S. Maitra. *On Obtaining New MUBs by Finding Points on Complete Intersection Varieties over* $\mathbb{R}$. International Journal of Theoretical Physics, 64 (227), 2025. doi: https://doi.org/10.1007/s10773-025-06094-3

[7] T. Baumgratz, M. Cramer, and M. B. Plenio. *Quantifying coherence.* Physical review letters, 113(14), 140401, (2014).

[8] I. Bengtsson. *MUBs, polytopes, and finite geometries.* American Institute of Physics - conference Proceedings, 750(1): 63–69, 2005. doi: https://doi.org/10.1063/1.1874558, arXiv: https://arxiv.org/abs/quant-ph/0406174, 2004

[9] I. Bengtsson, W. Bruzda, Å. Ericsson, J. Larsson, W. Tadej, and K. Życzkowski. *Mutually Unbiased Bases and Hadamard Matrices Of Order Six.* Journal of Mathematical Physics, 48, 052106, 2007. doi: https://doi.org/10.1063/1.2716990, arXiv: https://arxiv.org/abs/quant-ph/0610161, 2007

[10] I. Bengtsson and Å. Ericsson. *Mutually unbiased bases and the complementarity polytope.* Open Systems & Information Dynamics, 12(2): 107–120, 2005. doi: 10.1007/s11080-005-5721-3. URL: https://doi.org/10.1007/s11080-005-5721-3.

[11] C. H. Bennett and G. Brassard. *Quantum cryptography: public key distribution and coin tossing.* Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179, 1984. Theoretical Computer Science, 560(1): 7–11, 2014. doi: https://doi.org/10.1016/j.tcs.2014.05.025

[12] B. G. Bodmann and J. I. Haas. *Maximal orthoplectic fusion frames from mutually unbiased bases and block designs.* In Proceedings of the American Mathematical Society, 146(6): 2601–2616, 2018. doi: https://doi.org/10.1090/proc/13956

[13] R. C. Bose. *On the construction of balanced incomplete block designs.* Annals of Eugenics, 9(4): 353–399, 1939. doi: https://doi.org/10.1111/j.1469-1809.1939.tb02219.x

[14] R. C. Bose. *A note on resolvability of balanced incomplete block designs.* Sankhya: The Indian Journal of Statistics, 6(2): 105–110, 1942. URL: https://www.jstor.org/stable/25047747.

[15] R. C. Bose. *On a resolvable series of balanced incomplete block designs.* Sankhya: The Indian Journal of Statistics, 8(3): 249–256, 1947. URL: http://www.jstor.org/stable/25047951.

[16] P. O. Boykin, M. Sitharam, M. Tarifi, and P. Wocjan. *Real Mutually Unbiased Bases.* 2005. arXiv: https://arxiv.org/abs/quant-ph/0502024, 2005.

[17] P. O. Boykin, M. Sitharam, P. H. Tiep, and P. Wocjan. *MUBs and orthogonal decompositions of Lie algebras.* Quant. Inform. Comput. 7, 371 (2007). doi: https://doi.org/10.26421/QIC7.4-6

[18] S. Brierley and S. Weigert. *Maximal sets of mutually unbiased quantum states in dimension 6.* Physical Review A, (2008). doi: https://doi.org/10.1103/physreva.78.042312

[19] S. Brierley, S. Weigert, and I. Bengtsson. *All mutually unbiased bases in dimensions two to five.* Quantum Info. Comp. 10, 0803 (2010) doi: https://doi.org/10.48550/arXiv.0907.4097

[20] S. Brierley and S. Weigert. *Constructing mutually unbiased bases in dimension six.* Physical Review A—Atomic, Molecular, and Optical Physics, 79(5), 052316, 2009. doi: https://doi.org/10.1103/PhysRevA.79.052316

[21] D. Bruß. *Optimal Eavesdropping in Quantum Cryptography with Six States.* Phys. Rev. Lett. 81(14): 3018–3021, 1998. doi: https://doi.org/10.1103/PhysRevLett.81.3018

