On Combinatorial Constructions of Mutually Unbiased Bases (MUBs) with Approximations

Thesis submitted to Indian Statistical Institute

BY

AJEET KUMAR
APPLIED STATISTICS UNIT
INDIAN STATISTICAL INSTITUTE

2024

On Combinatorial Constructions of Mutually Unbiased Bases (MUBs) with Approximations

Thesis submitted to Indian Statistical Institute in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy in Computer Science

by

Ajeet Kumar
Applied Statistics Unit
Indian Statistical Institute
203, B. T. Road, Kolkata 700 108, INDIA
e-mail: ajeetk52@gmail.com

under the supervision of

Prof. Subhamoy Maitra
Applied Statistics Unit
Indian Statistical Institute
203, B. T. Road, Kolkata 700 108, INDIA
e-mail: subho@isical.ac.in, maitra.subhamoy@gmail.com

To one of the fundamentals in our CONSTITUTION

Article 51 (A) h.

–"To develop the scientific temper, humanism, and the spirit of inquiry and reform"

Acknowledgments

Preparing a thesis takes several years to be completed. In this period I have been enriched in numerous ways by interaction with many people. At this point, I like to thank them all.

First and foremost I must thank my supervisor Prof. Subhamoy Maitra. I met him in 2017 after I got selected in the research program at Indian Statistical Institute. In the next few years we became close friends. While the expression turned to an old cliche, I must reiterate that without his cooperation this thesis could not be completed. His interests have in many ways stimulated and shaped my approach to a problem. I must admire his great patience with his Ph.D. students and ability to bring the best out of them in research.

I am grateful to Prof. Bimal Roy for his keen interest in our combinatorial approach and his valuable insights which greatly helped in our research work. I must also thank Shri Gaurav Sinha for the valuable discussion on Number theoretic aspects, which proved valuable in our research. At the same time, I also acknowledge Dr. V. K. Senecha of BARC, who taught me computational methods long back that helped me in this thesis in many ways.

During the preparation of the thesis, I collaborated with several researchers. Some of them also joined me in writing peer-reviewed papers. In this regard I must acknowledge Dr. Shashi C. L. Srivastava (Scientific Officer 'F', VECC, Kolkata), Dr. Arindam Banerjee (Assistant Professor, IIT Kharagpur), Mr. Chandra Sekhar Mukherjee (an alumni of Indian Statistical Institute, now at University of Southern California, USA), Mr. Somjit Roy (Master's student of Statistics at University of Kolkata), Mr. Sreejit Chaudhury (Bachelor's of Engineering from Jadavpur University). I also like to thank my fellow research scholars Mr. Suman Dutta, Mr. Rakesh Kumar, Mr. Animesh Roy and Dr. Jyotirmoy Basak at Indian Statistical Institute. Other than the technical collaboration, they also helped me to handle various administrative issues.

I must also pay gratitude to my family, particularly to my brother, who provided me constant encouragement towards higher studies and research work. His encouragement led me to enroll for the PhD program. My wife and daughters provided very congenial atmosphere at home which helped me to sustain focus on my research work. Last, but not the least, my sister, brother-in-law and my parents provided extremely valuable support during this endeavour.

Abstract

Construction of Mutually Unbiased Bases (MUBs) is a very challenging combinatorial problem in the domain of quantum information theory with several long standing open questions. In the language of quantum information theory, two orthonormal bases in the d-dimensional complex Hilbert space $\mathbb{C}^d$, $\{|e_1\rangle, \ldots |e_d\rangle\}$ and $\{|f_1\rangle, \ldots |f_d\rangle\}$ are called Mutually Unbiased if we have

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

Similarly, some r orthonormal bases are called Mutually Unbiased Bases (MUBs) if they are pairwise Mutually Unbiased. Reaching the upper bound on this r is believed to be an extremely challenging problem for more than half a century. Because of the difficulties to construct significantly large number of MUBs, the problem is relaxed and the concept of Approximate Mutually Unbiased Bases (AMUBs) had been introduced by Klappenecker, Rötteler, Shparlinski and Winterhof in 2005. In this case the inner product of two vectors drawn from two different bases is relaxed, instead of being exactly $\frac{1}{\sqrt{d}}$.

In the initial contribution of our thesis, we provide a method to construct upto $(\sqrt{d}+1)$ many AMUBs in dimension $d = q^2$, where q is a positive integer. In particular, when d is of the form $(4x)^2$ where x is a prime, we obtain $(\frac{\sqrt{d}}{4}+1)$ many Approximate Mutually Unbiased Bases (ARMUBs) such that for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| \leq \frac{4}{\sqrt{d}}$.

The above results are then improved as well as generalized significantly with several constructions exploiting the more involved combinatorial structures such as Resolvable Block Designs (RBDs). We first explain the generic idea of our strategy in relating the RBDs with MUBs/ARMUBs, which are sparse (the basis vectors have small number of non-zero co-ordinates). To be specific, we present an infinite family of $\lceil\sqrt{d}\rceil$ many ARMUBs for dimension $d = q(q+1)$, where $q \equiv 3 \bmod 4$ and it is a prime power, such that for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| < \frac{2}{\sqrt{d}}$. We also analyze certain specific cases, such as $d = sq^2$, where q is a prime power and $sq \equiv 0 \bmod 4$.

We continue to improve our results in this direction and formalize the definition of approximate MUBs with more restrictions. We propose the concept of Almost Perfect MUBs (APMUB), where we restrict the absolute value of inner product $|\langle v_1|v_2\rangle|$ to be two-valued, one being zero and the other $\leq \frac{1+\mathcal{O}(d^{-\lambda})}{\sqrt{d}}$, such that $\lambda > 0$ and the numerator $1+\mathcal{O}(d^{-\lambda}) \leq 2$. We show that for a general composite dimension $d = k \times s$, $k, s \in \mathbb{N}$, with $k \leq s \leq 4k$, one can construct at least $N(s)+1$ many APMUBs, where $N(s)$ is the number of Mutually Orthogonal Latin Squares (MOLS) of order s. Even when restricted to $\mathbb{R}^d$, we can construct similar number of real APMUBs, whenever real Hadamard matrix of order k can be constructed. Further, if $s = q$, where q power of prime, we have $N(q) = q-1$, which enable

us to construct $q \sim \mathcal{O}(\sqrt{d})$ many APMUBs. More appropriate and novel combinatorial designs are presented in this regard which extend this to composite dimension of the form $d = (q-e)(q+f), e, f \in \mathbb{N}$, with $0 \leq f \leq e$ and q some power of prime. We also show that our result has important implications towards Bi-angular vectors.

With the understanding of APMUBs, we revisit a larger class of AMUBs, and improve the results further in terms of larger classes for composites that are not prime powers, and for both real and complex. The technique is more generalized in terms of exploring novel instances of RBDs that provide improved results.

Finally a heuristic framework is presented to search for AMUBs with significantly good parameters and experimental outcomes of the computer programs are studied. Given a non-prime dimension d, we note the closest prime $d' > d$ and form $d' + 1$ MUBs through the existing methods. Then our proposed idea considers two parts. First we apply basis reduction techniques (that are well studied in Machine Learning literature) in obtaining the initial solutions. Then we exploit the steepest ascent kind of search to improve the results further. The efficacy of our technique is shown through construction of AMUBs in dimensions $d = 6, 10, 46$ from $d' = 7, 11$ and 47 respectively. From a more generic view, this approach considers approximately solving a challenging (where efficient deterministic algorithms are not known) mathematical problem in discrete domain through state-of-the-art heuristic ideas.

To summarize, in this thesis we exploit several involved combinatorial techniques in a disciplined manner and also a heuristic to construct approximate MUBs.

Contents

List of Figures

List of Tables

List of Publications

Peer reviewed Journals

- 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: 10.1007/s12095-020-00468-6.
URL: https://doi.org/10.1007/s12095-020-00468-6.

- 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: 10.1007/s12095-021-00537-4.
URL: https://doi.org/10.1007/s12095-021-00537-4.

Peer Reviewed Conference

- S. Chaudhury, A. Kumar, S. Maitra, S. Roy and S. Sen Gupta. *A Heuristic Framework to Search for Approximate Mutually Unbiased Bases.* CSCML 2022: 208-223, Cyber Security, Cryptology, and Machine Learning - 6th International Symposium, Lecture Notes in Computer Science 13301, Springer 2022. URL: https://doi.org/10.1007/978-3-031-07689-3_16.

Preprints

- A. Kumar, S. Maitra and S. Roy. *Almost Perfect Mutually Unbiased Bases that are Sparse.* Preprint, https://arxiv.org/abs/2402.03964, 2024.

- A. Kumar and S. Maitra. *Further Constructions of AMUBs for Non-prime Power Composite Dimensions.* Preprint, https://arxiv.org/abs/2402.04231, 2024.

Chapter 1

Introduction

Mutually Unbiased Bases (MUBs) are important objects in various areas of Mathematics and Computer Science. The idea was initially described in [85] more than six decades back. The motivation was related to unitary operator bases and the work also considers maximum degree of incompatibility. Later in [52] such objects were used for state determination. Further it was noted that MUBs are directly related to Quantum Key Distribution (QKD) [10], in particular for the six-state scenario [19]. As it is well known that QKD is an integral part of Quantum Cryptology, the application of MUBs could be underlined immediately. For example, one may refer to [2] where certain connections between MUBs and Quantum Random Access Codes are noted. Other than the applications in the broad field of information theory, there are very interesting unsolved questions in this domain. For example, it is still open for more than half a century that exactly how many MUBs are there in the dimension six. While, the lower bound three could be achieved, no better result is known given that the upper bound is seven. To explain these in more details, let us formalize a few definitions in this regard. We begin with the notations from quantum information theory, and later move towards the combinatorial domain.

1.1 Presenting the problem

One can relate 'ket' with a unit vector, that can be written as $|v\rangle$. Such a vector belongs to some complex vector space, say V and physically can be understood as a quantum bit or qubit. One can define the inner product between two d-dimensional complex vectors $|u\rangle = (u_1, \ldots, u_d), |v\rangle = (v_1, \ldots, v_d)$ as $\langle u|v\rangle = u_1 v_1^* + \ldots + u_d v_d^*$, where v_i^* is complex conjugate of v_i. This produces a complex number. The modulus of a complex number $z = x + iy$ is $\sqrt{x^2 + y^2}$. This relates to the angle between two vectors, where the modulus of $\langle u|v\rangle$, denoted by $|\langle u|v\rangle|$ gives the cosine of the angle between $|u\rangle$ and $|v\rangle$. Here, $|u\rangle$ and

$|v\rangle$ are the unit vectors, and the angle lies between $\left[0, \frac{\pi}{2}\right]$. With this as background, let us present the definition of MUBs.

Definition 1.1.1. *Two orthonormal bases in the d-dimensional complex Hilbert space $\mathbb{C}^d$, $\{|e_1\rangle, \ldots, |e_d\rangle\}$ and $\{|f_1\rangle, \ldots, |f_d\rangle\}$ are called Mutually Unbiased if*

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

Similarly, some r orthonormal bases are called Mutually Unbiased Bases (MUBs) if they are pairwise Mutually Unbiased.

An example will be useful here for $d = 2$. Consider the bases

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

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

Now the question is how many such MUBs can be constructed for a dimension d. It was noted in [99] that for a dimension d, it is possible to construct at most $(d+1)$ MUBs. This bound can be achieved when d is a prime power [99], that has been proved in a constructive manner later [79]. A simplified proof of this, based on the estimation of exponential sums, was presented in [60]. Another important idea of proof, using maximally commuting bases of orthogonal unitary matrices, was presented in [6].

On the other hand, the construction methods cannot reach the upper bound when d is not a prime power. Given any $d = p_1^{k_1} p_2^{k_2} \ldots p_r^{k_r}$, in the form of its prime factorization, construction methods are known to obtain

$$\nu_d = \left(\min_{i \in \{1,\ldots,r\}} p_i^{k_i}\right) + 1$$

many MUBs. This is the lower bound and ν_d is much less than $d+1$ in many cases. Even after significant efforts in this direction for more than half a century, there is no evidence of beating the lower bound for the non prime power cases, and thus this problem remains quite interesting. One may refer to [64, Problem 13], where this question takes a place among the important open problems in quantum information theory. In fact there are a series of papers related to the case of $d = 6 = 2 \cdot 3$. As per the lower bound, $2 + 1 = 3$ MUBs could be constructed. However, the upper bound is $6 + 1 = 7$. Thus there is a gap and even this specific problem of dimension $d = 6$ is considered to be one of the most sought after questions in the domain of quantum information [81].

We like to clarify here the situation that there are cases where the lower bound of MUBs is strictly greater than ν_d, but the known constructions cannot reach $d + 1$ for a dimension d. Consider d as a perfect square written as $d = s^2$, where s is any positive integer. This construction [98] is based on Mutually Orthogonal Latin Squares (MOLS), and consider that there are $N(s)$ such objects for a dimension s. Then one may construct $N(s)+2$ many MUBs for the dimension d. Let us take an example with $s = 26$, i.e., $d = s^2 = 26^2 = 2^2 \cdot 13^2$. In this case, the lower bound $\nu_d = 2^2 + 1 = 5$. However, the number of MOLS is $N(26) \geq 4$. In this method, the number of MUBs generated will be at least $4 + 2 = 6$ which is greater than $\nu_d = 5$. To explain more such cases, note that $N(s) \geq 6$, for $s \geq 76$. For all $d = s^2 = (2p)^2$, where p is a prime and $s = 2p \geq 76$, we have $\nu_d = 5$. However, the construction using MOLS will always provide at least $N(s) + 2 = 6 + 2 = 8$ many MUBs.

From the above discussions, it is very clear that there are immense difficulties to construct increasing the number of MUBs, if not elusive. In this direction, the problem is comparatively simplified and the concept of Approximate Mutually Unbiased Bases (AMUBs) had been introduced in [61]. Here, the inner product of two vectors drawn from two different bases is relaxed, instead of being fixed to a single point. Note that we consider the approximation allowing the inner product for vectors coming from two different bases, but do not allow any relaxation inside a base. That is, the bases are always orthonormal in our study. We may define it formally as follows.

Definition 1.1.2. *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 $v_2 \in B_{i_2}$ $(i_1 \neq i_2)$,*

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

The domain of AMUBs has not been explored in-depth so far. In this thesis, our main motivation is to exploit combinatorial objects such as Hadamard matrices, Mutually Orthogonal Latin Squares (MOLS), Resolvable Block Designs (RBDs) etc. towards various construction techniques of AMUBs. Some computer-based heuristic searches in conjunction with dimension reduction techniques have also been studied towards the end. With this introduction, let us present the organization of the thesis and its contributions. Detailed background related to this topic will be explained in Chapter 2.

1.2 Thesis Plan

Chapter 3 presents the first contributory work of this thesis. In this initial effort, a construction method is described to obtain at most $(\sqrt{d}+1)$ many AMUBs in dimension $d = q^2$, where q is any positive integer. For $q \equiv 0 \bmod 4$, we obtain Approximate Real MUBs (ARMUBs) assuming that a Hadamard matrix of order q exists. In this effort, we further characterize the inner product values between the elements of two different bases. Given a prime x, when d is of the form $(4x)^2$, we obtain $(\frac{\sqrt{d}}{4}+1)$ many ARMUBs such that for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| \leq \frac{4}{\sqrt{d}}$. This work has been published in [67].

The results of Chapter 3 are then improved and generalized in Chapter 4. We propose various constructions exploiting involved combinatorial structures such as RBDs. First the generic construction idea is presented to relate the RBDs with MUBs/ARMUBs. We like to highlight that in these cases the basis vectors have small number of non-zero co-ordinates, i.e., the constructed bases are sparse. We take up specific parameters for which one can demonstrate new classes and improved results. In particular, we present an infinite family of $\lceil\sqrt{d}\rceil$ many ARMUBs for dimensions of the form $d = q(q+1)$, where q is a prime power and $q \equiv 3 \bmod 4$. In this case, for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| < \frac{2}{\sqrt{d}}$. We also analyze different cases such as $d = sq^2$, where q is a prime power and $sq \equiv 0 \bmod 4$. The work of this chapter is published in [65].

Next we formalize the definition of approximate MUBs with more restrictions in Chapter 5. We propose the concept of Almost Perfect MUBs (APMUBs), where the absolute value of inner product $|\langle v_1|v_2\rangle|$ is two-valued, one being zero and the other $\leq \frac{1+\mathcal{O}(d^{-\lambda})}{\sqrt{d}}$, such that $\lambda > 0$ and the numerator $1 + \mathcal{O}(d^{-\lambda}) \leq 2$. In this process, the vectors that we construct have important features, that large number of its components are zero (we already pointed this out) and the non-zero components are of equal magnitude. The techniques are sharpened exploiting combinatorial structures related to Resolvable Block Designs (RBDs). For a composite dimension $d = k \cdot s,\ k \leq s \leq 4k$, one can construct at least $N(s)+1$ many APMUBs, where $N(s)$ is the number of Mutually Orthogonal Latin Squares (MOLS) of order s. We also consider the cases when each component of the vectors are real, producing similar number of real APMUBs, whenever real Hadamard matrix of order k are available. Moreover, when $s = q$, where q is a prime power, we obtain $N(q) = q - 1$. This helps to construct $q \sim \mathcal{O}(\sqrt{d})$ many APMUBs. This technique is further extended to composite dimension of the form $d = (q-e)(q+f), e, f \in \mathbb{N}$, with $0 \leq f \leq e$ and a prime power q. Such cases are at least as dense as the prime numbers in the set of positive integers. These results are of importance in producing Bi-angular vectors. The APMUBs, so constructed in $\mathbb{C}^d$ or $\mathbb{R}^d$, provide sets of Bi-angular vectors which are of the order of $\mathcal{O}(d^{3/2})$ in numbers (here the upper bound is $\mathcal{O}(d^2)$). These results are presented in [68].

We further investigate a less restrictive, i.e., a more generalized class of AMUBs in Chapter 6, considering broader aspects over the results of Chapter 4. Broader classes of non-prime power composite dimensions are studied in this chapter for both real and complex AMUBs. Instead of constant block sizes, here we consider various values and thus consider several novel instances of RBDs suitable in this direction. These results are presented in [66].

We also explore a heuristic framework to search for AMUBs with significantly good parameters in Chapter 7. Note that these are not APMUBs as explained in the previous chapters. However, we obtain some interesting parameters when we compare them with AMUBs as presented in Chapters 3, 4. Here, instead of combinatorial techniques, heuristics are implemented and experimental outcomes of certain computer programs are reported. Given a non-prime dimension d, we first consider the closest prime $d' > d$ and form $d' + 1$ MUBs through the existing methods [79, 60, 6]. Then our proposed idea considers two techniques one after the other. First we apply basis reduction techniques from Machine Learning literature in obtaining the initial solutions. Then we exploit the steepest ascent kind of search to improve the results further. The experimental outcome is presented through construction of AMUBs for the dimensions $d = 6, 10, 46$ from $d' = 7, 11$ and 47 respectively. This technique provides a generic framework in construction of AMUBs heuristically. In fact, this approach attempts to solve a challenging (where efficient deterministic algorithms are not known) mathematical problem approximately in discrete domain through state-of-the-art heuristic ideas. The results of this chapter got published in [28].

Chapter 8 concludes the thesis with a summary of the results and several directions towards the open questions that might be interesting for future research efforts. In summary, we exploit several involved combinatorial techniques in a disciplined manner to construct Approximate MUBs. The constructions are based on simpler to more complicated combinatorial objects. Towards the end, we also explore certain heuristics and computer programs are executed to perform different experiments. Our constructions have applications in the broad area of quantum information. Several open questions are presented that could be important research problems in future.

1.3 Prerequisites

It is assumed that the reader is familiar with undergraduate level combinatorics, linear algebra and abstract algebra. We will present more details regarding the more involved algebraic and combinatorial structures in Chapter 2. Basic understanding of computer algorithms are necessary to understand the methodologies. The details of heuristics and basis reduction kinds of techniques will also be explained in Chapter 2 to follow the thesis. There is no requirement to have any background on Mutually Unbiased Bases (MUBs). We will develop the background with sufficient details in the following sections and introduce the ideas one by one, as and when required.

1.4 Conclusion

We have introduced the outline of the problem in this section. First we explain the MUBs and then pointed out that such constructions are quite hard for the dimensions which are not prime powers. That is the reason, certain approximations are necessary that may be useful for the application domain related to quantum information theory. Further, the relationship of MUBs with several combinatorial structures such as resolvable block designs are so intriguing that these problems are independently of theoretical interest. In this regard, certain relaxations over the MUBs are already considered and there are limited research efforts in the domain of Approximate MUBs. We consider this problem in a more detailed and disciplined manner, and propose a structure called Almost Perfect MUBs. In this thesis we provide several novel results in that direction. In the following chapter, we present the background material that would be helpful to understand the contributory sections of this thesis.

Chapter 2

Background

In this chapter we provide a brief introduction to existing research in the related areas and identify how our work fits in that framework. In the context of MUBs, a basis can be represented as a unitary matrix. That is, each row will be a unit vector. For dimension d, there will be d many components in the vector, and in our analysis those will be complex numbers. We will have d such orthonormal vectors. Such d rows will form a unitary matrix.

Let us now refer to the example in the previous chapter for $d = 2$, where we have considered:

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

Generally, the qubit $|0\rangle$ is represented as $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ and $|1\rangle$ can be represented as $\begin{bmatrix} 0 \\ 1 \end{bmatrix}$. That is, following the literature, we work with column vectors. However, for our purpose to connect a vector with a row, we will interpret $|0\rangle$ as $\begin{bmatrix} 1 & 0 \end{bmatrix}$ and $|1\rangle$ as $\begin{bmatrix} 0 & 1 \end{bmatrix}$.

Thus, we obtain $M_0^{(2)} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$. Note that while considering the MUBs, we can always consider the identity matrix as one basis. In this manner, we will have, $M_1^{(2)} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$ and $M_2^{(2)} = \begin{bmatrix} \frac{1}{\sqrt{2}} & \frac{i}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & -\frac{i}{\sqrt{2}} \end{bmatrix} = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix}$. For notational convenience in this chapter, we add a super-script in the first bracket to identify the dimension. One may note that $M_1^{(2)}$ is the well known Hadamard matrix of dimension 2 and referred to as H_2 in literature[1]. A general construction of Hadamard matrices H_{2^i} can be seen as $H_2 \otimes H_{2^{i-1}}$, where $\otimes$ is the tensor (Kronecker) product.

One can now check that if two different vectors from a matrix M_i are considered, they are orthonormal, i.e., the inner product will become zero. On the other hand, if one vector is chosen from M_i and the other from M_j, with $i \neq j$, then the inner product will produce the value $\frac{1}{\sqrt{2}}$. That is for dimension $d = 2$, $M_0^{(2)}, M_1^{(2)}, M_2^{(2)}$ are three MUBs. It is easy to see that if one considers any unitary matrix U of dimension 2, then $UM_0^{(2)}, UM_1^{(2)}, UM_2^{(2)}$ will also be a set of three MUBs.

Note that for $d = 3, 4, 5$, one can construct 4, 5, 6 many MUBs respectively. As it is discussed earlier, for any dimension d, the upper bound is $d + 1$ [99, 79, 60, 6]. The upper bound can be achieved for any prime power, and thus it works for $3, 4, 5$.

An example for four MUBs for $d = 3$ are as follows:

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

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

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

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

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

We like to point out that $M_1^{(4)} = H_{2^2} = H_2 \otimes H_2$, a Hadamard matrix. Note that the matrices $M_2^{(4)}, M_3^{(4)}$ and $M_4^{(4)}$ too can be seen as complex Hadamard matrices with the normalizing $\frac{1}{\sqrt{d}}$ taken out.

[1] Since we are working with unitary matrices, we have included the $\frac{1}{\sqrt{d}}$ for dimension d in this discussion. However, many authors defined Hadamard matrices without the normalizing factor.

2.1 MUBs and Hadamard matrices

Before proceeding, let us now explain a little bit more about unitary matrices. A unitary matrix U is a square one whose inverse is equal to its conjugate transpose ($U^\dagger$); that is $U^\dagger U = UU^\dagger = UU^{-1} = I$. One can verify that the rows (or columns) of U form an orthonormal basis of C^d with respect to the usual inner product. In fact, unitary matrices are the complex analog of real orthogonal matrices. Two simple examples of unitary matrices in dimensions 2 and 3 are $\frac{1}{2}\begin{bmatrix} 1+i & -1+i \\ 1+i & 1-i \end{bmatrix}$, $\frac{1}{2}\begin{bmatrix} 1 & -i & -1+i \\ i & 1 & 1+i \\ 1+i & -1+i & 0 \end{bmatrix}$ respectively.

We have already discussed that each MUB in the space C^d consists of d orthogonal unit vectors which, collectively, can be thought of as a unitary $d \times d$ matrix. Two (or more) MUBs thus correspond to two (or more) unitary matrices, one of which can always be mapped to the identity I of the space C^d, using a unitary transformation. For example, suppose we have r many MUBs $\{M_1, M_2, M_3, \ldots, M_r\}$ in C^d where $r \leq d+1$ and also we can thought them as a r numbers of $d \times d$ unitary matrices. If we multiply M_1^{-1} to each of the matrices at right, then one can obtain $\{I, M_2M_1^{-1}, M_3M_1^{-1}, \ldots, M_rM_1^{-1}\}$ as the transformed set of MUBs. As the inverse of any unitary matrix is equal to its conjugate transpose, to obtain $M_jM_i^{-1}$, for $i \neq j$, we are considering inner products of each row of the two matrices in the set of MUBs. Thus, the modulus of each element of the product matrix will be $\frac{1}{\sqrt{d}}$. Taking $\frac{1}{\sqrt{d}}$ common, the modulus of each of the elements will be 1, i.e., we will have complex Hadamard matrices. The result will be similar if we multiply the inverse from the left too. Let us explain this with the following example with three matrices, which are MUBs, but none of them is Hadamard.

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

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:

$$H_1 = M_1^{-1}M_2 = M_1^\dagger M_2 = \frac{1}{2}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{bmatrix}\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & -1 \end{bmatrix} = \frac{1}{2}\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

and

$$H_2 = M_1^{-1}M_3 = M_1^{\dagger}M_3 = \frac{1}{2}\begin{bmatrix}1 & 1 & 0 & 0\\ 1 & -1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\end{bmatrix}\begin{bmatrix}1 & 1 & 0 & 0\\ 0 & 0 & 1 & 1\\ 0 & 0 & 1 & -1\\ 1 & -1 & 0 & 0\end{bmatrix} = \frac{1}{2}\begin{bmatrix}1 & 1 & 1 & 1\\ 1 & 1 & -1 & -1\\ 1 & -1 & 1 & -1\\ -1 & 1 & 1 & -1\end{bmatrix}$$

as Hadamard matrices. As the examples contain real values only, the notation † works as simple transpose here. This is one relationship between MUBs and Hadamard matrices that we described. It is well known that Hadamard matrices have extremely rich combinatorial structures. In our contributory sections, we will use Hadamard matrices towards several kinds of constructions.

Definition 2.1.1 (Weighing matrix)**.** *A square matrix of order d and weight w is called a (complex) weighing matrix, denoted by $W(w,d)$, if its elements belong to the set $\left\{0, \frac{\exp(i\theta)}{\sqrt{w}}\right\}$ with $\theta \in \mathbb{R}$, and it satisfies $W(w,d)^{\dagger}W(w,d) = I$. If the elements are confined to the set $\left\{0, \pm\frac{1}{\sqrt{w}}\right\}$, it becomes a real weighing matrix.*

The use of complex weighing matrices in quantum error correcting codes has been explored in [41]. Furthermore, the connection between real weighing matrices and classical codes are also investigated, as evident from the studies such as [34, 54, 55, 4], which also delve into applications involving spherical codes [74]. For more analysis, one can refer to [62] and the references therein. This background is required to relate one of our constructions in Chapter 5.

2.2 Challenges in composite (but non prime power) dimensions

As we have already discussed, the smallest integer where the challenge appears is for $d = 6$. The lower bound provides the 3 MUBs that can be constructed and the upper bound is $6 + 1 = 7$.

Let us quickly provide an outline how one can construct the three MUBs of dimension 6. We already described $M_0^{(2)}, M_1^{(2)}, M_2^{(2)}$ as above for dimension 2. Similarly, consider the four MUBs of dimension 3, which are $M_0^{(3)}, M_1^{(3)}, M_2^{(3)}, M_3^{(3)}$. Now the matrices $M_{i_1}^{(2)} \otimes M_{j_1}^{(3)}$, $M_{i_2}^{(2)} \otimes M_{j_2}^{(3)}$, $M_{i_3}^{(2)} \otimes M_{j_3}^{(3)}$ will be three MUBs of dimension 6, where $i_1, i_2, i_3 \in \{0, 1, 2\}$ are distinct and $j_1, j_2, j_3 \in \{0, 1, 2, 3\}$ are distinct as well. It should be noted that if we consider $M_{i_1}^{(2)}, M_{j_1}^{(3)}$ as identity matrices of dimensions 2, 3 respectively, then $M_{i_1}^{(2)} \otimes M_{j_1}^{(3)}$ will also be an identity matrix of dimension 6. This actually outlines the proof of the minimum bound ν_d. It has been shown that for any $d = p_1^{k_1}p_2^{k_2}\dots p_r^{k_r}$, expressed in the form of its prime factorization, one can construct $\nu_d = \left(\min\limits_{i\in\{1,\dots,r\}} p_i^{k_i}\right) + 1$ many MUBs. The method should start from $p_s^{k_s}+1$ many MUBs for dimension $p_s^{k_s}$, where the minimum is for $i=s$. It is evident that any $p_i^{k_i} > p_s^{k_s}$, for $i \neq s$ and thus for the dimension $p_i^{k_i}$ we will have $p_i^{k_i}+1$ many MUBs, which is larger than $p_s^{k_s}+1$. Now for the r prime powers, we need to choose distinct matrices and get the tensor product of them to obtain each matrix of degree d. This way we can construct $p_s^{k_s}+1$ MUBs for dimension d.

However, even after very serious research efforts, the question remains unsolved whether the upper bound can be reached for composite (non prime power) dimensions. It is thus clearly understood that for composite numbers which are not prime powers, obtaining a conclusion is elusive [64, Problem 13]. In fact, this specific problem of dimension $d=6$ is a celebrated open question in quantum information [81]. One may refer to [32] and references therein to have an idea that how the numerical methods work towards obtaining approximate solutions. This also motivates our work that the approximate solutions are important while considering the MUBs. Our work in this thesis shows how combinatorial structures can be exploited to construct such approximate MUBs, with certain guarantees regarding the deviation from the exact ones. Our work in Chapter 3 considers Hadamard matrices for the constructions. However, more involved combinatorial structures are exploited in the following two chapters, namely Chapters 4, 5. In this direction, let us briefly explain the basics of Resolvable Block Design (RBD) in the following section (Section 2.3). We have also considered some numerical techniques in Chapter 7 of this thesis. That involves a heuristic framework exploiting certain basis reduction techniques that are frequently applied in Machine Learning literature. The background required there is briefly presented in that chapter itself in Section 7.1.2.

2.3 Basics of Resolvable Block Design

Let us now explain the combinatorial object that we relate to construct (approximate) MUBs. The notations for combinatorial designs are borrowed from [93, Chapter 1].

Definition 2.3.1. *A design can be expressed as a pair (X, A) such that the following properties are satisfied.*

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

A design is called simple, if there is no repeated block in A. In this chapter, we will restrict our analysis to simple designs only.

Definition 2.3.2. *A parallel class in design (X, A) is a subset of disjoint blocks in A whose union is X. For a design (X, A), if A can be partitioned into $r \geq 1$ parallel classes, called resolution, then the design (X, A) is called Resolvable Block Design (RBD).*

For example, consider the combinatorial design (X, A_1) and (X, A_2) with

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

Then (X, A_2) is a resolvable design since $A_2 = P_1 \cup P_2$ where $P_1 = \{(1, 2, 3), (6, 8), (4, 5, 7)\}$ and $P_2 = \{(1, 7), (2, 4, 6), (3, 5, 8)\}$ form two parallel classes consisting of disjoint sets whose union is set X. We say P_1 and P_2 form resolutions of A_2. However, the design (X, A_1) is not resolvable as such resolutions are not possible in this case.

Definition 2.3.3. *A Balanced Incomplete Block Design (BIBD) is a design (X, A), with parameters $\{v, k, \lambda\} \in \mathbb{N}$ and $v > k \geq 2$ and $\lambda \geq 1$ such that the following properties are satisfied:*

1. *$|X| = v$,*
2. *each block contains exactly k points, and*
3. *every pair of distinct points is contained in exactly λ blocks.*

The third property relates to balancedness. It can be shown that every point occurs in exactly $r = \frac{\lambda(v-1)}{k-1}$ blocks and a BIBD has exactly $b = \frac{vr}{k} = \frac{\lambda(v^2-v)}{k^2-k}$ blocks. A (v, k, λ)-BIBD (X, A) is resolvable if A has at least one resolution. Note that, the design (X, A_2) has resolution and hence it is a RBD. However, it is not a BIBD as properties 2, 3 are not satisfied.

The necessary condition for (v, k, λ)-BIBD to be resolvable is $b \geq v + r - 1$ or equivalently $r \geq k + \lambda$. A Resolvable (v, k, λ)-BIBD is called Affine Resolvable (ARBIBD) if $b = v + r - 1$ or equivalently $r = k + \lambda$. Further, any two blocks from different parallel classes of ARBIBD have exactly $\frac{k^2}{v}$ points in common.

An Affine Plane of order q is an example of $(q^2, q, 1)$-ARBIBD. The construction of such Affine Planes are known only when q is some power of a prime. A finite projective plane of order q is an example of $(q^2 + q + 1, q + 1, 1)$-BIBD. Finite projective planes are equivalent to finite affine planes and vice versa. Detailed understanding on these structures are presented in [93, Chapters 2, 5]. Another important and related combinatorial structure in this regard is the set of Mutually Orthogonal Latin Squares that we will explain next.

2.4 Mutually Orthogonal Latin Square (MOLS)

A Latin Square of order s is an $s \times s$ array, and a cell of the array consists of a single element from a set Y, such that $|Y| = s$. Every row of the Latin Square is a permutation of the elements of set Y and every column of the Latin square is also permutation of the elements from the set Y. For more details one may refer to [93, Definition 6.1] as well as [1, Example 1.1]. A pair of Latin Squares (L_1, L_2) of same order and having entries from same set Y (or, a different set having same number of elements) is called Mutually Orthogonal, if in the ordered pair $\{(Y, Y)\} = \{((L_1)_{ij}, (L_2)_{ij})\}$, every pair $x, y \in Y$ appears exactly once. That is, if two of the Latin Squares are superimposed, and the resulting entries in each cell is written as ordered pairs, then every $x, y \in Y$ appears exactly once in the cell. Further, if there is a set of w many Latin Squares, say $\{L_1, L_2, \dots, L_w\}$, each of order s, such that, every pair of Latin Squares is orthogonal, then the set is called Mutually Orthogonal Latin Square of order s, which we denote as w-MOLS(s).

Let $N(s)$ denote the maximal value of w such that, there are w many MOLS of order s [1, 30], [93, Chapter 6]. While using the numerical values of $N(s)$, in subsequent examples in this paper, we will use the currently known values of $N(s)$ from [1, Table 3.87, page 176]. Note that these are not always the actual values of $N(s)$ (except when s is some power prime or of small order) as the exact value of $N(s)$ is still an open question in most of the cases. It is known that, $N(s) \leq s - 1$, $\forall$ s. When this bound is attained, we say that there is a complete set of Mutually Orthogonal Latin Squares of order s. The construction for complete sets of MOLS(s) is known when s is some power of prime [93, Section 6.4]. When s is not a power of prime, $N(s)$ is much smaller than $s - 1$. A table with the largest known values for w is presented in [1] for $s < 10000$.

It is known that there exists a constant n_0, such that for all $s \geq n_0$, we have, $N(s) \geq \frac{1}{3}s^{\frac{1}{91}}$ [29], which was later improved by Wilson [97] to $N(s) \geq s^{\frac{1}{17}}$. Further, it was shown in [98, Section 4] that the exponent can be lower bounded by $\frac{1}{14.8}$. One may note that $N(s) \to \infty$ as $s \to \infty$ in general, but for the cases only when s is some power of prime then $N(s) = s - 1$, else it is considerably small. In this regard, one may also note that the Affine Planes of order q are equivalent to $(q - 1)$ MOLS(q) [93, Theorem 6.32]. For a brief survey on construction of MOLS, one may refer to [30]. In this direction we like to explain the following construction.

2.4.1 Combinatorial Construction of MUBs in Square Dimension

One important combinatorial construction of Mutually Unbiased Bases (MUBs) is given in [98], where it has been shown that $k = w + 2$ MUBs can be constructed in any square dimension $d = s^2$ provided there exists w Mutually Orthogonal Latin Squares (MOLS) of order s. The construction offered, broadly uses design-theoretic (combinatorial) objects viz., (k, s)-nets and generalized Hadamard matrices of size s. This construction obtains more number of mutually orthogonal bases in non-prime-power dimensions as compared to prime-power dimensions.

For this, let us explain Nets described as incidence vectors, which satisfies the conditions similar to MUBs. Consider a collection of k MUBs in $\mathbb{C}^d$ as

$$\mathcal{B}_l = \{|\psi_1^l\rangle, |\psi_2^l\rangle, \ldots, |\psi_d^l\rangle\}; 1 \leq l \leq k.$$

We have,

$$|\langle\psi_i^l|\psi_j^l\rangle|^2 = \delta_{ij};\ \forall\, 1 \leq l \leq k,\ \forall\, 1 \leq i, j \leq d \tag{2.1}$$

and,

$$|\langle\psi_i^l|\psi_j^m\rangle|^2 = \frac{1}{d};\ \forall\, 1 \leq l < m \leq k,\ \forall\, 1 \leq i \leq j \leq d \tag{2.2}$$

Now we take a collection of incidence vectors that satisfy "similar" conditions. A (column) vector, $\mathbf{m} = (\mathbf{m}[1], \ldots, \mathbf{m}[d])^T$ of size d is an incidence vector if its entries are either 0 or 1. The Hamming weight of $\mathbf{m}$ is the number of 1's, and denoted as s. With this background on incidence vectors, we define nets as follows.

Definition 2.4.1. *Let $\{\mathbf{m}_{11}, \ldots, \mathbf{m}_{1s}, \mathbf{m}_{21}, \ldots, \mathbf{m}_{2s}, \ldots, \mathbf{m}_{k1}, \ldots, \mathbf{m}_{ks}\}$ be a collection of ks incidence vectors of size $d = s^2$ that are partitioned into k blocks, where each block has s incidence vectors. Consider the i-th incidence vector in the l-th block, $\mathbf{m}_{li}. For 1 \leq l \leq k, 1 \leq i \leq s$, such a collection form a $(k, s)-$net if,*

$$\mathbf{m}_{li}^T\mathbf{m}_{lj} = 0; \forall\, 1 \leq l \leq k; \forall\, 1 \leq i \neq j \leq s \tag{2.3}$$

$$\mathbf{m}_{li}^T\mathbf{m}_{mj} = 1; \forall\, 1 \leq l \neq m \leq s; \forall\, 1 \leq i, j \leq s \tag{2.4}$$

Example 2.4.1. *Let $d = s^2 = 2^2$ with $s = 2$, we have $k = 3$ blocks. The incidence vectors for $(3, 2)$-net are,*

$\mathbf{m}_{11}$	$\mathbf{m}_{12}$	$\mathbf{m}_{21}$	$\mathbf{m}_{22}$	$\mathbf{m}_{31}$	$\mathbf{m}_{32}$
1	0	1	0	1	0
1	0	0	1	0	1
0	1	1	0	0	1
0	1	0	1	1	0

Table 2.1: Incidence vectors for $(3, 2)$-net.

Now let us elaborate generalized Hadamard matrices. Consider an $s \times s$ matrix

$$\mathbf{H} = \begin{pmatrix} h_{11} & h_{12} & \dots & h_{1s} \\ h_{21} & h_{22} & \dots & h_{2s} \\ \vdots & \vdots & \dots & \vdots \\ h_{s1} & h_{s2} & \dots & h_{ss} \end{pmatrix},$$

with entries $h_{ij} \in \mathbb{C}$. This is called a generalized Hadamard matrix with all entries have modulus 1 and $\mathbf{H}\mathbf{H}^\dagger = s\mathbf{1}_s$. Note that generalized Hadamard matrices exist for any dimension s. For example, one may consider a Fourier matrix such that,

$$DFT^{(s)}_{k,l} = (e^{\frac{2i\pi}{s}})^{kl}; k, l = 0, 1, 2, \dots, s-1,$$

i.e., each entry is an s-th root of unity.

Now let us explain the construction through embedding. Let $\mathbf{m} \in \{0,1\}^d$ be an incidence vector of Hamming weight s and an arbitrary vector $\mathbf{h} \in \mathbb{C}^s$. Then the "embedding of $\mathbf{h}$ into $\mathbb{C}^d$ controlled by $\mathbf{m}$", denoted by $\mathbf{h} \uparrow \mathbf{m}$, is the following vector in $\mathbb{C}^d$:

$$\mathbf{h} \uparrow \mathbf{m} = \sum_{r=1}^{s} \mathbf{h}[r] \left| j_r \right\rangle, \tag{2.5}$$

where $\mathbf{h}[r]$ is the r-th entry of $\mathbf{h}$, and $|j_r\rangle$ is the j_r-th standard basis of $\mathbb{C}^d$. Informally, $\mathbf{h} \uparrow \mathbf{m}$ is the first non-zero entry of $\mathbf{m}$ being replaced by the first entry of $\mathbf{h}$, the second non-zero entry of $\mathbf{m}$ replaced by the second entry of $\mathbf{h}$, and so on.

Example 2.4.2. $\mathbf{m} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \in \{0,1\}^9$, $\mathbf{h} = \begin{pmatrix} 1 \\ \omega \\ \omega^2 \end{pmatrix} \in \mathbb{C}^3$. *Therefore,* $\mathbf{h} \uparrow \mathbf{m} = \begin{pmatrix} 1 \\ 0 \\ \omega \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ \omega^2 \end{pmatrix} \in \mathbb{C}^9$.

The construction of MUBs using these combinatorial structures (as defined above) is summarized in the following theorem.

Theorem 2.4.1. *Let* $\{\mathbf{m}_{11}, \dots, \mathbf{m}_{1s}, \mathbf{m}_{21}, \dots, \mathbf{m}_{2s}, \dots, \mathbf{m}_{k1}, \dots, \mathbf{m}_{ks}\}$ *be a* $(k, s)-$*net and* $\mathbf{H}$ *an arbitrary generalized Hadamard matrix of order* s. *Then the* k *mutually orthogonal bases in* $\mathbb{C}^d$ *are*

$$\mathcal{B}_i = \left\{ \frac{1}{\sqrt{s}}(\mathbf{h}_l \uparrow \mathbf{m}_{ij}) | 1 \leq l \leq s; 1 \leq j \leq s \right\}, 1 \leq i \leq k.$$

The idea of constructing MUBs using the (k, s)-nets (described in terms of incidence vectors) provides an equivalence of the nets to MOLS as noted below.

Fact 2.4.1. *The existence of w-MOLS is equivalent to the existence of an (k, s)-net with $k = w + 2$.*

2.5 References to some Mathematical Tools

Various mathematical tools have been used to construct MUBs, among which noteworthy being the use of finite fields [99, 60] and maximal set of commuting bases [6]. For dimensions which are not power of primes, constructing large number of MUBs still remains elusive. This is the reason, various kinds of Approximate MUBs have been constructed using character sums over Galois Rings or Galois Fields [86, 61, 96, 23, 91, 71, 101].

When MUBs are constructed over $\mathbb{R}^d$, we get Real MUBs. They have interesting connections with Quadratic Forms [22], Association Schemes [70, 35], Equi-angular Lines, Equi-angular Tight Frames over $\mathbb{R}^d$ [14], Representation of Groups [44], Mutually Unbiased Real Hadamard Matrices, Bi-angular vectors over $\mathbb{R}^d$ [49, 59, 12] and Codes [20]. As we have noted out earlier, large number of Real MUBs are non-existent for most of the dimensions [18]. In fact only for $d = 4^s, s > 1$, we have $d/2 + 1$ many MUBs, whereas for most of the dimensions d, which are not perfect square, we have at best only 2 Real MUBs [18]. In view of this, attempts have been made to construct Approximate Real MUBs (ARMUBs) which are available in literature [101], other than our works in this thesis.

Various efforts have been made to explore connections between MUBs and geometrical objects such as polytopes and projective planes [7, 9, 84, 83, 3]. Since the known methods for the construction of MUBs provides complete sets only when d is some power of prime, there are conjectures related to the existence of complete sets of MUBs and finite projective plane, which are also currently known to exist only for prime power orders. If $d = p_1^{n_1} p_2^{n_2} \dots p_s^{n_s}$, then the lower bound on the number of MUBs is $p_r^{n_r} + 1$ where $p_r^{n_r} = \min\{p_1^{n_1}, p_2^{n_2}, \dots, p_s^{n_s}\}$. Thus, constructing a large number of MUBs for any composite dimension has proven to be elusive even over $\mathbb{C}^d$. In fact, the number of such bases is very small when we consider the problem over the real vector space $\mathbb{R}^d$ (see [18]).

2.6 Brief review of known constructions of Approximate MUBs

Various authors had shown existence and construction of set of orthonormal basis that does not exactly satisfy the criteria of MUB where $|\langle u|v\rangle| = \frac{1}{\sqrt{d}}$ when $|u\rangle$ and $|v\rangle$ are vectors from different basis. In order to relax this condition, Approximate MUBs have been defined differently in literature like $| \langle \psi_i^l | \psi_j^m \rangle | \leq \frac{1+o(1)}{\sqrt{d}}$, or $\frac{2+o(1)}{\sqrt{d}}$, or $\mathcal{O}\left(\frac{1}{\sqrt{d}}\right)$, or $\mathcal{O}\left(\frac{\log d}{\sqrt{d}}\right)$, or $\mathcal{O}\left(\frac{1}{\sqrt[4]{d}}\right)$ (for example see [61, 86]). Most authors considered $| \langle \psi_i^l | \psi_j^m \rangle | \leq \frac{1+o(1)}{\sqrt{d}}$ or $\mathcal{O}\left(\frac{1}{\sqrt{d}}\right)$ as the definition for AMUB. Hence to have uniformity and for ease of comparing the different approximations, we write $| \langle \psi_i^l | \psi_j^m \rangle | \leq \frac{\beta}{\sqrt{d}}$. Thus knowing the value of β, one can easily get its estimate of closeness to MUBs for the particular d. Further in this thesis we have introduced the notion of β-AMUB if $| \langle \psi_i^l | \psi_j^m \rangle | \leq \frac{\beta}{\sqrt{d}}$, where β is some small constant usually ≤ 2 which we define formally in next chapter. We subsequently demonstrate that our combinatorial method produces $\mathcal{O}(\sqrt{d})$ many β-AMUB for almost all composite d. The concept of β-AMUB also enable us to define and analyze concept of Almost Perfect AMUBs (APMUBs) in Chapter 5.

The first important work on AMUBs are by Klappenecker et al [61]. The authors constructed Approximate SIC-POVM using the complete set of MUBs. Since complete set of MUBs are known only for prime powers, for the non-prime powers they first constructed large set of Approximate MUBs, which then can be used to construct Approximate SIC-POVM. In this process they showed that [61, Theorem 11]] for all d, one can construct d many bases such that

$$| \langle \psi_i^l | \psi_j^m \rangle | = \mathcal{O}(d^{-\frac{1}{3}}) \Rightarrow \beta = \mathcal{O}(d^{\frac{1}{6}})$$

and can construct $d^t, t \geq 2$ many bases such that

$$| \langle \psi_i^l | \psi_j^m \rangle | = \mathcal{O}(d^{-\frac{1}{4}}) \Rightarrow \beta = \mathcal{O}(d^{\frac{1}{4}}),$$

where w$|\psi_i^l\rangle$ and $|\psi_j^m\rangle$ are basis vectors from different bases. Naturally β increases if the number of AMUBs increase. Finally in [61] this was improved for the dimensions of the form $d = p - 1$, where p is some prime. It was shown that there exists $d + 1$ bases such that

$$| \langle \psi_i^l | \psi_j^m \rangle | \leq \frac{1}{\sqrt{d}} + \mathcal{O}(d^{-1}) \text{ i.e., } \beta = 1 + \mathcal{O}(d^{-\frac{1}{2}}).$$

The results for all d have been improved in [86, Theorem 1], where a finite field based construction showed that for all d there are d many AMUBs such that

$$| \langle \psi_i^l | \psi_j^m \rangle | \leq \left(\frac{2}{\sqrt{\pi}} + \mathcal{O}\left(\log^{-1} d\right)\right) \left(\frac{\log d}{d}\right)^{\frac{1}{2}} \text{ i.e., } \beta = \mathcal{O}(\sqrt{\log d}).$$

This was further improved in the same paper using construction based on elliptic curves [86, Theorem 2] where the construction gave p^{t-1}, $t \geq 2$ where p is a prime such that $\sqrt{n} - 1 \leq \sqrt{p} \leq \sqrt{n} + 1$. The result shows

$$| \langle \psi_i^l | \psi_j^m \rangle | \leq \frac{2t + \mathcal{O}(d^{-\frac{1}{2}})}{\sqrt{d}} = \mathcal{O}(d^{-\frac{1}{2}}) \Rightarrow \beta = 2t + \mathcal{O}(d^{-\frac{1}{2}}).$$

These are the important results applicable for all dimensions [86] and we briefly recollect the construction which gives above two results. First the construction using finite field improves the bound on $|\langle\psi_i^l|\psi_j^m\rangle|$, from $\mathcal{O}(d^{-\frac{1}{3}})$ to $\mathcal{O}(d^{-\frac{1}{2}}\sqrt{\log d})$. This construction is motivated from the known construction of a set of $d+1$ MUBs in $\mathbb{C}^d$ for $d = p$, a power of prime, using Gaussian sums [60] for $p \geq 3$. This can be described as,

$$|\psi_k^h\rangle = \frac{1}{\sqrt{p}}\bigg(\mathbf{e}_p(hu^2 + ku)\bigg)_{u=1}^{p}; 1 \leq h, k \leq p,$$

where $\mathbf{e}_m(x) = e^{2\pi ix/m}$. Here $d = p$ a prime number and evaluating above expression for $u = 1$ to p, gives p components of $|\psi_k^h\rangle$ which is k^{th} basis vectors of h^{th} basis. The $\mathcal{B}_0$ being a standard orthonormal basis i.e., $\psi_j^0 = (\delta_{ju})_{u=1}^p$, is clearly mutually unbiased with each $|\psi_k^h\rangle$ above. Additive characters over an arbitrary finite field can be implemented to extend this construction to an arbitrary prime power $d = p^r$. However, this method cannot be applicable to composite d which is not power of some prime as we don't have finite filed corresponding to such a d. Hence the authors [86] consider the following modification shows $\beta = \mathcal{O}(\sqrt{\log d})$. For this let $h, k, d \in \mathbb{Z}^+$ and a prime $p \geq d$ and consider,

$$\mathcal{S}_{h,k}(p, d) = \sum_{u=1}^{d} \mathbf{e}_p(hu^2)\mathbf{e}_d(ku)$$

Lemma 2.6.1. *For $d \in \mathbb{Z}^+$ and a prime $p \geq d$ we have,*

$$\max_{0\leq k\leq d-1}\max_{1\leq h\leq p-1}|\mathcal{S}_{h,k}(p, d)| \leq \bigg(\frac{2}{\sqrt{\pi}} + \mathcal{O}(\frac{1}{\log p})\bigg)\sqrt{p\log p}$$

Let p be the smallest such prime $p \geq d$. By Prime Number Theorem there is a prime $p = \mathcal{O}(d)$. Now define the basis as follows,

$$\mathcal{B}_l = \{\mathbf{u}_1^l, \ldots, \mathbf{u}_d^l\}; \mathbf{u}_i^l = \frac{1}{\sqrt{d}}\bigg(\mathbf{e}_p(fu^2)\mathbf{e}_d(iu)\bigg)_{u=1}^{d}; 1 \leq f \leq d \tag{2.6}$$

The set of AMUBs obtained through this construction is presented in the theorem below in [86].

Theorem 2.6.1. *The standard basis $\mathcal{B}_0$ and the d bases $\mathcal{B}_f; 1 \leq f \leq d$ as given by 2.6 are orthonormal and also satisfy,*

$$|\langle u_i^l|u_j^m\rangle| \leq \bigg(\frac{2}{\sqrt{\pi}} + \mathcal{O}(\frac{1}{\log d})\bigg)\sqrt{\frac{\log d}{d}} \Rightarrow \beta = \mathcal{O}(\sqrt{\log d}),$$

where $0 \leq f \neq g \leq d$ and $1 \leq i, j \leq d$. This result is further improved using a new construction based on elliptic curves, in the same paper [86], where the bound is rendered as $\mathcal{O}(d^{-\frac{1}{2}})$. Following we reproduce important steps in it.

2.6.1 Construction based on Elliptic Curve

We refer to [89] and the references therein for technical details of elliptic curves. Consider a finite field $\mathbb{F}_p$ of prime order $p > 3$, and an elliptic curve $\mathcal{E}$ defined over $\mathbb{F}_p$ by the following affine Weierstrass equation,

$$Y^2 = X^3 + aX + b; a, b \in \mathbb{F}_p,$$

such that $4a^3 + 27b^2 \neq 0$. The cardinality $d = \#\mathcal{E}(\mathbb{F}_p)$ satisfies the Hasse-Weil inequality,

$$|d - p - 1| \leq 2\sqrt{p}$$

where $\mathcal{E}(\mathbb{F}_p)$ forms an Abelian group.

Each polynomial $f \in \mathbb{F}_p(\varepsilon)$ can be uniquely represented as $f(X, Y) = u(X) + v(x)Y$, where $u(X), v(X) \in \mathbb{F}_p(X)$ are polynomials as well. Note that, $\deg(f) = \max(2\deg(u), 3 + 2\deg(v))$ with the degree of zero polynomial being $-\infty$.

For $2 \leq t \leq d-1$, the set of polynomials of degree at most n with $f(0,0) = 0$, is denoted by $\mathcal{F}_t$. The following lemma and theorem presents the AMUBs with an improved bound on the inner product, obtained using elliptic curves.

Lemma 2.6.2. *The cardinality of $\mathcal{F}_t$ is $|\mathcal{F}_t| = p^{t-1}$.*

For $\mathcal{E}(\mathbb{F}_p)$ being an Abelian group, let χ denote the corresponding character group. Now for a polynomial $f \in \mathbb{F}_p[\varepsilon]$ define the set,

$$\mathcal{B}_f = \{\mathbf{v}_x^f : x \in \chi\} \tag{2.7}$$

where for each character $x \in \chi$, the vector $\mathbf{v}_x^f$ is given by,

$$\mathbf{v}_x^f = \frac{1}{\sqrt{d}} \bigg(\mathbf{e}_P(f(P)) x(P) \bigg)_{P \in \mathcal{E}} \tag{2.8}$$

where $f(\mathcal{O}) = 0$, $\mathcal{O}$ being the point at infinity for $\mathcal{O}(\mathbb{F}_p)$, termed as the neutral point.

Theorem 2.6.2. *For $2 \leq t \leq d-1$, the standard basis and the p^{t-1} sets, $\mathcal{B}_f = \{v_x^f : x \in \chi\}$ with $f \in \mathcal{F}_t$ are orthonormal and satisfy,*

$$|\langle \mathbf{v}_x^f | \mathbf{v}_\psi^g \rangle| \leq \frac{2t + (2t+1)d^{-\frac{1}{2}}}{\sqrt{d}} \Rightarrow \beta = 2t + \mathcal{O}(d^{-\frac{1}{2}})$$

where $f, g \in \mathcal{F}_n, f \neq g$ *and* $x, \psi \in \chi$.

Note that, for every prime $p > 3$, each integer d in the Hasse-Weil interval $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ is the cardinality of some elliptic curve over $\mathbb{F}_p$. Further, Cramér's conjecture ([33]) shows that the distance between the d^{th} and $(d+1)^{th}$ primes, i.e., p_d and p_{d+1} is,

$$p_{d+1} - p_d = \mathcal{O}((\log p_d)^2).$$

Under this conjecture, every $d \in \mathbb{Z}^+$ represents the cardinality of an elliptic curve defined over a finite field. However, finding such an elliptic curve poses a potential problem. Indeed the probability of an integer d not being in an interval of the Hasse-Weil type for some prime p is very small. Few important things to be noted in [86] are as follows.

1. The minimum possible value of t is 2, corresponding to which $\beta = 4 + \mathcal{O}(d^{-\frac{1}{2}})$, where one would obtain about n AMUBs. For $t > 2$ the β would be larger. Thus $\beta = 4 + \mathcal{O}(d^{-\frac{1}{2}})$ is minimum possible, which for large d approaches 4.

2. Since $\sqrt{n} - 1 \leq \sqrt{p} \leq \sqrt{n} + 1$, one can have $(n + 1 - 2\sqrt{n}) \leq p \leq (n + 1 + 2\sqrt{n})$. Thus for $t = 2$, the number of AMUBs would be equal to p which can be less than n, as the lower bound for p is $n - 2\sqrt{n} + 1$. Thus in order to obtain n many AMUBs, we may have to choose $t = 3$, which will give p^2 MUBS but will worsen the $\beta = 6 + \mathcal{O}(d^{-\frac{1}{2}})$.

3. Since all the components of each basis vectors consist of element on unit circle on complex plain, except the computational basis, the sparsity would be zero for all the AMUBs, except the computational basis.

4. This also implies that there is no possibility of obtaining real AMUBs using this construction as all the components of the basis vectors are product of Character of group elements and element on unit circle on the complex plain.

5. For constructing the AMUBs in $\mathbb{C}^d$, one has to find an elliptic curve $\mathcal{E}$ over finite filed $\mathbb{F}_p$, where p is a prime order $p > 3$, and the set of $\mathbb{F}_p$ rational points have cardinality d. For every prime $p > 3$, for every integer d in Hasse-Weil interval $[p+1-2\sqrt{p},\ p+1+2\sqrt{p}]$ there exists certain elliptic curve over $\mathbb{F}_p$ with cardinality d. However, there may not be computationally efficient methods to find such elliptic curve for a given d. Thus constructing such a large set of AMUBs using this construction method appears to be an expensive proposition.

6. Using unconditional result on the gap of primes, this method may not succeed to obtain a large set of AMUBs for n many dimensions $\leq d$, where $n = \mathcal{O}(d^{\frac{25}{36}+\epsilon})$. Here $\epsilon > 0$. However, assuming Cramér's conjecture [33] on the gap of primes, which says $p_{n+1} - p_n = \mathcal{O}(\log^2 p_n)$, the construction will provide a large set of AMUB for all d.

2.6.2 Other constructions of AMUBs for certain specific dimensions

In pursuit of better constructions of AMUBs, various authors have given other results, but they are not generic in nature, but rather for specific dimension. Some of them we summaries below. In the following, AMUBs are defined strictly when $\beta = 1 + \mathcal{O}(d^{-\frac{1}{2}})$.

In [71, Theorem 3.1], construction of AMUBs has been presented using Galois rings. The idea helps in constructing $q + 1$ many AMUBs for dimension $d = q(q - 1)$, where q is some power of prime where

$$|\langle \psi_i^l | \psi_j^m \rangle| \leq \frac{1}{q-1} \Rightarrow \beta = 1 + \mathcal{O}(d^{-\frac{1}{2}}).$$

The techniques include tensor products of MUBs and AMUBs. In fact, it has been shown in [71, Lemma 3.2] that tensor procdut of two AMUBs produces an AMUB in higher dimension.

In [23], AMUBs are constructed using orthogonality of character sum over Finite Fields for dimensions that are certain prime powers, i.e., $d = p^m$ over $\mathbb{C}^d$. Particularly when $p = 2$. It is to be noted that for such d there are well known constructions of compete set of MUBs itself. Hence they do not appear to be of any greater interest.

In [96], the authors provided construction for $d+1$ or $d+2$ many AMUBs over $\mathbb{C}^d$ when $d = q-1$ and q is a prime power. Thus it shows that one can obtain more than $d+1$ AMUBs with $\beta = 1 + \mathcal{O}(d^{-\frac{1}{2}})$, where as maximum only $d + 1$ many MUBs are possible for any d. The method employed mixed character sum of certain special functions over finite fields. In [96, Theorem 3.2], q many AMUBs could be constructed when $d = q - 1$, where

$$|\langle \psi_i^l | \psi_j^m \rangle| = \frac{1 + \sqrt{d}}{d} \text{ or } 0 \Rightarrow \beta = 1 + \mathcal{O}(d^{-\frac{1}{2}}).$$

Note that here that the there is equality in above relationship for value of $|\langle \psi_i^l | \psi_j^m \rangle|$ when the vectors are from different bases. Since $\Delta = \{0, \frac{1+\sqrt{d}}{d}\}$ is just two valued, that satisfies the condition of APMUB that we explain in detail in Chapter 5. The authors further showed [96, Theorem 3.5] that $q + 1$ AMUBs exist when $d = q - 1$ where

$$|\langle \psi_i^l | \psi_j^m \rangle| = \frac{\sqrt{d+1}}{d} \text{ or } \frac{1}{d} \Rightarrow \beta = 1 + \mathcal{O}(d^{-\frac{1}{2}}).$$

Again note that, there is equality in the above relationship for the value of $|\langle\psi_i^l|\psi_j^m\rangle|$ when vectors are from different bases. However, here $\Delta = \{0, \frac{1}{d}, \frac{\sqrt{d+1}}{d}\}$ is three valued and this is not APMUB, although the AMUBs are of very good quality.

In [91], the authors have shown the construction of AMUBs using Gauss sum over Frobenius Rings. In [91, Lemma 3.2], for any positive integer, one can construct p many AMUBs over $\mathbb{C}^{\phi(n)}$ where p is the smallest prime divisors of n and $\phi(n)$ is the Euler function. Here

$$|\langle\psi_i^l|\psi_j^m\rangle| \le \frac{1}{\sqrt{d}}\left(+\frac{n-d}{\sqrt{d}(\sqrt{n}+\sqrt{d})}\right) \Rightarrow \beta = 1 + \mathcal{O}(d^{-\frac{1}{2}}).$$

The asymptotic form of β is derived assuming $\phi(n) \approx \mathcal{O}(n)$. Note that number of MUBs is equal to the smallest prime divisor of n, which is restrictive and would be small even for $d = p^m$, for $m \ge 2$, as in such cases complete MUBs are known.

2.7 Conclusion

Towards concluding this background section, let us present certain salient features of all the above constructions.

1. All of the methods are based on the some kind of mix of exponential sum and characters of Abelian groups.
2. All the construction produces Complex AMUBs, i.e., the basis vectors are over $\mathbb{C}^d$.
3. The sparsity of all the basis constructed is zero, except the computational basis.
4. Though there are several combinatorial constructions of MUBs, but the corresponding techniques are not exploited for the AMUBs.
5. All the construction focus on the bounds of $|\langle\psi_i^l|\psi_j^m\rangle|$, which is characterized with β, but the idea of two-valued spectra as we present in Chapter 5 has not been explored.
6. Most of the constructions produce good quality AMUBs, only for certain specific forms of dimensions like $d = p-1, q+1, q$ etc., except for certain generalization in [86]. This we extend to a great extent in this thesis.

Generally, for $d = q-1$, where q is some power of prime, there are d or $d+1$ AMUBs [61, 96] where $\beta = 1+\mathcal{O}(d^{-\lambda})$ for $\lambda > 0$. The other known cases, when β is of this form, for $d = q(q-1)$, the number of AMUBs are $\mathcal{O}(\sqrt{d})$ and for $d = \phi(n)$ the number of AMUBs is equal to the smallest prime divisor of n, which is always less than $\sqrt{n}$ when n is not prime number [91]. Towards improving these results, in subsequent chapters we show that for all composite $d = k \times s$, when $|s - k| < d^{\frac{1}{2}}$, one can construct more that $\sqrt{d}$ many AMUBs with $\beta = 1 + \mathcal{O}(d^{-\lambda})$ for $\lambda > 0$. Thus, effectively we are able to construct such AMUBs for a very large set of dimensions d, and can also construct the real ones (ARMUBs) for such d's whenever real Hadamard matrices of order k or of order s are available. Further all these AMUBs constructed using RBDs are very sparse, i.e., basis vectors have very few non-zero components.

Chapter 3

On Approximate Real MUBs in Square Dimensions

As we have discussed, construction of Mutually Unbiased Bases (MUBs) is a very challenging combinatorial problem in quantum information theory with several long standing open questions in this domain. With certain relaxations, the object Approximate Mutually Unbiased Bases (AMUBs) has been defined in this context. In this chapter we provide a method to construct up to $(\sqrt{d}+1)$ many AMUBs in dimension $d = q^2$, where q is a positive integer. Our result is particularly important when $q \equiv 0 \bmod 4$, as we obtain Approximate Real MUBs (ARMUBs) assuming the cases where a Hadamard matrix of order q exists. In this construction, we also characterize the inner product values between the elements of two different bases. In particular, when d is of the form $(4x)^2$ where x is a prime, we obtain $(\frac{\sqrt{d}}{4} + 1)$ many ARMUBs such that for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| \leq \frac{4}{\sqrt{d}}$.

3.1 Introduction

Let us refer to Definition 1.1.1 in Chapter 1 first for a quick recapitulation of MUBs. For a dimension d, it is well known that there can be at most $(d+1)$ MUBs [39]. This bound can be achieved when d is a prime power. However, the result is not settled for the other cases. Given any d and its prime factorization $d = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, there exists a construction method to obtain $\nu_d = \left(min_{i\in[1,\dots,r]} p_i^{k_i}\right) + 1$ MUBs. Thus, this is a lower bound. For example, when $d = 2^4 x^2$, for some large prime x, then the lower bound will be $2^4 + 1 = 17$ only.

When d is not a prime power, the maximum possible number of MUBs are not known, although there has been progress in obtaining more than ν_d MUBs for certain special values of d. In [98], it was shown that $k = w + 2$ mutually unbiased bases can be constructed in any square dimension $d = q^2$ provided that there are w Mutually Orthogonal Latin Squares (MOLS) of order q. The asymptotic result of [98] states that one can obtain at least $q^{\frac{1}{14.8}}$ MUBs in dimension $d = q^2$, for all q but with finitely many exceptions. For example, the construction gives at least 8 MUBs for dimensions $d = q^2$ when $q = 76$, and higher values are not known due to difficulty in obtaining larger sets of MOLS.

Because of the difficulties in increasing the number of MUBs and proving upper bounds, there is a motivation to work on the the concept of Approximate Mutually Unbiased Bases, where the inner product of two vectors drawn from two different bases is upper bounded by some value. In this direction the works of [61, 86] are very important, the latest of which provided the following construction [86, Theorem 2].

Fact 3.1.1. *For any d, there are p^{y-1} orthonormal bases for any positive integer y indexed as B_i, where p is a prime satisfying $\sqrt{d} - 1 \leq \sqrt{p} \leq \sqrt{d} + 1$, such that for any two vectors $v_1 \in B_{i_1}$ and $v_2 \in B_{i_2}$ $(i_1 \neq i_2)$, one can obtain $|\langle v_1 | v_2 \rangle| \leq \frac{2y + \frac{2y+1}{\sqrt{d}}}{\sqrt{d}}$.*

This result provides an important construction of Approximate Mutually Unbiased Bases. However, it should be noted that the vectors in the bases due to this construction are inherently complex in nature. Thus it is interesting to explore some novel construction method when one considers only the real components. This is what we propose in this chapter (our work of [67]), and present a combinatorial construction to obtain $(\sqrt{d}+1)$ Approximate Real Mutually Unbiased Bases (ARMUBs) when $d = (4r)^2$. In [98], on assuming assume the widely accepted conjecture that for any integer $n \equiv 0 \bmod 4$ there exists an $n \times n$ real Hadamard matrix. The maximum number of Real MUBs known for this form of d is $\approx d^{\frac{1}{29.6}}$ [98] for sufficiently large values of d.

Let us now define ARMUBs formally.

Definition 3.1.1. *A set of k orthonormal bases $B_i, 0 \leq i \leq k-1$ of $\mathbb{R}^d$ are called β-ARMUBs if for two vectors $v_1 \in B_{i_1}$ and $v_2 \in B_{i_2}$ $(i_1 \neq i_2)$, $|\langle v_1 | v_2 \rangle| \leq \frac{\beta}{\sqrt{d}}$.*

In this direction we use elementary combinatorial and number-theoretic techniques to describe the construction method of obtaining a total of $\gamma + 2$ many $\Delta(q, \gamma)$-ARMUBs for any $d = q^2$ with $q \equiv 0 \bmod 4$. Let us now define $\Delta(q, \gamma)$.

Definition 3.1.2. *Let $\mathbb{Z}_q$ be the addition modulo q group consisting of the elements $\{0, 1, \ldots, q-1\}$ and $i\mathbb{Z}_q$ be the subgroup of $\mathbb{Z}_q$ generated by the element $i \in \mathbb{Z}_q$. Let $\gamma \leq q - 1$ where γ is a positive integer. Then we denote*

$$\Delta(q, \gamma) = \max_{1 \leq i \leq \gamma} \frac{|\mathbb{Z}_q|}{|i\mathbb{Z}_q|}.$$

Here $|S|$ denotes the cardinality of a set S .

In fact our construction forms a discrete spectrum with respect to the inner product of vectors from different bases, where the inner product values are all integer multiples of $\frac{1}{\sqrt{d}}$.

Thus, one may note that if $d = q^2 = (4x)^2$, where x is a large prime, then the generic lower bound will provide only $2^4 + 1 = 17$ MUBs, and the bound due to [98] will provide around $(4x)^{\frac{1}{14.8}}$ MUBs. The results of [61, 86] will provide p^{y-1} AMUBs where $\sqrt{p} \in [\sqrt{d}-1, \sqrt{d}+1]$ with the upper bound on the magnitude of inner products between vectors from different bases being at most $\frac{2y+\frac{2y+1}{\sqrt{d}}}{\sqrt{d}}$. For $y = 3$, one can obtain more than d AMUBs with maximum inner product between two vectors from two bases having at most $\frac{6+\frac{7}{\sqrt{d}}}{\sqrt{d}}$ magnitude. However these AMUBs are inherently complex.

In this context, if we set $\gamma = x - 1$ then we have $\Delta(q, x-1) = 4$ and thus we get $(\frac{\sqrt{d}}{4}+1)$ many bases where the inner product value will at most be $\frac{4}{\sqrt{d}}$. That is, the magnitude of the inner product values will be $\frac{i}{\sqrt{d}}$, $i \in \{0, 1, 2, 3, 4\}$.

Let us explain the development in terms of real MUBs a little more. In the latest version of the paper [18], towards a construction of real MUBs for $d = 4^i s^2$, only the work of [98] has been referred. The result is as follows:

> *"If $d = 4^i s^2$, where s is any positive integer, then the number of MUBs is $\geq MOLS(2^i s)+2$, provided that there exists a Hadamard matrix of order $2^i s$, where $MOLS(m)$ denotes the maximum number of MOLS of order m."*

As it is pointed out in [98], the construction gives at least 8 MUBs for dimensions $d = q^2$ when $q \geq 76$.

In our case, we depend on the famous conjecture on construction of real Hadamard matrices. It is stated in [21]:

> *"The Hadamard conjecture asserts that a Hadamard matrix exists of every order divisible by 4. The smallest multiple of 4 for which no such matrix is currently known is 668, the value 428 having been settled only in 2005 [58]."*

These are the real Hadamard matrices and hence according to our construction, we will have $(\frac{\sqrt{d}}{4}+1)$ Real Approximate MUBs. For $q = 76$, our result provides 20 ARMUBs. As the value of x increases, the number of 4-ARMUBs increases polynomially (at most 14-th power) compared to the results in [98].

3.2 Our Construction

Let us first describe the construction method. Then we will prove the related properties in Lemma 3.2.1 and Theorem 3.2.1. We also present certain examples to explain this construction.

Construction 3.2.1.

1. *First we choose an arbitrary orthonormal basis of* $\mathbb{R}^d$ *to begin with. For simplicity, let us consider the computational basis states* $I_d = \{|0\rangle, |1\rangle, \ldots, |d-1\rangle\}$. *Here* $|i\rangle$ *is a vector from the standard basis of unit vectors of* $\mathbb{R}^d$ *where the vector* $|i\rangle = \big[0, \ldots, 1, 0, \ldots, 0\big]$ *has the value* 1 *in the* i*-th position (we start with the zero-th one) and* 0 *in all other positions.*

2. *Next we form* $(\gamma + 2)$ *sets* $S_0, \ldots, S_\gamma, S_q$, $1 \leq \gamma \leq q-1$ *defined as follows.*

   (a) *Each set* S_i *is a partition of* I_d *into* q *subsets* $S_{i,j}$, $j \in \{0, 1, \ldots, q-1\}$, *each containing* q *vectors.*

   (b) *For any two subsets* S_{i_1,j_1} *and* S_{i_2,j_2}, $i_1 \neq i_2$, *the number of common vectors is upper bounded by* $\Delta(q, \gamma)$.

   These sets can be defined in many ways. Here we show one method of construction.

$$S_{i,j} = \left\{ s_t^{i,j} = |qt + (it + j) \bmod q\rangle_{t \in \{0,1,\ldots,q-1\}} \right\}, 0 \leq i \leq \gamma,\ 0 \leq j \leq q-1 \tag{3.1}$$

$$S_{q,j} = \left\{ |qj + t\rangle_{0 \leq t \leq q-1} \right\} \tag{3.2}$$

   Here note that S_q *is defined differently from* $S_i, i < q$. *Moreover the construction for the sets* $S_i, i < q$ *cannot be extended beyond* $q - 1$ *as that would lead to repetition because* $((q + l)t + j) \bmod q = (lt + j) \bmod q$.

3. *Next we choose a* $q \times q$ *matrix* H, *expressed as* $H[i, j]$, $0 \leq i, j \leq q-1$, *with the following properties*

   (a) *The magnitude of all entries of the matrix is* $\frac{1}{\sqrt{q}}$.

   (b) *For any two rows* i_1 *and* i_2 *with* $i_1 \neq i_2$, *we have* $\sum_{t=0}^{q-1}(H[i_1, t] \cdot H[i_2, t]) = 0$.

   One should note here that any normalized Hadamard matrix satisfies these properties. The first property of the matrix H *is needed to maintain that the inner product of two vectors from the formed bases are a multiple of* $\frac{1}{\sqrt{d}}$.

4. *Finally, we form a basis* B_i *corresponding to each set* S_i *in the following manner.*

- *Corresponding to each set $S_{i,j} = \{s_t^{i,j}\}_{0 \leq t \leq q-1}$ we form $B_{i,j} = \{b_t^{i,j}\}_{0 \leq t \leq q-1}$ consisting of q pairwise orthogonal vectors as*

$$b_t^{i,j} = \sum_{u=0}^{q-1} H[t,u] s_u^{i,j}.$$

Finally we define $B_i = \{B_{i,j}\}_{0 \leq j \leq q-1}$. The second property of H is needed to ensure that the vectors of $B_{i,j}$, which are all different combinations of the elements of $S_{i,j}$ are all pairwise orthogonal in nature. This is essential in making B_i an orthonormal basis of $\mathbb{R}^d$. The proofs are explained in Theorem 3.2.1.

- *The resultant bases B_i thus consist of the vectors $\{b_t^{i,j}\}_{0 \leq j,t \leq q-1}$.*

Let us first formally analyze the sets $S_i, 0 \leq i \leq \gamma$ and S_q.

Lemma 3.2.1. *The set $S_i = \{S_{i,0}, \ldots, S_{i,d-1}\}$ is a disjoint partition of $I_d = |k\rangle_{k=0}^{d-1}$ with every set $S_{i,j}$ containing $q = \sqrt{d}$ elements. Furthermore, for any two sets S_{i_1,j_1} and S_{i_2,j_2} with $i_1 \neq i_2$ there are at most $\Delta(q,\gamma)$ elements in $S_{i_1,j_1} \cap S_{i_2,j_2}$.*

Proof. We first show that S_i is indeed a partition of I_d. In this regard, refer to item 1 of Construction 3.2.1. Consider two non-negative integers $a \neq b$. For the two vectors, $|a\rangle, |b\rangle$, we have $\langle a|b\rangle = 0 \; \forall a \neq b$. Therefore, it is sufficient to show that the d vectors of S_i are different elements of I_d. This is trivially true for S_d. For any $i \in \{0, \ldots, \gamma\}$, let us consider two different vectors $s_{t_1}^{i,j_1} = s_{t_2}^{i,j_2}$. That is $(j_1, t_1) \neq (j_2, t_2)$. Then

$$qt_1 + (it_1 + j_1) \bmod q = qt_2 + (it_2 + j_2) \bmod q.$$

This can only be true if $t_1 = t_2 = t$ (say). Then we have

$$\begin{gathered} qt + (it + j_1) \bmod q = qt + (it + j_2) \bmod q \\ \implies qt + it + j_1 = qt + it + j_2 + qz \implies j_1 = j_2 + qz \end{gathered}$$

This can only happen if $z = 0$ and thus $j_1 = j_2$, which is a contradiction.

Now let us observe the situation when $i_1 \neq i_2$. Then the number of common elements in two vectors $s_{t_1}^{i_1,j_1}$ and $s_{t_2}^{i_2,j_2}$ is equal to the number of pairs (t_1, t_2) for which we have

$$qt_1 + (i_1t_1 + j_1) \bmod q = qt_2 + (i_2t_2 + j_2) \bmod q. \tag{3.3}$$

Again for all such solutions we will have $t_1 = t_2 = t$ (say). Let us assume without loss of generality that $i_1 > i_2$. Then the solution to Equation (3.3) is same as the solution to

$$\begin{aligned} & qt + (i_1t + j_1) \bmod q = qt + (i_2t + j_2) \bmod q \\ \implies & (i_1 - i_2)t \equiv (j_2 - j_1) \bmod q \\ \implies & \alpha t \equiv \beta \bmod q, 0 \leq t \leq q-1 \end{aligned}$$

The values $(\alpha t) \bmod q$ form the subgroup $\alpha\mathbb{Z}_q$ generated by α of $\mathbb{Z}_q$. Then if $\beta \in \alpha\mathbb{Z}_q$ then the number of values of t for which this equation is satisfied is same as $\frac{|\mathbb{Z}_q|}{|\alpha\mathbb{Z}_q|}$. Now if we have $i \leq \gamma$ then so is $i_1 - i_2$.

For the pairs S_{q,j_1} and S_{i,j_2}, $i \neq q$ the situation is simpler. In S_{q,j_1} the elements are $|qj + t\rangle, 0 \leq t \leq q-1$. By definition in S_{i,j_2} there is only one element in the range $|qj\rangle$ to $|qj + q - 1\rangle$. This completes the proof. □

Let us now consider an example with $d = (12)^2$. If we form γ $(3 \leq \gamma \leq 5)$ bases then $\Delta(12, \gamma) = 4$. However, if we consider $6 \leq \gamma \leq 11$, then $\Delta(12, \gamma) = 6$.

Suppose we take $\gamma = 5$ and consider the sets $S_{0,1}$ and $S_{5,1}$. Then the number of duplicates is equivalent to the number of solutions for $5t \equiv 0 \bmod 12$, which is satisfied for only $t = 0$. Indeed the two sets are

(i) $S_{0,1} = \{|1\rangle, |13\rangle, |25\rangle, |37\rangle, |49\rangle, |61\rangle, |73\rangle, |85\rangle, |97\rangle, |109\rangle, |121\rangle, |133\rangle\}$,

(ii) $S_{5,1} = \{|1\rangle, |18\rangle, |35\rangle, |40\rangle, |57\rangle, |62\rangle, |79\rangle, |84\rangle, |101\rangle, |118\rangle, |123\rangle, |140\rangle\}$,

and the only element common is $|1\rangle$.

On the other hand if we look at $S_{0,2}$ and $S_{4,2}$ then the number of common elements increase, as the the equation $4t \equiv 0 \bmod 12$ has four solutions, $0, 3, 6$ and 9. The elements of the sets are

(i) $S_{0,2} = \{|2\rangle, |14\rangle, |26\rangle, |38\rangle, |50\rangle, |62\rangle, |74\rangle, |86\rangle, |98\rangle, |110\rangle, |122\rangle, |134\rangle\}$,

(ii) $S_{4,2} = \{|2\rangle, |18\rangle, |34\rangle, |38\rangle, |54\rangle, |70\rangle, |74\rangle, |90\rangle, |106\rangle, |110\rangle, |126\rangle, |142\rangle\}$.

In this case the common elements are $|2\rangle, |38\rangle, |74\rangle$ and $|110\rangle$.

Having described the properties of the set S_i, we now complete the construction of the $\Delta(q, \gamma)$-ARMUBs.

Theorem 3.2.1. *Consider that $d = q^2$, where $q \equiv 0 \bmod 4$ and a $q \times q$ Hadamard Matrix exists. Further, consider the $(\gamma + 2)$ orthonormal bases $B_i = \{b_t^{i,j}\}_{0 \leq j,t < q}$, as described in Construction 3.2.1. Then they form $\Delta(q, \gamma)$-ARMUBs, i.e., for any two vectors $b_{t_1}^{i_1,j_1}$ and $b_{t_2}^{i_2,j_2}$ belonging to two different bases $(i_1 \neq i_2)$ we have*

$$|\langle b_{t_1}^{i_1,j_1} | b_{t_2}^{i_2,j_2} \rangle| \in \left\{ \frac{i}{\sqrt{d}} : i = 0, 1, \ldots, \Delta(q, \gamma) \right\}.$$

Proof. Let us first show that each of the set of vectors B_i are all indeed orthonormal bases. The vectors of a basis B_i are designed in the following way. The sets $\{S_{i,j}\}_{0 \leq j \leq q-1}$ contain q

vectors from I_d each. Each set $S_{i,j}$ is converted to $B_{i,j}$ where each vector in $B_{i,j}$ is a different combination of the vectors in $S_{i,j}$, formed using the Hadamard matrix as

$$b_t^{i,j} = \sum_{u=0}^{q-1} H[t,u] s_u^{i,j},$$

and $B_i = \{B_{i,j}\}_{0 \le j \le q-1}$. Now since $S_{i,j_1} \cap S_{i,j_2} = \{\phi\}$ for all $j_1 \neq j_2$ there is no common vector from I_d between any two vectors of B_i, $b_{t_1}^{i,j_1}$ and $b_{t_2}^{i,j_2}$ with $j_1 \neq j_2$ and thus $\langle b_{t_1}^{i,j_1} | b_{t_2}^{i,j_2} \rangle = 0$.

Now let us consider two vectors from the same set $B_{i,j}$, $b_{t_1}^{i,j}$ and $b_{t_2}^{i,j}$. Then we have

$$\begin{aligned}
\langle b_{t_1}^{i,j} | b_{t_2}^{i,j} \rangle &= \left\langle \sum_{u=0}^{q-1} H[t_1,u] s_u^{i,j} \middle| \sum_{u=0}^{q-1} H[t_2,u] s_u^{i,j} \right\rangle \\
&= \sum_{u_1=0}^{q-1} \sum_{u_2=0}^{q-1} H[t_1,u_1] H[t_2,u_2] \langle s_{u_1}^{i,j} | s_{u_2}^{i,j} \rangle \\
&= \sum_{u=0}^{q-1} H[t_1,u] H[t_2,u] \langle s_{u_1}^{i,j} | s_{u_2}^{i,j} \rangle \ [\text{as } \langle s_{u_1}^{i,j} | s_{u_2}^{i,j} \rangle = 0 \ \forall \ u_1 \neq u_2] \\
&= \sum_{u=0}^{q-1} H[t_1,u] H[t_2,u]
\end{aligned}$$

Now we know from the property of Hadamard matrices that the sum of position-wise product of any two rows is zero. Which implies $\langle b_{t_1}^{i,j} | b_{t_2}^{i,j} \rangle = 0$. This implies the d vectors in B_i are all orthogonal to each other and thus $B_i, 0 \le i \le q$ are all orthonormal bases.