[22] Č. Brukner,and A. Zeilinger. *Information and fundamental elements of the structure of quantum theory* In Time, quantum and information (pp. 323-354). Berlin, Heidelberg: Springer Berlin Heidelberg, 2003

[23] X. Cao and W. S. Chou. *More constructions of approximately mutually unbiased bases.* Bulletin of the Australian Mathematical Society, 93(2): 211–222, 2016. doi: https://doi.org/10.1017/S0004972715000994

[24] N.J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin. *Security of quantum key distribution using d-level systems.* Physical Review Letters, 88(12), 127902, 2002. doi: https://doi.org/10.1103/PhysRevLett.88.127902

[25] S. Chaturvedi, S. Ghosh, K.R. Parthasarathy, and A.I. Singh. *Optimal quantum tomography with constrained measurements arising from unitary bases.* Reviews

in Mathematical Physics, 33(07), 2130005, 2021. doi: https://doi.org/10.1142/S0129055X21300053

[26] S. Chowla, P. Erdös, and E. G. Straus. *On the maximal number of pairwise orthogonal latin squares of a given order*. Canadian Journal of Mathematics, 12: 204–208, 1960. doi: https://doi.org/10.4153/CJM-1960-017-2.

[27] C. J. Colbourn and J. H. Dinitz. *Mutually orthogonal latin squares: a brief survey of constructions*. Journal of Statistical Planning and Inference, 95(1): 9–48, 2001. doi: https://doi.org/10.1016/S0378-3758(00)00276-7

[28] S. Designolle, M. Farkas, and J. Kaniewski. *Incompatibility robustness of quantum measurements: a unified framework.* New Journal of Physics, 21(11), 113053, 2019. doi: 10.1088/1367-2630/ab5020

[29] P. Dita. *Some results on the parametrization of complex Hadamard matrices*. Journal of Physics A: Mathematical and General, 37(20), 5355 (2004). doi : 10.1088/0305-4470/37/20/008

[30] T. Durt, B. G. Englert, I. Bengtsson, and K. Życzkowski. *On mutually unbiased bases.* International journal of quantum information, 8(4): 535–640, 2010. doi: https://doi.org/10.1142/S0219749910006502

[31] C. Eltschka, M. Huber, S. Morelli, and J. Siewert. *The shape of higher-dimensional state space: Bloch-ball analog for a qutrit.* Quantum, 5, 485, 2021. doi: https://doi.org/10.22331/q-2021-06-29-485

[32] B.G. Englert, and Y. Aharonov. *The mean king's problem: prime degrees of freedom.* Physics Letters A, 284(1), 1-5, 2001. doi: https://doi.org/10.1016/S0375-9601(01)00271-7

[33] D. Goyeneche. *A new method to construct families of complex Hadamard matrices in even dimensions.* J. Math. Phys. 54, 032201 (2013). doi: 10.1063/1.4794068, arXiv: https://arxiv.org/abs/1210.7673, April 2013

[34] D. Goyeneche and S. Gomez. *Mutually unbiased bases with free parameters.* Phys. Rev. A 92(6): 23-25 (2015). doi: 10.1103/PhysRevA.92.062325, arXiv: https://arxiv.org/abs/1506.08283, June 2015

[35] M. Grassl. *On SIC-POVMs and MUBs in dimension 6.* doi: https://doi.org/10.48550/arXiv.quant-ph/0406175

[36] U. Haagerup. *Orthogonal maximal Abelian-subalgebras of the $n \times n$ matrices and cyclic n-roots.* Odense Universitet, 1996

[37] J. I. Haas, J. Cahill, J. Tremain, and P. G. Casazza. *Constructions of biangular tight frames and their relationships with equiangular tight frames.* arXiv: https://arxiv.org/abs/1703.01786, 2017

[38] N. Hao, Z.H. Li, H.Y. Bai, and C.M. Bai. *A new quantum secret sharing scheme based on mutually unbiased bases.* International Journal of Theoretical Physics, 58, 1249-1261, (2019).