Let us now consider the dot product between any two vectors taken from different Bases B_{i_1} and B_{i_2}. When $i_1 \neq i_2$ we have

$$\begin{aligned}
\langle b_{t_1}^{i_1,j_1} | b_{t_2}^{i_2,j_2} \rangle &= \left\langle \sum_{u=0}^{q-1} H[t_1,u] s_u^{i_1,j_1} \middle| \sum_{u=0}^{q-1} H[t_2,u] s_u^{i_2,j_2} \right\rangle \\
&= \sum_{u=0}^{q-1} \sum_{j=0}^{q-1} \langle H[t_1,u] s_u^{i_1,j_1} | H[t_2,u] s_v^{i_2,j_2} \rangle \\
\implies |\langle b_{t_1}^{i_1,j_1} | b_{t_2}^{i_2,j_2} \rangle| &\le \sum_{u=0}^{q-1} \sum_{j=0}^{q-1} \left\langle \frac{s_u^{i_1,j_1}}{\sqrt{q}} \middle| \frac{s_v^{i_2,j_2}}{\sqrt{q}} \right\rangle \le \frac{|S_{i_1,j_1} \cap S_{i_2,j_2}|}{q} \\
&= \frac{\Delta(q,\gamma)}{\sqrt{d}} (\text{from Lemma 3.2.1}).
\end{aligned}$$

As all the values $\langle H[t_1,u] s_u^{i_1,j_1} | H[t_2,u] s_v^{i_2,j_2} \rangle$ are integer multiple of $\frac{1}{\sqrt{d}}$, it implies that $\langle b_{t_1}^{i_1,j_1} | b_{t_2}^{i_2,j_2} \rangle$ is an integer multiple of $\frac{1}{\sqrt{d}}$. This completes the proof. □

Remark 3.2.1.

1. *Once we have a set $S_{i,j}$ we denote its element as $s_t^{i,j}, 0 \leq t \leq q-1$ before applying the Hadamard matrices to form the bases. Note that $S_{i,j}$ is in fact an unordered set and $s_t^{i,j}$ is an ordering of the elements. As it can be observed from Theorem 3.2.1, the particular ordering does not affect the upper bound on the magnitude of the dot products across bases, however as we shall see with an example the exact spectrum is indeed dependent on this ordering.*

2. *For any $d = q^2$, corresponding to any two different sets S_{i_1,j_2} and S_{i_2,j_2} one can use two different $q \times q$ Hadamard Matrices as it does not affect any of the constraints. However, it will affect the spectrum and it is an interesting problem to observe how much the spectrum can be smoothened with the choice of these matrices.*

Finally we show two examples of the final dot product values, assuming that only a single Hadamard matrix is being used for all transformations. Let us again look into the cases of $S_{0,1}, S_{5,1}$ and $S_{0,2}, S_{4,2}$. We first need a 12×12 Hadamard Matrix to construct the vectors of $B_{0,1}, B_{5,1}, B_{0,2}$ and $B_{4,2}$. Let the Hadamard Matrix be H^{12} described below:

$$H^{12} = \frac{1}{\sqrt{12}} \begin{pmatrix}
1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\
1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 \\
1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 \\
1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 \\
1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\
1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\
1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \\
1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\
1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 & -1 \\
1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 & 1 \\
1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1 & -1 \\
1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 & 1 & -1 & 1 & 1
\end{pmatrix}$$

Let us first consider the vectors $v_{t_1} = b_{t_1}^{0,1}$ and $v_{t_2} = b_{t_2}^{5,1}$. Then we have $v_{t_1} = \sum H^{12}[t_1, u] s_u^{0,1}$ and $v_{t_2} = \sum H^{12}[t_2, u] s_u^{5,1}$. Now when we consider $\langle v_{t_1} | v_{t_2} \rangle$ only the basis state $|1\rangle$ is common between the two vectors, and thus the inner product is always $H^{12}[t_1, 0] H^{12}[t_2, 0] = \pm \frac{1}{12}$.

However, since there are multiple common elements between $S_{0,2}$ and $S_{4,2}$ the final dot product of two vectors $b_{t_1}^{0,2}$ and $b_{t_2}^{4,2}$ is dependent on the choice of the Hadamard matrix and the ordering of the elements in the set.

For example, we have,

(i) $b_1^{0,2} = \frac{1}{\sqrt{12}}(|2\rangle + |14\rangle - |26\rangle + |38\rangle - |50\rangle - |62\rangle - |74\rangle + |86\rangle + |98\rangle + |110\rangle - |122\rangle + |134\rangle)$,

(ii) $b_2^{4,2} = \frac{1}{\sqrt{12}}(|2\rangle + |18\rangle + |34\rangle - |38\rangle + |54\rangle - |70\rangle - |74\rangle - |90\rangle + |106\rangle + |110\rangle + |126\rangle + |142\rangle)$.

Now note that although there are 4 basis states are common between the two vectors we have $\langle b_1^{0,2} | b_2^{4,2} \rangle = \frac{2}{12}$. In fact we swap the vectors $|74\rangle$ and $|84\rangle$ in $b_t^{0,2}$ then we will in fact have $\langle b_1^{0,2} | b_2^{4,2} \rangle = 0$. Therefore understanding how to best permute the subsets $S_{i,j}$ before applying the Hadamard matrices and the choice of the particular Hadamard matrix should have significant impact on the different dot product values that constitute the spectrum.

This construction gives particularly close results when $d = (4x)^2$ where x is a prime number in which case $\Delta(q, \frac{q}{4} - 1) = 4$. We note this as the following corollary.

Corollary 3.2.1. *Given $d = q^2$ such that $q = 4x$ where x is a prime then there are $(\frac{\sqrt{d}}{4} + 1)$ orthonormal real bases (assuming existence of a real Hadamard matrix of size $4x \times 4x$) $B_i = \{b_t^{i,j}\}_{0 \leq j,t < q}$, such that for any two vectors $b_{t_1}^{i_1,j_1}$ and $b_{t_2}^{i_2,j_2}$ taken from two different bases we have*

$$|\langle b_{t_1}^{i_1,j_1} | b_{t_2}^{i_2,j_2} \rangle| \in \left\{ \frac{i}{\sqrt{d}} : i = 0, 1, \ldots, 4 \right\}.$$

Proof. In this case the non trivial factors of q are $2, 4, x, 2x$. If we choose $0 \leq i \leq x-1, i = q$ for the sets S_i, then $\alpha = |i_1 - i_2| \in \{0, 1, \ldots x-1\}$ and therefore $\Delta(q, \gamma) \leq 4$. This combined with Theorem 3.2.1 gives us the result. □

Here one should also note that for many values of q we are aware of constructions for $q \times q$ Hadamard matrices, namely the Paley construction [13], which makes our results not dependent on the Hadamard conjecture for infinitely many values of q, which we note down in the following corollary.

Corollary 3.2.2. *If $d = q^2$, where $q = (p+1)2^k, k \geq 1$ where $q \equiv 0 \bmod 4$ and p is a prime, then we have $\gamma + 2$ many $\Delta(q, \gamma)$-ARMUBs defined on $\mathbb{R}^d$ for all such values of d.*

The result of Corollary 3.2.1 and Corollary 3.2.2 can be further combined to state the following result.

Corollary 3.2.3. *If p is a prime such that $\frac{p+1}{2}$ is also a prime, then there exists $(\frac{\sqrt{d}}{4} + 1)$ 4-ARMUBs in $\mathbb{R}^d$ where $d = (2(p+1))^2$.*

Proof. If $\hat{p} = \frac{p+1}{2}$ is a prime then q is in fact of the form $4r$ and there exists a $q \times q$ Hadamard matrix due to Paley construction [13]. This combined with Corollary 3.2.2 forms the result. □

Whether infinitely many such pairs $(p, \frac{p+1}{2})$ exist is not known. The case of $(p, \frac{p-1}{2})$, p is known as the Sophie Germain primes, and this is also an open problem. One can refer to [95] for more information in this area.

3.3 Conclusion

In this chapter we described a simple construction method for designing a set of $(\gamma+2)$ many $\Delta(q,\gamma)$-Approximate Real Mutually Unbiased Bases in $\mathbb{R}^d$, where $d = q^2$ and $q \equiv 0 \bmod 4$. Here, $\Delta(q,\gamma)$ denotes the maximum index among the subgroups generated by elements less than γ in the addition modulo q group. The number of bases that we obtain is more than 14-th power of the best known results for MUBs [98], although we achieve that at the cost of $\Delta(q,\gamma)$-approximation. We also characterize the exact spectrum of the dot product values between different vectors taken from different bases. As a special case, when $d = (4x)^2$, where x is a prime, we obtain $(\frac{\sqrt{d}}{4}+1)$ orthonormal bases where for any two vectors v_1 and v_2 taken from different bases we have $|\langle v_1|v_2\rangle| \in \left\{\frac{i}{\sqrt{d}} : i = 0, 1, \ldots, 4\right\}$. When both x and $2x-1$ are primes, we use Paley construction to obtain $4x \times 4x$ Hadamard matrix and complete the construction of 4-ARMUBs. The impact of the ordering of the sets $S_{i,j}$ described in our construction and choices of the Hadamard matrices on this spectrum remains a very interesting combinatorial problem and needs further investigation. In the next chapter, we will present further results in this direction using more involved combinatorial objects like Resolvable Block Designs in conjunction with Hadamard matrices.

Chapter 4

Resolvable Block Designs in Construction of Approximate Real MUBs that are Sparse

As we have discussed so far, several constructions of Mutually Unbiased Bases (MUBs) borrow tools from combinatorial objects. In this contributory chapter, we focus on how one can construct Approximate Real MUBs (ARMUBs) with improved parameters, using the results from the domain of Resolvable Block Designs (RBDs). We first explain the generic idea of our strategy in relating the RBDs with MUBs/ARMUBs, which are sparse (the basis vectors have small number of non-zero co-ordinates). Then specific parameters are presented, for which we can obtain new classes and improve the existing results. To be specific, we present an infinite family of $\lceil\sqrt{d}\rceil$ many ARMUBs for dimension $d = q(q+1)$, where $q \equiv 3 \bmod 4$ and it is a prime power, such that for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| < \frac{2}{\sqrt{d}}$. We also demonstrate certain cases, such as $d = sq^2$, where q is a prime power and $sq \equiv 0 \bmod 4$. These findings subsume and improve some of our results from the previous chapter. This present construction idea provides several infinite families of such objects, not known earlier in the literature, which can find efficient applications in quantum information processing for the sparsity, apart from suggesting that parallel classes of RBDs are intimately linked with MUBs/ARMUBs.

4.1 Introduction

Inspired by the fact that known methods to construct MUBs provide complete set only when dimension is certain power of a prime, there are strong conjectures relating existence of the complete set of MUBs and objects from combinatorial design. Though it is to be noted that the MUBs are constructed on Hilbert spaces which are continuum, whereas structures of combinatorial design like affine planes are built on finite number of points and lines for any order. Hence, the conjectures connecting existence of complete set of MUBs and certain combinatorial designs are intriguing. For example, one can refer to the conjecture [84] that states "non existence of a projective plane of the given order d implies that there are less than $d + 1$ MUBs in $\mathbb{C}^d$."

Zauner studied quantum designs [102], which are orthogonal projection matrices on finite dimensional Hilbert space ($\mathbb{C}^d$) with certain features, and emphasized its parallel with combinatorial design theory. Noteworthy is the analogy with regular affine quantum design, which are equivalent to MUBs for rank one projection matrices, with combinatorial affine designs that consist of resolvable parallel classes. In the thesis [102], he also provided the solution of maximal regular affine quantum design, drawing parallels from combinatorial affine 2-design. The solution was shown to exist for prime power dimensions as was the case for combinatorial affine 2-design. However, for composite dimensions, the method did not offer solution.

Wooters [100] drew a parallel between the known numbers of Mutually Orthogonal Latin Square (MOLS) of order q with the number of known MUBs in $\mathbb{C}^d$, where $d = q^2$. Based on this parallel, the analogy between lines in finite geometry and pure state in quantum mechanics can be understood. The study further argues that the complete set of MUBs in d-dimensional Hilbert space are analogous to combinatorial structure of affine plane of order d. In order to prove or disprove the conjecture, attempts had been made to construct MUBs from MOLS(q) and vice versa. One interesting work in this direction was by Wocjan [98] who used MOLS(q) to construct MUBs in $\mathbb{C}^d$, when $d = q^2$. This also improves the lower bound of MUBs for many different dimensions. Further, Paterek [76] devised a method to generate complete set of MUBs in prime power dimension using augmented set of MOLS(q) and Weyl-Schwinger unitary operators. However, in [77], the authors analyzed the idea deeply and concluded that the method cannot relate the MUBs to MOLSs completely. They further concluded that the "problem of MUBs might not be equivalent to the mathematical problem of MOLS".

Our construction for ARMUBs (see Construction 4.3.1 later) is an independent and generalized approach based on RBDs, but it should be noted that for special cases related to exact MUBs, the MOLS based approach of [98] uses similar kind of combinatorial objects. The main difference is corresponding to each block. The construction idea of [98, Theorem 3, Example 4] considered different components of a vector in dimension d and a single Hadamard matrix of a specific order has been used. In our case, same sub-components of a vector are used corresponding to the elements of a block and those are disjoint for different blocks inside the same parallel class. In a special case, while generating exact real MUBs, we obtain similar results as in [98], but have the flexibility of exploiting different non-equivalent

Hadamard matrices of the same order. Further, we have the advantage of using unitary matrices of different orders to provide approximate MUBs, in case of different block sizes in designs which are not regular or balanced. These are not achievable for a large range of parameters by tweaking the construction idea in [98].

It has been well known for decades that obtaining new classes of MUBs and reaching the upper bounds are quite challenging problems. Some relaxation is thus considered in literature and there are efforts towards the concept of Approximate Mutually Unbiased Bases (AMUBs), where the inner product of two vectors drawn from two different bases is upper bounded by some value, rather than the optimal $\frac{1}{\sqrt{d}}$ for dimension d. In this direction the works of [61, 86] are pioneering, particularly, the result [86, Theorem 2] remains the best known construction of Approximate Mutually Unbiased Bases in $\mathbb{C}^d$. The vectors in the bases due to this construction are inherently complex in nature. Thus it is interesting to explore some novel construction method when one considers only the real components. In this direction we have studied certain results in [67], that has been presented in the previous chapter.

However, further examination pointed out that the work of previous chapter [67] considered a restricted class and further generalization beyond that is possible given richer combinatorial structures in literature. In this direction, we propose a generic method to construct Approximate MUBs (AMUBs) using Resolvable Block Designs (RBDs). RBDs consist of parallel classes. We provide a method to convert each parallel class into an orthonormal basis and show that these bases are intimately linked with AMUBs. Certain kinds of parallel classes in RBDs, meeting appropriate exact conditions can generate exact MUBs too. When these conditions are not met with, the parallel classes will generate approximate ones. The number of such MUBs or AMUBs depends on the number of parallel classes in RBDs. To convert parallel classes of RBDs into orthonormal bases, our construction strategy exploits unitary matrices, mostly in smaller dimension, depending on the parameters of the resolvable design.

In this chapter, our main focus is to construct RBDs with suitable parameters where real Hadamard matrix (a subset of unitary matrices) can be used. The technique described here provides novel results in obtaining very sparse Approximate Real MUBs (ARMUBs), that can find application in quantum information processing. It is well known that sparsity can be exploited for efficient computations. With this backdrop, let us present the organization and contribution of this chapter.

4.1.1 Organization & Contribution

In Section 4.2 we begin with various terms and notations formally. We define parameters to characterize Approximate MUBs and its sparsity. Let us refer to Section 2.3 from Chapter 2 to revisit the basics of Resolvable Block Design (RBD), Balanced Incomplete Block Design (BIBD) and Affine Resolvable BIBD and some examples. The relationships between the parameters of block designs and the necessary conditions are instrumental for our techniques. Thereafter, we present the novel results of this work [65].

- In Section 4.3, we present the generic method to construct an orthonormal basis using a parallel class of RBD. This is explained in Construction 4.3.1. We also prove important bound on inner product between basis vectors from different orthonormal bases constructed from different parallel classes in the RBD. These are presented in Lemma 4.3.1 and Theorem 4.3.1.
- Then, in Section 4.4, we use different Resolvable Balanced Incomplete Block Designs (RBIBDs) to construct ARMUBs. The parameters of the BIBDs and the existence of certain matrices, particularly Hadamard, are identified from literature and then we plug those into our construction. Our main result is presented in Theorem 4.4.1. Several novel structures with new parameters are identified in this process in Section 4.4.1 through Affine Resolvable BIBDs (ARBIBDs).
    - Finally in Remark 4.4.1, we explain the construction of exact real MUBs as a special case. We can attain the results of similar quality as it is mentioned in [98]. However, the focus of this chapter is on ARMUBs, and it will be evident that our proposal is more generalized and tuned towards the approximate results, that cannot be achieved through [98] or any other existing methods.
- In Section 4.5 we exploit the RBDs which are not balanced. We construct the unbalanced designs mostly by assimilating or modifying the Affine Resolvable $(q^2, q, 1)$-BIBDs, whose construction are known to exist for whenever q is some power of prime. Clear improvements over presently known parameters are described here. The treatment here provides significant generalization and improvement over our earlier result in [67] (last chapter) in different aspects. In the last chapter [67], it was shown that $\frac{\sqrt{d}}{4} + 1$ ARMUBs with maximum value of inner product as $\frac{4}{\sqrt{d}}$ could be achieved.
    - To show the breadth of this new approach, one special case under Theorem 4.5.1 provides ARMUBs with the same quality as described in the last chapter [67]. This happens when $d = sq^2$, where q is a prime power and $sq \equiv 0 \bmod 4$. The special case, $s = 16$ as well as q a prime itself, takes care of our earlier result in [67].
    - The parameters are improved too in some other classes. Theorem 4.5.2 shows that it is possible to construct $\lceil \sqrt{d} \rceil$ many ARMUBs with the maximum value of inner product (between the vectors of two different bases) less than $\frac{2}{\sqrt{d}}$. That is, we have more number of classes with improved counts of MUBs and a better

upper bound on the absolute values of the inner products. This happens when $d = q(q+1)$, where q is a prime power and $q \equiv 3 \bmod 4$.

We conclude this chapter in Section 4.6 with directions towards future research. While constructing the approximate MUBs, sometimes we also refer how exact MUBs can be obtained from our strategy. Indeed, this is not the main focus of this chapter and those results are not better than the state-of-the-art ones, in terms of number of MUBs constructed. However, large sparsity is a novel feature of our construction, which is almost absent in the existing methods. However, we expect to obtain certain improvements if these techniques can be explored further. Before proceeding, let us now define various notations and parameters characterizing the MUBs and the AMUBs.

4.2 Background and Preliminaries

As we have already discussed, the well known problem is to maximize the number of MUBs for a dimension d and it is still open in composite dimensions. Further, the situation is more complicated in $\mathbb{R}^d$, where very few MUBs are known in general. Knowledge of relatively large number of Approximate MUBs can be helpful in practical situations.

Given a set of orthonormal bases $\mathbb{M} = \{M_1, M_2, \ldots, M_r\}$ (may not be MUBs) of dimension d, we define Δ to be the set of inner products between the vectors from different orthonormal bases. That is, Δ contains the distinct values of $\left|\langle\psi_i^l|\psi_j^m\rangle\right|$ for all $i, j \in \{1, 2, \ldots, d\}$ and $l \neq m \in \{1, \ldots, r\}$. In case $\mathbb{M}$ is an MUB, Δ is a singleton set with the only element $\frac{1}{\sqrt{d}}$. However, for the AMUBs, there will be more than one value in the set and we will try to minimize the maximum absolute value. In this regard, we like to define β-AMUB or β-ARMUB, for which the maximum value in Δ is bounded by $\frac{\beta}{\sqrt{d}}$.

To characterize the closeness of orthonormal bases M_l and M_m to MUBs, we define the variance of the inner products between the vectors of M_l and M_m from $\dfrac{1}{\sqrt{d}}$. For this we define $\sigma^{l,m} = \frac{1}{d}\sqrt{\sum_{i,j}\left(\frac{1}{\sqrt{d}} - \left|\langle\psi_j^l|\psi_i^m\rangle\right|\right)^2}$, as there are d^2 different elements in the calculation. For the set $\mathbb{M}$ of orthonormal bases, σ is accordingly defined as $\sigma = \max_{l\neq m}\{\sigma^{l,m}\}$.

Another way to characterize the closeness of a pair of orthonormal bases to MUBs is by the value of maximum difference of the inner product between any pair of vectors, say from M_l and M_m, with the value of $\frac{1}{\sqrt{d}}$. For this we define, $\tau^{l,m} = \max\left\{\left|\frac{1}{\sqrt{d}} - |\langle\psi_j^l|\psi_i^m\rangle|\right|\right\}\ \forall i, j$. For a set $\mathbb{M}$ of orthonormal bases, τ is accordingly defined as maximum of $\tau^{l,m}$, i.e., $\tau = \max_{l\neq m}\{\tau^{l,m}\}$.

Note that if M_l and M_m constitute a pair of MUBs, then $\beta = 1$, $\Delta = \left\{\frac{1}{\sqrt{d}}\right\}$, $\sigma^{l,m} = 0$

and $\tau^{l,m} = 0$. Similarly, if $\mathbb{M} = \{M_1, M_2, \ldots, M_r\}$ is a set of MUBs, then $\beta = 1, \Delta = \left\{\frac{1}{\sqrt{d}}\right\}$, $\sigma = 0$ and $\tau = 0$. In a certain sense, the vectors in two different bases in an MUB set should make maximum and same angles with others. Thus, the projective measurements associated with them are maximally uncorrelated. This will be deviated for the approximate MUBs.

It is clear that a particular basis of MUBs or AMUBs in $\mathbb{C}^d$ (resp. ARMUBs in $\mathbb{R}^d$) can be thought of as a $d \times d$ unitary matrix (resp. orthogonal matrix in real case) with their columns as orthonormal basis vectors. To characterize the sparsity of such matrices, we define ϵ as the ratio of the number of zero elements in the matrix to the total number of elements, i.e., d^2. It is clear to see that, $0 \leq \epsilon \leq 1$. The closer the value of ϵ to 1, more the number of zeros in the matrix and therefore larger the sparsity. MUBs, which have been constructed for prime or prime power dimensions using finite fields [99] or those constructed using maximal class of commuting operators [6], are invariably having almost all nonzero entries in the MUBs except for the standard basis. Thus, ϵ is close to 0 in these constructions. Regarding sparsity, the situation is similar with real MUBs constructed in [22]. The construction provided mutually unbiased Hadamard matrices, which by nature has all the entries $\{1, -1\}$, thereby ϵ is 0, i.e., not sparse at all. The MUBs constructed using MOLS [98, 18] show relatively better sparsity. This is because the MOLS related constructions are equivalent to the RBDs in certain cases [31, Part III.3]. We like to reiterate that this is the first time the sparsity of the (approximate) MUBs is being quantified in literature. In case of actual implementation or computation, the sparsity might provide efficiency in practice.

4.3 Our Generic idea of Construction

Here we connect how one can design MUBs or approximate MUBs from the above mentioned combinatorial objects, namely RBDs. We provide a generic construction of an orthonormal basis from a parallel class of any Resolvable Block Design (RBD). If the parallel class contain s blocks then the construction would also require s many unitary matrices each of the order which would be equal to the the size of blocks in the parallel class under consideration. If there are r many parallel classes in (X, A), then each one of them can be used to construct an orthonormal basis in $\mathbb{C}^d$ or $\mathbb{R}^d$. Next we show that the inner product between two vectors, each from different orthonormal basis, constructed using parallel classes from design (X, A), are bounded if the Hadamard matrices are exploited as unitary matrices. The set of orthonormal basis so constructed are β-AMUBs (see Theorem 4.3.1 later). This β will depend on the parameters of the RBD and if the parameters are such that $\beta = 1$ then the set of orthonormal bases, constructed using parallel classes, will be MUBs.

Let us now describe the steps for construction of an orthonormal basis using a parallel class from an RBD (X, A). Then we present a simple example to explain the technique.

Construction 4.3.1.

1. *In a design (X, A), choose the elements of X as some 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 consisting of elements from X, would consist of blocks consisting 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 $X = b_1 \cup b_2 \cup \ldots \cup b_s$.*

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 fashion, 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.*

Note that if all the blocks in a parallel class used in the above construction consist of only a single element, then it will result into vectors which will be some permutation of X. Similarly if identity matrices are chosen corresponding to all blocks b_j of the parallel class, again the above construction will result into vectors which will be some permutation of X. Hence, in order to get vectors different from the initial chosen orthonormal vectors X, at least one of the blocks of the parallel class should have more than one element and at least one of the unitary matrices, chosen corresponding to some block of the parallel class, should be different from the identity matrix.

Lemma 4.3.1. *Refer to Construction 4.3.1. The vectors, $|\phi^r_i\rangle$ for $i = 1, 2, \ldots, n_r$ and $r = 1, 2, \ldots, s$, such that $\sum_{j=1}^{s} n_j = d$, form an orthonormal basis.*

Proof. Consider n_r many vectors constructed from the block b_r of a parallel class B. The inner product of any two vectors constructed from b_r would give

$$\langle\phi^r_j|\phi^r_i\rangle = \sum_{k,l=1}^{n_r} \overline{u^r_{jl}}\, u^r_{ik}\, \langle\psi_{r_l}|\psi_{r_k}\rangle = \sum_{k,l=1}^{n_r} \overline{u^r_{jl}}\, u^r_{ik}\, \delta_{kl} = \sum_{k=1}^{n_r} \overline{u^r_{jk}}\, u^r_{ik} = \delta_{ij}.$$

Hence n_r many vectors constructed from the block b_r are orthogonal. Note that, the vectors constructed from a block are linear combinations of vectors $\{|\psi_i\rangle\} \in X$ in the corresponding block. Since different blocks of the parallel class are disjoint subsets of X, the vectors constructed from different blocks of the parallel class would lie on the orthogonal subspace of $\mathbb{C}^d$ and hence will be orthogonal. Since $\sum_{j=1}^{s} n_j = d$, the construction will generate an orthonormal basis in $\mathbb{C}^d$. □

Note that in Construction 4.3.1, if X is chosen from some orthonormal basis vectors of $\mathbb{R}^d$ along with the orthogonal matrix (i.e., all the entries are real) corresponding to each b_r in step 1 and 3 respectively, then the Construction 4.3.1 will result into real orthonormal basis vectors in $\mathbb{R}^d$ corresponding to the parallel class under consideration. Similarly, as noted above, the construction will provide vectors different from X in $\mathbb{R}^d$, if at least one block of the parallel class consist of more than one elements or at least one orthogonal matrix corresponding to some block is chosen different from the identity matrix.

Let us illustrate the above construction method by applying it on Resolvable Block Design (X, A_2) mentioned in Section 2.3 of Chapter 2. The two resolutions of A_2 are P_1 and P_2, where $P_1 = \{(1,2,3),(6,8),(4,5,7)\}$ and $P_2 = \{(1,7),(2,4,6),(3,5,8)\}$. We will show how to convert P_1 into one orthonormal basis and in a similar manner P_2 can be converted to another orthonormal basis. Let $X = \{|1\rangle, |2\rangle, \ldots, |8\rangle\}$ be the computational basis in $\mathbb{C}^8$. Using above notations, consider the parallel class $P_1 = \{b_1, b_2, b_3\}$, where $b_1 = (1,2,3)$, $b_2 = (6,8)$ and $b_3 = (4,5,7)$. Thus we see that, $|b_1| = |b_3| = 3$ and $|b_2| = 2$. Hence, we require at least two unitary matrices, one of order 2 and another of order 3. We will choose the Hadamard matrices in this direction. Let us choose $U_2 = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $U_3 = \frac{1}{\sqrt{3}}\begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}$. For simplicity, we will use the same U_3 for both the blocks, b_1 and b_3. Following the notations and methods given in Construction 4.3.1, we obtain total eight orthogonal vectors of $\mathbb{C}^8$ from the parallel class P_1. Two orthogonal vectors are constructed from b_2 and three each from b_1 and b_3 in the following manner.

$$
\begin{aligned}
|\phi_1^1\rangle &= \frac{1}{\sqrt{3}}\left(|1\rangle + |2\rangle + |3\rangle\right) = \frac{1}{\sqrt{3}}(1\ 1\ 1\ 0\ 0\ 0\ 0\ 0)^T \\
|\phi_2^1\rangle &= \frac{1}{\sqrt{3}}\left(|1\rangle + \omega\,|2\rangle + \omega^2\,|3\rangle\right) = \frac{1}{\sqrt{3}}(1\ \omega\ \omega^2\ 0\ 0\ 0\ 0\ 0)^T \\
|\phi_3^1\rangle &= \frac{1}{\sqrt{3}}\left(|1\rangle + \omega^2\,|2\rangle + \omega\,|3\rangle\right) = \frac{1}{\sqrt{3}}(1\ \omega^2\ \omega\ 0\ 0\ 0\ 0\ 0)^T \\
|\phi_1^2\rangle &= \frac{1}{\sqrt{2}}\left(|6\rangle + |8\rangle\right) = \frac{1}{\sqrt{2}}(0\ 0\ 0\ 0\ 0\ 1\ 0\ 1)^T \\
|\phi_1^2\rangle &= \frac{1}{\sqrt{2}}\left(|6\rangle - |8\rangle\right) = \frac{1}{\sqrt{2}}(0\ 0\ 0\ 0\ 0\ 1\ 0\ \ -1)^T \\
|\phi_1^3\rangle &= \frac{1}{\sqrt{3}}\left(|4\rangle + |5\rangle + |7\rangle\right) = \frac{1}{\sqrt{3}}(0\ 0\ 0\ 1\ 1\ 0\ 1\ 0)^T \\
|\phi_2^3\rangle &= \frac{1}{\sqrt{3}}\left(|4\rangle + \omega\,|5\rangle + \omega^2\,|7\rangle\right) = \frac{1}{\sqrt{3}}(0\ 0\ 0\ 1\ \omega\ 0\ \omega^2\ 0)^T \\
|\phi_3^3\rangle &= \frac{1}{\sqrt{3}}\left(|4\rangle + \omega^2\,|5\rangle + \omega\,|7\rangle\right) = \frac{1}{\sqrt{3}}(0\ 0\ 0\ 1\ \omega^2\ 0\ \omega\ 0)^T.
\end{aligned}
$$

Note that the first three vectors $|\phi_1^1\rangle, |\phi_2^1\rangle, |\phi_3^1\rangle$ corresponding to one block in a parallel class works with $|1\rangle, |2\rangle, |3\rangle$ only, and the orthogonality among themselves is achieved by using U_3. This is different from [98, Theorem 3, Example 4] as there the vectors corresponding to each block may have other components of the vector. The kind of separate grouping that we use here and use the unitary matrices for orthogonality between the vectors is different from that of [98]. In our case the between block orthogonality in the same parallel class is achieved as the components of the vectors are different. This helps us to exactly calculate the different inner product values (as we are considering approximate MUBs rather than exact MUBs) when blocks (and the vectors corresponding to that) from two different parallel classes (different orthogonal bases) interact.

Now arranging the above eight orthogonal vectors as columns of 8 × 8 unitary matrix we have the following.

$$
M_1 = \frac{1}{\sqrt{6}}
\begin{pmatrix}
\sqrt{2} & \sqrt{2} & \sqrt{2} & 0 & 0 & 0 & 0 & 0 \\
\sqrt{2} & \sqrt{2}\omega & \sqrt{2}\omega^2 & 0 & 0 & 0 & 0 & 0 \\
\sqrt{2} & \sqrt{2}\omega^2 & \sqrt{2}\omega & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & \sqrt{2} \\
0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2}\omega & \sqrt{2}\omega^2 \\
0 & 0 & 0 & \sqrt{3} & \sqrt{3} & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2}\omega^2 & \sqrt{2}\omega \\
0 & 0 & 0 & \sqrt{3} & -\sqrt{3} & 0 & 0 & 0
\end{pmatrix}.
$$

In a similar manner, the parallel class P_2 can be converted into another orthonormal basis of $\mathbb{C}^8$. Following the Construction 4.3.1 in a similar manner, and using the unitary matrix U_2 for block $(1,7)$ and U_3 for both the blocks $(2,4,6)$ and $(3,5,8)$ we obtain the following.

$$M_2 = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{3} & \sqrt{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2} & \sqrt{2} & \sqrt{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2} & \sqrt{2} \\ 0 & 0 & \sqrt{2} & \sqrt{2}\omega & \sqrt{2}\omega^2 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2}\omega & \sqrt{2}\omega^2 \\ 0 & 0 & \sqrt{2} & \sqrt{2}\omega^2 & \sqrt{2}\omega & 0 & 0 & 0 \\ \sqrt{3} & -\sqrt{3} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & \sqrt{2} & \sqrt{2}\omega^2 & \sqrt{2}\omega \end{pmatrix}.$$

Let us now denote $\{|\psi_i^1\rangle\}, 1 \leq i \leq 8$ for column vectors of M_1 and $\{|\psi_j^2\rangle\}, 1 \leq j \leq 8$ for column vectors of M_2. Through explicit calculations we obtain,

$$\Delta = \big\{ |\langle \psi_i^1 | \psi_j^2 \rangle| \text{ where } i,j = 1, \ldots, 8 \big\} = \left\{ \frac{1}{2}, \frac{1}{\sqrt{6}}, \frac{1}{3} \right\}.$$

In order to calculate $\sigma^{1,2}$, note that out of 64 many inner products formed between the vectors of M_1 and M_2, 36 of them have the value $\frac{1}{3}$, 24 of them have the value of $\frac{1}{\sqrt{6}}$ and remaining 4 has the value $\frac{1}{2}$, whereas MUBs in $\mathbb{C}^8$ would have inner product value of $\frac{1}{\sqrt{8}}$ for all the cases. Hence,

$$\left(\sigma^{1,2}\right)^2 = \frac{1}{64}\left(36\left(\frac{1}{3} - \frac{1}{\sqrt{8}}\right)^2 + 24\left(\frac{1}{\sqrt{6}} - \frac{1}{\sqrt{8}}\right)^2 + 4\left(\frac{1}{2} - \frac{1}{\sqrt{8}}\right)^2\right),$$

which evaluates to $\sigma^{1,2} \approx 0.052$. Note that $\max_{i,j} \left|\langle \psi_i^1 | \psi_j^2 \rangle\right| = \frac{1}{2}$. Hence $\tau^{1,2} = \left|\frac{1}{2} - \frac{1}{\sqrt{8}}\right| \approx 0.12$. We also obtain $\beta_{1,2} = \frac{\sqrt{8}}{2} = \sqrt{2}$ and the sparsity $\epsilon = \frac{42}{64} \approx 0.66$ for both M_1 and M_2. From calculations it is evident that the $\max_{i,j} \left|\langle \psi_i^1 | \psi_j^2 \rangle\right|$ is dependent on the block sizes and number of points common between the blocks from which $|\psi_i^1\rangle, |\psi_j^2\rangle$ are constructed. The following proposition examines the same, when Hadamard matrices are used as unitary matrices, and presents an upper bound on this value. The Hadamard matrices are subset of unitary matrices, and at least one such (Fourier) matrix exists for every dimension. In the following proposition, and the subsequent constructions, we will use Hadamard matrices of order dependent on the block size of parallel class under consideration. That is, in this initiative we will use the real Hadamard matrices for unitarity/orthogonality.

Theorem 4.3.1. *Let P_1 and P_2 be two parallel classes of Resolvable Block Design (X, A) having constant block sizes k_1 and k_2 respectively, such that the maximum intersection points* *between the blocks of parallel classes is μ. Then corresponding to the parallel classes P_1 and P_2, orthonormal bases in $\mathbb{C}^d$ can be constructed which is β-AMUB with $\beta = \mu\sqrt{\frac{d}{k_1k_2}}$ where $|X| = d$.*

Proof. The proof follows from Construction 4.3.1, where the Hadamard matrices are chosen as the unitary matrices in step 3. We show this as follows.

Let $X = \{|\psi_1\rangle, |\psi_2\rangle, \ldots, |\psi_d\rangle\}$ be an orthonormal basis in $\mathbb{C}^d$. Let the blocks in the parallel classes be $P_1 = \{b_1^1, b_2^1, \ldots, b_p^1\}$ and $P_2 = \{b_1^2, b_2^2, \ldots, b_q^2\}$. We have $|b_1^1| = |b_2^1| = \ldots = |b_p^1| = k_1$ and $|b_1^2| = |b_1^2| = \ldots = |b_q^2| = k_2$ and $X = b_1^1 \cup b_2^1 \cup \ldots \cup b_p^1 = b_1^2 \cup b_2^2 \cup \ldots \cup b_q^2$.

Following the steps of the Construction 4.3.1, let $M_1 = \{|\zeta_1\rangle, |\zeta_2\rangle, \ldots, |\zeta_d\rangle\}$ and $M_2 = \{|\phi_1\rangle, |\phi_2\rangle, \ldots, |\phi_d\rangle\}$ be the orthonormal matrices constructed from parallel classes P_1 and P_2 respectively of the RBD (X, A). Consider the vectors constructed from r^{th} $(r \leq p)$ block of P_1, say $|\zeta_{r_i}\rangle$, and from s^{th} $(s \leq q)$ block of P_2, say $|\phi_{s_j}\rangle$. Let H_{k_1} be the Hadamard matrix of order k_1 used for constructing $|\zeta_{r_i}\rangle$ and H_{k_2} be the Hadamard matrix of order k_2 used for constructing $|\phi_{s_j}\rangle$. Then we have

$$|\zeta_{r_i}\rangle = h_{i1}^1 |\psi_{r_1}\rangle + h_{i2}^1 |\psi_{r_2}\rangle + \ldots + h_{ik_1}^1 |\psi_{r_{k_1}}\rangle = \sum_{u=1}^{k_1} h_{iu}^1 |\psi_{r_u}\rangle : b_r^1 = \{|\psi_{r_u}\rangle\} \subset X,$$

$$|\phi_{s_j}\rangle = h_{j1}^2 |\psi_{s_1}\rangle + h_{j2}^2 |\psi_{s_2}\rangle + \ldots + h_{jk_2}^2 |\psi_{s_{k_2}}\rangle = \sum_{v=1}^{k_2} h_{jv}^2 |\psi_{s_v}\rangle : b_s^2 = \{|\psi_{s_v}\rangle\} \subset X,$$

where $(H_{k_1})_{i,j} = h_{i,j}^1$ and $(H_{k_2})_{i,j} = h_{i,j}^2$. Hence,

$$\langle\zeta_{r_i}|\phi_{s_j}\rangle = \sum_{u,v=1}^{k_1,k_2} \overline{h_{iu}^1}\ h_{jv}^2 \ \langle\psi_{r_u}|\psi_{s_v}\rangle = \sum_{u,v=1}^{k_1,k_2} \overline{h_{iu}^1}\ h_{jv}^2 \ \delta_{r_u,s_v}.$$

Since $\{|\psi_{r_u}\rangle\}$ and $\{|\psi_{s_v}\rangle\}$ are subsets of X, which consist of orthonormal basis vectors, therefore $\langle\psi_{r_u}|\psi_{s_v}\rangle = \delta_{r_u,s_v}$. Let $b_r^1 \cap b_s^2$ be the set of points common in the two blocks, which has been used in the construction for $|\zeta_{r_i}\rangle$ and $|\phi_{s_j}\rangle$. It is given that $\max_{i,j}\left\{\left|b_i^1 \cap b_j^2\right|\right\} = \mu$, where $i = 1, 2, \ldots, p$ and $j = 1, 2, \ldots, q$. Hence $|b_r^1 \cap b_s^2| \leq \mu$. Further, note that $\left|h_{r_u}^1\right| = \frac{1}{\sqrt{k_1}}$ and $\left|h_{s_v}^2\right| = \frac{1}{\sqrt{k_2}}$. Hence

$$\langle\zeta_{r_i}|\phi_{s_j}\rangle = \sum_{b_r^1 \cap b_s^2} \overline{h_{iu}^1}\ h_{jv}^2 \leq \sum_{b_r^1 \cap b_s^2} |\overline{h_{iu}^1}|\ |h_{jv}^2| = \sum_{b_r^1 \cap b_s^2} \frac{1}{\sqrt{k_1k_2}} \leq \frac{\mu}{\sqrt{k_1k_2}} = \frac{\mu\sqrt{\frac{d}{k_1k_2}}}{\sqrt{d}},$$

where $\beta = \mu\sqrt{\frac{d}{k_1k_2}}$. The vectors $|\zeta_{r_i}\rangle$ and $|\phi_{s_j}\rangle$ are constructed from any r^{th} and s^{th} block of P_1 and P_2 respectively. Hence the above relationship will hold for any two vectors constructed from different parallel classes. Hence $|\langle\zeta_i|\phi_j\rangle| \leq \frac{\mu}{\sqrt{k_1 k_2}}$ for any $1 \leq i, j \leq d$. Thereby, the orthonormal bases constructed corresponding to the parallel classes P_1 and P_2 are β-AMUB. □

Suitable choices of Hadamard matrices, for specific situations may improve the inequality. Particularly, whenever parametric form of Hadamard matrices are available, they may be used and parameters may be optimized, which can result into orthonormal bases closer to MUBs. Another method to improve this inequality would be through reducing the μ, which is dependent on parameters of the Resolvable Block Design. In fact, if $\mu = 1$ and $d = k_1 \cdot k_2$ then $\beta = 1$, and the above constructions will present MUBs. In our present work we will focus on making β close to 1 (from the higher side) by altering the parameters of RBD.

In a similar manner, we can convert Resolvable Block Design consisting of r resolutions into set of r orthonormal bases for $\mathbb{R}^d$ using real Hadamard matrices in set 3 of Construction 4.3.1. A real Hadamard matrix exists for $d = 2^s, s \in \mathbb{N}$ (Sylvester Construction [48]) and for $d = 2^s(q+1)$, where q is some power of odd prime (Paley Construction [75]), apart from other known constructions [48]. In fact, the Hadamard Conjecture [37] says that the real Hadamard matrix exists for all dimensions $d > 2$ such that $4|d$. This is a long standing unproven conjecture which has been found to be true for all $d < 668$ [37].

The order of Hadamard matrix to be exploited in the step 3 of construction 4.3.1, is decided by the block size of the corresponding parallel class. Hence to obtain real MUBs, we will ensure that the block size (denoted by k) is either 2 or divisible by 4. Though our focus is on ARMUBs, the results hold equally well for complex AMUBs. In fact to obtain complex AMUBs, there would be no restriction on the parameters of the Resolvable Block Design (X, A), as there are Hadamard matrices available for every order, namely the Fourier matrices.

For all our examples and constructions in following sections, the points (or elements) in X would consist of computational basis vectors and would be simply denoted as $\{1, 2, \ldots, d\}$. For example, $|X| = 4$ implies $X = \{1, 2, 3, 4\}$ where 1 represents $(1, 0, 0, 0)^T$, 2 represents $(0, 1, 0, 0)^T$, 3 represent $(0, 0, 1, 0)^T$ and 4 represent $(0, 0, 0, 1)^T$. Since a real Hadamard matrix consists of only $\{-1, +1\}$ entries, our construction for ARMUBs will have vectors whose entries will consist of $\{-1, 0, +1\}$ with some normalization factor for the corresponding vectors.

4.4 ARMUBs using Resolvable BIBDs

In this section, we will explore the designs which are resolvable and also $(v, k, 1)$-BIBDs. Necessary condition for a $(v, k, 1)$-BIBD to be resolvable can be derived by the fact that $k|v$

and $(k-1)|(v-1)$ for b and r to be integers. It turns out that the necessary condition for resolvable $(v,k,1)$-BIBD is $v = k(k-1)t + k$ for $t \in \mathbb{N}$ [46]. It has been shown that with finitely many exceptions, resolvable $(v,k,1)$-BIBDs exist whenever necessary condition is satisfied. More specifically, given $k \geq 2$, there exists a constant $C(k)$ such that if $v \geq C(k)$ and $v \equiv k \mod [k(k-1)]$, then $(v,k,1)$-resolvable BIBDs exist [80]. This implies that there exist infinite families of resolvable $(v,k,1)$-BIBDs for every $k \in \mathbb{N}$. In all the following theorems and constructions, the dimension d of the underlying vector space will be equal to v i.e., $d = v$.

Theorem 4.4.1. *Suppose, there exists a resolvable $(v,k,1)$-BIBD. Let $d = v = k(k-1)t+k$, where $t \in \mathbb{N}$. If $t > 1$, then one can construct $(kt+1)$ many Approximate MUBs in $\mathbb{C}^d$ with $\Delta = \left\{0, \frac{1}{k}\right\}$, $\beta = \sqrt{\frac{(k-1)t+1}{k}}$, $\sigma^2 = \frac{2}{d}\left[1 - \frac{k}{\sqrt{d}}\right]$, $\tau < \frac{1}{k}$ and the sparsity $\epsilon = 1 - \frac{1}{(k-1)t+1}$. If $t = 1$, then one can construct $(k+1)$ many MUBs in $\mathbb{C}^d$ with $\Delta = \left\{\frac{1}{k}\right\}$, $\beta = 1$, $\sigma = \tau = 0$ and the sparsity $\epsilon = \left(1 - \frac{1}{k}\right)$. Further, if a real Hadamard matrix of order k exists, then one can construct ARMUBs in $\mathbb{R}^d$ with the same parameters.*

Proof. The necessary condition for the existence of a Resolvable $(v,k,1)$-BIBD is $v = k(k-1)t + k$ for some $t \in \mathbb{N}$ [46]. Let us consider $t > 1$. Since $\lambda = 1$ in this BIBD, every pair of points will occur in a single block. Thus, any two blocks will have maximum one point in common. This implies that the blocks from different parallel classes will have at most one point in common. Now we can use any Hadamard matrix of order k to convert each parallel class having block size k into orthonormal basis as per Construction 4.3.1. The Δ would consist of $\left\{\frac{1}{k}, 0\right\}$ corresponding to whether there is one point in common or there is no point is common between the blocks used to generate corresponding vectors of the orthonormal basis. Hence $\beta = \frac{\sqrt{d}}{k} = \frac{\sqrt{k(k-1)t+k}}{k} = \sqrt{\frac{(k-1)t+1}{k}}$. Now to compute σ, note that each vector in an orthonormal basis will have inner product value equal to $\frac{1}{k}$ with k^2 vectors of any other orthonormal basis and will have inner product equal to 0 with remaining $(d-k^2)$ basis vectors. Hence,

$$\sigma^2 = \frac{1}{d}\left[k^2\left(\frac{1}{\sqrt{d}} - \frac{1}{k}\right)^2 + \left(d - k^2\right)\left(\frac{1}{\sqrt{d}} - 0\right)^2\right] = \frac{2}{d}\left[1 - \frac{k}{\sqrt{d}}\right].$$

In order to calculate τ, note that $\left|\frac{1}{k} - \frac{1}{\sqrt{d}}\right| \geq \frac{1}{\sqrt{d}}$ for $d \geq 4k^2$ which implies $t \geq \frac{4k-1}{k-1} \approx 4$ for sufficiently large k. Hence,

$$\tau = \begin{cases} \frac{1}{\sqrt{d}}, \text{ for } 1 < t \leq \frac{4k-1}{k-1} \text{ (i.e., } k^2 < d \leq 4k^2) \\ \frac{1}{k} - \frac{1}{\sqrt{d}}, \text{ for } t > \frac{4k-1}{k-1} \text{ (i.e., } d > 4k^2) \end{cases}.$$

Hence $\tau \leq \frac{1}{k}$ for any d. Note that for for a fixed k, σ decreases as the dimension d increases, whereas τ goes towards $\frac{1}{k}$. In this construction Δ is independent of the dimension but σ and τ are not.

To calculate sparsity, note that each vector in $\mathbb{C}^d$ (or $\mathbb{R}^d$), constructed from block of size k, will have exactly k many non-zero and $d-k$ many zero entries. Since the construction provides d orthonormal basis vectors, we get

$$\epsilon = \frac{d^2 - dk}{d^2} = 1 - \frac{k}{d} = 1 - \frac{1}{(k-1)t+1}.$$

Now consider the case $t = 1$. Here $d = v = k^2$ which implies combinatorial design is $(k^2, k, 1)$-ARBIBD. Hence blocks from different parallel classes have exactly one point in common. Hence $\Delta = \left\{\frac{1}{k}\right\}$. But in this case $\frac{1}{k} = \frac{1}{\sqrt{d}}$. Hence $\sigma = \tau = 0$. The expression for sparsity will remain unchanged, i.e. $\epsilon = 1 - \frac{k}{d} = 1 - \frac{1}{k}$. This completes the proof. □

Hence the constructed orthonormal bases are very sparse even for moderate size k and t. Let us consider two simple cases, for $k = 2, 4$. This will enable us to choose real Hadamard matrices for converting the parallel classes of resolvable $(v, k, 1)$-BIBD into orthonormal bases. It has been shown in [80, 46] that for these values of k, necessary condition is also a sufficient condition for the existence of resolvable $(v, k, 1)$-BIBD without any exception. Hence we obtain the following result.

Corollary 4.4.1. *For any even dimension $d > 4$, there exist $d-1$ ARMUBs in $\mathbb{R}^d$ such that $\Delta = \left\{\frac{1}{2}, 0\right\}$, $\beta = \sqrt{\frac{d}{4}}$, $\sigma^2 = \frac{2}{d}\left[1 - \frac{2}{\sqrt{d}}\right]$, $\tau < \frac{1}{2}$ and sparsity $\epsilon = 1 - \frac{2}{d}$. Further, for $d = 4$ we can construct three real MUBs with sparsity $\epsilon = \frac{1}{2}$*

Proof. This directly follows from Theorem 4.4.1. Taking $k = 2$ gives $d = 2t + 2$. Hence for $t > 1$, we can construct $2t + 1 = d - 1$ many Approximate MUBs in $\mathbb{R}^d$ with $\Delta = \left\{0, \frac{1}{2}\right\}$, $\beta = \sqrt{\frac{t+1}{2}} = \sqrt{\frac{d}{4}}$, $\sigma^2 = \frac{2}{d}\left[1 - \frac{2}{\sqrt{d}}\right]$, $\tau < \frac{1}{2}$ and the sparsity $\epsilon = \left(1 - \frac{2}{d}\right)$. If $t = 1$, then $d = 2 + 2 = 4$ and we can construct $(2 + 1) = 3$ many MUBs in $\mathbb{R}^d$ with $\Delta = \left\{\frac{1}{2}\right\}$, $\beta = 1$, $\sigma = \tau = 0$ and the sparsity $\epsilon = 1 - \frac{1}{2} = \frac{1}{2}$. This completes the proof. □

To explicitly demonstrate the construction of real MUBs in $\mathbb{R}^4$, using Resolvable $(4, 2, 1)$-BIBD, let $X = \{1, 2, 3, 4\}$ be the four standard basis vectors in $\mathbb{R}^4$ and let $A = \{P_1, P_2, P_3\}$ be the three parallel classes of the resolvable design. Explicitly, one such design would be:

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

Now using $H_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ for each block of parallel class, and exploiting Construction 4.3.1, we obtain three set of orthonormal basis vectors corresponding to each parallel class as follows.

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

The columns of $\{M_1, M_2, M_3\}$ form the orthonormal basis vectors, and these orthonormal bases are MUBs in $\mathbb{R}^4$. Note that maximum number of real MUBs in $d = 4^s, s \in \mathbb{N}$ is equal to $\frac{d}{2} + 1$ [18]. Hence for $d = 4$, the three MUBs constructed are also maximal for $\mathbb{R}^4$.

To illustrate construction of ARMUBs with a specific example, let us consider $d = 6$. Let $X = \{1, 2, 3, 4, 5, 6\}$ be the six standard basis vectors in $\mathbb{R}^6$ and let $A = \{P_1, P_2, P_3, P_4, P_5\}$ be the five parallel classes of the design. Explicitly, one such design would be

$P_1 = \{(1,4), (2,3), (5,6)\}$, $P_2 = \{(2,6), (3,4), (1,5)\}$, $P_3 = \{(5,2), (3,1), (4,6)\}$, $P_4 = \{(5,3), (4,2), (6,1)\}$, $P_5 = \{(5,4), (6,3), (1,2)\}$.

Now again using $H_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}$ for each block of parallel class, and following Construction 4.3.1, we obtain five set of orthonormal basis vectors as follows.

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

$$M_3 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 1 & 1 & 0 & 0\\ 1 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & -1 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & 1\\ 1 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & -1\end{pmatrix}, M_4 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 1 & 1 & 0 & 0\\ 1 & 1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & -1 & 0 & 0\\ 1 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 0 & 0 & 1 & -1\end{pmatrix},$$

$$M_5 = \frac{1}{\sqrt{2}}\begin{pmatrix}0 & 0 & 0 & 0 & 1 & 1\\ 0 & 0 & 0 & 0 & 1 & -1\\ 0 & 0 & 1 & 1 & 0 & 0\\ 1 & 1 & 0 & 0 & 0 & 0\\ 1 & -1 & 0 & 0 & 0 & 0\\ 0 & 0 & 1 & -1 & 0 & 0\end{pmatrix}.$$

Here again, the columns form the orthonormal basis vectors. Note that, for any basis vector say from M_1, there are four vectors in M_2 which has inner product value of $\frac{1}{2}$ and the remaining two have the values 0 i.e., two of them are orthogonal. Here $\Delta = \left\{0, \frac{1}{2}\right\}$, $\beta = \frac{\sqrt{6}}{2} \approx 1.22$. Further, for this construction $\sigma = \sqrt{\frac{2}{6}\left(1 - \frac{2}{\sqrt{6}}\right)} \approx 0.247$, $\tau = \max\left\{\frac{1}{\sqrt{6}}, |\frac{1}{2} - \frac{1}{\sqrt{6}}|\right\} = \frac{1}{\sqrt{6}} \approx 0.408$ and sparsity $\epsilon = 1 - \frac{2}{6} = \frac{2}{3}$. Now let us consider the case for $k = 4$.

Corollary 4.4.2. *For any dimension $d > 16$ where $d \equiv 4 \bmod 12$, there exist $\frac{d-1}{3}$ many ARMUBs in $\mathbb{R}^d$ such that $\Delta = \left\{0, \frac{1}{4}\right\}$, $\beta = \dfrac{\sqrt{d}}{4}$, $\sigma^2 = \frac{2}{d}\left(1 - \frac{4}{\sqrt{d}}\right)$, $\tau < \frac{1}{4}$ and the sparsity $\epsilon = 1 - \frac{4}{d}$. For $d = 16$, we can construct five real MUBs with sparsity $\epsilon = \frac{3}{4}$.*

Proof. The result follows directly from Theorem 4.4.1 by taking $k = 4$. This gives $d = 4 \times 3t + 4 \equiv 4 \bmod 12$. Hence for $t > 1$, using Theorem 4.4.1, we get $4t + 1 = \frac{d-1}{3}$ many ARMUBs with $\Delta = \left\{0, \frac{1}{4}\right\}$, $\beta = \sqrt{\frac{3t+1}{4}} = \frac{\sqrt{d}}{4}$, $\sigma^2 = \frac{2}{d}\left(1 - \frac{4}{\sqrt{d}}\right)$, $\tau < \frac{1}{4}$ and the sparsity $\epsilon = 1 - \frac{4}{d}$.

If $t = 1$, then in $d = 4 \times 3 + 4 = 16$ and we can construct $(4 + 1) = 5$ many MUBs in $\mathbb{R}^d$ with $\Delta = \left\{\frac{1}{4}\right\}$, $\beta = 1$, $\sigma = \tau = 0$ and the sparsity $\epsilon = 1 - \frac{1}{4} = \frac{3}{4}$. This completes the proof. □

Note that in $d = 4^2$, the maximum number of real MUBs are $\frac{4^2}{2} + 1 = 9$ [18]. However, from our construction, we only obtain five MUBs which is not maximal. However, we like to point out here that these 5 MUBs are very sparse ($\epsilon = 0.75$), whereas 9 real MUBs constructed using [22] would give MUBs in the form of mutually unbiased Hadamard matrices, where all the entries from $\{+1, -1\}$ hence no sparsity, except the standard basis.

Note that the construction using Theorem 4.4.1 gives very good Approximate MUBs for a fixed k ($d \geq k^2$) in lower dimensions, with β close to 1. However, as dimension increases β increases as $\sqrt{d}$ hence approximation deteriorates. On the other hand, as d increases the sparsity also increases. In this regard, let us present two instances.

Example 4.4.1. *The resolvable $(28, 4, 1)$-BIBD will provide 9 ARMUBs in $\mathbb{R}^{28}$ with $\beta = \sqrt{\frac{7}{4}} \approx 1.3$ and $\epsilon = \frac{6}{7}$. Similarly, the resolvable $(40, 4, 1)$-BIBD will generate 13 ARMUBs in $\mathbb{R}^{40}$ with $\beta = \sqrt{\frac{5}{2}} \approx 1.6$ and $\epsilon = \frac{9}{10}$. Note that for both of the dimension only a pair of real MUBs can exist.*

4.4.1 Constructions following ARBIBD

Among all the resolvable BIBDs, Affine Resolvable BIBDs ($r = k+\lambda$) provide very interesting class of MUBs and AMUBs because of the fact that any two blocks from different parallel classes intersect at exactly $\frac{k^2}{v}$ points. By using the Hadamard matrices in Construction 4.3.1 at Step 3 provides approximate MUBs with small values of σ and τ, as well as β close to 1.

The Affine Resolvable BIBD (v, k, λ) can be parameterized in terms of two positive integer variables n and μ. The other parameters of the design in terms of n and μ are given as $v = n^2\mu$, $k = n\mu$, $\lambda = \frac{n\mu-1}{n-1}$, $b = \frac{n(n^2\mu-1)}{n-1}$, $r = \frac{n^2\mu-1}{n-1}$, and $\frac{k^2}{v} = \mu$. Hence one may consider it as $(n^2\mu, n\mu, \frac{n\mu-1}{n-1})$-ARBIBD. Conversely, any resolvable BIBD having parameters of this form is Affine Resolvable. We will denote such BIBD as an (n, μ)-ARBIBD [93, Chapter 5].

Lemma 4.4.1. *If there exists an Affine Resolvable BIBD of the form $(n^2\mu, n\mu, \frac{n\mu-1}{n-1})$, then for $d = n^2\mu$, we can construct $\frac{n^2\mu-1}{n-1}$ many approximate MUBs with $\beta = \sqrt{\mu}$, $\sigma \leq \frac{1}{n}$, $\tau \leq \frac{1}{n}$ and sparsity $\epsilon = 1 - \frac{1}{n}$. If real Hadamard matrix of order $n\mu$ exist, then we can construct Approximate Real MUBs with the same parameters.*

Proof. Using Affine resolvable $(n^2\mu, n\mu, \frac{n\mu-1}{n-1})$-BIBD, we can convert $r = \frac{n^2\mu-1}{n-1}$ number of parallel classes using Hadamard matrix of order $n\mu$ into r many orthonormal basis. Since exactly μ points are common between any two blocks from different parallel classes, maximum inner product between vectors from different orthonormal bases should be less than or equal to $\mu \times \frac{1}{n\mu} = \frac{1}{n}$.

Now, $\max\left\{\frac{1}{n\sqrt{\mu}}, \left|\frac{1}{n} - \frac{1}{n\sqrt{\mu}}\right|\right\}$ is equal to $\frac{\sqrt{\mu}-1}{\sqrt{d}}$ for $\mu \geq 4$ and it is equal to $\frac{1}{\sqrt{d}}$ for $1 < \mu < 4$. Therefore $\sigma^2 \leq \left(\frac{1}{n} - \frac{1}{\sqrt{n^2\mu}}\right)^2 = \frac{\left(\sqrt{\mu}-1\right)^2}{d}$ for $\mu \geq 4$ and $\sigma^2 \leq \left(\frac{1}{n\sqrt{\mu}} - 0\right)^2 = \frac{1}{d}$ for $1 < \mu < 4$. Hence $\sigma^2 \leq \frac{\mu}{d} = \frac{1}{n^2}$ $\forall \mu > 1$. That is, $\sigma \leq \frac{1}{n}$ for $\mu > 1$. Similarly $\tau = \max\left\{\frac{1}{n\sqrt{\mu}}, \left|\frac{1}{n} - \frac{1}{n\sqrt{\mu}}\right|\right\}$, which implies $\tau \leq \sqrt{\frac{\mu}{d}} = \frac{1}{n}$ $\forall\, \mu > 1$.

Note that when $\mu = 1$, both σ and $\tau = 0$. This happens because, $\mu = 1$ means, between a pair of blocks from different parallel classes has exactly one point in common, implying $\beta = 1$, and we will get exact MUBs.

The sparsity can be calculated as $\epsilon = 1 - \frac{k}{d} = 1 - \frac{1}{n}$. Moreover, if real Hadamard matrix of order $n\mu$ exists, then we can choose them as the unitary matrix in step 3 of Construction 4.3.1 to construct ARMUBs, where the parameters will remain unchanged. As noted, if $\mu = 1$ then both σ and τ will be zero, hence we will get exactly $n + 1$ many MUBs. □

However, there are not many known families of Affine Resolvable $(n^2\mu, n\mu, \frac{n\mu-1}{n-1})$-BIBDs [87, 93]. One well known family of ARBIBD can be constructed from affine geometry of order

d. However, this construction is known only if d is some power of prime. In particular when $d = q^2$, where q is some power of prime, Affine Resolvable $(q^2, q, 1)$-BIBDs can be constructed. This immediately gives the following corollary.

Corollary 4.4.3. *When $d = q^2$ where q is some power of prime, then we can construct $q+1$ MUBs in $\mathbb{C}^d$ with $\epsilon = 1 - \frac{1}{q}$.*

Proof. For any prime power, an Affine Resolvable $(q^2, q, 1)$-BIBD exists, such that between any two blocks from different parallel classes there is only one point in common. Thus, using any Hadamard matrix of order q in Step 3 of Construction 4.3.1, we obtain $q+1$ many MUBs in $\mathbb{C}^d$. If Fourier matrix of order q is used, then resulting entries of MUBs will consist of only q^{th} roots of unity and zeros. These $q+1$ MUBs so constructed have sparsity $\epsilon = 1 - \frac{1}{q}$. □

In such constructions of MUBs, any kind of Hadamard matrix can be used in step 3 of Construction 4.3.1. This immediately suggests the ways to generate MUBs in a dimension q^2, where q is some power of a prime. Such constructions are not possible using Galois Field [99, 39] or through construction of maximal commuting unitary operators using generalized Pauli matrices [6]. The caveat here is, using Construction 4.3.1, the number of MUBs would be $q+1$, which is considerably less than the upper bound of q^2+1. For example, we can construct five MUBs in $d = 4^2$ using Affine Resolvable $(4^2, 4, 1)$-BIBD and using parametric form of Hadamard matrix $F_4^{(1)(a)}$ [94, Example 1.2.1]. Similarly, using Buston Hadamard matrices like $BH(n^{2k}, 6)$ [94, Corollary 1.4.42], which exist for every $n, k \in \mathbb{N}$, we can construct q^2+1 many MUBs in $\mathbb{C}^{q^4}$ where q is some power of prime. Here we need to use Affine Resolvable $(q^4, q^2, 1)$-BIBD, whose non-zero entries would consist of only sixth roots of unity. Further, using Petrescu's construction for parametric form of Hadamard matrices, for primes $p = 7, 13, 19, 31$ [94, Theorem 3.1.2], one can construct corresponding parametric MUBs in $d = 7^2, 13^2, 19^2, 31^2$, which would not be equivalent to the MUBs from known methods, based on Galois Field [99, 39] or through construction of maximal commuting unitary operators using generalized Pauli matrices [6]. Further knowledge of Hadamard matrices, whose orders are some powers of prime, can be exploited to construct interesting sparse MUBs using this method.

Since there always exist real Hadamard matrices of order $2^s, s \in \mathbb{N}$ [48], we have the following corollary.

Corollary 4.4.4. *For $d = 4^s, s \in \mathbb{N}$, there exist $2^s + 1$ many real MUBs with sparsity $\epsilon = 1 - 2^{-s}$.*

Note that these are very sparse real MUBs and hence can be used for efficient computations. However, these do not improve the existing parameters in literature. However, we present these for exposure as we expect that further analysis of our techniques may improve the parameters.

It should also be noted that the existence of real Hadamard matrix of order $4m$ implies the existence for Affine Resolvable $(4m, 2m, 2m-1)$-BIBD [93, 87]. Thus we have the following result.

Proposition 4.4.1. *Consider that a real Hadamard matrix of order $2m$ $(m > 1)$ exists. Then for $d = 4m$, we can construct $4m - 1$ many β-ARMUBs where $\beta \leq \sqrt{m}$. Further, $\Delta = \frac{1}{\sqrt{d}} \times \left\{0, \frac{2}{\sqrt{m}}, \frac{4}{\sqrt{m}}, \ldots, \frac{m}{\sqrt{m}}\right\}$, $\sigma \leq \frac{1}{2}$, $\tau \leq \frac{1}{2}$ and the sparsity $\epsilon = \frac{1}{2}$.*

Proof. The case for $m = 1$, i.e., $d = 4$, is covered in Corollary 4.4.1. Hence we assume $m > 1$ here. If there exists a Hadamard matrix of order $2m$, then for $m > 1$, m must be even. We can use this Hadamard matrix of order $2m$ to construct Hadamard matrix of order $4m$ by taking its tensor product with the Hadamard matrix of order 2 [48]. Then using Hadamard matrix of order $4m$, we obtain Affine Resolvable $(4m, 2m, 2m-1)$-BIBD [93, 87]. Now following the Construction 4.3.1 and choosing the given real Hadamard matrix of order $2m$ in step 3, we obtain the desired ARMUB.

Since the design is Affine Resolvable, there are exactly same number of points are common between blocks from different resolution, which is $\frac{k^2}{v} = \frac{(2m)^2}{4m} = m$ implying $\beta = \sqrt{m}$. This also implies that the inner product between vectors from different basis would be of the form $\frac{1}{2m} \times w$, where w will be the sum of m many 1's putting ± before each 1. Since m is even and $d = 4m$, this implies $\Delta = \left\{0, \frac{2}{2m}, \frac{4}{2m}, \ldots, \frac{m}{2m}\right\} = \frac{1}{\sqrt{d}} \times \left\{0, \frac{2}{\sqrt{m}}, \frac{4}{\sqrt{m}}, \ldots, \frac{m}{\sqrt{m}}\right\}$.

In order to estimate σ, note that the maximum inner product between the vectors from different bases is $\frac{m}{2m} = \frac{1}{2}$ which implies $\sigma^2 \leq \left(\frac{1}{\sqrt{4m}} - \frac{1}{2}\right)^2 = \frac{1}{4} + \frac{1}{4m} - \frac{1}{\sqrt{4m}} \leq \frac{1}{4}$. Similarly $\tau \leq \left|\frac{1}{\sqrt{4m}} - \frac{1}{2}\right| \leq \frac{1}{2}$ and the sparsity $\epsilon = 1 - \frac{k}{d} = \frac{1}{2}$. Note that this k is the block size. □

In a first look, it appears that ARMUBs with $\beta = \sqrt{m}$ might not be very interesting. However, using this construction we get $d - 1$ many ARMUBs and β is not very large for certain moderate values of d. Let us take the example for $d = 64 = 4 \cdot 16$ and thus, $\beta \leq 4$. Here we obtain 63 ARMUBs. However, for the same dimension, our construction in the earlier work [67] provided only three β-ARMUBs respectively with $\beta \leq 4$. This is a significant improvement for this specific $d = 64$. For larger dimensions, this construction will provide significantly more number of ARMUBs than [67] but the value of β will be greater than 4.

Now we present the case for $d = 2^s$, where the existence of Hadamard matrix is guaranteed.

Corollary 4.4.5. *For $d = 2^s, s \geq 2$ there exist $2^s - 1$ many β-ARMUBs where $\beta \leq \sqrt{2^{s-2}}$, with $\sigma \leq \frac{1}{2}$, $\tau \leq \frac{1}{2}$ and with sparsity $\epsilon = \frac{1}{2}$.*

Proof. There always exists a Hadamard matrix of the order 2^n where $n \in \mathbb{N}$ (Sylvester construction [48]). Then in the Affine Resolvable $(4m, 2m, 2m-1)$-BIBD, one can substitute $m = 2^{s-2}$ with $s > 2$, and the result follows immediately. □

We conclude this section with the following remark that compares our construction idea for exact real MUBs with [98].

Remark 4.4.1. *Consider that w many MOLS(q) are available. Such a structure can be used to construct an RBD (X, A), such that $|X| = q^2$ having $w+2$ parallel classes, each having q blocks of constant size q and any two blocks from different parallel classes will have exactly one point in common. This idea follows from [93, Section 6.4.1, Theorem 6.32] in relating MOLS and Affine Plane. One may note that such an RBD will provide $w+2$ MUBs in $\mathbb{C}^d$ following our Construction 4.3.1. Further, if real Hadamard matrix of order q exists, then the construction will provide $w+2$ real MUBs in $\mathbb{R}^d$. Our numerical results related to exact MUBs in this direction will be the same as [98], but our construction is different and we have more flexibility of using different suitable unitary matrices. Further, our main focus here is the relaxed model of approximate MUBs, rather that exact ones, and their we have the opportunity of different avenues to explore through Construction 4.3.1, which we could not see immediately through the work of [98].*

In the next section we explore the designs which are not balanced, and that provide us further results in this direction.

4.5 ARMUBs using Resolvable Block Designs that are not Balanced

Now we will focus on resolvable block designs which are not balanced. This implies that either one or both the conditions given in 2 or 3 of BIBD (Definition 2.3.3) are not satisfied. However, these kinds of customized designs, for the purpose of obtaining ARMUBs provide generic and improved results. In the first construction, we use multiple Affine Resolvable BIBDs which are identical, and in the next one we add new elements in the design.

Theorem 4.5.1. *Consider $d = sq^2$, where q is a prime power and $sq \equiv 0 \bmod 4$. Assuming a real Hadamard matrix of order sq exists, we can construct $q+1$ many β-ARMUBs, where $\beta \leq \sqrt{s}$. Further, $\sigma \leq \sqrt{\frac{s}{d}}$, $\tau = \frac{1}{\sqrt{d}}$ for $1 \leq s \leq 4$ and $\tau = \frac{\sqrt{s}-1}{\sqrt{d}}$ for $s > 4$ and the sparsity $\epsilon = 1 - \frac{1}{q}$.*

Proof. We split $d = sq^2$ orthonormal vectors in s sets of q^2 vectors. Now for each set of q^2 vectors, one can construct Affine Resolvable $(q^2, q, 1)$-BIBD, where each one of them will have all blocks of size q and total $q+1$ many parallel classes, such that blocks from different parallel classes will have only one point in common. Now, consider the union of s such ARBIBDs, each having an identical structure, but different points. It will give resolvable design of sq^2 points, with each block of size of sq, consisting of $q+1$ many parallel classes, such that blocks from two different parallel classes will have exactly s points in common. If we assume that Hadamard matrix of order sq exits, that can be used to convert each parallel classes into orthonormal bases as in Construction 4.3.1. Thus we obtain $q+1$ many β-ARMUBs.

To explain the values in Δ, note that inner products between the vectors from different parallel classes would be of the form $\frac{1}{sq} \times w$, where w will be the sum of s many 1's putting $\pm$ before each 1. This implies $\Delta = \left\{0, \frac{2}{sq}, \frac{4}{sq}, \ldots, \frac{s}{sq}\right\}$ if s is even and $\Delta = \left\{\frac{1}{sq}, \frac{3}{sq}, \frac{5}{sq}, \ldots, \frac{s}{sq}\right\}$ if s is odd. Hence $\beta = \frac{\sqrt{d}}{q} = \sqrt{s}$.

The largest inner product value between the vectors from different parallel classes is equal to $\frac{1}{q}$. Further, we have $\max\left\{\frac{1}{\sqrt{d}}, \left|\frac{1}{\sqrt{d}} - \frac{1}{q}\right|\right\}$ is equal to $\frac{1}{\sqrt{d}}$ for $1 \leq s \leq 4$ and is equal to $\frac{1}{q} - \frac{1}{\sqrt{d}}$ for $s \geq 4$. Hence $\sigma^2 \leq \left(\frac{1}{\sqrt{sq}} - 0\right)^2$ for $1 < s \leq 4$, and $\sigma^2 \leq \left(\frac{1}{\sqrt{sq}} - \frac{1}{q}\right)^2$, for $s \geq 4$ which we can conveniently state as $\sigma \leq \sqrt{\frac{s}{d}}$. In order to ascertain τ, we have $\max\left\{\frac{1}{\sqrt{d}}, \left|\frac{1}{\sqrt{d}} - \frac{1}{q}\right|\right\}$ is equal to $\frac{1}{\sqrt{d}}$ for $1 \leq s \leq 4$ and is equal to $\frac{1}{q} - \frac{1}{\sqrt{d}}$ for $s \geq 4$. Hence $\tau = \frac{\sqrt{s}-1}{\sqrt{d}}$ for $s > 4$, else $\tau = \frac{1}{\sqrt{d}}$ for $s \leq 4$. The sparsity $\epsilon = 1 - \frac{k}{d} = 1 - \frac{1}{q}$, where k is the block size. □

This case subsumes the result in the previous chapter[67] for $s = 16$ and a prime q, i.e., $d = (4q)^2$. That is, with the method of [67], one can obtain $q + 1 = \frac{\sqrt{d}}{4} + 1$ ARMUBs such that for two vectors from different orthogonal bases, the inner product will be upper bounded by $\frac{4}{\sqrt{d}}$. This is the same quality result presented in Corollary 3.2.1 in the previous chapter (also available in [67, Corollary 1]). The clear extension in our case is that, here u can be any power of prime, whereas the construction given by [67] (as explained in the previous chapter) was applicable only to $d = (4q)^2$ for a prime q. For example, using above corollary, we can construct β-ARMUBs with $\beta \leq 4$, even for dimensions 4×9, 4×25 etc. However, one can not construct β-ARMUBs for these dimensions using the construction given in the last chapter. Thus this result subsumes the result of our previous work [67].

Now we present a result, where we can improve the number of MUBs as well as upper bound the inner product value. This we explore for a case where real Hadamard matrices exist. For this we have the following result.

Theorem 4.5.2. *Consider $d = q(q+1)$ such that q is a prime power and $q \equiv 3 \bmod 4$. Then we can construct $(q+1)$ many ARMUBs with $\Delta = \left\{0, \frac{1}{q+1}, \frac{2}{q+1}\right\}$, $\beta = 2\sqrt{\frac{q}{q+1}}$ and*

$\sigma_o^2\left(1-\frac{1}{\sqrt{d}}\right) \leq \sigma^2 \leq \sigma_o^2\left(1+\frac{1}{\sqrt{d}}\right)$, where $\sigma_o^2 = \frac{2}{d}\left(1-\sqrt{\frac{q}{q+1}}\right)$. Further, $\tau = \frac{1}{\sqrt{d}}$ and the sparsity is given by $\epsilon = 1-\frac{1}{q}$.

Proof. Consider an Affine Resolvable $(q^2, q, 1)$-BIBD. There will be $r = q+1$ parallel classes, consisting of q blocks each having q elements. Any two blocks from different parallel classes will have only one point in common. Add q more elements in the set X, which implies $|X| = q^2+q$. Add these q elements, one in each block of every parallel class. Now all the parallel classes will have blocks of size $q+1$ and the number of blocks will remain unchanged, which is q. In this situation, any block in a parallel class will have one element in common with $q-1$ blocks and two elements in common with the remaining block of any other parallel class. Hence we obtain a set of $q+1$ parallel classes each having q blocks and each block consisting of $q+1$ elements. This is the desired resolvable design.

Since $q \equiv 3 \bmod 4$, the Paley construction [75] will always provide real Hadamard matrix of order $q+1$. Hence we use this for constructing ARMUBs following Construction 4.3.1. Note that the blocks from different parallel classes have maximum two points in common, implying $\Delta = \left\{0, \frac{1}{q+1}, \frac{2}{q+1}\right\}$. In order to calculate σ, note that every block has only one point in common with $q-1$ blocks of any other parallel class and two points in common with the remaining blocks of that parallel class. Thus, any vector from one basis will have the inner product value of $\frac{1}{q+1}$ with $(q-1)(q+1)$ vectors and will have inner product either 0 or $\frac{2}{q+1}$ with $(q+1)$ vectors of any other orthogonal basis. Thus, we have

$$\left(\frac{1}{\sqrt{q(q+1)}}-\frac{1}{q+1}\right)^2(q-1)(q+1)+\left(\frac{1}{\sqrt{q(q+1)}}-\frac{2}{q+1}\right)^2(q+1) \leq d\times\sigma^2$$
$$\leq \left(\frac{1}{\sqrt{q(q+1)}}-\frac{1}{q+1}\right)^2(q-1)(q+1)+\left(\frac{1}{\sqrt{q(q+1)}}-0\right)^2(q+1).$$

This simplifies to $\sigma_o^2\left(1-\frac{1}{\sqrt{d}}\right) \leq \sigma^2 \leq \sigma_o^2\left(1+\frac{1}{\sqrt{d}}\right)$ where $\sigma_o^2 = \frac{2}{d}\left(1-\sqrt{\frac{q}{q+1}}\right)$.

On the other hand, there will be vectors between two different orthonormal bases which will also be orthogonal, corresponding to blocks having two points in common such that one gives $+1$ and another provides -1 in the inner product or vice versa, thereby, making the inner product between the vectors 0. Hence $\tau = \frac{1}{\sqrt{q(q+1)}} = \frac{1}{\sqrt{d}}$ and the sparsity would be given by $\epsilon = 1-\frac{1}{q}$. □

This result clearly shows that there are $\lceil\sqrt{d}\rceil$ real MUBs with $\beta < 2$ and it substantially improves the result of the last chapter [67] from both in number of MUBs as well as in terms of upper bound of the inner products. As numerical examples, for $d = 12, 56$, there would be respectively $4, 8$ ARMUBs of the above type.

For clarity, let us present the case for $q = 3$, i.e., $d = 3(3 + 1) = 12$. To begin with, consider the design of Affine Resolvable $(3^2, 3, 1)$-BIBD. Below we represent each parallel class as 3×3 matrix, where each row represent one block of the parallel class. Hence there would be 4 such matrices. Writing them explicitly

$$P_1 = \begin{pmatrix} 1 & 5 & 9 \\ 2 & 6 & 7 \\ 3 & 4 & 8 \end{pmatrix}, P_2 = \begin{pmatrix} 1 & 6 & 8 \\ 2 & 4 & 9 \\ 3 & 5 & 7 \end{pmatrix}, P_3 = \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}, P_4 = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}.$$

Now add three more points in the design, namely $\{10, 11, 12\}$, and as stated, one point is added in each block of every parallel class. The resulting parallel classes would be

$$P_1 = \begin{pmatrix} 1 & 5 & 9 & 10 \\ 2 & 6 & 7 & 11 \\ 3 & 4 & 8 & 12 \end{pmatrix}, P_2 = \begin{pmatrix} 1 & 6 & 8 & 10 \\ 2 & 4 & 9 & 11 \\ 3 & 5 & 7 & 12 \end{pmatrix}, P_3 = \begin{pmatrix} 1 & 4 & 7 & 10 \\ 2 & 5 & 8 & 11 \\ 3 & 6 & 9 & 12 \end{pmatrix}, P_4 = \begin{pmatrix} 1 & 2 & 3 & 10 \\ 4 & 5 & 6 & 11 \\ 7 & 8 & 9 & 12 \end{pmatrix}.$$

Above is the desired RBD, consisting of four parallel class, each having 3 blocks of constant size 4, such that between any two blocks from different parallel classes, either one or two points will be in common. The existence of real Hadamard matrix of order 4 will produce four ARMUBs here, with the inner product value bounded by $\frac{2}{q+1} = \frac{2}{4} = \frac{1}{2} < \frac{2}{\sqrt{d}} = \frac{2}{\sqrt{12}} = \frac{1}{\sqrt{3}}$.

As a passing remark, in the above construction of RBD, we can add q elements as one block in say, $(q + 1)$-th parallel class, and then one element of this block, into each block of all other parallel classes. This will make all the parallel classes to have q blocks of size $q + 1$ except the $(q + 1)$-th parallel class which will have $q + 1$ blocks each having size q. Each block of this parallel class will have only one element in common with any block of other parallel classes. Since q is a prime power, and if it is odd, we need a complex Hadamard matrix to convert $(q + 1)$-th parallel class into an orthonormal basis. This complex orthonormal basis would be mutually unbiased with all the other q sets of real orthonormal bases so constructed.

4.6 Conclusion

In this chapter we have described a generic approach that connects an object of combinatorial design, namely Resolvable Block Design (RBD) with Mutually Unbiased Bases (MUBs) which are structures on Hilbert spaces. We have presented a method which takes an RBD as input and use this to construct the orthonormal bases. The parallel classes of RBD play the most important role here. Each orthonormal basis is constructed out of a parallel class, and the parameters of the approximate MUBs are dependent on that of the parallel classes. Our construction method also exploits unitary matrices, dependent on the block sizes of a parallel class to generate the Approximate Real MUBs (in some cases MUBs too, but those are not main focus of this work). Throughout this chapter, we mostly concentrate on Hadamard construction while using the unitary matrices.

To characterize the approximate nature of the MUBs, we define certain parameters namely β, Δ, σ and τ. It has been shown that in most of the cases variance goes to zero as dimension increases, hence making the approximation quite close to the actual MUBs. In certain cases, where the variance is zero, exact MUBs are obtained. The sparsity ϵ has been characterized as the simple ratio of the number of zero elements divided by the total elements in the matrix that corresponds to a basis. In general, our construction provides very high sparsity and we obtain $\epsilon = 1 - \frac{1}{\sqrt{d}}$, in most of the cases.

In summary, we provide a generic approach for the first time to obtain ARMUBs for a large class of parameters that were not known earlier. The kinds of constructions we studied are different from the existing efforts in this domain of research. Thus, it will be interesting if these ideas can be extended further to obtain ARMUBs with improved inner product values or exact MUBs with more numbers than what is available in the state of the art literature. In this direction we present the idea of Almost Perfect MUBs in the next chapter where the conditions are more restrictive in terms of inner products.

Chapter 5

Almost Perfect MUBs

In this chapter we present a formalization of a specific subclass of Approximate MUBs. We propose the notion of Almost Perfect MUBs (APMUBs), where the absolute value of the inner product $|\langle v_1|v_2\rangle|$ can be restricted to two values, one being 0 and the other $\leq \frac{1+\mathcal{O}(d^{-\lambda})}{\sqrt{d}}$, such that $\lambda > 0$ and the numerator $1 + \mathcal{O}(d^{-\lambda}) \leq 2$. The vectors so constructed has the important features that large number of its component are zero (similar to what we noted in the previous chapter) and more than that, the non-zero components are of equal magnitude. Our techniques in this chapter are based on combinatorial structures related to Resolvable Block Designs (RBDs) as in the previous chapter, but we exploit the combinatorial structures more cleverly to produce large number of APMUBs having very good parameters for composite dimensions.

First we show that for a general composite dimension $d = k \times s$, $k, s \in \mathbb{N}$, with $k \leq s \leq 4k$, one can construct at least $N(s) + 1$ many APMUBs, where $N(s)$ is the number of Mutually Orthogonal Latin Squares (MOLS) of order s. Even when restricted to $\mathbb{R}^d$, we can construct similar number of real APMUBs, whenever real Hadamard matrix of order k can be constructed. Further, if $s = q$, where q power of prime, we have $N(q) = q - 1$. This enables us to construct $q \sim \mathcal{O}(\sqrt{d})$ many APMUBs.