[39] J. Herzog, and T. Hibi. *Monomial ideals.* Graduate Texts in Mathematics, Springer-Verlag London, Ltd., London, 260, 2011. doi: https://doi.org/10.1007/978-0-85729-106-6

[40] J. Herzog, T. Hibi, and H. Ohsugi. *Binomial ideals.* Graduate Texts in Mathematics, Springer, Cham, 279, 2018. doi: https://doi.org/10.1007/978-3-319-95349-6

[41] P. Horodecki, L. Rudnicki, and K. Życzkowski. *Five open problems in quantum information theory.* PRX Quantum, 3(1), 010101, 2022. doi: https://doi.org/10.1103/PRXQuantum.3.010101

[42] C. J. Huang, G. Y. Xiang, Y. Guo, K.D. Wu, B. H. Liu, C. F. Li, G. C. Guo, and A. Tavakoli. *Nonlocality, steering, and quantum state tomography in a single experiment.* Physical Review Letters, 127(2), 020401,2021. doi: https://doi.org/10.1103/PhysRevLett.127.020401

[43] I. D. Ivanovic. *Geometrical description of quantal state determination.* Journal of Physics A, 14(12): 3241-3245, 1981. doi: http://dx.doi.org/10.1088/0305-4470/14/12/019

[44] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner. *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6.* Journal of Physics A: Mathematical and Theoretical, 42(24), 245305, 2009. doi: 10.1088/1751-8113/42/24/245305

[45] W. M. Kantor. *MUBs inequivalence and affine planes.* Journal of Mathematical Physics, 53(3),2012. doi: https://doi.org/10.1063/1.3690050

[46] M. R. Kibler and M. Planat. *A SU(2) recipe for MUBs.* Int. J. Mod. Phys. B 20, 1802 (2006). doi: https://doi.org/10.1142/S0217979206034303

[47] G. Kimura, H. Tanaka, and M. Ozawa. *Solution to the mean king's problem with mutually unbiased bases for arbitrary levels.* Physical Review A—Atomic, Molecular, and Optical Physics, 73(5), 050301, 2006. doi: https://doi.org/10.1103/PhysRevA.73.050301

[48] J. Kiukas, D. McNulty, and J. P. Pellonpää. *Amount of quantum coherence needed for measurement incompatibility.* Physical Review A, 105(1), 012205, 2022 doi: https://doi.org/10.1103/PhysRevA.105.012205

[49] A. Klappenecker, M. Röetteler. *Constructions of Mutually Unbiased Bases.* Finite Fields and Applications, pp. 137–144, Berlin, Heidelberg, Springer Berlin Heidelberg, 2004. doi: https://doi.org/10.1007/978-3-540-24633-6_10

[50] A. Klappenecker, M. Rötteler, I. E. Shparlinski, and A. Winterhof. *On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states.* Journal of Mathematical Physics, 46(8): 082104, 2005. doi: https://doi.org/10.1063/1.1998831

[51] A. B. Klimov, L. L. Sánchez-Soto, and H. de Guise. *A complementarity-based approach to phase in finite-dimensional quantum systems.* arXiv preprint quant-ph/0410135, 2004. doi: 10.1088/1464-4266/7/9/008

[52] M. N. Kolountzakis, M. Matolcsi, and M. Weiner. *An application of positive definite functions to the problem of MUBs.* Proc. Amer. Math. Soc. 146, 1143 (2018). doi: https://doi.org/10.1090/proc/13829

[53] O. Krueger and R. F. Werner. *Some Open Problems in Quantum Information Theory.* arXiv https://arxiv.org/abs/quant-ph/0504166, 2005

[54] A. Kumar, R. Kumar and S. Maitra. *A Parametric Class of Mutually Unbiased Bases Using Resolvable Block Designs.* INDOCRYPT (1), Lecture Notes in Computer Sci-

ence 15495, 356-373, 2024. doi: https://link.springer.com/chapter/10.1007/978-3-031-80308-6_16

[55] A. Kumar, R. Kumar, S. Maitra and S. Sarangi. *Exploring the presence of* 4*-th MUB as a product basis in* $\mathbb{C}^6$. 8th Workshop on Design Theory, Hadamard Matrices and Applications (Hadamard 2025), 26-30 May, 2025, Sevilla. doi: https://gestioneventos.us.es/hadamard2025

[56] A. Kumar, R. Kumar, S. Maitra and U. Mandal. *On Construction of Approximate Real Mutually Unbiased Bases for an infinite class of dimensions* $d \not\equiv 0 \bmod 4$. doi: https://doi.org/10.48550/arXiv.2507.07028

[57] A. Kumar and S. Maitra. *Resolvable block designs in construction of approximate real MUBs that are sparse.* Cryptography and Communications, 14(3):527-549, 2022. doi: https://doi.org/10.1007/s12095-021-00537-4

[58] A. Kumar and S. Maitra. *Further Constructions of AMUBs for Non-prime Power Composite Dimensions*. Preprint. arXiv: https://arxiv.org/abs/2402.04231, 2024.

[59] A. Kumar, S. Maitra, and C. S. Mukherjee. *On approximate real mutually unbiased bases in square dimension*. Cryptography and Communications, 13(2): 321–329, 2021. doi: https://doi.org/10.1007/s12095-020-00468-6

[60] A. Kumar. S. Maitra and S. Roy. *Almost Perfect Mutually Unbiased Bases that are Sparse*. Preprint. arXiv: https://arxiv.org/abs/2402.03964, 2024.

[61] N. LeCompte, W. J. Martin, and W. Owens. *On the equivalence between real mutually unbiased bases and a certain class of association schemes*. European Journal of Combinatorics, 31(6): 1499–1512, 2010. doi: https://doi.org/10.1016/j.ejc.2009.11.014

[62] H. Matsumura. *Commutative Ring Theory*. Cambridge Studies in Advanced Mathematics, 8, Translated from the Japanese by M. Reid (1986).

[63] D. McNulty and S. Weigert. *Isolated Hadamard matrices from mutually unbiased product bases*. Journal of mathematical physics, 53(12) (2012). doi: https://doi.org/10.1063/1.4764884

[64] D. McNulty, and S. Weigert. *All mutually unbiased product bases in dimension six.* arXiv preprint arXiv:1111.3632, 2011. doi: https://doi.org/10.1088/1751-8113/45/13/13530

[65] D. McNulty, and S. Weigert. *On the impossibility to extend triples of mutually unbiased product bases in dimension six.* International Journal of Quantum Information 10.05, 1250056, 2012. doi: https://doi.org/10.1142/S0219749912500566

[66] D. McNulty and S. Weigert. *Mutually Unbiased Bases in Composite Dimensions–A Review.* arXiv preprint arXiv:2410.23997, 2024. doi: https://doi.org/10.48550/arXiv.2410.23997

[67] M. Nathanson, and M. B. Ruskai (2007). *Pauli diagonal channels constant on axes.* Journal of Physics A: Mathematical and Theoretical, 40(28), 8171. doi: 10.1088/1751-8113/40/28/S22

[68] A. Fernández-Pérez, A.B. Klimov, and C. Saavedra. *Quantum process reconstruction based on mutually unbiased basis.* Physical Review A—Atomic, Molecular, and Optical Physics, 83(5), 052332, 2011. doi: https://doi.org/10.1103/PhysRevA.83.052332

[69] T. Paterek, M. Pawłowski, M. Grassl, and Č. Brukner. *On the connection between mutually unbiased bases and orthogonal Latin squares.* Physica Scripta, 2010(T140):014031, 2010. doi: https://doi.org/10.1088/0031-8949/2010/T140/014031

[70] M. Planat, H. Rosu, and S. Perrine. *A survey of finite algebraic geometrical structures underlying mutually unbiased quantum measurements.* Foundations Of Physics, 36, 1662-1680 (2006). doi: https://doi.org/10.1007/s10701-006-9079-3

[71] M. Saniga, M. Planat, and H. Rosu. *Mutually unbiased bases and finite projective planes.* Journal of Optics B: Quantum and Semiclassical Optics, 6(9): L19, 2004. doi: https://doi.org/10.1088/1464-4266/6/9/L01