More appropriate and novel combinatorial designs are presented in this regard that extend to composite dimensions of the form $d = (q - e)(q + f), e, f \in \mathbb{N}$, with $0 \leq f \leq e$ and q some power of prime. Our technique produces $\mathcal{O}(\sqrt{d})$ many APMUBs for these cases, when e, f are constants. We estimate that, such kind of composite dimensions are at least as numerous as the prime numbers in the set of positive integers $\mathbb{N}$. Our result has important implications towards Bi-angular vectors. We show that, APMUBs so constructed in $\mathbb{C}^d$ or $\mathbb{R}^d$, provide sets of Bi-angular vectors which are of the order of $\mathcal{O}(d^{3/2})$ in numbers (here the upper bound is $\mathcal{O}(d^2)$). These constructions of APMUBs have several interesting properties and the resulting structures may have applications in quantum information, coding theory, weighing matrices and association schemes.

5.1 Introduction

In the two previous contributory chapters, we have used different combinatorial structures to produce Approximate MUBs. We obtain a significant number of orthonormal bases on dimension d such that for any two vectors from two different bases, the inner product may deviate from $\frac{1}{\sqrt{d}}$. Now accepting the approximation, what could be the logical way of formalization. In this direction two points are important.

1. Can we restrict the nonzero values in $[\frac{1}{\sqrt{d}}, \frac{2}{\sqrt{d}}]$, and more towards $\frac{1}{\sqrt{d}}$?
2. Can we have only two-valued spectra? That is, for inner products between the vectors from two different matrices, the magnitude of nonzero values should be the same. In fact, some of the values may be zero too considering the vectors from two matrices.

We answer both questions affirmatively. The second point can be seen as follows. In the set of an orthonormal basis, any two vectors are perpendicular to each other. As d grows larger, it is clear that $\frac{\beta}{\sqrt{d}}$ becomes small, for $1 \leq \beta \leq 2$. Now if the inner product between two vectors from different bases is zero, then they are orthogonal. Else, if it is $\frac{\beta}{\sqrt{d}}$, then also being very small, the angle between them is close to a right angle. Now each basis has d many vectors, and for certain parameters we show that we can have $\mathcal{O}(\sqrt{d})$ such APMUBs. Thus, in total we obtain $\mathcal{O}(d^{3/2})$ vectors which are either perpendicular or almost perpendicular (having the same angle) to each other. These are known as Bi-angular vectors. Such vectors have received serious attention in literature [73], and constructions have been proposed for $\mathcal{O}(d^2)$ vectors. However, the angles are smaller in the construction of [73] compared to our results that are achieved through the APMUBs.

That is, our formalization of the approximation provides connections to interesting combinatorial structures. Let us now explain the contribution and organization of this chapter in more details.

5.2 Contribution & Organization

In this chapter we begin with Section 5.3 to present a background of related combinatorial objects. Then towards the constructions, in Section 5.4, we show bounds on the values of certain parameters, expressed in terms of the block size k and number of elements in the RBD, i.e., d. In this regard, we define a combinatorial quantity $\mathcal{T}(d, k, \mu)$, relevant to our analysis, which can be of its own independent interest. Thereafter in Lemma 5.4.3 we describe an interesting class of RBDs which can be constructed from MOLS(s) yielding $\mu = 1$ and $r = N(s) + 2$. A constructive proof to obtain the same from MOLS(s) has also been given and in Lemma 5.4.4. We further show that the converse of Lemma 5.4.3 is also true. The results are further explained with illustrative examples.

Then we consider the Almost Perfect MUBs (APMUBs) and some generic ideas of construction in Section 5.5. The basic motivation and its relationship with Bi-angular vectors are presented in Section 5.5.1. In Section 5.5.2, we analyze certain properties of the AMUBs which can be constructed using RBDs having blocks of constant size. In this direction, we consider RBD(X, A) with $|X| = d = k \times s = (q - e)(q + f)$ and A with resolution r, where each block is of size $(q - e)$. We study the asymptotic behaviours of the parameters of AMUBs thus generated. It is also shown that our construction can provide APMUBs only when $\mu = 1$, therefore putting strong constraints over the nature of the RBDs required for this kind of constructions.

Section 5.6 contains our algorithms towards constructing RBDs that can be consequently used for obtaining APMUB's with parameters that could be achieved for the first time. We first show that whenever the dimension d is a composite number and can be expressed as $k \times s, k \leq s$, such that $\beta = \sqrt{\frac{s}{k}} \leq 2$, one can construct $N(s) + 1$ many APMUBs, where $N(s)$ is the number of MOLS(s). We refer to this as the MOLS Lower Bound Construction for APMUBs. Since a composite number d can be factored in multiple ways ensuring $\beta \leq 2$, there can be more than one MOLS Lower Bound Constructions for a dimension d. It is to be noted that if $s = q$, some power of prime, then $N(q) = q - 1$. Hence in such situations we get q many APMUBs. The best known asymptotic bound for $N(s)$ is given by $N(s) \to \mathcal{O}(s^{\frac{1}{14.8}})$, which generally results into a small number of APMUBs. In this direction we show that when $d = (q - e)(q + f), e, f \in \mathbb{N}$ and $e \geq f$, where q is some power of prime, we can obtain $\mathcal{O}(q)$ many APMUBs. Illustrative examples to describe the above construction have also been provided. In addition to this, we have highlighted that for a certain form of the composite dimension d, it might be hard to obtain construction techniques for developing APMUBs that could beat the MOLS Lower Bound Construction.

5.3 Background

Let us recapitulate a few definitions that were already discussed in the background (Chapter 2). We describe it again here towards better consistency in following the technical results in this chapter. A combinatorial block design is a pair (X, A), where X is a set of elements, called elements, and A is a collection of non-empty subsets of X, called blocks. A combinatorial design is called simple, if there is no repeated block in A. Generally all the combinatorial designs are assumed to be simple, i.e., they do not have any repeated blocks.

Definition 5.3.1. *A combinatorial design (X, A) is a t-(d, k, λ) design if each block in A is of size k, and that any set of t elements from X, appears as subset of exactly λ blocks in A. Note that here t, d, k and λ are positive integers with $1 < k < d$.*

As we have already discussed, Resolvable Block Design (RBD) is a special kind of Combinatorial design, where the set A can be partitioned into parallel classes which are called resolutions of A. This combinatorial structure was proposed in the context of Balanced Incomplete Block Design [15, 16, 17]. Later various generalizations could be achieved as explained in varied literatures [88, 56, 78, 53].

Definition 5.3.2. *Combinatorial design (X, A), is called a Resolvable Block Design (RBD), if A can be partitioned into $r \geq 1$ parallel classes, called resolutions. Where a parallel class in design (X, A) is a subset of the disjoint blocks in A whose union is X.*

As discussed earlier, there is a special kind of RBD called the Affine Resolvable BIBD (ARBIBD) [16, 17, 87] (see also [93, Chapter 5]). It is well known that whenever q is some power of a prime, one can construct $(q^2, q, 1)$ ARBIBD. An Affine plane of order q is an example of this. Here $|X| = q^2$, and A consists of $q(q+1)$ blocks, which can be resolved into $q+1$ many parallel classes. Each parallel class consists of q many blocks of constant size q. Most importantly, any pair of blocks from different parallel classes has exactly one element in common. Affine Planes are known only when q is power of a prime. For more details, one may refer to [93, Sections 2.3, 5.2, 5.3, 6.4].

Let us define a few notations that we will use in the context of this chapter. For RBD(X, A), with $|X| = d$, we will indicate the elements (also called elements) of X by simple numbering, i.e., $X = \{1, 2, 3, \ldots, d\}$. Here r will denote the number of parallel classes in RBD and parallel class will be represented by $P_1, P_2, \ldots, P_r$. The blocks in the l^{th} parallel class will be represented by $\{b_1^l, b_2^l, \ldots, b_s^l\}$, indicating that the l^{th} parallel class has s many blocks. Since in our entire analysis we will be using RBDs with constant block size, let us denote the block size by k. Further, we denote the number of blocks in a parallel class of RBD by s. Since in our analysis we are making of use of RBDs with constant block size, hence each parallel class will always have s many blocks and $|X| = d = k \times s$. The notation b_{ij}^l would represent the j^{th} element of the i^{th} block in the l^{th} parallel class. Further, the notation b_i^l would represent i^{th} block of l^{th} parallel class. Note that $b_{ij}^l \in X$. In every block, we will arrange the elements in increasing order, and we will follow this convention throughout the paper, unless mentioned specifically. Thus $b_{ij}^l \leq b_{i,j+1}^l$, $\forall j$. This will be important to revisit when we convert the parallel classes into orthonormal bases. Another important parameter for our construction is the value of the maximum number of common elements between any pair of blocks from different parallel classes. We denote this positive integer by μ. Note that $\mu \geq 1$ for any RBD, with $r \geq 2$. One may further refer to Lemma 5.4.2 of Section 5.4 in this regard. We also like to refer to Section 2.4 in Chapter 2 for the background on MOLS (Mutually Orthogonal Latin Square). With this, let us describe a few technical results.

5.4 Some Important Technical Results

Let us now consider a counting of combinatorial objects that is relevant to us.

Definition 5.4.1. *Let $\mathcal{T}(d,k,\mu)$, $0 \leq \mu < k < d$ be the maximum number of subsets each of size k, that can be constructed from d distinct objects, such that, between any two different subsets there is a maximum of μ objects in common.*

First we should relate with the error correcting codes, as this can be seen as the maximum number of codewords of the binary constant weight codes of length d and weight k with minimum distance $2(k-\mu)$. For more details in this regard one may refer to [51, Theorem 2.3.6], but we will only restrict here to some technical results only. One may immediately note that $\mathcal{T}(d,k,0) = \left\lfloor \frac{d}{k} \right\rfloor$, and $\mathcal{T}(d,k,k-1) = \binom{d}{k}$. For arbitrary $d,k,\mu \in \mathbb{N}$, the following result provides an estimate of $\mathcal{T}(d,k,\mu)$.

Lemma 5.4.1. $\mathcal{T}(d,k,\mu) \leq \left\lfloor \frac{\binom{d}{\mu+1}}{\binom{k}{\mu+1}} \right\rfloor = \left\lfloor \frac{d!(k-\mu-1)!}{k!(d-\mu-1)!} \right\rfloor$. *The upper bound of* $\left\lfloor \frac{d!(k-\mu-1)!}{k!(d-\mu-1)!} \right\rfloor$ *is achieved whenever $(\mu+1)-(d,k,1)$ design exists and in such cases $\mathcal{T}(d,k,\mu)$ is the same as the number of blocks in $(\mu+1)-(d,k,1)$ design as in Definition 5.3.1.*

Proof. Given a set of d distinct elements, we like to construct the maximum number of subsets each of size k, such that any two subsets has μ elements in common. Let us label these blocks as $\{b_1, b_2, \ldots b_r\}$, with $r = \mathcal{T}(d,k,\mu)$.

Now consider all the $(\mu+1)$-element subsets of d distinct elements. They will be $\binom{d}{\mu+1}$ in numbers. Now consider the blocks b_i and b_j. Since there are a maximum of μ elements in common, any $(\mu+1)$-element subset of d elements cannot exist, which occur in both the blocks b_i and b_j. Since each block b_i is of size k, the number of $(\mu+1)$-element subsets which can be constructed by the k elements in b_i is $\binom{k}{\mu+1}$. Let us denote this set by S_i. Similarly for block b_j the number of $(\mu+1)$-element subsets which can be constructed with its k elements is $\binom{k}{\mu+1}$. Let us denote this set by S_j. We have already seen $S_i \cap S_j = \phi$, else there would be $\mu+1$ element common between b_i and b_j. Now since there are r such blocks each of size k, hence $|S_1| + |S_2| + \ldots |S_r| = r\binom{k}{\mu+1}$. This must be less than or equal to $\binom{d}{\mu+1}$, which is the maximum possible $(\mu+1)$-element subsets that can be constructed from d distinct elements. This implies $r\binom{k}{\mu+1} \leq \binom{d}{\mu+1} \Rightarrow \mathcal{T}(d,k,\mu) = r \leq \left\lfloor \frac{\binom{d}{\mu+1}}{\binom{k}{\mu+1}} \right\rfloor = \left\lfloor \frac{d!(k-\mu-1)!}{k!(d-\mu-1)!} \right\rfloor$.

To see the second part of the lemma, note that $t-(d,k,1)$ design is a design (X,A) where A contains the subsets of X called blocks, such that $|X|=d$ and each block contains exactly k elements. Every t-element subset of X is contained in exactly one block. Hence this implies that any two blocks of the design has maximum $t-1$ elements in common. Thus it immediately follows that if $(\mu+1)-(d,k,1)$ design exists, then blocks of the design satisfies the property of $\mathcal{T}(d,k,\mu)$, and since number of blocks in $(\mu+1)-(d,k,1)$ design is $\frac{\binom{d}{\mu+1}}{\binom{k}{\mu+1}}$ [93, Chapter 9, Theorem 9.4 and the following observation], which is exactly the upper bound of $\mathcal{T}(d,k,\mu)$ as proven above. □

The upper bound of $\mathcal{T}(d,k,\mu)$ is achieved whenever a $(\mu+1)-(d,k,1)$ design exists, which is known for many values of $0\leq\mu<k<d$. This implies that the bound for $\mathcal{T}(d,k,\mu)$ given by the above result is tight. However, getting an exact value/expression of $\mathcal{T}(d,k,\mu)$ appears to be an open and challenging problem.

To construct the AMUBs, our focus has been on RBDs with constant block size. In this connection we now focus on few results that are relevant to our constructions of APMUBs in Section 5.6. Following is a lemma related to an RBD providing a bound for μ and r in terms of the block size and the number of blocks in parallel classes where, as defined previously, μ is the maximum number of common elements between any pair of blocks from different parallel classes and r is the number of parallel classes.

Lemma 5.4.2. *Consider an RBD(X,A) with $|X|=d=k\times s$ where $k,s\in\mathbb{N}$, consisting of $r>1$ parallel classes, each having blocks of size k. Then $\mu\geq\lceil\frac{k}{s}\rceil$, where μ is the maximum number of common elements between any pair of blocks from different parallel classes and $r\leq\mathcal{T}(d-1,k-1,\mu-1)$. Further, if $\mu=1$, then $r\leq\lfloor\frac{d-1}{k-1}\rfloor=s+\lfloor\frac{s-1}{k-1}\rfloor$.*

Proof. Since $r>1$, consider any pair of parallel classes of RBD say (P_l,P_m). Denote the blocks of P_l be as $b_1^l,b_2^l,\ldots,b_s^l$. Since blocks are of constant size $\Rightarrow|b_i^l|=k$ and the blocks belonging to the same parallel class have no element in common, $\Rightarrow b_i^l\cap b_j^l=\phi\;\forall\,i,j=1,2,\ldots,s$ and $X=b_1^l\cup b_2^l\cup\ldots\cup b_s^l$, $|X|=k\times s$. Similar relations will hold for blocks of any other parallel class.

Consider any block of P_l, say b_i^l. Since, $\mu=\max_m|b_i^l\cap b_j^m|$, we have $b_i^l\cap b_j^m\leq\mu,\;\forall\;j=1,2,\ldots,s$. Since $X=b_1^m\cup b_2^m\cup\ldots\cup b_s^m$, hence, $\sum_{j=1}^s|b_i^l\cap b_j^m|=|b_i^l|=k$. We also have $\sum_{m=1}^s|b_i^l\cap b_j^m|\leq\sum_{m=1}^s\mu=\mu s\Rightarrow k\leq\mu s$. Since $k,s,\mu\in\mathbb{N}$, we get $\mu\geq\lceil\frac{k}{s}\rceil$. This implies minimum value of $\mu=1$ which is possible only if $k\leq s$ and on the other hand if $k>s$, then minimum value of $\mu=2$. Thus, for $\mu=1$, we must have $k\leq s$, i.e., number of blocks must be greater than or equal to the block size of the RBD.

To obtain a bound on r, fix an element, say $x\in X$. Since the blocks of a parallel class are mutually disjoint and their union is X, each parallel class will have exactly one block which will contain x. Collect all the blocks that contain the element x and we will obtain a set of r such blocks. Denote this set by S. Now, remove x from every block in the set S. Hence S will consist of blocks of size $k-1$, the maximum number of common elements between any two blocks in S would be now $(\mu - 1)$ and the total number of elements contained in these r blocks will be $\leq (d-1)$. Therefore, we obtain $r \leq \mathcal{T}(d-1, k-1, \mu-1)$. Thus if $\mu = 1$ we have $r \leq \mathcal{T}(d-1, k-1, 0) = \lfloor \frac{d-1}{k-1} \rfloor = \lfloor \frac{s \cdot k-1}{k-1} \rfloor = s + \lfloor \frac{s-1}{k-1} \rfloor$. □

We will see that, using our construction method for APMUBs, the necessary condition on RBDs is $\mu = 1$. Hence our effort will be to construct RBDs with $\mu = 1$. For this to happen, $k \leq s$ and $r \leq s + \lfloor \frac{s-1}{k-1} \rfloor$.

5.4.1 Results relating to MOLS

We will now consider a class of Resolvable Block Designs (X, A) such that $|X| = s^2$, which can be constructed from a set of w-MOLS(s). Here A consists of blocks having constant size s, which can be resolved into $w+2$ many parallel classes, each having s many blocks, such that blocks from two different parallel classes have exactly one element in common. Through the following construction, we explain a simple and direct way to convert a set of w many MOLS(s) into such an RBD(X, A).

Construction 5.4.1. *To construct an RBD having $w+2$ number of parallel classes from w-MOLS(s) using the following steps.*

1. *Define M_{ref}, which is a $s \times s$ array where each cell consists of one of the elements from $X = \{1, 2, \ldots, s^2\}$, as follows:*

$$M_{ref} = \begin{bmatrix} 1 & 2 & 3 & \ldots & s \\ s+1 & s+2 & s+3 & \ldots & 2s \\ 2s+1 & 2s+2 & 2s+3 & \ldots & 3s \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (s-1)s+1 & (s-1)s+2 & (s-1)s+3 & \ldots & s^2 \end{bmatrix}, L_k = \begin{bmatrix} l^k_{11} & l^k_{12} & \ldots & l^k_{1s} \\ l^k_{21} & l^k_{22} & \ldots & l^k_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ l^k_{s1} & l^k_{n2} & \ldots & l^k_{ss} \end{bmatrix}$$

2. *Consider a Latin Square L_k, from the set of w-MOLS(s). Let $(L_k)_{ij} = l^k_{ij}$ as indicated above.*

3. *Corresponding to the Latin Square L_k, construct a parallel class P_k consisting of s disjoint blocks b^k_t, each of size s as follows,*

$$b^k_t = \{(M_{ref})_{ij} : l^k_{ij} = t\}, \ \textit{where } i, j \in \{1, 2, \ldots, s\}.$$

Each row of the the Latin Square is a permutation of $\{1, 2, \ldots, s\}$. Hence, there will be a pair (i, j) in each row for which $l^k_{ij} = t$. Thus, the blocks P^k_t will have a total s elements, one from each row and column of M_{ref}. Since $t = \{1, 2, \ldots, s\}$, there will be s blocks. Thus we are essentially collecting all the elements of M_{ref} corresponding to a particular symbol t of L_k in one block b^k_t, and together the blocks b^k_i where $i = \{1, 2, \ldots, s\}$ form a parallel class P_k.

4. *Repeat the above step for all Latin Squares in the set of w-$MOLS(s)$, thereby giving w many parallel classes.*

5. *Construct two more parallel classes, one using the horizontal rows of M_{ref}, and other using the vertical rows of M_{ref} as follows:*

$$P_0 = \big\{(1, 2, \ldots, s), (s + 1, s + 2, \ldots, 2s), \ldots ((s - 1)s + 1, (s - 1)s + 2, \ldots, s^2)\big\}$$
$$P_\infty = \big\{(1, s + 1, \ldots, (s - 1)s + 1), (2, s + 2, \ldots, (s - 1)s + 2), \ldots, (s, 2s, \ldots, s^2)\big\}$$

6. *The $RBD(X, A)$ with $X = \{1, 2, 3, \ldots, s^2\}$ and $A = \{P_0, P_\infty, P_1, P_2, \ldots, P_w\}$ is the desired outcome.*

Lemma 5.4.3. *A set of w many MOLS(s) can be used to construct an RBD(X, A) such that $|X| = s^2$, consisting of constant block sizes, each having s elements, that can be resolved into $w + 2$ many parallel classes. Here, any two blocks from different parallel classes will have exactly one element in common.*

Proof. We claim that, any pair of blocks from different parallel classes $\{P_0, P_\infty, P_1, P_2, \ldots P_w\}$ constructed above has exactly one element in common. Consider the t^{th} and s^{th} blocks of k^{th} and m^{th} parallel classes respectively. Then

$$P^k_t \cap P^m_s = \{(M_{ref})_{ij} : l^k_{ij} = t\} \cap \{(M_{ref})_{ij} : l^m_{ij} = s\}.$$

Now since L^k and L^m are the orthogonal Latin Squares, there will be exactly one pair (i, j) such that, $(L^k)_{ij} = t$ and $(L^m)_{ij} = s$. Hence exactly one element will be common between the blocks P^k_t and P^m_s.

From the construction of P_0 and P_∞, it is clear that any block has exactly one element in common. Since any block of P^k_t is picking one element from each row and each column of M_{ref}, each block of P^k_t will have exactly one element in common with blocks of P_0 and P_∞, which are collection of horizontal rows (P_0) and vertical rows (P_∞) of M_{ref}. □

We will now sketch the idea of the above method with a simple example to convert a 2-MOLS(5) into 4 parallel classes.

Example 5.4.1. *Let us consider the* 2*-MOLS*(5) *and* M_{ref} *as follows.*

$$L_1 = \begin{bmatrix} 5 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \end{bmatrix}, L_2 = \begin{bmatrix} 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}, M_{ref} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{bmatrix}.$$

We use a 5×5 *Reference Matrix* M_{ref} *consisting of elements indicated by* $\{1, 2, \ldots, 25\}$. *We put them in a simple row wise increasing sequence, which is to ensure that each element occur only once in the matrix* M_{ref}. *Now corresponding to each MOLS* L_1 *and* L_2, *we construct a parallel class, as per the Construction 5.4.1, thereby forming blocks of* P_1 *and* P_2 *by picking elements from* M_{ref}.

$$P_1 = \{(2,6,15,19,23),(3,7,11,20,24),(4,8,12,16,25),(5,9,13,17,21),(10,14,18,22,1)\},$$
$$P_2 = \{(2,10,13,16,24),(3,6,14,17,25),(4,7,15,18,21),(5,8,11,19,22),(1,9,12,20,23)\}.$$

The remaining two parallel classes will be constructed using horizontal and vertical elements of M_{ref} *as follows:*

$$P_0 = \{(1,2,3,4,5),(6,7,8,9,10),(11,12,13,14,15),(16,17,18,19,20),(21,22,23,24,25)\},$$
$$P_\infty = \{(1,6,11,16,21),(2,7,12,17,22),(3,8,13,18,23),(4,9,14,19,24),(5,10,15,20,25)\}.$$

Let us now consider the construction in the other way, i.e., the converse.

Construction 5.4.2. *Consider an RBD*(X, A), *where* $|X| = s^2$ *and* A *consist of* $w + 2$ *numbers of parallel classes such that, each block of a parallel class is of a constant size* s *and any pair of blocks from different parallel classes have exactly one element in common. Let us denote the elements of* X *by* $\{1, 2, \ldots, s^2\}$, *parallel classes by* $\{P_0, P_\infty, P_1, \ldots, P_w\}$, *and the blocks of* P_l *by* b_i^l. *Since there are* s *blocks in each parallel class, therefore* $P_l = \{b_1^l, b_2^l, \ldots, b_s^l\}$. *Let* s *distinct symbols for construction of the Latin Squares be denoted by* $Y = \{y_1, y_2, \ldots, y_s\}$. *Now construct* w*-MOLS*(s) *using RBD*(X, A) *as follows.*

1. *Use* P_0 *and* P_∞ *to construct a reference matrix* M_{ref} *having elements from* $\{1, 2, \ldots, s^2\}$ *in the following manner:*

$$M_{ref} = \begin{bmatrix} b_1^0 \cap b_1^\infty & b_1^0 \cap b_2^\infty & \ldots & b_1^0 \cap b_s^\infty \\ b_2^0 \cap b_1^\infty & b_2^0 \cap b_2^\infty & \ldots & b_2^0 \cap b_s^\infty \\ \vdots & \vdots & \ldots & \vdots \\ b_s^0 \cap b_1^\infty & b_s^0 \cap b_2^\infty & \ldots & b_s^0 \cap b_s^\infty \end{bmatrix}.$$

Here M_{ref} *contains all the elements of* X *exactly once. As any two blocks from different parallel classes have exactly one element in common, if* $(M_{ref})_{ij} = (M_{ref})_{lm}$ *then* $b_i^0 \cap$

$b_j^{\infty} = b_l^0 \cap b_m^{\infty}$, and that implies all the blocks $\{b_i^0, b_l^0, b_j^{\infty}, b_m^{\infty}\}$ have one element in common. Here, b_i^0 and b_l^0 are the blocks in the Parallel class P_0. Similarly, b_j^{∞} and b_m^{∞} are the blocks of the parallel class P_{∞}. Since blocks in a Parallel class are mutually disjoint, this is not possible, i.e., $(M_{ref})_{ij} \neq (M_{ref})_{lm}$.

2. *Corresponding to the parallel class P_k, construct the Latin Squares L_k as follows*

$$\textit{if } (M_{ref})_{ij} \in b_t^k \textit{ then } (L_k)_{ij} = y_t.$$

That is, we are substituting y_t, wherever the element of the block b_t^k is appearing in M_{ref} to construct L_k. Note that L_k is a Latin Square. Since $X = b_1^k \cup b_2^k \dots b_s^k$, for every $(M_{ref})_{ij}$ there will be one b_t^k such that $(M_{ref})_{ij} \in b_t^k$ and since $b_i^k \cap b_j^k = \phi$, $i, j \in \{1, 2, \dots, s\}$, for each $(M_{ref})_{ij}$, there will be a unique b_t^k such that $(M_{ref})_{ij} \in b_t^k$. Now if L_k is not a Latin square, then there would be at least a pair of (i_1, i_2) corresponding to which $(L_k)_{i_1 j} = (L_k)_{i_2 j}$ or a pair of (j_1, j_2) corresponding to which $(L_k)_{ij_1} = (L_k)_{ij_j}$. Consider $(L_k)_{i_1 j} = (L_k)_{i_2 j}$. This implies if $x_1 = (M_{ref})_{i_1 j} = b_{i_1}^0 \cap b_j^{\infty} \in b_t^k$ and $x_2 = (M_{ref})_{i_2 j} = b_{i_2}^0 \cap b_j^{\infty} \in b_t^k$. Thus x_1 and $x_2 \in b_j^{\infty}$. Hence $|b_t^k \cap b_j^{\infty}| \geq |\{x_1, x_2\}| = 2$ as $x_1 = (M_{ref})_{i_1 j} \neq (M_{ref})_{i_2 j} = x_2$. This is a contradiction as there is exactly one element common between the blocks of different parallel classes, here P^{∞} and P^k. Similarly it can be argued that $(L_k)_{ij_1} \neq (L_k)_{ij_j}$ for any pair of (j_1, j_2).

3. *Repeat the above step for each of the parallel class P_k, $k = 1, 2, \dots, w$, thereby constructing the set of w Latin squares viz $\{L_1, L_2, \dots, L_w\}$.*

The converse of Lemma 5.4.3 is as follows.

Lemma 5.4.4. *Given an RBD(X, A), where $|X| = s^2$ and consisting of $w + 2$ many parallel classes such that, each block of a parallel class is of a constant size s and any pair of blocks from different parallel classes have exactly one element in common. Then RBD(X, A) can be used to construct w-MOLS(s).*

Proof. We claim that the set of Latin squares $L_1, L_2, \dots, L_w$ as constructed above are Mutually Orthogonal Latin Squares of order s.

Recalling that a pair of Latin Squares L_1 and L_2 of same order and constructed from the entries from the same set Y is called mutually orthogonal, if the ordered pair $((L_1)_{ij}, (L_2)_{ij}) \in \{(Y, Y)\}$ appears exactly once.

Consider the ordered pair, $((L_k)_{ij}, (L_m)_{ij})$. Assume that, L_k and L_m are not Mutually Orthogonal Latin Squares, which implies that, there would be at least one pair of Indices $\{(i, j), (u, v) : (i, j) \neq (u, v)\}$ such that, $((L_k)_{ij}, (L_m)_{ij}) = ((L_k)_{uv}, (L_m)_{uv}) = (y_p, y_q)$. Let $y_p = (L_k)_{ij} \in b_p^k$ and $y_q = (L_m)_{ij} \in b_q^m$. This implies $(M_{ref})_{ij} \in b_p^k$ and b_q^m. Similarly, $y_p = (L_k)_{uv} \in b_p^k$ and $y_q = (L_m)_{uv} \in b_q^m$ which implies $(M_{ref})_{uv} \in b_p^k$ and b_q^m. However, then we will have, $b_p^k \cap b_q^m = \{(M_{ref})_{ij}, (M_{ref})_{uv}\}$, but if $(i,j) \neq (u,v)$ then $(M_{ref})_{ij} \neq (M_{ref})_{uv}$. Thus, $|b_p^k \cap b_q^m| \geq 2$ which contradicts the fact that $|b_p^k \cap b_q^m| = 1$. Hence we conclude that L_k and L_m are Mutually Orthogonal Latin Squares. □

We now sketch the above method with an example to obtain a 2-MOLS(5) from 4 parallel classes.

Example 5.4.2. *If we proceed with the same set of* 4 *parallel classes obtained as in Example 5.4.1, it would naturally result into the same pair of MOLS*(5)*, i.e., L_1 and L_2, with which we have started Example 5.4.1. Therefore, we consider a different set of* 4 *parallel classes as follows:*

$$\begin{aligned}
P_0 &= \{(1,2,3,4,5),(6,7,8,9,10),(11,12,13,14,15),(16,17,18,19,20),(21,22,23,24,25)\}\,,\\
P_\infty &= \{(1,6,11,16,21),(2,7,12,17,22),(3,8,13,18,23),(4,9,14,19,24),(5,10,15,20,25)\}\,,\\
P_1 &= \{(1,9,12,20,23),(2,10,13,16,24),(3,6,14,17,25),(4,7,15,18,21),(5,8,11,19,22)\}\,,\\
P_2 &= \{(1,7,13,19,25),(2,8,14,20,21),(3,9,15,16,22),(4,10,11,17,23),(5,6,12,18,24)\}\,.
\end{aligned}$$

Note that, P_0 and P_∞ are taken as above for convenience, providing the M_{ref} with elements from $X = \{1,2,\ldots,25\}$. Observe that any pair of blocks from different parallel classes have exactly one element in common. Now corresponding to $s = 5$, we simply use $Y = \{1,2,3,4,5\}$ as five symbols to construct the Latin square. The remaining parallel classes P_1 and P_2 are used to construct L_1 and L_2 respectively, which are the required 2*-MOLS*(5)*. Following the Construction 5.4.2 above, we obtain Orthogonal Latin Squares L_1 and L_2 as follows:*

$$M_{ref} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{bmatrix}, \quad L_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{bmatrix}, \quad L_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}.$$

Based on this we now proceed for our generic construction idea in the next section.

5.5 Definition of APMUBs and general construction ideas

In this section we first present the motivation of proposing such a combinatorial object and then proceed with the general construction ideas.

5.5.1 Motivation for defining APMUBs and its Characteristics

Consider a pair of orthonormal bases, say M_l and M_m. If they are β-AMUBs then $|\langle\psi_i^l|\psi_j^m\rangle| \leq \frac{\beta}{\sqrt{d}}$, where β is bounded by some constant. The definition of β-AMUBs does not rule out $|\langle\psi_i^l|\psi_j^m\rangle| = 0$. Let for $\mathfrak{n}_1$ pairs, the value of $|\langle\psi_i^l|\psi_j^m\rangle|$ be 0, and for the remaining pairs $\mathfrak{n}_2$, the value of $|\langle\psi_i^l|\psi_j^m\rangle|$ be non-zero ($\neq 0$). If $|\langle\psi_i^l|\psi_j^m\rangle| = \frac{\beta_{ij}}{\sqrt{d}}$ (say), then $\frac{\beta_{ij}}{\sqrt{d}} \leq \frac{\beta}{\sqrt{d}}$. Since $\sum_{ij}^{d} |\langle\psi_i^l|\psi_j^m\rangle|^2 = d$. Therefore,

$$\mathfrak{n}_1 \cdot 0 + \sum_{\substack{i,j=1 \\ |\langle\psi_i^l|\psi_j^m\rangle|\neq 0}}^{d} \left(\frac{\beta_{ij}}{\sqrt{d}}\right)^2 = d \Rightarrow \mathfrak{n}_2 \frac{\beta_{\min}^2}{d} \leq d \leq \mathfrak{n}_2 \frac{\beta_{\max}^2}{d},$$

where, $\beta_{\min} = \min_{ij} \beta_{ij}$ and $\beta_{\max} = \max_{ij} \beta_{ij}$ This implies,

$$\mathfrak{n}_2 \frac{\beta_{\min}^2}{d^2} \leq 1 \leq \mathfrak{n}_2 \frac{\beta_{\max}^2}{d^2}.$$

Note that, $\mathfrak{n}_1 + \mathfrak{n}_2 = d^2 \Rightarrow \frac{\mathfrak{n}_1}{d^2} = 1 - \frac{\mathfrak{n}_2}{d^2}$, then we have,

$$1 - \frac{1}{\beta_{\min}^2} \leq \frac{\mathfrak{n}_1}{d^2} \leq 1 - \frac{1}{\beta_{\max}^2}. \tag{5.1}$$

Note that, $\frac{\mathfrak{n}_1}{d^2}$ is the probability of randomly selecting two orthogonal vectors from two different bases. Therefore, if $\beta_{\min} = \beta = \beta_{\max}$, i.e., $\Delta = \{0, \frac{\beta}{\sqrt{d}}\}$ and $\beta = 1 + \mathcal{O}(d^{-\lambda}), \lambda > 0$, then, $\frac{\mathfrak{n}_1}{d^2} = \mathcal{O}(d^{-\lambda}),\ \lambda > 0$. Hence, with these conditions on Δ and β, the probability of any pair randomly selected vectors from different orthonormal bases being orthogonal, tends to 0. Similarly, the probability that the angle between them is $\frac{\beta}{\sqrt{d}}$ tends to 1 asymptotically. Since $\beta \to 1$, as d increases, the bases of APMUBs would behave like MUBs in this sense.

Further note that, the vectors from a set of MUBs form a set of Bi-angular vectors as $\Delta = \{0, \frac{1}{\sqrt{d}}\}$. Now if we restrict $\Delta = \{0, \frac{\beta}{\sqrt{d}}\}$, then basis vectors of AMUBs would form set of Bi-angular vectors. Thus analysis of such AMUBs would also shed light on the study of Bi-angular vectors that has close connections with Weighing Matrices, Error Correcting Codes, Orthogonal spreads, Frame theory, Association Schemes etc. [20, 11, 12, 50, 72, 45, 24, 49, 59].

With this motivation, let us define Almost Perfect MUBs (APMUBs), which is the main focus of this paper.

Definition 5.5.1. *The set $\mathbb{M} = \{M_1, M_2, \ldots, M_r\}$ will be called Almost Perfect MUBs (APMUBs) if $\Delta = \left\{0, \frac{\beta}{\sqrt{d}}\right\}$, i.e., the set contains just two values, such that $\beta = 1 + \mathcal{O}(d^{-\lambda}) \leq 2,\ \lambda > 0$. When the bases are real, we call them Almost Perfect Real MUBs (APRMUBs).*

If the vectors are understood as states of a quantum system then the absolute value of an inner product essentially indicates the overlap between these states. Hence randomly picking two quantum states corresponding to different basis of above set of APMUBs, the overlap will have magnitude equal to $\frac{\beta}{\sqrt{d}}$ with probability almost 1. With negligible probability it will be 0 which corresponds to the quantum sates being orthogonal.

The sets of basis vectors of APMUB are Bi-angular as they are either orthogonal or have constant absolute value of inner product, i.e., $\Delta = \{0, \frac{\beta}{\sqrt{d}}\}$. Hence APMUBs form set of Bi-angular vectors with 0 being one of the value of inner product. Thus, for any pair of APMUBs in $\mathbb{C}^d$(or $\mathbb{R}^d$) we have the following lemma.

Lemma 5.5.1. *Consider any pair of APMUBs in $\mathbb{C}^d$ with $\Delta = \{0, \frac{\beta}{\sqrt{d}}\}$. Then any basis vector of an APMUB will be orthogonal to $(1-\frac{1}{\beta^2}) \times d$ many basis vectors of another APMUB and will be at angle $\frac{\beta}{\sqrt{d}}$ with remaining $\frac{d}{\beta^2}$ many basis vectors.*

Proof. Let M_l and M_n be any pair of APMUBs over $\mathbb{C}^d$ and let $\{|\psi_i^l\rangle : i = 1, 2, \ldots, d\}$ and $\{|\psi_j^m\rangle : j = 1, 2, \ldots, d\}$ be the corresponding basis vectors. Expressing $|\psi_i^l\rangle$ as a linear combination of $\{|\psi_j^m\rangle : j = 1, 2, \ldots, d\}$, we get,

$$|\psi_i^l\rangle = \alpha_{i1} |\psi_1^m\rangle + \alpha_{i2} |\psi_2^m\rangle + \ldots + \alpha_{id} |\psi_d^m\rangle ,$$

where $\alpha_{ij} = \langle\psi_i^l|\psi_j^m\rangle$. Since the bases consist of unit vectors, i.e., $\langle\psi_i^l|\psi_i^l\rangle = 1 \forall l, i$ hence,

$$\langle\psi_i^l|\psi_i^l\rangle = |\alpha_{i1}|^2 + |\alpha_{i2}|^2 + \ldots + |\alpha_{id}|^2 = \sum_{j=1}^{d} | \langle\psi_i^l|\psi_j^m\rangle |^2 = 1.$$

Since $\Delta = \{0, \frac{\beta}{\sqrt{d}}\}$, let us assume that $|\psi_i^l\rangle$ is orthogonal, i.e., $| \langle\psi_i^l|\psi_j^m\rangle | = 0$ with $\mathfrak{t}_1$ many basis vectors of M^m, and make an angle of $\frac{\beta}{\sqrt{d}}$ with remaining $\mathfrak{t}_2 = d - \mathfrak{t}_1$ many basis vectors of M^m. Hence we have,

$$\sum_{j=1}^{d} | \langle\psi_i^l|\psi_j^m\rangle |^2 = 1 \Rightarrow \mathfrak{t}_1 \cdot 0 + \mathfrak{t}_2 \times \left(\frac{\beta}{\sqrt{d}}\right)^2 = 1 \ \Rightarrow \ \mathfrak{t}_1 = \left(1 - \frac{1}{\beta^2}\right) \times d \text{ and } \mathfrak{t}_2 = \frac{d}{\beta^2}.$$

Since $|\psi_i^l\rangle$ is arbitrary basis vector of M^l, hence the result. □

The above result tells that β^2 can only be a rational number. Further, we have the following corollary considering all the vectors in the set of APMUBs.

Corollary 5.5.1. *Consider a set of r many APMUBs on dimension d with $\Delta = \{0, \frac{\beta}{\sqrt{d}}\}$, that will produce $r \times d$ vectors. In this set, each vector will have $(d-1) + (r-1)(1-\frac{1}{\beta^2})d$ many vectors as its orthogonal and $(r-1)\frac{d}{\beta^2}$ many vectors having the dot product $\frac{\beta}{\sqrt{d}}$.*

The main contribution here is to show that one can construct $\mathcal{O}(\sqrt{d})$ many APMUBs with values of β slightly more than one. This says that our method can provide $\mathcal{O}(d^{\frac{3}{2}})$ many Bi-angular vectors where the dot product values are 0 and $\frac{\beta}{\sqrt{d}}$. While there are constructions of $\mathcal{O}(d^2)$ Bi-angular vectors [73], but the angles we obtain with our methods are quite high than the existing constructions. Further we achieve large sparsity and non-zero components of equal magnitude. This is related to coherence property of unit norm vectors. This shows that the construction of APMUBs may produce interesting results in related domain. Further note that any set of Orthonormal Basis vectors always form Unit Norm Tight Frames (UNTF). For a brief introduction on Frame theory and its application in Hilbert space one may refer to [26, 25]. Thus the basis vectors of the set of APMUBs also constitute a Unit Norm Tight Frames apart from being Bi-angular, whereas in general the Bi-angular vectors constructed in [73] do not constitute tight frame. To see this, note that since APMUBs are orthonormal basis vectors, hence any arbitrary vector $|u\rangle$ can be uniquely expressed in terms of each of the APMUBs. Thus in this context also the construction of APMUBs may be of independent interest.

Let us now demonstrate how the construction of APMUBs bears implications to the existence of mutually unbiased weighing matrices (MUWM).

Definition 5.5.2. *Let W_1 and W_2 be a pair of weighing matrices of order d and weight w. If $W_1^\dagger W_2$ is again a weighing matrix with order d and weight w, then the pair is called mutually unbiased weighing matrices (MUWM). Moreover, let $W = \{W_1, W_2, \dots, W_r\}$ be a set of weighing matrices such that every pair is mutually unbiased. Then W is referred to as a set of mutually unbiased weighing matrices. If W consists solely of real weighing matrices, it is called a set of mutually unbiased real weighing matrices (MURWM).*

Note that, the MUWMs generalize mutually unbiased Hadamard matrices. The study of mutually unbiased weighing matrices of small orders has been conducted in [12], where computer searches and some analytical methods were predominantly employed. Moreover, in [47], mutually unbiased real weighing matrices have been used to study the binary codes. In this regard, we like to underline the following technical result.