[72] J. Schwinger. *Unitary Operator Bases.* Proc. Natl. Acad. Sci. U.S.A. 46(4): 570-579, 1960. doi: https://doi.org/10.1073/pnas.46.4.570

[73] I. E. Shparlinski and A. Winterhof. *Constructions of approximately mutually unbiased bases.* LATIN 2006: Theoretical Informatics, vol. 3887: 793–799, 2006. doi: https://doi.org/10.1007/11682462_72

[74] C. Spengler, M. Huber, S. Brierley, T. Adaktylos, and B.C. Hiesmayr. *Entanglement detection via mutually unbiased bases.* Physical Review A—Atomic, Molecular, and Optical Physics, 86(2), 022311, 2012. doi: https://doi.org/10.1103/PhysRevA.86.022311

[75] D. R. Stinson. *Combinatorial designs: constructions and analysis.* Springer Science & Business Media, 2007.

[76] Y. Sun, M.J. Zhao, and P.T. Li. *Applications of Geometric Coherence with Respect to Mutually Unbiased Bases.* International Journal of Theoretical Physics, 63(10), 264, (2024).

[77] W. Tadej and K. Zyczkowski. *A concise guide to complex Hadamard matrices.* Open Systems Information Dynamics, 13(2), 133-177 (2006). doi: https://doi.org/10.1007/s11080-006-8220-2

[78] A. Tavakoli, I. Bengtsson, N. Gisin, and J. M. Renes. *Compounds of symmetric informationally complete measurements and their application in quantum key distribution.* Physical Review Research, 2(4), 043122, 2020. doi: https://doi.org/10.1103/PhysRevResearch.2.043122

[79] A. Tavakoli, I. Herbauts, M. Żukowski and M. Bourennane. *Secret sharing with a single d-level quantum system.* Physical Review A, 92(3), 030302 (2015).

[80] A. Tavakoli, A. Hameedi, B. Marques, and M. Bourennane. *Quantum random access codes using single d-level systems.* Physical Review Letters, 114(17), 170502, (2015). doi: https://doi.org/10.1103/PhysRevLett.114.170502

[81] M. Weiner. *A gap for the maximum number of mutually unbiased bases.* Proceedings of the American Mathematical Society, 141(6), 1963-1969, 2013. doi: https://doi.org/10.48550/arXiv.0902.0635

[82] M. Wieśniak, T. Paterek, and A. Zeilinger. *Entanglement in mutually unbiased bases.* New Journal of Physics, 13(5), 053047, 2011. doi: 10.1088/1367-2630/13/5/053047

[83] R. M. Wilson. *Concerning the number of mutually orthogonal latin squares.* Discrete Mathematics, 9(2): 181–198, 1974. doi: https://doi.org/10.1016/0012-365X(74)90148-4

[84] P. Wocjan and T. Beth. *New Construction of Mutually Unbiased Bases In Square Dimensions.* Quantum Information and Computation, 5(2): 93–101, 2005. doi: https://dl.acm.org/doi/abs/10.5555/2011626.2011627 arXiv: https://arxiv.org/abs/quant-ph/0407081, 2004

[85] W. K. Wootters and B. D. Fields. *Optimal state-determination by mutually unbiased measurements.* Annals of Physics, 191(2): 363–381, 1989. doi: https://doi.org/10.1016/0003-4916(89)90322-9

[86] M. Yang, A. Zhang, J. Wen, and K. Feng. *Constructions on real approximate mutually unbiased bases*, 2021. arXiv: https://arxiv.org/abs/2110.06665, 2021

[87] G. Zauner. *Quantum designs: foundations of a noncommutative design theory.* International Journal of Quantum Information, 9(1): 445–507, 2011. doi: https://doi.org/10.1142/S0219749911006776

[88] F. Zhang. *Matrix theory: basic results and techniques.* Springer Science and Business Media, 2011.

[89] Github: https://github.com/UddiptoMandal/ARMUB