Lemma 5.5.2. *The existences of the following combinatorial objects are equivalent:*

1. *r many APMUBs with $\Delta = \left\{0, \frac{\beta}{\sqrt{d}}\right\}$, and*

2. *$(r-1)$ many mutually unbiased weighing matrices of order d and weight $\frac{d}{\beta^2}$.*

Proof. (1) ⇒ (2): Let $\{M_1, M_2, \dots, M_r\}$ be a set of r many APMUB. Choose any weighing matrix, say M_1 and consider the set $\left\{M_1^\dagger M_1, M_1^\dagger M_2, \dots, M_1^\dagger M_r\right\} = \{I, W_2, W_3, \dots, W_r\}$.

Since M_i's are unitary matrices, W_i are also unitary. Moreover, since M_1 and M_i are APMUB, the elements of $W_i = M_1^\dagger M_i$ are from the set $\left\{0, \frac{\beta \exp(i\theta)}{\sqrt{d}}\right\}$ where $\theta \in \mathbb{R}$. Hence, W_i is a weighing matrices with weight $\frac{d}{\beta^2}$.

Further, $W_i^\dagger W_j = (M_1^\dagger M_i)^\dagger (M_1^\dagger M_j) = M_i^\dagger M_1 M_1^\dagger M_j = M_i^\dagger M_j$. Since M_i and M_j are APMUB, the elements of $M_i^\dagger M_j$ are from the set $\left\{0, \frac{\beta \exp(i\theta)}{\sqrt{d}}\right\}$ where $\theta \in \mathbb{R}$, making $W_i^\dagger W_j$ a weighing matrices with weight $\frac{d}{\beta^2}$. Hence, W_i and W_j are mutually unbiased weighing matrices, for any pair of W_i, W_j. Thus $\{W_2, W_3, \ldots, W_r\}$ is a set of $(r-1)$ mutually unbiased weighing matrices of weight $\frac{d}{\beta^2}$.

(2) $\Rightarrow$ (1) The set of $(r-1)$ mutually unbiased weighing matrices along with identity matrix (I), constitute the set of r many APMUB. □

In the lemma above, when we restrict the matrices to APRMUB, we obtain a set of mutually unbiased real weighing matrices (MURWM). It's also noteworthy that this lemma parallels the connection between MUBs and mutually unbiased Hadamard matrices (MUHM) [39, Section 5], where r MUBs are equivalent to $(r-1)$ MUHMs and vice versa.

5.5.2 Our general construction ideas

Let us now refer to the construction method of orthonormal bases using RBDs as given in [65, Section 3]. The construction idea of [65] is generic in nature, where unitary matrices can be employed to construct orthogonal bases corresponding to each parallel class of an RBD. However, here we will confine ourselves to the choice of Hadamard Matrices (which are special kind of unitary matrices) for constructing orthonormal bases from parallel classes of an RBD. This will enable us to bound β as per [65, Theorem 1], which is required for constructing APMUBs with good parameters. The order of the Hadamard matrices used in this construction must be same as the block size of each parallel class. With this method in place for constructing the set of orthonormal bases from RBD, our work here primarily focuses on constructing suitable RBDs, and consequently analyzing the parameters Δ, β and ϵ of corresponding AMUBs constructed from them.

We focus on constructing RBDs, having constant block size. The constant block size is essential if we want to use Hadamard matrices of same order (real or complex) for all the blocks of the RBD. This is required as it renders all the components of the basis finally constructed to be either zero or of a constant magnitude ($\frac{1}{\sqrt{k}}$), which is the normalizing factor of each basis vector. We will examine when they can satisfy the conditions of APMUBs (APRMUBs). Our construction method results into vectors which are vary sparse with the non-zero components of constant magnitude. This provides large sets of both real as well as complex AMUBs for the dimensions where it is known that not more that two or three real MUBs exist.

We first present a generic result, which is dependent on the existence of suitable RBDs. Thereafter, we explore the methods to construct such RBDs. We further show that if an RBD satisfy $\mu = 1$, then it will result into an APMUB. In fact, μ is the most critical parameter which we control in the construction of RBDs. In all the constructions of AMUBs, the number of elements in an RBD, i.e., $|X|$ can be increased without bound whereas, the parameter μ remains constant. All our constructions will have this property, which justifies asymptotic analysis of the parameters for AMUBs thus constructed.

Theorem 5.5.1. *Consider an RBD(X, A) with $|X| = d = (q-e)(q+f)$, with $q, e, f \in \mathbb{N}$. If the said RBD(X, A) consists of r parallel classes, each having blocks of size $(q-e)$, and if $0 \leq (e+f) \leq \left(\frac{c^2-\mu^2}{\mu c}\right) d^{\frac{1}{2}}$ where c is some constant, then one can construct r many β-AMUBs in dimension d, where $\beta = \mu\sqrt{\frac{q+f}{q-e}} \leq c$ and $\epsilon = 1 - \frac{1}{q+f}$. When $\mu = 1$ and $c = 2$, we will get r many APMUBs with $\beta = 1 + \frac{e+f}{2\sqrt{d}} + \mathcal{O}(d^{-1}) \leq 2$ and $\Delta = \{0, \frac{1}{q-e}\}$. Further, if there exists a real Hadamard matrix of order $(q-e)$, we can construct r many APRMUBs with the same parameters.*

Proof. We have $|X| = (q-e)(q+f)$ with each parallel class having the block size $k = (q-e)$. Here μ is the maximum number of elements that are common between two blocks from different parallel classes. Following [65, Theorem 1], this implies that, $\beta = \frac{\mu\sqrt{d}}{q-e} = \mu\sqrt{\frac{q+f}{q-e}}$. Further, using the relation $d = q^2 + (f-e)q - ef$, we obtain $\beta = \mu(\sqrt{1+x^2} + x)$, where $x = \frac{e+f}{2\sqrt{d}}$. From the definition of β-AMUBs, β must be bounded for all values of d. Let this bound for β be c, then $\mu(\sqrt{1+x^2}+x) \leq c \Rightarrow 0 \leq (e+f) \leq \left(\frac{c^2-\mu^2}{\mu c}\right) d^{\frac{1}{2}}$. This inequality can be restated in terms of q as $0 \leq (c^2 e + \mu^2 f) \leq (c^2 - \mu^2)q$, which is the condition for β being bounded above by the constant c.

In order to see the asymptotic variation of β in terms of q, we consider the expansion of terms as follows:

$$\beta = \mu\left(1 + \frac{e+f}{2q} + \frac{(e+f)(3e-f)}{2^3q^2} + \frac{(e+f)(5e^2-2ef+f^2)}{2^4q^3} + \dots\right). \tag{5.2}$$

To understand the asymptotic variation of β in terms of d, we again use the relation $d = q^2 + (f-e)q - ef$ to express q in terms of $\sqrt{d}$ and thereafter, expanding the expression for $\beta = \mu\sqrt{\frac{q+f}{q-e}} = \mu(\sqrt{1+x^2}+x)$, where $x = \frac{f+e}{2\sqrt{d}}$, in terms of negative power of $\sqrt{d}$ and we obtain

$$\beta = \mu\left(1 + \frac{e+f}{2\sqrt{d}} + \frac{(e+f)^2}{2^3d} - \frac{(e+f)^4}{2^7d^2} + \frac{(e+f)^6}{2^{10}d^3} - \frac{5(e+f)^8}{2^{15}d^4} + \dots\right). \tag{5.3}$$

Thus, for a given e and f, for large d (or q), asymptotically $\beta = \mu + \mathcal{O}(\frac{1}{q}) = \mu + \mathcal{O}(\frac{1}{\sqrt{d}})$. Therefore, if $\mu = 1$, the construction yields APMUBs, provided $\beta \leq 2 \Rightarrow c = 2$ as we have seen above that β is bounded by c. And in this situation we get $0 \leq (e+f) \leq \frac{3}{2}d^{\frac{1}{2}}$.

To get the values of the set Δ, note that when $\mu = 1$, there is maximum one element common between any pair of blocks from different parallel classes. And since Hadamard matrices are used for constructing orthonormal bases, thus $|\langle u|v\rangle| = \frac{1}{q-e}$ corresponding to the situations when one element is common between the pair of blocks and $|\langle u|v\rangle| = 0$ corresponding to situation, when no elements are common between the pair of blocks. Thus $\Delta = \{0, \frac{1}{q-e}\}$.

To calculate sparsity, note that for each vector constructed from a block of size k, we will have exactly k many non-zero and $d-k$ many zero entries, hence

$$\epsilon = \frac{d-k}{d} = 1 - \frac{k}{d} = 1 - \frac{q-e}{(q+f)(q-e)} = 1 - \frac{1}{q+f}.$$

If a real Hadamard matrix of order $(q-e)$ exists, we can exploit it to obtain r many real approximate MUBs in $\mathbb{R}^d$, with same values of the parameters β, Δ and ϵ. □

If the construction in [65] is to be used for APMUBs, then μ should be 1. Thus μ, which is the maximum number of elements common between any pair of blocks from different parallel classes, is the most critical parameter here. Further note that, μ is always greater than or equal to 1, hence, a very limited kinds of RBDs can be used to construct APMUBs. As per Lemma 5.4.2, $\mu \geq \lceil \frac{k}{s} \rceil$. Thus, for $\mu = 1$, an RBD having a constant block size must have $k \leq s$, i.e., the block size must not be greater than the number of blocks in the parallel class. In this connection, we have noted that an RBD constructed using MOLS have $\mu = 1$. In fact, between any pair of blocks from different parallel classes, in such an RBD, there is exactly one element in common.

In our above theorem, we have $|X| = d = (q-e)(q+f)$, where number of elements in a block is $(q-e)$, i.e., $k = (q-e)$, and number of blocks in a parallel class is $(q+f)$, hence $s = (q+f)$. The reason we are expressing it like this will be clear in Theorem 5.6.2 where we demonstrate the construction of such an RBD. Since e and f are bounded by a positive integer, if $e \geq f$, it will ensure that $k \leq s$. Since$\beta = \mu\sqrt{\frac{s}{k}} = \mu\sqrt{\frac{q+f}{q-e}}$, hence for large $d = (q-e)(q+f)$ we obtain $\beta \to \mu$, which is also evident from the asymptotic expansion of β above.

For $|X| = d = (q-e)(q+f)$, we can have an RBD, where the block size is $(q+f)$, hence having $(q-e)$ blocks in each parallel class. However, in such a situation, $\mu > 1$ Lemma 5.4.2, and hence we cannot get APMUBs. However, they can provide AMUBs as in [65]. The result of [65, Theorem 4] is a particular case of this situation, with $e = 0, f = 1$ and $\mu = 2$.

In this case, $q+1$ many parallel classes are there in an RBD, each having a constant block size of $(q+1)$. In this case, $\beta = 2\sqrt{\frac{q}{q+1}} = 2 - \mathcal{O}(\frac{1}{\sqrt{d}})$, i.e., though the maximum value of the inner product was slightly less than $\frac{2}{\sqrt{d}}$, but asymptotically β converges to 2. Further Δ is also not two-valued. Thus the construction did not satisfy the conditions needed for Almost Perfect MUBs which is $\beta = 1 + \mathcal{O}(d^{-\lambda})$, for some $\lambda > 0$ and Δ being the set consisting of just two elements with one being 0.

Thus, in order to obtain APMUBs, the RBDs in use must have $\mu = 1$ and all the block sizes must be same. With this understanding, we will explore more suitable designs in the following sections, so that the upper bound on the absolute inner product values can be improved than the results presented in [65] to obtain Almost Perfect MUBs.

5.6 Exact constructions of APMUBs through RBDs

As followed from previous section, an RBD having constant block size must have $\mu = 1$, in order to obtain APMUBs. In this section we explain the constructions of such RBDs. Since our focus is to build APMUBs in composite, we concentrate on $d = k \times s$, and consider two categories.

- The first construction, being generic in nature, will work for any composite $d = k \times s = (s-e)s$ with $0 \le e \le \frac{3}{2}d^{\frac{1}{2}}$. Here the number of APMUBs is at least $N(s)+1$ when $e > 0$ and $N(s)+2$ when $e = 0$.
- The second one is considered when d can be expressed as $(q-e)(q+f),\ 0 < \ f \le e$, where q is some power of prime. Here the number of APMUBs is at least $\lfloor \frac{q-e}{f} \rfloor + 1$.

These are presented in the Sections 5.6.1 and 5.6.2 respectively as below. Thus here our approach to is to obtain large numbers of APMUBs, if the composite dimension d can be expressed in some generic form. In the first category our starting point is w-MOLS(s) and in the second category we initiate with $(q^2, q, 1)$-ARBIBD. In each case, we will first demonstrate the construction with an example, then outline the algorithm for the respective construction and then provide the proof of correctness.

5.6.1 $d = k \times s = (s-e)s,\ 0 \le e \le \frac{3}{2}d^{\frac{1}{2}}$

Let us first demonstrate the method by explicitly constructing RBD(X, A) with $|X| = 2\times 5 = 10$, i.e., here $s = 5$ and $k = 2$.

1. To begin with, consider the following 4-MOLS(5) and the M_{ref}:

$$LS_1 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 2 & 3 & 4 \\ 4 & 5 & 1 & 2 & 3 \\ 3 & 4 & 5 & 1 & 2 \\ 2 & 3 & 4 & 5 & 1 \end{bmatrix}, LS_2 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 5 & 1 & 2 & 3 \\ 2 & 3 & 4 & 5 & 1 \\ 5 & 1 & 2 & 3 & 4 \\ 3 & 4 & 5 & 1 & 2 \end{bmatrix}, LS_3 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 1 & 2 \\ 5 & 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 & 1 \\ 4 & 5 & 1 & 2 & 3 \end{bmatrix},$$

$$LS_4 = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \\ 3 & 4 & 5 & 1 & 2 \\ 4 & 5 & 1 & 2 & 3 \\ 5 & 1 & 2 & 3 & 4 \end{bmatrix}, M_{ref} = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \\ 16 & 17 & 18 & 19 & 20 \\ 21 & 22 & 23 & 24 & 25 \end{bmatrix}.$$

2. Using Construction 5.4.1, we construct RBD$(\bar{X}, \bar{A})$, with $|\bar{X}| = 25$ and $\bar{A}$ having 6 parallel classes. We used M_{ref} as shown above to obtain the following RBD. We collect blocks from each parallel class, in a 5×5 matrix, where each row represents one block of the parallel class, and index the blocks as $\bar{b}_i^l$, where l represents the index of parallel class and i represents the block number within the parallel class.

$$\bar{P}_1 = \begin{bmatrix} \bar{b}_5^1 = \{1 & 7 & 13 & 19 & 25\} \\ \bar{b}_4^1 = \{2 & 8 & 14 & 20 & 21\} \\ \bar{b}_3^1 = \{3 & 9 & 15 & 16 & 22\} \\ \bar{b}_2^1 = \{4 & 10 & 11 & 17 & 23\} \\ \bar{b}_1^1 = \{5 & 6 & 12 & 18 & 24\} \end{bmatrix}, \bar{P}_2 = \begin{bmatrix} \bar{b}_5^2 = \{1 & 8 & 15 & 17 & 24\} \\ \bar{b}_4^2 = \{2 & 9 & 11 & 18 & 25\} \\ \bar{b}_3^2 = \{3 & 10 & 12 & 19 & 21\} \\ \bar{b}_2^2 = \{4 & 6 & 13 & 20 & 22\} \\ \bar{b}_1^2 = \{5 & 7 & 14 & 16 & 23\} \end{bmatrix},$$

$$\bar{P}_3 = \begin{bmatrix} \bar{b}_5^3 = \{1 & 9 & 12 & 20 & 23\} \\ \bar{b}_4^3 = \{2 & 10 & 13 & 16 & 24\} \\ \bar{b}_3^3 = \{3 & 6 & 14 & 17 & 25\} \\ \bar{b}_2^3 = \{4 & 7 & 15 & 18 & 21\} \\ \bar{b}_1^3 = \{5 & 8 & 11 & 19 & 22\} \end{bmatrix}, \bar{P}_4 = \begin{bmatrix} \bar{b}_5^4 = \{1 & 10 & 14 & 18 & 22\} \\ \bar{b}_4^4 = \{2 & 6 & 15 & 19 & 23\} \\ \bar{b}_3^4 = \{3 & 7 & 11 & 20 & 24\} \\ \bar{b}_2^4 = \{4 & 8 & 12 & 16 & 25\} \\ \bar{b}_1^4 = \{5 & 9 & 13 & 17 & 21\} \end{bmatrix},$$

$$\bar{P}_\infty = \begin{bmatrix} \bar{b}_5^5 = \{1 & 6 & 11 & 16 & 21\} \\ \bar{b}_4^5 = \{2 & 7 & 12 & 17 & 22\} \\ \bar{b}_3^5 = \{3 & 8 & 13 & 18 & 23\} \\ \bar{b}_2^5 = \{4 & 9 & 14 & 19 & 24\} \\ \bar{b}_1^5 = \{5 & 10 & 15 & 20 & 25\} \end{bmatrix}, \bar{P}_0 = \begin{bmatrix} \bar{b}_5^6 = \{1 & 2 & 3 & 4 & 5\} \\ \bar{b}_4^6 = \{6 & 7 & 8 & 9 & 10\} \\ \bar{b}_3^6 = \{11 & 12 & 13 & 14 & 15\} \\ \bar{b}_2^6 = \{16 & 17 & 18 & 19 & 20\} \\ \bar{b}_1^6 = \{21 & 22 & 23 & 24 & 25\} \end{bmatrix}.$$

Here $\bar{A} = \{\bar{P}_1 \cup \bar{P}_2 \cup \bar{P}_3 \cup \bar{P}_4 \cup \bar{P}_0 \cup \bar{P}_\infty\}$. Note that, any pair of blocks from different parallel classes has exactly one element in common.

3. Now we remove any 3 blocks from the parallel class $\bar{P}_0$, say $\{\bar{b}_1^6, \bar{b}_2^6, \bar{b}_3^6\}$.

4. Next we remove the elements contained in this block from the entire design $(\bar{X}, \bar{A})$.

5. Then we discard $\bar{P}_0$ from the design. Here we get RBD(X, A) consisting of 5 parallel classes, each having 5 blocks of size 2, where $X = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ and $A = \{P_1 \cup P_2 \cup P_3 \cup P_4 \cup P_\infty\}$. Explicitly, we have,

$$P_1 = \begin{bmatrix} b_5^1 = \{1 & 7\} \\ b_4^1 = \{2 & 8\} \\ b_3^1 = \{3 & 9\} \\ b_2^1 = \{4 & 10\} \\ b_1^1 = \{5 & 6\} \end{bmatrix}, P_2 = \begin{bmatrix} b_5^2 = \{1 & 8\} \\ b_4^2 = \{2 & 9\} \\ b_3^2 = \{3 & 10\} \\ b_2^2 = \{4 & 6\} \\ b_1^2 = \{5 & 7\} \end{bmatrix}, P_3 = \begin{bmatrix} b_5^3 = \{1 & 9\} \\ b_4^3 = \{2 & 10\} \\ b_3^3 = \{3 & 6\} \\ b_2^3 = \{4 & 7\} \\ b_1^3 = \{5 & 8\} \end{bmatrix},$$

$$P_4 = \begin{bmatrix} b_5^4 = \{1 & 10\} \\ b_4^4 = \{2 & 6\} \\ b_3^4 = \{3 & 7\} \\ b_2^4 = \{4 & 8\} \\ b_1^4 = \{5 & 9\} \end{bmatrix}, P_\infty = \begin{bmatrix} b_5^5 = \{1 & 6\} \\ b_4^5 = \{2 & 7\} \\ b_3^5 = \{3 & 8\} \\ b_2^5 = \{4 & 9\} \\ b_1^5 = \{5 & 10\} \end{bmatrix}.$$

Note that, for this particular case using $(10, 2, 1)$-BIBD, one can construct an RBD with 9 parallel classes each having 5 many blocks of constant block size 2. One must note that this construction may not provide RBDs having maximum number of parallel classes, with constant block size and $\mu = 1$. Even if we include the parallel class $P_0 = \bar{P}_0 \setminus \{\bar{b}_1^6, \bar{b}_2^6, \bar{b}_3^6\}$ in the RBD(X, A), it will not change the value of μ which will remain equal to 1. However, the block size of P_0 will be 5 then and hence RBD(X,A) will contain two different block sizes. Therefore we discard the P_0. Nevertheless we will see that even P_0 can be used to construct orthonormal basis which will be mutually unbiased with all the orthonormal basis constructed using $\{P_1 \cup P_2 \cup P_3 \cup P_4 \cup P_\infty\}$.

The technique is more formally explained for the general case in Construction 5.6.1 below.

Construction 5.6.1. Let $d = k \times s = (s - e)s$, with $0 < e \leq s$.

1. Using Construction 5.4.1, construct $RBD(\bar{X}, \bar{A})$, where $\bar{X} = \{1, 2, \ldots, s^2\}$. It will have $r = N(s) + 2$ many parallel classes, namely $\{\bar{P}_1, \bar{P}_2, \ldots, \bar{P}_w, \bar{P}_0, \bar{P}_\infty\}$, each having s many blocks of constant size s. Denoting blocks of the parallel class $\bar{P}_l$ with $\bar{b}_i^l$, for $i = 1, 2, \ldots, s$, we note that between any two blocks from different parallel classes, there is exactly one element in common, i.e., $|\bar{b}_i^l \cap \bar{b}_j^m| = 1, \ \forall \ l \neq m$.

2. Pick a parallel class, say $\bar{P}_0$. Remove e many blocks from it and denote as $S = \{\bar{b}_1^0 \cup \bar{b}_2^0 \cup \ldots \cup \bar{b}_e^0\}$.

3. Remove the elements in S from $\bar{X}$ and let us denote the new set with X, i.e., $X = \bar{X} \backslash S$. Further, we remove the elements in S from the parallel classes $\{\bar{P}_2, \bar{P}_3, \ldots, \bar{P}_w, \bar{P}_\infty\}$ and denote them by P_l, for $l = 2, 3, \ldots, r$, i.e., $P_l = \bar{P}_l \setminus S$. Then $A = \{P_2, P_3, \ldots, P_w, P_\infty\}$ with $P_l = \{b_1^l, b_2^l, \ldots, b_q^l\}$, where $b_i^l = \bar{b}_i^l \setminus S$.

4. Discard the parallel class $\bar{P}_0$. The resulting RBD(X, A) is the required design. For convenience, rename the elements from 1 to $(s-e)s$.

We claim that the above design (X, A) is an RBD, such that $|X| = (s-e)s$ and A consist of $N(s)+1$ many parallel classes, i.e., $A = \{P_2, P_3, \ldots, P_w, P_\infty\}$, each having s many blocks, i.e., $P_l = \{b_1^l, b_2^l, \ldots, b_s^l\}, l = 1, 2, \ldots, s$, each of size $(s-e)$, i.e., $|b_i^l| = (s-e)\ \forall i, l$, such that blocks from different parallel classes have at most one element in common, i.e., $|b_i^l \cap b_j^m| \leq 1\ \forall\, l \neq m$. We formalize this in the form of a lemma below.

Lemma 5.6.1. *Let $d = (s-e)s$ for $s, e \in \mathbb{N}$ with $0 < e \leq s$. Then one can construct an RBD(X, A), with $|X| = d$ having constant block size $(s-e)$ with $\mu = 1$, and having $N(s)+1$ many parallel classes, where $N(s)$ is the number of MOLS(s).*

Proof. Refer to Construction 5.6.1 above. In RBD$(\bar{X}, \bar{A})$ any pair of blocks from different parallel classes is of size s and has exactly one element in common, i.e., $|\bar{b}_i^l \cap \bar{b}_j^m| = 1\ \forall\ l \neq m$. Hence removal of the elements $S = \{\bar{b}_1^1 \cup \bar{b}_2^1 \cup \ldots \cup \bar{b}_e^1\}$ from entire design will discard exactly e elements from each block $\bar{b}_i^l, l \neq 1$. Hence, the blocks $b_i^l = \bar{b}_i^l \backslash S$ will be of constant size $|b_i^l| = s-e$ and $|b_i^l \cap b_j^m| \leq 1\ \forall\, l \neq m$. □

Now we can use this RBD(X, A) to construct APMUBs in dimension $d = |X| = (s-e)s$ following Theorem 5.5.1.

Theorem 5.6.1. *Let $d = (s-e)s$ for $s, e \in \mathbb{N}$ with $0 < e \leq \frac{3}{2}d^{\frac{1}{2}}$. Then there exist $N(s)+1$ many APMUBs with $\Delta = \{0, \frac{1}{s-e}\}$ and $\beta = \sqrt{\frac{s}{s-e}} = 1 + \mathcal{O}(d^{-\lambda}) \leq 2$, where $\lambda = \frac{1}{2}$ and sparsity $\epsilon = 1 - \frac{1}{s}$. Further, if there exists a real Hadamard matrix of order $(s-e)$, then we can construct $N(s)+1$ many APRMUBs with the same parameters. For the case e $= 0$, there exist $N(s)+2$ many MUBs, and if there exists a real Hadamard matrix of order s, then we can construct $N(s)+2$ many Real MUBs.*

Proof. In order to show that we can produce such number of APMUBs, let us consider an RBD(X, A) with $|X| = (s-e)s$ having $N(s)+1$ parallel classes of constant block size $(s-e)$ such that between the blocks from different parallel classes, there is at most one element in common, and hence $\mu = 1$. This follows from Lemma 5.6.1. Then using this RBD along with a Hadamard matrix of order $(s-e)$, we can construct orthonormal bases following Theorem 5.5.1, with the values of Δ, β, ϵ by substituting $q = s$, and $f = 0$. Further, the condition that $\beta \leq 2$ for APMUB gives $e \leq \frac{3}{2}d^{\frac{1}{2}}$. In terms of s this inequality becomes $e \leq \frac{3}{4}s$ and in terms of $k = (s-e)$, the inequality becomes $s \leq 4k$ so that $\beta \leq 2$. The parameters of APMUBs are $\Delta = \{0, \frac{1}{s-e}\}$, $\beta = \sqrt{\frac{s}{s-e}} = 1 + \mathcal{O}(d^{-\frac{1}{2}}) \leq 2$ and $\epsilon = 1 - \frac{1}{s}$. Since the number of parallel classes is one more than number of Mutually Orthogonal Latin Squares of Order s, we have $r = N(s)+1$.

In the situation when $d = s^2$, i.e., $e = 0$, using Construction 5.4.1 above, we obtain RBD(X, A) having $N(s) + 2$ parallel classes, such that any pair of blocks have exactly one point in common. Now using this RBD(X, A), along with a Hadamard matrix of order s, we can construct orthonormal bases following Theorem 5.5.1 which will provide $N(s)+2$ many MUBs. Hence for $e = 0$, the result follows directly. Construction 5.6.1 is applied only when $e > 0$. Thus when $d = s^2$, we get $N(s) + 2$ MUBs, and when real Hadamard matrix of order s is available, that can be used to construct $N(s) + 2$ real MUBs. □

Remark 5.6.1. *Note that we can construct an orthonormal basis corresponding to the parallel class $P_0 = \bar{P}_0 \setminus S$, again having $(s-e)s$ elements. These basis vectors will be mutually unbiased with all the orthonormal bases constructed using the parallel classes $P_1, P_2, \ldots P_w, P_\infty$. However, if we include it in the set of orthonormal bases then $\Delta = \{0, \frac{1}{\sqrt{d}}, \frac{\beta}{\sqrt{d}}\}$ will have three values, and the condition of APMUB will not be satisfied. Thus we ignore P_0, even though it provides an orthonormal basis which is mutually unbiased with all the bases constructed above.*

For a composite s, $N(s) \to \mathcal{O}(s^{\frac{1}{14.8}}) \ll s - 1$, which is an upper bound [1, 93, 98]. Thus in case d can be expressed as $d = k \times s = (s - e)s$, where $s, e \in \mathbb{N}$ with $k < s \leq 4k$ (or $0 < e \leq \frac{3}{4}s$), we can always construct $N(s) + 1$ many APMUBs. We refer to this as Mutually Orthogonal Latin Square Lower Bound construction for APMUBs. For example, given $d = 2^2 \times 3^2 \times 5 \times 7$,

- this can be factored as $d = 35 \times 36$, which will provide $N(36) + 1 = 9$ many APMUBs with $\beta = 1.01$,
- or $d = 30 \times 42$ which will give $N(42) + 1 = 6$ many APMUBs with $\beta = 1.18$,
- or $d = 28 \times 45$, which will give $N(45) + 1 = 7$ many APMUB with $\beta = 1.27$.

Here, $N(36) = 8, N(42) = 5$ and $N(45) = 6$ are the presently known values of the maximum number of MOLS of these orders [1]. Let us now explain the significance of our construction method through this example.

- The number of complex MUBs for this $d = 2^2 \times 3^2 \times 5 \times 7$ which can be constructed using prime power decomposition, and then taking tensor product, would be $2^2+1 = 5$. This is the lower bound and there is no better known result than this in the number of MUBs in this dimension. The value of β is 1 in this case as exact MUBs are referred.
- Expressing $d = 35 \times 36$, we have more number of APMUBs (9 many) than MUBs, with $\beta = 1.01$.

- Further, expressing $d = 28 \times 45$, we can get 7 many APRMUBs with $\beta = 1.27$. This is because, we have real Hadamard matrix on the dimension $4 \times 7 = 28$.

Our Theorem 5.6.1 can be compared with that of [98, Theorem 3], where the result could be achieved using (k, s)-nets. This, in turn, can be constructed from Mutually Orthogonal Latin Squares of order s. Thus, for a square dimension $d = s^2$, there would be $N(s) + 2$ many MUBs. Moreover, the result in [65, Corollary 3] points out that using RBDs, one can construct $q + 1$ many MUBs of dimension d when $d = q^2$. Note that $N(q) = q - 1$ and thus the number of MUBs from [65, Corollary 3] is same as that presented in [98, Theorem 3]. The construction of [65, Corollary 3] had the advantage of using different Hadamard matrices for the construction of each MUBs, whereas a single Hadamard matrix can be used for construction of MUBs in [98, Theorem 3].

Since Theorem 5.6.1 is based on RBDs as in [65, Corollary 3], here also different Hadamard matrices can be used for the construction of each MUBs. Hence, Theorem 5.6.1 is a generalization of [98, Theorem 3] and [65, Corollary 3] as enumerated below.

1. For $d = s^2$, Theorem 5.6.1 reproduces the results of [98, Theorem 3] in terms of number of MUBs constructed.

2. For $d = q^2$, Theorem 5.6.1 reproduces the results of [65, Corollary 3], in terms of having the advantage of using different Hadamard matrices for the construction of each MUBs and the number of MUBs constructed.

3. As the additional contribution, for any composite $d = k \times s = (s - e) \times s$, with $0 < e \leq \frac{3}{2}d^{\frac{1}{2}}$, Theorem 5.6.1 provides MOLS$(s) + 1$ many APMUBs and one can also use different Hadamard matrices for the construction of each basis.

The case $N(s) = s - 1$ corresponds to affine plane of order s and the corresponding RBD is called Affine Resolvable BIBD. When $s = q$, where q is a prime power, we have well known methods to construct Affine Resolvable $(q^2, q, 1)$-BIBDs. Hence in such a situation we will have $q \sim \mathcal{O}(\sqrt{d})$ many APMUBs for composite dimensions which are not square. For example, if $d = 3^4 \times 7 = 21 \times 27$, we have 29 APMUBs with $\beta = 1.13$ or for $d = 2^4 \times 3 = 6 \times 8$ we obtain 9 APMUBs, with $\beta = 1.15$ whereas number of MUBs is 8 and 4 respectively in these cases.

Now let us explain the consequences for Approximate Real MUBs. When q is a prime power, and real Hadamard matrix of order $(q - e)$ exists, then we will obtain $(q + 1) > \sqrt{d}$ many APRMUBs, which provides large numbers of such objects over $\mathbb{R}^d$. This is presented in the following result.

Corollary 5.6.1. *Let $d = (q - e)q$, where q is a prime power and $e \in \mathbb{N}$, with $0 < e \leq \frac{3}{2}d^{\frac{1}{2}}$. Then there exist $q + 1$ many APMUBs with $\Delta = \{0, \frac{1}{q-e}\}$, $\beta = \sqrt{\frac{q}{q-e}} = 1 + \mathcal{O}(d^{-\lambda})$, where*

$\lambda = \frac{1}{2}$ and $\epsilon = 1 - \frac{1}{q}$. Further, if there exist real Hadamard matrices of order $(q-e)$, then one can construct $q+1$ many Almost Perfect Real MUBs with same parameters.

The condition $e \leq \frac{3}{2}d^{\frac{1}{2}}$ is because we require $\beta \leq 2$ for APMUBs. If $e > \frac{3}{2}d^{\frac{1}{2}}$ then $\beta > 2$, hence the constructed Approximate MUBs will not satisfy the criteria for APMUBs [Definition 5.5.1]. Further examining the expression for β in Equation 5.3, for this particular construction with $\mu = 1, f = 0$, we obtain the best possible APRMUBs when $e = 1$. That is, we have this situation when the dimensions are of the form $d = (q-1)q$. This we formally state in the following corollary.

Corollary 5.6.2. *Consider $d = (q-1)q$, such that q is a prime power and assume that a real Hadamard matrix of order $(q-1)$ exists. Then one can construct q many Almost Perfect Real MUBs in dimension d with $\Delta = \left\{0, \frac{1}{q-1}\right\}$, $\beta = \sqrt{\frac{q}{q-1}} = 1 + \mathcal{O}(d^{-\frac{1}{2}})$, and $\epsilon = 1 - \frac{1}{q}$.*

For example, when $d = 20$ and 156, there would be respectively 5 and 13 APRMUBs of the above type. One may note that we have $\lceil\sqrt{d}\rceil$ many APRMUBs in this case. If $m = \frac{q-3}{2} \equiv 1 \bmod 4$ and m is some prime power, then using the Paley Construction [75], one can obtain Hadamard matrix of order $2(m+1) = q-1$. Hence for any prime power $q \equiv 1 \bmod 4$, if $\frac{q-3}{2}$ is also some prime power and is equal to 1 mod 4, then the real Hadamard matrix of order $q-1$ will necessarily exist through the Paley Construction. For example, one can consider $q = 13, 29, 5^3$ etc. For such q's, the result will become independent of the Hadamard Conjecture.

5.6.2 $d = k \times s = (q-e)(q+f),\ 0 < f \leq e$ and $0 < (e+f) \leq \frac{3}{2}d^{\frac{1}{2}}$

As noted in Corollary 5.6.1 that if d can be expresses as $k \times s = (q-e)q$ with $\beta = \sqrt{\frac{s}{k}} = \sqrt{\frac{q}{q-e}} \leq 2$, then there we can construct $q = \mathcal{O}(\sqrt{d})$ many APMUBs. However, if d can not be expressed in this form then one can construct $N(s)$ many APMUBs if d can be expressed as $k \times s$ with s a composite such that $k \leq s \leq 4k$, i.e., for example in the cases $d = \{2 \times 3^2,\ 2 \times 11,\ 2 \times 3 \times 7,\ 2^2 \times 3 \times 7, \ldots\}$ etc. The condition $k \leq s \leq 4k$ ensures $\beta \leq 2$ and if d can be expressed as $(s-e) \times s$ then it is equivalent to $0 \leq e \leq \frac{3}{2}d^{\frac{1}{2}}$. The best known lower bound for general s is $N(s) \sim s^{\frac{1}{14.8}}$ which is much less than s.

In order to obtain significantly larger number of APMUBs, for the dimensions that cannot be expressed in the form $d = (q-e)q$ where q is some prime power with $0 < e \leq \frac{3}{2}d^{\frac{1}{2}}$, we now consider the form of $d = (q-e)(q+f)$, such that q is a prime power with $e, f \in \mathbb{N}$. First we show that, in such a case if $e \geq f$, then we can construct RBD(X, A) with $|X| = d$ having constant block size $(q-e)$ such that A can be partitioned into at least $r = \lfloor\frac{q-(e-f)}{f}\rfloor = \lfloor\frac{q-e}{f}\rfloor + 1$ many parallel classes. Hence such an RBD(X, A) can be used to construct $\lfloor\frac{q-e}{f}\rfloor + 1$

many orthonormal bases following [65, Theorem 1]. Further, if $0 < (e+f) \leq \frac{3}{2}d^{\frac{1}{2}}$, then $\beta \leq 2$, and these orthonormal bases would be APMUBs, thus providing us $\mathcal{O}(q)$ many APMUBs in such a situation.

We explain this construction in two parts. First we consider a $(q^2, q, 1)$ Affine Resolvable BIBD as the input. We call this $\mathrm{RBD}(\bar{X}, \bar{A})$ where $|\bar{X}| = q^2$ and all the blocks of A is of the same size q and number of parallel classes in A is $q+1$. We use this to construct $\mathrm{RBD}(\widetilde{X}, \widetilde{A})$, where $|\widetilde{X}| = (q-e)(q+f)$ having same number of parallel class $(q+1)$, but the blocks are not of the same size. The sizes of the blocks are from set $\{(q-e), (q-e+1), \ldots, (q-e+f), q\}$.

In the second part we use the $\mathrm{RBD}(\widetilde{X}, \widetilde{A})$ as input and construct $\mathrm{RBD}(X, A)$ where $|X| = (q-e)(q+f)$ such that each block in A is of size $(q-e)$. However, now the number of parallel class reduces to $\lfloor \frac{q-e}{f} \rfloor + 1$.

To demonstrate the first part of the construction, we take $|X| = (7-3)(7+1) = 4 \cdot 8 = 32$, where $q = 7, e = 3$ and $f = 1$. We use an Affine Resolvable $(7^2, 7, 1)$-BIBD which we call $\mathrm{RBD}(\bar{X}, \bar{A})$. It will consist of eight parallel classes. Each parallel class would consist of seven blocks of constant size 7. We represent each parallel class as a 7×7 matrix, where each row represent one block of the parallel class. Hence there would be eight such matrices as below to represent the design.

$$\bar{P}_1 = \begin{bmatrix} \bar{b}^1_7 = \{1 & 2 & 3 & 4 & 5 & 6 & 7\} \\ \bar{b}^1_6 = \{8 & 9 & 10 & 11 & 12 & 13 & 14\} \\ \bar{b}^1_5 = \{15 & 16 & 17 & 18 & 19 & 20 & 21\} \\ \bar{b}^1_4 = \{22 & 23 & 24 & 25 & 26 & 27 & 28\} \\ \bar{b}^1_3 = \{29 & 30 & 31 & 32 & 33 & 34 & 35\} \\ \bar{b}^1_2 = \{36 & 37 & 38 & 39 & 40 & 41 & 42\} \\ \bar{b}^1_1 = \{43 & 44 & 45 & 46 & 47 & 48 & 49\} \end{bmatrix}, \bar{P}_2 = \begin{bmatrix} \bar{b}^2_7 = \{1 & 9 & 17 & 25 & 33 & 41 & 49\} \\ \bar{b}^2_6 = \{2 & 10 & 18 & 26 & 34 & 42 & 43\} \\ \bar{b}^2_5 = \{3 & 11 & 19 & 27 & 35 & 36 & 44\} \\ \bar{b}^2_4 = \{4 & 12 & 20 & 28 & 29 & 37 & 45\} \\ \bar{b}^2_3 = \{5 & 13 & 21 & 22 & 30 & 38 & 46\} \\ \bar{b}^2_2 = \{6 & 14 & 15 & 23 & 31 & 39 & 47\} \\ \bar{b}^2_1 = \{7 & 8 & 16 & 24 & 32 & 40 & 48\} \end{bmatrix},$$

$$\bar{P}_3 = \begin{bmatrix} \bar{b}^3_7 = \{1 & 10 & 19 & 28 & 30 & 39 & 48\} \\ \bar{b}^3_6 = \{2 & 11 & 20 & 22 & 31 & 40 & 49\} \\ \bar{b}^3_5 = \{3 & 12 & 21 & 23 & 32 & 41 & 43\} \\ \bar{b}^3_4 = \{4 & 13 & 15 & 24 & 33 & 42 & 44\} \\ \bar{b}^3_3 = \{5 & 14 & 16 & 25 & 34 & 36 & 45\} \\ \bar{b}^3_2 = \{6 & 8 & 17 & 26 & 35 & 37 & 46\} \\ \bar{b}^3_1 = \{7 & 9 & 18 & 27 & 29 & 38 & 47\} \end{bmatrix}, \bar{P}_4 = \begin{bmatrix} \bar{b}^4_7 = \{1 & 11 & 21 & 24 & 34 & 37 & 47\} \\ \bar{b}^4_6 = \{2 & 12 & 15 & 25 & 35 & 38 & 48\} \\ \bar{b}^4_5 = \{3 & 13 & 16 & 26 & 29 & 39 & 49\} \\ \bar{b}^4_4 = \{4 & 14 & 17 & 27 & 30 & 40 & 43\} \\ \bar{b}^4_3 = \{5 & 8 & 18 & 28 & 31 & 41 & 44\} \\ \bar{b}^4_2 = \{6 & 9 & 19 & 22 & 32 & 42 & 45\} \\ \bar{b}^4_1 = \{7 & 10 & 20 & 23 & 33 & 36 & 46\} \end{bmatrix},$$

$$\bar{P}_5 = \begin{bmatrix} \bar{b}^5_7 = \{1 & 12 & 16 & 27 & 31 & 42 & 46\} \\ \bar{b}^5_6 = \{2 & 13 & 17 & 28 & 32 & 36 & 47\} \\ \bar{b}^5_5 = \{3 & 14 & 18 & 22 & 33 & 37 & 48\} \\ \bar{b}^5_4 = \{4 & 8 & 19 & 23 & 34 & 38 & 49\} \\ \bar{b}^5_3 = \{5 & 9 & 20 & 24 & 35 & 39 & 43\} \\ \bar{b}^5_2 = \{6 & 10 & 21 & 25 & 29 & 40 & 44\} \\ \bar{b}^5_1 = \{7 & 11 & 15 & 26 & 30 & 41 & 45\} \end{bmatrix}, \bar{P}_6 = \begin{bmatrix} \bar{b}^6_7 = \{1 & 13 & 18 & 23 & 35 & 40 & 45\} \\ \bar{b}^6_6 = \{2 & 14 & 19 & 24 & 29 & 41 & 46\} \\ \bar{b}^6_5 = \{3 & 8 & 20 & 25 & 30 & 42 & 47\} \\ \bar{b}^6_4 = \{4 & 9 & 21 & 26 & 31 & 36 & 48\} \\ \bar{b}^6_3 = \{5 & 10 & 15 & 27 & 32 & 37 & 49\} \\ \bar{b}^6_2 = \{6 & 11 & 16 & 28 & 33 & 38 & 43\} \\ \bar{b}^6_1 = \{7 & 12 & 17 & 22 & 34 & 39 & 44\} \end{bmatrix},$$

$$\bar{P}_7 = \begin{bmatrix} \bar{b}^7_7 = \{1 & 14 & 20 & 26 & 32 & 38 & 44\} \\ \bar{b}^7_6 = \{2 & 8 & 21 & 27 & 33 & 39 & 45\} \\ \bar{b}^7_5 = \{3 & 9 & 15 & 28 & 34 & 40 & 46\} \\ \bar{b}^7_4 = \{4 & 10 & 16 & 22 & 35 & 41 & 47\} \\ \bar{b}^7_3 = \{5 & 11 & 17 & 23 & 29 & 42 & 48\} \\ \bar{b}^7_2 = \{6 & 12 & 18 & 24 & 30 & 36 & 49\} \\ \bar{b}^7_1 = \{7 & 13 & 19 & 25 & 31 & 37 & 43\} \end{bmatrix}, \bar{P}_8 = \begin{bmatrix} \bar{b}^8_7 = \{1 & 8 & 15 & 22 & 29 & 36 & 43\} \\ \bar{b}^8_6 = \{2 & 9 & 16 & 23 & 30 & 37 & 44\} \\ \bar{b}^8_5 = \{3 & 10 & 17 & 24 & 31 & 38 & 45\} \\ \bar{b}^8_4 = \{4 & 11 & 18 & 25 & 32 & 39 & 46\} \\ \bar{b}^8_3 = \{5 & 12 & 19 & 26 & 33 & 40 & 47\} \\ \bar{b}^8_2 = \{6 & 13 & 20 & 27 & 34 & 41 & 48\} \\ \bar{b}^8_1 = \{7 & 14 & 21 & 28 & 35 & 42 & 49\} \end{bmatrix},$$

In order to construct RBD$(\widetilde{X}, \widetilde{A})$, where $|\widetilde{X}| = (q-e)(q+f) = (7-3)(7+1) = 32$ such that $\mu = 1$, we consider the following steps.

1. Choose any $h = e - f = 3 - 1 = 2$ blocks from $\bar{P}_1$. Let these blocks be $\bar{b}^1_1$ and $\bar{b}^1_2$. Let $S_1 = \bar{b}^1_1 \cup \bar{b}^1_2 = \{36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49\}$, as annotated in red in the above matrices.

2. Choose another $f = 1$ block from $\bar{P}_1$. Let it be $\bar{b}^1_3$. Now choose any $e = 3$ elements from it. Let these be $S_2 = \{33, 34, 35\}$. Set $S = S_1 \cup S_2 = \{33, 34, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49\}$ (indicated in red).

3. Remove the elements of set S from RBD$(\bar{X}, \bar{A})$. Call the resulting combinatorial design RBD$(\widetilde{X}, \widetilde{A})$, where $|\widetilde{X}| = 32$ and $\widetilde{A} = \{\widetilde{P}_1, \widetilde{P}_2, \widetilde{P}_3, \widetilde{P}_4, \widetilde{P}_5, \widetilde{P}_6, \widetilde{P}_7, \widetilde{P}_8\}$, presented as below.

$$\widetilde{P}_1 = \begin{bmatrix} \widetilde{b}^1_7 = \{1 & 2 & 3 & 4 & 5 & 6 & 7\} \\ \widetilde{b}^1_6 = \{8 & 9 & 10 & 11 & 12 & 13 & 14\} \\ \widetilde{b}^1_5 = \{15 & 16 & 17 & 18 & 19 & 20 & 21\} \\ \widetilde{b}^1_4 = \{22 & 23 & 24 & 25 & 26 & 27 & 28\} \\ \widetilde{b}^1_3 = \{29 & 30 & 31 & 32\} & & & \end{bmatrix}, \widetilde{P}_2 = \begin{bmatrix} \widetilde{b}^2_7 = \{1 & 9 & 17 & 25\} & \\ \widetilde{b}^2_6 = \{2 & 10 & 18 & 26\} & \\ \widetilde{b}^2_5 = \{3 & 11 & 19 & 27\} & \\ \widetilde{b}^2_4 = \{4 & 12 & 20 & 28 & 29\} \\ \widetilde{b}^2_3 = \{5 & 13 & 21 & 22 & 30\} \\ \widetilde{b}^2_2 = \{6 & 14 & 15 & 23 & 31\} \\ \widetilde{b}^2_1 = \{7 & 8 & 16 & 24 & 32\} \end{bmatrix},$$

$$\widetilde{P}_3 = \begin{bmatrix} \widetilde{b}^3_7 = \{1 & 10 & 19 & 28 & 30\} \\ \widetilde{b}^3_6 = \{2 & 11 & 20 & 22 & 31\} \\ \widetilde{b}^3_5 = \{3 & 12 & 21 & 23 & 32\} \\ \widetilde{b}^3_4 = \{4 & 13 & 15 & 24\} & \\ \widetilde{b}^3_3 = \{5 & 14 & 16 & 25\} & \\ \widetilde{b}^3_2 = \{6 & 8 & 17 & 26\} & \\ \widetilde{b}^3_1 = \{7 & 9 & 18 & 27 & 29\} \end{bmatrix}, \widetilde{P}_4 = \begin{bmatrix} \widetilde{b}^4_7 = \{1 & 11 & 21 & 24\} & \\ \widetilde{b}^4_6 = \{2 & 12 & 15 & 25\} & \\ \widetilde{b}^4_5 = \{3 & 13 & 16 & 26 & 29\} \\ \widetilde{b}^4_4 = \{4 & 14 & 17 & 27 & 30\} \\ \widetilde{b}^4_3 = \{5 & 8 & 18 & 28 & 31\} \\ \widetilde{b}^4_2 = \{6 & 9 & 19 & 22 & 32\} \\ \widetilde{b}^4_1 = \{7 & 10 & 20 & 23\} & \end{bmatrix},$$

$$\widetilde{P}_5 = \begin{bmatrix} \widetilde{b}^5_7 = \{1 & 12 & 16 & 27 & 31\} \\ \widetilde{b}^5_6 = \{2 & 13 & 17 & 28 & 32\} \\ \widetilde{b}^5_5 = \{3 & 14 & 18 & 22\} & \\ \widetilde{b}^5_4 = \{4 & 8 & 19 & 23\} & \\ \widetilde{b}^5_3 = \{5 & 9 & 20 & 24\} & \\ \widetilde{b}^5_2 = \{6 & 10 & 21 & 25 & 29\} \\ \widetilde{b}^5_1 = \{7 & 11 & 15 & 26 & 30\} \end{bmatrix}, \widetilde{P}_6 = \begin{bmatrix} \widetilde{b}^6_7 = \{1 & 13 & 18 & 23\} & \\ \widetilde{b}^6_6 = \{2 & 14 & 19 & 24 & 29\} \\ \widetilde{b}^6_5 = \{3 & 8 & 20 & 25 & 30\} \\ \widetilde{b}^6_4 = \{4 & 9 & 21 & 26 & 31\} \\ \widetilde{b}^6_3 = \{5 & 10 & 15 & 27 & 32\} \\ \widetilde{b}^6_2 = \{6 & 11 & 16 & 28\} & \\ \widetilde{b}^6_1 = \{7 & 12 & 17 & 22\} & \end{bmatrix},$$

$$\widetilde{P}_7 = \begin{bmatrix} \widetilde{b}^7_7 = \{1 & 14 & 20 & 26 & 32\} \\ \widetilde{b}^7_6 = \{2 & 8 & 21 & 27\} & \\ \widetilde{b}^7_5 = \{3 & 9 & 15 & 28\} & \\ \widetilde{b}^7_4 = \{4 & 10 & 16 & 22\} & \\ \widetilde{b}^7_3 = \{5 & 11 & 17 & 23 & 29\} \\ \widetilde{b}^7_2 = \{6 & 12 & 18 & 24 & 30\} \\ \widetilde{b}^7_1 = \{7 & 13 & 19 & 25 & 31\} \end{bmatrix}, \widetilde{P}_8 = \begin{bmatrix} \widetilde{b}^8_7 = \{1 & 8 & 15 & 22 & 29\} \\ \widetilde{b}^8_6 = \{2 & 9 & 16 & 23 & 30\} \\ \widetilde{b}^8_5 = \{3 & 10 & 17 & 24 & 31\} \\ \widetilde{b}^8_4 = \{4 & 11 & 18 & 25 & 32\} \\ \widetilde{b}^8_3 = \{5 & 12 & 19 & 26\} & \\ \widetilde{b}^8_2 = \{6 & 13 & 20 & 27\} & \\ \widetilde{b}^8_1 = \{7 & 14 & 21 & 28\} & \end{bmatrix}.$$

Note that here all the blocks are not of the same sizes, but any two blocks from different parallel classes have at most 1 element in common, i.e., $\mu = 1$. The blocks sizes are in the set $\{(q-3), (q-2), q\} = \{4, 5, 7\}$. The number of parallel classes in $\widetilde{A}$ remains $q + 1 = 8$. This technique is now more formally explained for the general case in Construction 5.6.2 below. Let $d = k \times s = (q-e)(q+f)$, with $0 < f \leq e \leq q$. The steps for constructing the RBD(X, A) are as follows.

Construction 5.6.2. Given q, a prime power, construct $(q^2, q, 1)$-ARBIBD. Call this design $(\bar{X}, \bar{A})$ with $\bar{X} = \{1, 2, \ldots, q^2\}$ and $|\bar{A}| = q(q+1)$ many blocks, each block is of constant size q. It will have $r = q+1$ many parallel classes, call them $\{\bar{P}_1, \bar{P}_2, \ldots, \bar{P}_{q+1}\}$, each parallel class having q many blocks of constant size q. Between any two blocks from different parallel classes, exactly one element will be common, i.e., $|\bar{b}^l_i \cap \bar{b}^m_j| = 1, \forall\ l \neq m$.

1. Given $e \geq f$, choose $h = e - f \geq 0$ many blocks from $\bar{P}_1$, which are $\{\bar{b}^1_1, \bar{b}^1_2, \ldots, \bar{b}^1_h\}$. Let $S_1 = \bar{b}^1_1 \cup \bar{b}^1_2 \cup \ldots \cup \bar{b}^1_h$. Therefore, $|S_1| = h \times q$.

2. From $\{\bar{b}^1_{h+1}, \bar{b}^1_{h+2}, \ldots, \bar{b}^1_{h+f}\}$ blocks of $\bar{P}_1$, choose any e number of elements from each of them. Let S_2 be the union of all these elements. Therefore, $|S_2| = e \times f$. Let $S = S_1 \cup S_2$.

3. Remove the elements of set S from RBD $(\bar{X}, \bar{A})$ and call the resulting design as RBD$(\widetilde{X}, \widetilde{A})$.

We claim that the above RBD$(\widetilde{X}, \widetilde{A})$ is such that $|\widetilde{X}| = (q - e)(q + f)$ and $\widetilde{A}$ consists of $q + 1$ many parallel classes having different block sizes, such that blocks from different parallel classes have at most one element in common, i.e., $|b^l_i \cap b^m_j| \leq 1, \forall\ l \neq m$. Hence $\mu = 1$. We formalize this in the form of a lemma below.

Lemma 5.6.2. *Let $d = (q - e)(q + f)$ for $f, e \in \mathbb{N}$ with $0 < f \leq e \leq q$ and some prime power q. Then one can construct an RBD$(\widetilde{X}, \widetilde{A})$, with $|X| = d$ having block sizes from the set of integers $\{(q-e), (q-e+1), \ldots, (q-e+f), q\}$ with $\mu = 1$, and having $r = q+1$ many parallel classes.*

Proof. Refer to Construction 5.6.2 above. Here RBD$(\bar{X}, \bar{A})$ is an ARBIBD with $|\bar{X}| = q^2$, having constant block size q. Note that any pair of blocks from different parallel classes have exactly one element in common, i.e., $|\bar{b}^l_i \cap \bar{b}^m_j| = 1\ \forall\ l \neq m$. The number of elements in the set $|S| = |S_1 \cup S_2| = |S_1| + |S_2| = (e - f)q + ef < q^2$, which is a proper subset of $\bar{X}$. These are removed from all the parallel classes of RBD$(\bar{X}, \bar{A})$. Hence, the resulting design RBD$(\widetilde{X}, \widetilde{A})$ is such that $|\widetilde{X}| = q^2 - (e - f)q + ef = (q - e)(q + f) = d$, having same number of parallel classes as in $\bar{A}$. The number of element common between any two blocks from different parallel classes would be at most 1, i.e., $|\widetilde{b}^l_i \cap \widetilde{b}^m_j| \leq 1, \forall\ l \neq m$.

To obtain the sizes of the blocks in RBD$(\widetilde{X}, \widetilde{A})$, note that S_1 contains all elements from $h = (e - f)$ number of blocks of $\bar{P}_1$. Hence S_1 would have at least h elements in common with all the blocks of remaining parallel classes. Thus, removal of the elements in S_1 from the parallel classes $\bar{P}_l, l \geq 2$ will remove at least h elements from each block of $\bar{P}_l$ which implies $|\bar{b}^l_i \setminus S_1| = q - (e - f)$. Further S_2 contains e elements from f many blocks of $\bar{P}_1$. Thus, the blocks in $\bar{P}_2, \bar{P}_3, \ldots, \bar{P}_{q+1}$ will have at most f many elements in common with S_2. Consequently, after removal of all the elements in S, from the parallel class $\bar{P}_l$, the block size $|\widetilde{b}^l_i|,\ l \geq 2$ will be maximum $q - (e - f) = (q - h)$ and minimum $q - (e - f) - f = (q - e)$. Further, the blocks in $\widetilde{P}_1$ will be of sizes $q, (q-e)$ and have total $(q-h)$ number of blocks. □

We will now show how one can use f many blocks of the parallel class $\widetilde{P}_1$ in RBD$(\widetilde{X}, \widetilde{A})$, as constructed above, to reshape any one of the parallel classes $\widetilde{P}_l,\ l \neq 1$ into a parallel class having $(q + f)$ many blocks each of size $(q - e)$, which we denote by P_l and the resulting combinatorial design by RBD(X, A). Since $\widetilde{P}_1$ have $q - h$ number of blocks, thus $\lfloor \frac{q-h}{f} \rfloor$ many parallel classes of $\bar{A}$ can be reshaped into a parallel class of A.

Let us first demonstrate the construction by using RBD$(\widetilde{X}, \widetilde{A})$, as constructed in the example earlier in this section, where $|\widetilde{X}| = (7-3)(7+1) = 4 \cdot 8 = 32$, with $q = 7, e = 3$, $f = 1$ and $h = e - f = 2$. Note that $\widetilde{P}_1$ has $q - h = 5$ blocks, and all the other parallel classes have $q = 7$ blocks each. Let us denote the excess number of elements on each block of $\widetilde{b}_j^l$, $l \geq 2$ than $(q - e)$ by m_j^l. Hence $m_i^l = |\widetilde{b}_i^l| - (q - e)$. Here for each block of the parallel class $\widetilde{P}_l$, $l \geq 2$, the value of m_i^l is either 0 or 1. If the block $|\widetilde{b}_i^l| = 5$, then $m_i^l = |\widetilde{b}_i^l| - (q-e) = 5 - (7-3) = 1$ and similarly for block $|\widetilde{b}_i^l| = 4$, $m_i^l = 0$. Note that $\sum_{i=1}^{q} m_i^l = (q-e) \cdot f = (7-3) \cdot 1 = 4, \forall\, l \geq 2$. We modify this RBD$(\widetilde{X}, \widetilde{A})$ as follows.

1. Since $f = 1$, consider one block $\widetilde{b}_3^1$ of $\widetilde{P}_1$, which has 4 elements in it. Remove these elements from different blocks of $\widetilde{P}_2$ and add them as separate block in $\widetilde{P}_2$. Denote the resulting parallel class as P_2.

2. Consider the parallel class $\widetilde{P}_3$ and the next $f = 1$ block of $\widetilde{P}_1$, i.e., the block $\widetilde{b}_4^1$. Choose a block from $\widetilde{P}_3$, say $\widetilde{b}_1^3$. Since $|\widetilde{b}_1^3| = 5$, i.e., it has one element more than $q - e = 4$, hence mark one common element between $\widetilde{b}_4^1$ and $\widetilde{b}_1^3$ which is 27 in this case. Sequentially execute this for all the blocks of $\widetilde{P}_1$. This will mark the elements $\{27, 23, 22, 28\}$ on $\widetilde{b}_4^1$.

3. Since $m_j^3 = 0$ or 1, the above step will mark exactly $(q - e) = 4$ elements on $\widetilde{b}_4^1$. In a situation, if m_i^l has more than one elements, then further iterations are required to mark exactly $(q-e)$ elements on the blocks of $\widetilde{P}_1$. Refer to Step 3 of Construction 5.6.3 later for the exact strategy in this regard.

4. Now remove the elements marked on $\widetilde{b}_4^1$, i.e., $\{27, 23, 22, 28\}$ from $\widetilde{P}_3$ and add them as a separate block of $\widetilde{P}_3$ and denote the resulting parallel class as P_3.

5. Consider the next parallel class $\widetilde{P}_4$ and the next $f = 1$ block of $\widetilde{P}_1$, i.e., the block $\widetilde{b}_5^1$. Then repeat the Steps 2, 3, 4 to obtain P_4.

6. Since the number of blocks in $\widetilde{P}_1 = 5$, in this way $r = \frac{5}{1} = 5$ parallel classes, i.e., $\widetilde{P}_l$, $l = 2, 3, 4, 5, 6$ can be modified. Discard $\widetilde{P}_7$ and $\widetilde{P}_8$. The resulting RBD(X, A) is such that $|X| = 32$ with A consisting of parallel classes $\{P_2, P_3, P_4, P_5, P_6\}$ as shown below.

$$P_2 = \begin{bmatrix} b_8^2 = \{29 & 30 & 31 & 32\} \\ b_7^2 = \{1 & 9 & 17 & 25\} \\ b_6^2 = \{2 & 10 & 18 & 26\} \\ b_5^2 = \{3 & 11 & 19 & 27\} \\ b_4^2 = \{4 & 12 & 20 & 28\} \\ b_3^2 = \{5 & 13 & 21 & 22\} \\ b_2^2 = \{6 & 14 & 15 & 23\} \\ b_1^2 = \{7 & 8 & 16 & 24\} \end{bmatrix}, P_3 = \begin{bmatrix} b_8^3 = \{22 & 23 & 27 & 28\} \\ b_7^3 = \{1 & 10 & 19 & 30\} \\ b_6^3 = \{2 & 11 & 20 & 31\} \\ b_5^3 = \{3 & 12 & 21 & 32\} \\ b_4^3 = \{4 & 13 & 15 & 24\} \\ b_3^3 = \{5 & 14 & 16 & 25\} \\ b_2^3 = \{6 & 8 & 17 & 26\} \\ b_1^3 = \{7 & 9 & 18 & 29\} \end{bmatrix}, P_4 = \begin{bmatrix} b_8^4 = \{16 & 17 & 18 & 19\} \\ b_7^4 = \{1 & 11 & 21 & 24\} \\ b_6^4 = \{2 & 12 & 15 & 25\} \\ b_5^4 = \{3 & 13 & 26 & 29\} \\ b_4^4 = \{4 & 14 & 27 & 30\} \\ b_3^4 = \{5 & 8 & 28 & 31\} \\ b_2^4 = \{6 & 9 & 22 & 32\} \\ b_1^4 = \{7 & 10 & 20 & 23\} \end{bmatrix},$$

$$P_5 = \begin{bmatrix} b_8^5 = \{10 & 11 & 12 & 13\} \\ b_7^5 = \{1 & 16 & 27 & 31\} \\ b_6^5 = \{2 & 17 & 28 & 32\} \\ b_5^5 = \{3 & 14 & 18 & 22\} \\ b_4^5 = \{4 & 8 & 19 & 23\} \\ b_3^5 = \{5 & 9 & 20 & 24\} \\ b_2^5 = \{6 & 21 & 25 & 29\} \\ b_1^5 = \{7 & 15 & 26 & 30\} \end{bmatrix}, P_6 = \begin{bmatrix} b_8^6 = \{2 & 3 & 4 & 5\} \\ b_7^6 = \{1 & 13 & 18 & 23\} \\ b_6^6 = \{14 & 19 & 24 & 29\} \\ b_5^6 = \{8 & 20 & 25 & 30\} \\ b_4^6 = \{9 & 21 & 26 & 31\} \\ b_3^6 = \{10 & 15 & 27 & 32\} \\ b_2^6 = \{6 & 11 & 16 & 28\} \\ b_1^6 = \{7 & 12 & 17 & 22\} \end{bmatrix}, P_7 = \begin{bmatrix} b_8^7 = \{5 & 12 & 19 & 26\} \\ b_7^7 = \{1 & 14 & 20 & 32\} \\ b_6^7 = \{2 & 8 & 21 & 27\} \\ b_5^7 = \{3 & 9 & 15 & 28\} \\ b_4^7 = \{4 & 10 & 16 & 22\} \\ b_3^7 = \{11 & 17 & 23 & 29\} \\ b_2^7 = \{6 & 18 & 24 & 30\} \\ b_1^7 = \{7 & 13 & 25 & 31\} \end{bmatrix}.$$

We will now discuss about P_7 as presented above. From the two discarded parallel classes $\widetilde{P}_7$ and $\widetilde{P}_8$, we find that one can use the block $\widetilde{b}_3^8$ and remove the elements in it from $\widetilde{P}_7$, and place them as a separate block of parallel class $\widetilde{P}_7$, resulting into another parallel class having $(q+f) = 8$ many blocks each block having $(q-e) = 4$ elements each. We denote this parallel class as P_7. Certainly this is not unique as there are other possibilities to obtain a parallel class using $\widetilde{P}_7$ and $\widetilde{P}_8$. Thus here we actually obtain $r = 6 > \left\lfloor \frac{q-e}{f} \right\rfloor + 1 = 5$, indicating that $\left\lfloor \frac{q-e}{f} \right\rfloor + 1$ is not a tight lower bound in this example.

The above construction is formally explained for the general case in Construction 5.6.3 below. We consider RBD$(\widetilde{X}, \widetilde{A})$ constructed in 5.6.2 with $|\widetilde{X}| = (q-e)(q+f)$ as the input for following construction. To begin with, compute $m_j^l = |\widetilde{b}_j^l| - (q-e),\ l \geq 2$ for each block of $\widetilde{P}_l,\ l \geq 2$, which is the count of the excess number of elements on each block of $\widetilde{b}_j^l,\ l \geq 2$ than what is required, which is $q-e$. Note that $\sum_{j=1}^q m_j^l = \sum_{j=1}^q \Big(|\widetilde{b}_j^l| - (q-e)\Big) = \sum_{j=1}^q |\widetilde{b}_j^l| - q(q-e) = (q-e)(q+f) - q(q-e) = (q-e)f,\ \forall\, l \geq 2$. Thus $\sum_{j=1}^q m_j^l = (q-e)f$ is constant for all the parallel classes of RBD$(\widetilde{X}, \widetilde{A})$ except $\widetilde{P}_1$, which consists of $q-h$ blocks of sizes $\{(q-e), q\}$ and are being used to modify the r number of other parallel classes and will be discarded in the end.

Construction 5.6.3. Let $d = k \times s = (q-e)(q+f)$, with $0 < f \leq e \leq q$ and we consider RBD$(\widetilde{X}, \widetilde{A})$ from Construction 5.6.2 with $|\widetilde{X}| = (q-e)(q+f)$ as the input.

1. Consider f many blocks of $\widetilde{P}_1$, which has $(q-e)$ elements, i.e., the blocks $\{\widetilde{b}^1_{h+1}, \widetilde{b}^1_{h+2}, \ldots, \widetilde{b}^1_{h+f}\}$. Remove the elements in the blocks $\{\widetilde{b}^1_{h+1}, \widetilde{b}^1_{h+2}, \ldots, \widetilde{b}^1_{h+f}\}$ from different blocks of $\widetilde{P}_2$ and add the blocks $\{\widetilde{b}^1_{h+1}, \widetilde{b}^1_{h+2}, \ldots, \widetilde{b}^1_{h+f}\}$ as blocks of $\widetilde{P}_2$. Name the resulting parallel class as P_2.

2. Consider the parallel class $\widetilde{P}_3$ and next f many blocks of $\widetilde{P}_1$, i.e., $\{\widetilde{b}^1_{(h+f+1)}, \widetilde{b}^1_{(h+f+2)}, \ldots, \widetilde{b}^1_{(h+2f)}\}$, each consisting of q many elements. Call this set of blocks as S_3^1. Select a block

from $\widetilde{P}_3$, say $\widetilde{b}_1^3$. Corresponding to this block, mark m_1^3 number of elements which are common with the blocks in set S_3^1. Then move them to the next block of $\widetilde{P}_3$, namely $\widetilde{b}_2^3$, and mark m_2^3 number of elements common with the blocks in S_3^1. Sequentially continue this for all the blocks of $\widetilde{P}_3$.

3. Now consider $\widetilde{b}_u^1$, $\widetilde{b}_v^1 \in S_3^1$, such that $\widetilde{b}_u^1$ has more elements marked than $(q-e)$ and $\widetilde{b}_v^1$ has less elements marked than $(q-e)$. Identify the blocks of $\widetilde{P}_3$ which have a marked element common with $\widetilde{b}_u^1$, but has an unmarked element common with $\widetilde{b}_v^1$, say block $\widetilde{b}_j^3$. Then unmark this element in $\widetilde{b}_u^1$, and mark the common element between the block $\widetilde{b}_j^3$ and $\widetilde{b}_v^1$ on the block $\widetilde{b}_v^1$. Thus, the marked element on $\widetilde{b}_u^1$ is removed and the marked on $\widetilde{b}_v^1$ is added. Iterate this for all such blocks in S_3^1 which has marked elements different from $(q-e)$ and continue this till all the blocks in set S_3^1 have exactly $(q-e)$ marked element.

   Later in Lemma 5.6.3, we will show that such a block $\widetilde{b}_j^3$ will always exist. Further this process will terminate in a finite number of steps as there are finite number of blocks and elements, and every iteration adds the marked element of a block having less elements marked than $(q-e)$ and removes the mark element of a block having more elements marked than $(q-e)$.

4. Remove the elements marked on each of the blocks in the set S_3^1 from the parallel class $\widetilde{P}_3$ and add the elements marked on the block, say $\widetilde{b}_{h+f+1}^1$ as separate blocks in $\widetilde{P}_3$. Similarly add elements marked on the block $\widetilde{b}_{h+f+2}^1$ as separate blocks in $\widetilde{P}_3$ and so on for all the blocks in S_3^1. Call the resulting parallel class as P_3.

5. Then consider the next parallel class $\widetilde{P}_4$ and the next f many blocks of $\widetilde{P}_1$ and repeat the steps 2, 3 and 4 as mentioned above. Denote the resulting class as P_4 and continue till the number of blocks in $\widetilde{P}_1$ becomes less than f .

6. Since the number of blocks in $\widetilde{P}_1$ is $q-h = q-(e-f)$, in this way $r = \left\lfloor \frac{q-(e-f)}{f} \right\rfloor = \left\lfloor \frac{q-e}{f} \right\rfloor + 1$ many parallel classes $\widetilde{P}_r$ can be modified. Then the RBD(X, A), where $X = \{1, 2, \ldots, (q-e)(q+f)\}$ and $A = \{P_2, P_3, \ldots, P_{r+1}\}$ is the required design.

Note that in Step 4 above, since each block in the set S_3^1 has $q-e$ elements marked and total number of blocks is f, hence total number of elements removed from $\widetilde{P}_3$ are $(q-e) \times f$. Thus, we are basically using a set of f blocks from the parallel classes $\widetilde{P}_1$ to reshape one of the remaining parallel class, into blocks of size $(q-e)$, having $(q+f)$ blocks. This is achieved by identifying $(q-e)$ elements of one block from the parallel classes $\widetilde{P}_1$, and in different blocks of parallel class say $\widetilde{P}_l$. Thereafter, we delete these elements from different blocks $\widetilde{P}_l$, and add these elements as a separate block in $\widetilde{P}_l$. Thus, the resulting parallel class will consist of $(q+f)$ blocks, each having $(q-e)$ elements.

We claim that the above design (X, A) is a RBD, such that $|X| = (q-e)(q+f)$ and A consists of $r = \left\lfloor \frac{q-e}{f} \right\rfloor + 1$ many parallel classes each having $(q+f)$ many blocks each of size $(q-e)$, such that the blocks from different parallel classes have at most one element in common, i.e., $|b_i^l \cap b_j^m| \leq 1 \; \forall \; i \neq j$. We formalize this in the following lemma.

Lemma 5.6.3. *Let $d = (q-e)(q+f)$, for $f, e \in \mathbb{N}$ with $0 < f \leq e \leq q$ and q some power of prime. Then one can construct an RBD(X, A), with $|X| = d$ having constant block size $(q-e)$ with $\mu = 1$, and having at least $r = \left\lfloor \frac{q-e)}{f} \right\rfloor + 1$ many parallel classes.*

Proof. Refer to Construction 5.6.3 above. Since in RBD$(\widetilde{X}, \widetilde{A})$ any pair of blocks from different parallel classes has at most one element in common, we have $|\bar{b}_i^l \cap \bar{b}_j^m| \leq 1 \; \forall \; l \neq m$. Since no element of RBD$(\widetilde{X}, \widetilde{A})$ has been deleted or added to it to obtain RBD(X, A), hence $d = |\widetilde{X}| = |X| = (q-e)(q+f)$. From the Step 6 of Construction 5.6.3, we obtain $r = \left\lfloor \frac{q-e)}{f} \right\rfloor + 1$.

Now we show that Step 2 can be successfully executed. That is, from the set of f many blocks of $\widetilde{P}_1$, it will be possible to mark $\sum_{i=1}^{q} m_i^l = (q-e) \times f, \; \forall \; l \geq 2$. Note that each block $\widetilde{b}_j^1, \; j > e$ has exactly one element common with $\widetilde{b}_j^l, \; j = 1, 2, \ldots, q, \; l \geq 2$. As $0 \leq m_j^l \leq f$, corresponding to each block $\widetilde{b}_j^l$, there will always be m_j^l elements on different blocks, which is total f in number. Hence Step 2 can be successfully executed.

Steps 3 and 4 are related to the construction where elements are to be marked on blocks in the set S_3^1 having f many blocks. These steps will finally result into $(q-e)$ elements being marked on each of these blocks. For this, note that $\sum_{i=1}^{q} m_i^l = (q-e)f$. That means, if it is not possible to mark $q-e$ elements on each of the blocks in the set S_3^1, then on some block there will have more elements marked than $q-e$ and on some blocks there are less element marked than $q-e$. It is not possible that all the blocks have less than $(q-e)$ elements marked or all the blocks have more than $(q-e)$ elements marked as in that case $\sum_{i=1}^{q} m_i^l < (q-e)f$ or $> (q-e)f$ accordingly.

In case there is a block $\widetilde{b}_u^1, \; \widetilde{b}_v^1 \in S_3^1$, such the $\widetilde{b}_u^1$ has more elements marked than $(q-e)$ and $\widetilde{b}_v^1$ has less element marked than $(q-e)$, then there will exist a block of $\widetilde{P}_3$ which have marked element common with $\widetilde{b}_u^1$, but non-marked element common with $\widetilde{b}_v^1$. Suppose there is no such block in $\widetilde{P}_3$. Then the marked elements of block $\widetilde{b}_u^1$ (which is $> q-e$) and the unmarked elements of $\widetilde{b}_v^1$ (which is $> e$) would all lie on the different blocks of $\widetilde{P}_3$. However, this would imply number of blocks in $|\widetilde{P}_3| > q - e + e = q$, which is a contradiction as $|\widetilde{P}_3| = q$.

Finally, we show that $\mu = 1$. Note that the blocks which has been added in the parallel classes $\widetilde{P_2}, \widetilde{P_3}, \ldots, \widetilde{P}_{r+1}$ to construct the parallel classes $P_2, P_3, \ldots, P_{r+1}$ are respectively part of the blocks of $\widetilde{P_1}$. Since any block of $\widetilde{P_1}$ has at most one element common with any other block of $\widetilde{P_l}$, $l \geq 2$, μ will be 1 for RBD(X, A). □

Now we can use this RBD(X, A) to construct APMUBs in dimension $d = |X| = (q - e)(q + f)$ having parameters as given by Theorem 5.5.1, which we formally state and prove in the next theorem.

Theorem 5.6.2. *Let $d = (q - e)(q + f)$, for some prime power q, where $0 < f \leq e$ and $0 < (e + f) \leq \frac{3}{2}d^{\frac{1}{2}}$, $e, f \in \mathbb{N}$. Then there exist at least $r = \left\lfloor \frac{q-e}{f} \right\rfloor + 1$ many Almost Perfect MUBs, with $\Delta = \{0, \frac{1}{q-e}\}$, $\beta = \sqrt{\frac{q+f}{q-e}} = 1 + \mathcal{O}(d^{-\lambda}) \leq 2$, where $\lambda = \frac{1}{2}$ and $\epsilon = 1 - \frac{1}{q+f}$. Further, if there exists a Real Hadamard matrix of order $(q - e)$, then one can construct r many Almost Perfect Real MUBs with same parameters.*

Proof. In order to show that we can produce such APMUBs, let us consider an RBD(X, A) with $|X| = (q - e)(q + f)$ having r parallel classes of constant block size $(q - e)$, such that between the blocks from different parallel classes, there is at most one element in common, and hence $\mu = 1$.Then using this RBD along with a Hadamard matrix of order $(q - e)$, we can construct orthonormal bases following Theorem 5.5.1. Further, the condition that $\beta < 2$ for APMUB gives $(e + f) \leq \frac{3}{2}d^{\frac{1}{2}}$. In terms of q, this inequality becomes $4e + f \leq 3q$. The parameters of APMUBs are $\Delta = \{0, \frac{1}{q-e}\}$, $\beta = \sqrt{\frac{q+f}{q-e}} = 1 + \mathcal{O}(d^{-\frac{1}{2}}) \leq 2$ and sparsity $\epsilon = 1 - \frac{1}{q+f}$. Further when a real Hadamard matrix of order $(q-e)$ is available, the same can be used in the construction of Approximate Real MUBs. Since number of parallel classes r is at least $\lfloor \frac{q-e}{f} \rfloor + 1$, hence we get at least these many APMUBs. □

Remark 5.6.2. *Note that $\frac{q-e}{f}$ is $\mathcal{O}(\sqrt{d})$, when e, f are considered to be constants. That is, in such cases we obtain $\mathcal{O}(\sqrt{d})$ many APMUBs for the dimension d.*

Following Theorem 5.6.2, we can get at least $r = \left\lfloor \frac{q-e}{f} \right\rfloor + 1$ many APMUBs. This can enable us to beat the Mutually Orthogonal Latin Square (MOLS) Lower Bound construction for APMUBs (Theorem 5.6.1), according to which we obtain $N(q + f) + 1$ many APMUBs. Let us present a few illustrative examples in this regard.

- For $d = 60 = 6 \times 10$, the known value of $N(10)$ is 2 hence MOLS Lower Bound construction provides three APMUBs with β value of 1.29. On the other hand, if we use above construction method, by expressing $d = (9 - 3)(9 + 1)$, we obtain $\frac{9-(3-1)}{1} = 7$ many APMUBs with $\beta = 1.29$. In this case the number of complex MUBs, that can be constructed following prime factorization formula, is $3 + 1 = 4$ only.

- For $d = 24 = 4 \times 6$, with $N(6) = 1$, the MOLS Lower Bound construction generates 2 APRMUBs with $\beta = 1.22$. On the other hand, expressing $d = 24 = (5-1)(5+1)$ we obtain 5 APRMUBs with $\beta = 1.22$. The number of real MUBs for $d = 24$ is 2 [18] only.

Further, to illustrate the advantage of Construction 5.6.3 over Construction 5.6.1, consider the example of $d = 2^2 \times 3^2 \times 5 \times 7$ and different ways of expressing it as product of two factors, that we considered earlier following Theorem 5.6.1.

- Expressing $d = 30 \times 42$, the MOLS Lower Bound construction will provide $N(42)+1 = 6$ many APMUBs with $\beta = 1.18$, where as expressing $d = (41-11)(41+1)$ and using Theorem 5.6.2 will provide 31 many APMUBs with $\beta = 1.18$.
- or expressing $d = 28 \times 45$, the MOLS Lower Bound construction will provide $N(45)+1 = 7$ many APRMUB with $\beta = 1.27$, where as expressing $d = (43-15)(43+2)$ and using Theorem 5.6.2 will provide 15 many APRMUB with $\beta = 1.27$.

Note that, $N(42) = 5$ and $N(45) = 6$ are the presently known values of the maximum number of MOLS of these orders [1]. Here expressing $d = 35 \times 36$, we cannot use Theorem 5.6.2 as it cannot be expressed as $(q-e)(q+f)$, with q some power of prime and $0 \leq f \leq e$. Thus with this factorization of d, MOLS Lower Bound construction provides $N(36)+1 = 9$ APMUBs with $\beta = 1.01$.

Note that, $r = \left\lfloor \frac{q-(e-f)}{f} \right\rfloor$, with condition $0 < f \leq e$, is maximum for a given q when $f = e = 1$. From the asymptotic expression of β, it is clear that for $0 < f \leq e$ we will obtain β closest to 1 when $e = f = 1$. Thus for $e = f = 1$, we state the result of APMUB as a corollary below.

Corollary 5.6.3. *Let $d = q^2 - 1 = (q-1)(q+1)$ where q is a prime power. Then one can construct q many Almost Perfect MUBs with $\Delta = \left\{0, \frac{1}{q-1}\right\}$ and $\beta = \sqrt{\frac{q+1}{q-1}}$ with sparsity $\epsilon = 1 - \frac{1}{q+1}$. If a real Hadamard Matrix of order $q-1$ exists, then we have q many APRMUBs with the same parameters.*

Our observation made in connection with Hadamard matrix of order $(q-1)$, constructed through Paley method [75] after Corollary 5.6.2 is applicable here as well. That is, if $m = \frac{q-3}{2} \equiv 1 \bmod 4$ and m is some prime power, then using the Paley Construction [75], one can obtain Hadamard matrix of order $2(m+1) = q-1$. Hence for any prime power $q \equiv 1 \bmod 4$, if $\frac{q-3}{2}$ is also some prime power and is equivalent to 1 mod 4, then the real Hadamard matrix of order $q-1$ will necessarily exist through the Paley Construction. For all such q's, there exist q APRMUBs in $\mathbb{R}^{q^2-1}$ and the above corollary will become independent of the Hadamard Conjecture. Examples of such q are $13, 29, 5^3$ etc.

- For $d = (13-1)(13+1) = 2^3 \times 3 \times 7$, we obtain 13 many APRMUBs with $\beta = 1.080$. In this case number of real MUBs is only 2 and complex MUBs is 4.
- For $d = (29-1)(29+1) = 2^3 \times 3 \times 5 \times 7$, we obtain 29 many APRMUBs with $\beta = 1.035$. In this case also the number of real MUBs is only 2 and complex MUBs is 4.

The above examples clearly indicates that as d increases, β approaches closer to 1, hence we obtain APRMUBs which are significantly close to the MUBs.

5.6.3 Some problems that require further attention

It was pointed out in the example constructed above for RBD(X, A), that for $|X| = d = 4 \times 8 = (7-3)(7+1)$, one could construct more number of parallel classes than $r = \left\lfloor \frac{q-e}{f} \right\rfloor + 1 = 5$ in this case, $q = 7, e = 3, f = 1$. From our experience of constructing RBD(X, A), for the situation when $|X|$ can be expressed as $(q-e)(q+e) = q^2 - e^2$, i.e., for the situation $e = f > 0$, there appears to be always more than $r = \left\lfloor \frac{q}{f} \right\rfloor + 1$ many parallel classes. In this situation it is possible to use other parallel classes, apart from the first one of $(q^2, q, 1)$-ARBIBD, which enable us to obtain more parallel classes for RBD(X, A) than $r = \left\lfloor \frac{q}{f} \right\rfloor + 1$. A proof of this in the following form in a general setting might be an interesting open problem.

Let $d = (q-e)(q+e)$, for $e \in \mathbb{N}$ with $0 \leq e \leq q$ and q a prime power. Then one can construct an RBD(X, A), with $|X| = d$ having constant block size $(q-e)$ with maximum intersection number $\mu = 1$, and having $r \geq \frac{q}{2}$ many parallel classes.

Further our efforts for the following form of composite d could not result into number of APMUBs of the order of $\mathcal{O}(\sqrt{d})$, where q is a prime power.

- For $d = q(q+f)$, RBD having block size q, with $q+f$ many blocks in each parallel classes.
- For $d = (q-e)(q+f), 0 < e < f$, RBD having block size $q-e$ with $q+f$ many blocks in each parallel classes.

For the above forms of d, we could not construct more number of APMUBs than what is given by Mutually Orthogonal Latin Square Lower Bound construction. Further efforts in this direction or new ideas may be required for this. We believe that it should be possible to improve the MOLS lower bound in such cases as well.

Note that our construction of APMUBs are very sparse and hence the set of Bi-angular vectors are very sparse. The sparsity of each vector inner constructions, is $\epsilon = 1 - \frac{1}{s} \approx 1 - \frac{1}{\sqrt{d}}$.

Also the non zero components of the vectors are all of the same absolute value, which is $\frac{1}{s-e} \approx \frac{1}{\sqrt{d}}$. Our extensive search of literature could not find any study on bounds on the cardinality of such kind of sparse vectors, each having same sparsity. Nevertheless, there are bounds on the cardinality of flat equiangular lines. Here flat signifies that all the component of the vectors are of same magnitude. In such situation the cardinality of set of equiangular lines in $\mathbb{C}^d$ is bounded by $(d^2 - d - 1)$, Refer to [43, Lemma 2.2] which is less than d^2, which is cardinality when the constrain of flatness is relaxed. We similarly believe that the cardinality of such Bi-angular set, with with such large sparsity would be significantly less than those given in [36, Table I] and [20, Equations 3.9,5.9]]. Hence we subsequently intend to study the bounds on the cardinality of the set of Bi-angular vectors, with large sparsity.

5.7 Conclusion

In this chapter we consider construction of APMUBs, which are significantly good approximation of MUBs. In asymptotic sense, the APMUBs are almost as good as the MUBs. That is, for a dimension d, the value of the dot product between two vectors from different bases will be very close to $\frac{1}{\sqrt{d}}$, and in a few cases 0. In this paper we have formalized the definition of APMUBs and shown that for a good proportion of integers, we can construct $\mathcal{O}(\sqrt{d})$ many APMUBs. Such a generic result is elusive in cases of perfect MUBs. Thus, for all practical purposes in the domain of quantum information, or related areas, our construction ideas open up a larger possibility of obtaining required combinatorial structures. How dense are these values of d for which we can construct such APMUBs is an important research question. As the main scope of this thesis is understanding the combinatorial techniques, we leave this as a future research effort. Another important issue in this regard is that our constructions are directly related to the concept of Bi-angular vectors. We primarily note that when two vectors are randomly selected from the set of such Bi-angular vectors, there exists a very large probability that they will be making an angle of $\frac{\beta}{\sqrt{d}}$. In fact as d increases, the probability converges to certainty. This is the scenario that happens in our APMUB related constructions. We leave this too for future investigation in a disciplined manner.

Chapter 6

Further Constructions of AMUBs for Non-prime power Composite Dimensions

As discussed so far, the construction of a large class of Mutually Unbiased Bases (MUBs) for non-prime power composite dimensions ($d = k \times s$) is a long standing open problem, which leads to different construction methods for the class Approximate MUBs (AMUBs) by relaxing the criterion that the absolute value of the dot product between two vectors chosen from different bases should be $\leq \frac{\beta}{\sqrt{d}}$. In this chapter, we consider a more general class of AMUBs (ARMUBs, considering the real ones too), compared to Chapter 4. We note that the quality of AMUBs (ARMUBs) constructed using RBD(X, A) with $|X| = d$, critically depends on the parameters, $|s - k|$, μ (maximum number of elements common between any pair of blocks), and the set of block sizes. We present the construction of $\mathcal{O}\left(\sqrt{d}\right)$ many β-AMUBs for composite d when $|s-k| < \sqrt{d}$, using RBDs having block sizes approximately $\sqrt{d}$, such that $|\langle\psi_i^l|\psi_j^m\rangle| \leq \frac{\beta}{\sqrt{d}}$ where $\beta = 1 + \frac{|s-k|}{2\sqrt{d}} + \mathcal{O}\left(d^{-1}\right) \leq 2$. Moreover, if real Hadamard matrix of order k or s exists, then one can construct at least $N\left(k\right)+1$ (or $N\left(s\right)+1$) many β-ARMUBs for dimension d, with $\beta \leq 2 - \frac{|s-k|}{2\sqrt{d}} + \mathcal{O}\left(d^{-1}\right) < 2$, where $N\left(w\right)$ is the number of MOLS(w). This improves and generalizes some of our previous results for ARMUBs in Chapter 4 from two points, viz., the real cases are now extended to complex ones too. The earlier efforts use some existing RBDs, whereas here we consider new instances of RBDs that provide better results. Similar to the earlier cases, the AMUBs (ARMUBs) constructed using RBDs are in general very sparse, where the sparsity (ϵ) is $1 - \mathcal{O}\left(d^{-\frac{1}{2}}\right)$.

6.1 Introduction

In this chapter we analyze general characteristics of AMUBs constructed using combinatorial design techniques, using objects called Resolvable Block Designs, as in the earlier two chapters. We have identified parameters that critically influence the quality of AMUBs. We show that, large sets of real and complex class of Approximate MUBs, which we call β-AMUBs (not APMUBs) can be constructed, in composite dimensions ($d = k \times s$) with $|s - k| < \sqrt{d}$ using RBD. In general, for the composite dimensions (non-prime power), only a very small set of MUBs is known, even in the complex case.

In this work, we derive how β depends on the nature of RBD(X, A), with $|X| = d$. To explore this, we broadly categorize RBD(X, A) into two categories, one where all the parallel classes have a constant block size and the other, where the block sizes differ. When parallel classes have a constant size, say k, in such RBD(X, A), a single Hadamard matrix of order k can be used to yield AMUBs over $\mathbb{C}^d$ (or $\mathbb{R}^d$), depending on whether complex or real Hadamard matrices are used. Here, for the cases where parallel classes do not have a constant block size, one needs to use Hadamard matrices of the order of block sizes.

On the basis of our analysis and construction under various settings, we conclude that $|s - k|$, μ and set of Block sizes K are most critical parameters determining the closeness of AMUBs to the MUBs constructed over $\mathbb{C}^d$ (or $\mathbb{R}^d$). When block sizes are near $\sqrt{d}$ and μ is 1, we get $\mathcal{O}(\sqrt{d})$ many AMUBs for all d's with $2\delta = |s - k| < \sqrt{d}$, $\beta = 1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}(\frac{\delta^2}{d}) \leq 2$ and $\epsilon = 1 - \mathcal{O}(d^{-\frac{1}{2}})$. Further, once a real Hadamard matrix of order k or s is available, we obtain $N(s) + 1$ or $N(k) + 1$ many ARMUBs with similar characteristics.

6.2 Organization and Contribution

In Section 6.3, we provide a theoretical analysis of AMUBs that could be constructed using RBD and describe the important parameters of RBD that affect the quality of the constructed AMUBs using RBDs. For this, we categorize RBD into two categories: one having variable block size and another having constant block size. We first show that the sparsity of the AMUBs constructed using RBD is approximately $1 - \frac{1}{\sqrt{d}}$ if block sizes are around $\sqrt{d}$. Then, we present a general theorem on AMUBs, assuming the existence of a certain kind of RBD. The block sizes and the maximum number of elements common between any pair of blocks in the RBD play a crucial role in the value of β. We demonstrate that when block sizes are around $\sqrt{d}$, we obtain very sparse β-AMUBs with $\beta = \mu + \mathcal{O}\left(d^{-\frac{1}{2}}\right)$ and sparsity $\epsilon \sim 1 - \frac{1}{\sqrt{d}}$, thus showing that as d increases, β approaches μ and the sparsity approaches 1. For RBDs (X, A), with $|X| = d = k \times s$ having constant block size either k or s, we show that $\delta = \frac{|s-k|}{2}$ plays a crucial role in deciding the quality of AMUBs apart from μ. For constant block sizes, we express $d = (q-e)(q \pm f)$ where q is some power of a prime. After that, we provide an estimate of e and f using unconditional results on the gaps between primes and Cramér's conjecture.

Section 6.4 discusses algorithms for constructing the RBDs for composite d. And then we give result about β-AMUBs, which can be constructed using such RBD. In the first subsection, we give the construction for variable block sizes of RBD, with $\mu = 1$, and the number of parallel classes is greater than $\sqrt{d}$. In the following subsection, we provide construction using the RBD with constant block sizes, where μ is either 1 or 2, and the number of parallel classes is $N(s)$ or $N(k)$. We show that RBDs having constant block size can be used to construct β-ARMUBs if a Hadamard matrix of order s or k is available. We also illustrate our constructions with examples and show how these constructions improve and generalize the previous results.

In Section 6.5, we discuss and compare the present results with existing results. In Section 6.6, we summarize the main ideas of this work and conclude by suggesting further research possibilities in this direction.

6.3 Theoretical Analysis

In this section, we present a generic result dependent on the existence of a suitable RBD, achieved by appropriately categorizing RBD. After that, we explore methods to construct such RBDs. We again emphasize that in the present theoretical analysis, we assume that the points of RBD, i.e., $|X| = d$, can be increased without bound while the parameter μ remains constant. All our constructions will have this property, justifying the asymptotic analysis of the quality of AMUBs thus constructed. We categorize the analysis into two part, one where all the blocks are of constant size and the other where the blocks are not of constant size in RBD(X, A) with $|X| = d$, a composite number.

6.3.1 RBD(X, A) with variable block size.

In general, RBD(X, A) with $|X| = d$ can have block sizes varying from 1 to d. Before presenting the theorem demonstrating how RBD can be used to construct high-quality AMUBs, we provide the following lemma regarding the sparsity of the orthonormal basis constructed [65, Construction 1], having different block sizes.

Lemma 6.3.1. *Refer to [65, Construction 1]. If a parallel class P_l of RBD(X, A) has b blocks of sizes $\left\{k_1^l, k_2^l, \ldots, k_b^l\right\}$, where $\sum_i k_i^l = |P_l| = |X| = d$, then the sparsity (ϵ) of the* *orthonormal basis constructed using P_l is:*

$$\epsilon = 1 - \frac{{k_1^l}^2 + {k_2^l}^2 + \ldots + {k_b^l}^2}{d^2} \leq 1 - \frac{1}{b}.$$

Proof. To estimate sparsity, refer the construction of an orthonormal basis using RBD(X, A) as in [65, Theorem 1]. Each block within any parallel class, denoted as P_l, consisting of k_i elements, which yields k_i basis vectors. Each of these basis vectors contains k_i many non-zero elements and $(d - k_i)$ zeros. Consequently, a block with k_i elements will contribute k_i^2 non-zero elements and $k_i(d - k_i)$ zero elements. Therefore, if a parallel class P_l comprises b blocks of sizes $k_1^l, k_2^l, \ldots, k_b^l$, the total number of non-zero components across all the basis vectors is given by $\sum_i {k_i^l}^2 = {k_1^l}^2 + \ldots + {k_b^l}^2$. The constraint $\sum_i k_i^l = |P_l| = |X| = d$ represents the total number of elements in the combinatorial design. Under this constraint, $\sum_i {k_i^l}^2$ is minimized when $k_1^l = k_2^l = \ldots = k_b^l = \frac{d}{b}$, resulting in maximum sparsity giving $\sum_i {k_i^l}^2 = \frac{d^2}{b} \Rightarrow \epsilon \leq 1 - \frac{1}{b}$. □

When we know the bounds on the block size of the RBD but do not know the number of blocks, in such situation we can derive bounds on the sparsity using above result, which we state in following corollary

Corollary 6.3.1. *Refer to [65, Construction 1]. If a parallel class P_l of RBD(X, A), with $|X| = d$, has block sizes bounded below by k_o and above by k_m, then the sparsity (ϵ) of the orthonormal basis constructed using P_l*

$$1 - \frac{k_m}{d} \leq \epsilon \leq 1 - \frac{k_o}{d}.$$

Proof. From Lemma 6.3.1, the $\epsilon = 1 - \frac{{k_1^l}^2 + {k_2^l}^2 + \ldots + {k_b^l}^2}{d^2}$ where $\sum_i k_i^l = d$. To determine the minimum or maximum value of $\sum_i {k_i^l}^2$, consider that if $x + y = c$ is a constant, with $x > y$, then $(x + u)^2 + (y - u)^2 > x^2 + y^2$. Hence, the maximum value of $\sum_i {k_i^l}^2$ occurs when the maximum number of k_i^l is as large as possible, while the minimum occurs when maximum number of k_i^l is as small as possible. But since the $k_o \leq k_i^l \leq k_m$, hence when all the blocks are of size k_o, the number of blocks would be $\frac{d}{k_o}$ and when all the blocks would be size k_o, the number of blocks would be $\frac{d}{k_m}$. Thus $\frac{d}{k_o}\ k_o^2 \leq \sum_i {k_i^l}^2 \leq \frac{d}{k_m}\ k_m^2 \Rightarrow 1 - \frac{k_m}{d} \leq \epsilon \leq 1 - \frac{k_o}{d}$. □

Note that $0 \leq \epsilon \leq 1 - \frac{1}{d}$, where the upper bound corresponds to diagonal unitary matrix, which corresponds to the parallel class having d singleton blocks and the lower bound corresponds to Unitary matrix having no zero entry in it, which corresponds to parallel class having just one block consisting of all the elements of the design. RBDs can be used to construct set of orthonormal basis as given in [65, Construction 1], but all of them might not be good quality AMUBs. In this direction, we give the following theorem, where if the block sizes are $\mathcal{O}(d^{\frac{1}{2}})$, then we can get good quality sparse β-AMUBs, even when blocks are of different sizes. As noted previously, we call the largest number of elements common between any pair of blocks from different parallel classes the intersection number and denoted as μ.

Theorem 6.3.1. *Let (X, A) be an RBD with $|X| = d$ and μ, containing r parallel classes, with block sizes from the set $K = \{q-m, q-m+1, \ldots, q-m+t\}$ with $q, m, t \in \mathbb{N}$. Let $q = \sqrt{d} + \eta$, with $\eta \in \mathbb{R}$. If $(m-\eta) \leq \left(\frac{c-\mu}{c}\right)\sqrt{d}$, then we can construct r many β-AMUBs in dimension d, where $\beta = (\frac{\mu}{q-m})\sqrt{d} = \mu + \frac{\mu(m-\eta)}{\sqrt{d}} + \mathcal{O}(d^{-1}) \leq c$. Additionally, the sparsity (ϵ) is bounded by Furthermore, if real Hadamard matrices of order equal to every block size exist, then we can construct r many ARMUBs with the same β and ϵ.*

Proof. We have $|X| = d$ and each parallel class has block size from the set $K = \{q-m, q-m+1, \ldots, q-m+t\}$, with $\mu(\geq 1)$ being the maximum number of points being common between any two blocks from different parallel classes. Now, we obtain the maximum value of the dot product between two vectors from different bases would when the vectors are constructed from minimum block sizes. Thus $|\langle v_1|v_2\rangle| \leq \frac{\mu}{q-m}$ This implies, $\beta = \frac{\mu\sqrt{d}}{q-m}$ and if $\eta = q - \sqrt{d}$, then $\beta \leq c \Rightarrow (m-\eta) \leq \left(\frac{c-\mu}{c}\right)\sqrt{d}$. Since $1 \leq \mu \leq c$, we have $\left(\frac{m-\eta}{\sqrt{d}}\right) \leq \left(\frac{c-\mu}{c}\right) < 1$. Thus series expansion of β in terms of d, is given by

$$\beta = \mu\left(1 + \frac{m-\eta}{\sqrt{d}} + \frac{(m-\eta)^2}{d} + \frac{(m-\eta)^3}{d\sqrt{d}} + \ldots\right)$$

showing that $\beta = \mu + \frac{\mu(m-\eta)}{\sqrt{d}} + \mathcal{O}(d^{-1})$. Now to estimate the sparsity, we use Corollary 6.3.1 above. The block size are bounded between $(q-m)$ and $(q-m+t)$, thus,

$$1 - \frac{q-m+t}{d} \leq \epsilon \leq 1 - \frac{q-m}{d},$$

which implies $\epsilon_o - \frac{t}{d} \leq \epsilon \leq \epsilon_o$, where $\epsilon_o = 1 - \frac{q-m}{d}$. And if real Hadamard matrices of order equal to every block size exist, then they can be used as unitary matrices in the [65, Construction 1] to get real AMUBs with the same parameters, as the choice of Hadamard matrix does not affect the parameters β and ϵ of the constructed AMUBs. □

Note that the parameter β is independent of t and depends solely on μ, m, and η. This is because β, being an upper bound, is determined by the smallest block size of the RBD(X, A) and the intersection number, whereas the sparsity depends on m and t, as the block sizes determine it.

6.3.2 RBD having constant block size

In this section, we focus on analyzing the properties of AMUBs constructed using RBDs with a constant block size. The constant block size is essential if we want to utilize Hadamard matrices of the same order (equal to the block size) for all the blocks of the RBD. This is necessary as it ensures that all the basis components finally constructed are either zero or of a constant magnitude ($= 1/\sqrt{k}$), the normalizing factor for each basis vector. If the RBD has a constant block size (denoted as k), then the total number of elements, denoted as $|X| = d$, would be a multiple of k, thus $d = k \times s$. Now, two situations arise, one when $k \leq s$ and the other when $k > s$, corresponding to the scenarios where block sizes are less than or equal to the number of blocks in a parallel class and vice versa.

The case where $k \leq s$ has been analyzed in [68] in constructing APMUBs. For APMUBs, $\mu = 1$ was identified as a necessary condition, and a construction was provided for specific forms of $d = k \times s = (q - e)(q + f), 0 < f \leq e$, where $\mathcal{O}(\sqrt{d})$ many APMUBs could be constructed. The [68, Theorem 1] outlines general features of such AMUBs, concluding that for APMUB construction, one of the crucial requirements was $\mu = 1$, achievable only when $k \leq s$. This is because, when the blocks are of constant sizes, as shown in the previous chapter, $\mu \geq \lceil \frac{k}{s} \rceil$. Hence, for $\mu = 1$, it necessitates that $k \leq s$.

The constant block size is very useful for constructing ARMUB, as it necessitates the existence of only one real Hadamard matrix of order k. Otherwise, a real Hadamard matrix corresponding to all the different block sizes is needed to obtain ARMUB, which is difficult, as real Hadamard matrices are only possible of order 2 and multiples of 4. However, if the Hadamard matrix of order s is available and not k, we would require RBDs to have a block size of order s. Thus, in such a situation, we need RBDs to have a larger block size than the number of blocks in each parallel class. Toward this, we provide a general result, for $d = k \times s$, constructed using RBDs, without assuming $k \leq s$, as was done in [65, Theorem 4]. This can also be viewed as a generalization of the result of [65, Theorem 4] so that a larger class of d can be covered. For this, we state and prove the following theorem.

Theorem 6.3.2. *Suppose there exists an RBD(X, A) with an intersection number μ, having constant block size k and consisting of r parallel classes, where $|X| = d = k \times s$, with $k, s \in \mathbb{N}$ and $2\delta = (s - k)$ such that $\delta \leq \sqrt{d}$. Then, one can construct r β-AMUBs in dimension d, where $\beta = \mu\sqrt{\frac{s}{k}} = \mu\left(1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}(d^{-1})\right) \leq \left(1 + \sqrt{2}\right)\mu$, and sparsity $\epsilon = 1 - \frac{1}{s}$. Furthermore, if there exists a real Hadamard matrix of order k, we can construct r APRMUBs with the same β and ϵ values and $\Delta = 0, \frac{1}{k}, \frac{2}{k}, \dots, \frac{\mu}{k}$.*

Proof. We have $|X| = d = k \times s$, where each parallel class has a block size of k and μ represents the maximum number of points common between blocks from different parallel classes. Consequently, $\beta = \frac{\mu\sqrt{d}}{k} = \mu\sqrt{\frac{s}{k}}$. If $2\delta = s - k$, then $d = (s - 2\delta)s$, and solving for s and k, we obtain $s = \sqrt{d+\delta^2} + \delta$ and $k = \sqrt{d+\delta^2} - \delta$. Therefore, if $\beta = \mu\sqrt{\frac{s}{k}} \leq c$, it follows that $\delta \leq \left(\frac{c^2-\mu^2}{2\mu c}\right)\sqrt{d}$. Assuming δ to be small and bounded, we have $\beta = \mu\left(1 + \frac{\delta}{\sqrt{d}} + \frac{\delta^2}{2d} + \dots\right)$.

The sparsity, as defined in Lemma 6.3.1, is given by $\epsilon = 1 - \frac{k}{d} = 1 - \frac{1}{s}$. If a real Hadamard matrix of order k exists, we can use them in the construction to obtain r many real approximate MUBs in $\mathbb{R}^d$, with the same β and sparsity (ϵ). In the case of real approximate MUBs over $\mathbb{R}^d$, the Δ values, representing different possible absolute values of the inner product, would be $\Delta = \left\{0, \frac{1}{k}, \frac{2}{k}, \dots, \frac{\mu}{k}\right\}$. This implies that in the case of ARMUBs constructed using RBD(X, A) with a constant block size k, $|\Delta| = \mu + 1$, and since μ is usually a small positive integer, Δ constitutes a small set. □

The form of d as $(q-e)(q+f)$ in [68] was chosen because when q is some power of a prime, using $(q^2, q, 1)$-RBIBD, one could construct having $\mathcal{O}(\sqrt{d})$ many parallel classes. In [68], the focus was to construct RBD(X, A) such that $\mu = 1$, hence the block size could only be $(q-e)$ and not $(q+f)$. Not all composite d could be written in this form as it required the existence of prime power q, such that $\frac{k+s}{2} \leq q \leq s$. Nevertheless, expressing $d = (q-e)(q+f)$ proved beneficial in increasing the number of AMUBs to $\mathcal{O}(\sqrt{d})$. In the similar direction of constructing $\mathcal{O}(\sqrt{d})$ many parallel classes, for a larger class of composite d, we now express composite d as $(q-e)(q \pm f), 0 < f \leq e$, where q is some suitable prime power depending on factors of d and then we focus on constructing RBD(X, A) with $|X| = d$ and having q many parallel classes, with intersection number μ. The condition $0 < f \leq e$ will ensure $(q-e) \leq (q \pm f)$. Also note that when $d = q^2$, i.e., corresponding to $e = f = 0$, the RBD method gives $q+1$ many Orthonormal bases, which are MUBs [65, Corollary 3 and Corollary 4]. Hence, expressing a composite d which is not some power of a prime number, as $(q-e)(q \pm f), 0 < f \leq e$ for small values of e and f, will also help in understanding how the small perturbation in q affects the nature of the constructed orthonormal basis and its deviation from MUBs.

Using the theorem above along with [68, Theorem 1], and expressing $d = k \times s = (q-e)(q \pm f)$, where $0 < f \leq e$, we summarize the results, providing the values of its β and sparsity ϵ for the AMUBs constructed under various situations for RBD(X, A), where $|X| = d$, and all blocks of the design are of constant size, depicted as follows.

$d = k \times s$	Block size	$\mu_{\min}$	β	ϵ	β/μ
$(q-e)(q+f)$	$(q-e)$	1	$\mu\sqrt{\frac{q+f}{q-e}}$	$1-\frac{1}{q+f}$	$1+\frac{e+f}{2\sqrt{d}}+\dots$
$(q-e)(q+f)$	$(q+f)$	2	$\mu\sqrt{\frac{q-e}{q+f}}$	$1-\frac{1}{q-e}$	$1-\frac{e+f}{2\sqrt{d}}+\dots$
$(q-e)(q-f)$	$(q-e)$	1	$\mu\sqrt{\frac{q-f}{q-e}}$	$1-\frac{1}{q-f}$	$1+\frac{e-f}{2\sqrt{d}}+\dots$
$(q-e)(q-f)$	$(q-f)$	2	$\mu\sqrt{\frac{q-e}{q-f}}$	$1-\frac{1}{q-e}$	$1-\frac{e-f}{2\sqrt{d}}+\dots$

We have ignored the higher-order terms in the expansion of β as a function of $1/\sqrt{d}$. Furthermore, it is worth noting that $(e+f)$ and $(e-f)$, which appear above, are equivalent to $2\delta = s-k$ for their respective cases. Although in the cases where $\mu_{\min} = 2$, APMUBs cannot be obtained, it still qualifies as a β-AMUBs, with β bounded above by μ. Therefore, for constructing high-quality β-AMUBs, it is desirable to use RBD(X, A), ensuring that μ is minimized as much as possible. In this connection let us following lemma on Absolute Lower Bound on β

Lemma 6.3.2. *Let RBD(X,A) with $|X| = d = k \times s$ having constant block size k, is used to construct β-AMUBs where each parallel class has s many blocks, then $\beta \geq \sqrt{\frac{k}{s}}$.*

Proof. From [68, Lemma 2] for $d = k \times s$, where k is the block size and s is the number of blocks in a parallel class, then $\mu \geq \lceil \frac{k}{s} \rceil \geq \frac{k}{s}$. Thus, we have $\beta = \mu\sqrt{\frac{s}{k}} \geq \sqrt{\frac{k}{s}}$ □

Note that $\beta \geq 1$ in all cases, thus this provides a better lower bound for β than the trivial lower bound of 1, in situations where the block size exceeds the number of blocks i.e., $k > s$, in the RBD(X, A), having a constant block size.

Since, we are interested in expressing factors of $d = k \times s$ as $(q-e)(q+f)$ where q is some power of prime, we now state some facts about the gaps between two consecutive primes. In [5] it was shown that there is prime in interval$[x - x^{\theta}, x]$ for x greater than sufficiently large integer say n_o where $\theta = 0.525$. Hence, for any two consecutive prime we have, $p_{n+1} - p_n = \mathcal{O}(p_n^{0.525})$ for all prime, larger than n_o. If we define $g_n = p_{n+1} - p_n$ then the ratio $\frac{g_n}{\log(p_n)}$ is known as merit of the gap g_n. There is another important figure of merit for gap between the consecutive prime, is called Cramér - Shanks - Granville ratio based on Cramér conjecture [33]. It is defined as the ratio $\frac{g_n}{\log(p_n)^2}$. Shanks conjectured that this ratio will always be less than 1, where as Granville conjectured, that the ratio will exceed 1 or come arbitrarily close to $2/e^{\gamma} = 1.1229$ [69, 90]. On the other hand Firoozbakht's conjecture implies that the ratio is below $1 - \frac{1}{\log(p)}$ for all primes $p \geq 11$ [63]. The greatest known value of this ratio is about 0.92, after discarding the anomalously high values of the ratio for the small primes less than or equal to 7. Thus assuming Cramér conjecture, there is a prime number in interval $[x, x+\varrho\log^2 x]$ for all $x \geq 7$ where currently all the known value of $\varrho < 1$.

We now state and prove the following lemma related to expressing any composite $d = k \times s = (q-e)(q \pm f)$ and examine the availability of such q to express d in the above form and examine the asymptotic dependence of β on q, e, f, and get an estimate of these values in terms of d and its factors k and s. These will help in analyzing constructions in the next section. We state and prove the following lemmas.

Lemma 6.3.3. *If $d = k \times s$ such that $\delta = \frac{s-k}{2} \geq s^\theta$, then there exists a prime number q such that $d = (q-e)(q+f)$. Here $\theta = 0.525$ for sufficiently large s.*

Proof. We are looking for a prime number q between k and s such that $d = (q-e)(q+f)$ with $0 \leq f \leq e \Rightarrow s - q \leq q - k \Rightarrow \frac{s+k}{2} \leq q$. Hence $\frac{s+k}{2} \leq q \leq s$. The unconditional result on the gaps in the prime [5] implies the existence of a prime number in the interval $[s - s^\theta, s]$ for sufficiently large s. The current known value of $\theta = 0.525$. Applying this, we get $s - \frac{s+k}{2} = \delta \geq s^\theta$ as a sufficient condition for the existence of such prime number q. □

Since $\frac{k+s}{2} \leq q \leq s$, hence $\delta = \frac{k+s}{2} - k \leq e = q - k \leq s - k = 2\delta$ and $0 \leq f = s - q \leq s - \frac{k+s}{2} = \delta$. Thus $0 \leq f \leq \delta \leq e \leq 2\delta$ such that $\frac{e+f}{2} = \delta$. Now assuming Cramér conjecture [33] on the gap in prime number in terms of Cramér - Granville - Shanks ratio, which is less than 1, we have $\delta \geq \varrho\log^2 s$ as a sufficient condition for the existence of such a prime power q. Therefore, if it is impossible to find such prime between k and s only in situation when there is no 'sufficient' gap between them. In such a situation, we find q closest to s but greater than s and express $d = (q-e)(q-f)$. In this direction, we have the following lemma.

Lemma 6.3.4. *Let $d = k \times s$, and there is no prime power between k and s, then $d = \mathcal{O}(s^2)$ and we can express $d = (q-e)(q-f)$, with q being some prime power greater than s, such that $f = \mathcal{O}(d^{\frac{\theta}{2}})$ and $e = 2\delta + \mathcal{O}(d^{\frac{\theta}{2}})$ where $\delta = \frac{s-k}{2}$ and $\theta = 0.525$.*

Proof. The result on prime power gaps states that for sufficiently large x, there is a prime number between $[x - x^\theta, x]$. Given that there is no prime power between k and s, this implies $(s-k) = 2\delta < s^\theta$. In such a situation, choose the smallest prime power q such that $q \geq s$ and express $d = k \times s = (q-e)(q-f)$ where $f = \mathcal{O}(s^\theta)$ and $e = 2\delta + \mathcal{O}(s^\theta)$. Further note that in this situation, since $2\delta \leq s^\theta \Rightarrow k \geq s - s^\theta$. Thus $(s - s^\theta)s \leq d \leq s^2 \Rightarrow s^2 - s^{1+\theta} \leq d \leq s^2$. Hence $d = \mathcal{O}(s^2)$. Also note that $d = (s-2\delta)s \Rightarrow s = d^{\frac{1}{2}} + \delta + \frac{\delta^2}{4\sqrt{d}} + ..$ and since $\delta \leq s^\theta$, hence $s = \mathcal{O}(\sqrt{d})$ thereby implying $f = \mathcal{O}(d^{\frac{\theta}{2}})$ and $e = 2\delta + \mathcal{O}(d^{\frac{\theta}{2}})$. □

Note that in this case $\frac{e+f}{2} = \delta + f = \delta + \mathcal{O}(d^{\frac{\theta}{2}})$. And again if we assume Cramér conjecture [33] on the gap in prime number, then in terms of Cramér - Granville - Shanks ratio we have $f = \mathcal{O}(\log^2 s)$ and $e = 2\delta + \mathcal{O}(\log^2 s)$ and $\frac{e+f}{2} = \delta + \mathcal{O}(\log^2 s)$.

6.4 Construction of AMUBs through RBDs

We will characterize an AMUB by the values of β, Δ and ϵ, which we call as the parameters of the AMUB. We now present the construction of several sets of β-AMUBs, which could be useful in information processing in classical and quantum domains. We demonstrate that for a given d, there can be varying number of AMUBs having same β but different ϵ and Δ. We will compare the parameters of our construction with known constructions of AMUBs, illustrating and highlighting salient features of the present construction and how it surpasses known AMUBs in certain aspects.

To construct AMUBs through RBD, we proceed in two steps. First, we construct suitable RBDs. Then, we using the steps of [65, Construction 1] to construct a set of unitary matrices corresponding to each parallel class of RBD, having values of parameters following the results provided in Section 6.3. For ease of understanding, we will initially demonstrate each construction with a simple example, followed by a general algorithm for construction and then proof of the correctness of the construction in the form of a lemma. This will be followed by Theorem/Lemma concerning AMUB for the given form of d for which the construction has been demonstrated.

We present this in two parts: one devoted to constructing AMUBs using RBDs with non-constant block size and another devoted to constructing AMUBs using RBDs with constant block size.

6.4.1 Construction of β-AMUBs through RBD having non-constant block size

In this section, we demonstrate that for any composite $d = k \times s$ such that $|k - s| < \sqrt{d}$, we can construct an RBD(X, A) with $\mu = 1$ containing more than $\sqrt{d}$ parallel classes with non-constant block sizes which in turn will fetch $\mathcal{O}(\sqrt{d})$ many sparse β-AMUBs with $\beta = 1 + \mathcal{O}(d^{-\frac{1}{2}})$, indicating that for large d, it approaches very close to MUBs. To achieve this, we express d as either $d = (q-e)(q+f)$ or $(q-e)(q-f)$, where q is some power of prime, and e and f satisfy some suitable condition.

Let us first consider the case for $d = (q-e)(q+f)$ with $0 < f \leq e$. In [68, Theorem 3] we have shown that when d is of the form $(q-e)(q+f)$, then we can construct $\lfloor \frac{q-e}{f} \rfloor + 1$ many APMUBs, with $\beta = 1 + \mathcal{O}(d^{-\frac{1}{2}})$. Toward the proof of this theorem, the [68, Construction 4] and corresponding [68, Lemma 7] shows the existence of RBD$(\widetilde{X}, \widetilde{A})$, where $|\tilde{X}| = d = (q-e)(q+f)$ with $f \leq e$ having $r = q + 1$ parallel classes, and $\mu = 1$. The block sizes are from set $\{(q-e), (q-e+1), \ldots, (q-e+f)\}$. Now in Theorem 6.3.2, one can use RBD$(\widetilde{X}, \widetilde{A})$ to construct $q + 1$ many β-AMUBs. But since the block sizes are not constant, hence Δ will consist of more than two elements, and thus it will not satisfy the criteria of APMUB, even though $\beta = 1 + \mathcal{O}(d^{-\lambda})$ with $\lambda = \frac{1}{2}$ and $\beta \leq 2$ if $0 \leq (e+f) \leq \frac{3}{2}\sqrt{d}$. To characterize the Δ of resulting AMUBs from RBD$(\widetilde{X}, \widetilde{A})$, we define the following.

Definition 6.4.1. *For $d = (q-e)(q+f)$, where $e \geq f$ and let $\theta_1 = \frac{1}{\sqrt{q-e}}$, $\theta_2 = \frac{1}{\sqrt{q-e+1}}$, $\ldots$, $\theta_{f+1} = \frac{1}{\sqrt{q-e+f}}$, $\theta_{f+2} = \frac{1}{\sqrt{q}}$, then define $\Delta_1 = \{\theta_i\theta_j\} \cup \{0\}$ where $i, j = 1, 2, \ldots, (f+1), (f+2)$.*

Note that $|\Delta_1| = \binom{f+2}{2} + (f+2) + 1 = \frac{(f+3)(f+2)}{2} + 1 = \mathcal{O}(f^2)$. Thus the number of elements in Δ_1 is only dependent on the value of f and is proportional to the square of it. We now state and prove the result on β-AMUBs, using such RBD$(\widetilde{X}, \widetilde{A})$ as follows

Corollary 6.4.1. *If $d = (q-e)(q+f)$, for some prime-power q, and $e, f \in \mathbb{N}$ satisfying $0 < f \leq e$ and $0 < (e+f) \leq \frac{3}{2}\sqrt{d}$, then there exist at least $r = q+1$ many β-AMUBs, with $\Delta \subseteq \Delta_1$, $\beta = \sqrt{\frac{q+f}{q-e}} = 1 + \frac{e+f}{2\sqrt{d}} + \mathcal{O}(d^{-1}) \leq 2$, and $1 - \frac{q-e+f}{d} \leq \epsilon \leq 1 - \frac{1}{q}$ where ϵ denotes the sparsity.*

Proof. Consider the RBD$(\widetilde{X}, \widetilde{A})$ as constructed in [68, Construction 4], and its property given in [68, Lemma 7]. The $|\widetilde{X}| = (q-e)(q+f)$ with $f \leq e$. The block sizes of RBD$(\widetilde{X}, \widetilde{A})$ are from the set $(q-e), (q-e+1), \ldots, (q-e+f), q$. Now using Hadamard matrices of the order of the block sizes, we get the set of $q+1$ orthonormal basis. Thus, the normalizing factors of Hadamard matrices of different orders would be from set $\left\{\frac{1}{\sqrt{q-e}}, \frac{1}{\sqrt{q-e+1}}, \ldots, \frac{1}{\sqrt{q-e+f}}, \frac{1}{\sqrt{q}}\right\}$. Let's denote this set by $S_\theta = \{\theta_1, \theta_2, \ldots, \theta_{f+2}\}$ where $\theta_1 = \frac{1}{\sqrt{q-e}}$, $\theta_2 = \frac{1}{\sqrt{q-e+1}}$, $\ldots$, $\theta_{f+1} = \frac{1}{\sqrt{q-e+f}}$, and $\theta_{f+2} = \frac{1}{\sqrt{q}}$. The set has $f+2$ elements. Since $\mu = 1$ for RBD$(\widetilde{X}, \widetilde{A})$, we have $|\langle \psi_i^l | \psi_j^m \rangle| = \theta_i\theta_j$ or 0, where $|\psi_i^l\rangle$ and $|\psi_i^m\rangle$ are the vectors from two different orthonormal bases constructed using the parallel class of RBD$(\widetilde{X}, \widetilde{A})$ and $\theta_i, \theta_j \in S_\theta$. Thus, $\Delta \subseteq \Delta_1$.

Now, $\max\left\{|\langle \psi_i^l | \psi_j^m \rangle|\right\} = \max\{\theta_i\theta_j\} = \frac{1}{q-e}$ corresponding to the maximum value of $\theta_i = \theta_j = \frac{1}{\sqrt{q-e}}$. Thus, $\beta = \frac{d}{q-e} = \sqrt{\frac{q+f}{q-e}} = 1 + \frac{e-f}{2\sqrt{d}} + \mathcal{O}(d^{-1})$. And for $\beta \leq 2$ as stated in [68, Theorem 3] we should have $0 < (e+f) \leq \frac{3}{2}d^{\frac{1}{2}}$.

To estimate the value of sparsity, refer to the Lemma 6.3.1, since there are q blocks in each parallel class, thus Sparsity(ϵ) is bounded above by $1 - \frac{1}{q}$ and using Corollary 6.3.1, the lower bound of ϵ is $1 - \frac{q-e+f}{d}$. Hence $1 - \frac{q-e+f}{d} \leq \epsilon \leq 1 - \frac{1}{q}$. □

Note the that here we have improved the number of β-AMUBs for dimensions of the form $d = (q-e)(q+f)$ from $\lfloor \frac{q-e}{f} \rfloor + 1$ to $(q+1)$ many β-AMUBs with the same $\beta = 1 + \mathcal{O}(d^{-\frac{1}{2}})$. However, the order of set Δ has now increased from two valued viz. $\left\{0, \frac{\beta}{\sqrt{d}}\right\}$ to Δ_s as in Definition 6.4.1. Hence, it is also not APMUB. Also as stated in [68, Theorem 3], if there exists a real Hadamard matrix of order $(q-e)$, then there exists at least $r = \lfloor \frac{q-e}{f} \rfloor + 1$ many Almost Perfect Real MUBs (APRMUBs). However, the same cannot be applicable here, since from Corollary 6.4.1, the block sizes vary from $(q-e)$ to $(q-e+f)$ and q. Hence for ARMUBs, we require real Hadamard matrices of all these orders. Since a real Hadamard matrix can only exist when the order is divisible by 4, it is not possible to construct ARMUBs using RBD$(\widetilde{X}, \widetilde{A})$. Also the sparsity in the above case is bounded above by $1 - \frac{1}{q}$, whereas the sparsity in the case of APMUB [68, Theorem 3] is $1 - \frac{1}{q+f}$. Hence, for $f > 0$, the APMUBs are sparser than the AMUBs constructed here for same $d = (q-e)(q+f)$.

For example, when the RBD$(\widetilde{X}, \widetilde{A})$ with $d = 4 \times 8 = (7-3)(7+1)$, is used for constructing β-AMUBs, we obtain $\Delta = \frac{1}{\sqrt{d}} \times \{\beta_i\}$ where $\beta_i = \{0,\ 0.79,\ 0.96,\ 1.07,\ 1.13,\ 1.24,\ 1.41\}$. Note that, $\beta = \sqrt{\frac{q+f}{q-e}} = \sqrt{2} = 1.41$ in this case, and the sparsity $\epsilon \leq 1 - \frac{1}{7} = 0.86$. On the other hand, the APMUB for the same $d = 4 \times 8$, we obtain $\Delta = \left\{0, \frac{\beta}{\sqrt{d}}\right\} = \{0, 1.41\}$ and sparsity $\epsilon = 1 - \frac{1}{7+1} = 0.88$. Thus, the Δ reduces to two elements, and the sparsity increases slightly. Note that, $\beta = \sqrt{\frac{q+f}{q-e}} = \sqrt{2} = 1.41$ remain same for both the cases. But the advantage here is that we have 8 many β-AMUBs where as there were only 5 APMUBs.

As we have noted that when there is not sufficient gap between k and s, there need not be any prime power q between k and s, hence we can not express $d = (q-e)(q+f)$ with $f \leq e$. In such situation we find q greater than s and express $d = (q-e)(q-f)$ for suitable e and f. Refer Lemma 6.3.3 and Lemma 6.3.4 in this connection.

Let us now consider d of the form $(q-e)(q-f)$, where q is a prime power with $0 < f \leq e$. First, we demonstrate that in such cases, we can construct an RBD(X, A) with $|X| = d$ having q many parallel classes, where block sizes in the parallel classes are from set $\{q-(e+f), q-(e+f)+1, \ldots, q-e\}$. Consequently, such an RBD(X, A) can be utilized to construct q orthonormal bases following Theorem 6.3.1 thus providing $\mathcal{O}(q)$ many AMUBs in such scenarios.

For constructing such an RBD, we consider a $(q^2, q, 1)$-Affine Resolvable BIBD as the input. We denote this RBD$(\bar{X}, \bar{A})$, where $|\bar{X}| = q^2$ and all blocks of A have the same size q, with the number of parallel classes in A being $q+1$. Utilizing this, we construct RBD(X, A), where $|X| = (q-e)(q-f)$ with the same number of parallel classes q, but the blocks do not have the same size.

Let us illustrate this construction with an example. Consider $|X| = (7-2)(7-1) = 5 \times 6 = 30$, where $q = 7$, $e = 2$, and $f = 1$. We employ an Affine Resolvable $(7^2, 7, 1)$-BIBD, call it as RBD$(\bar{X}, \bar{A})$, which comprises of eight parallel classes. Each parallel class comprises seven blocks of constant size 7. We represent each parallel class as a 7×7 matrix, with each row representing one block of the parallel class. Therefore, there would be 8 such matrices as shown below to depict the combinatorial design.

$$\bar{P}_1 = \begin{bmatrix} \bar{b}_7^1 = \{1 & 2 & 3 & 4 & 5 & 6 & 7\} \\ \bar{b}_6^1 = \{8 & 9 & 10 & 11 & 12 & 13 & 14\} \\ \bar{b}_5^1 = \{15 & 16 & 17 & 18 & 19 & 20 & 21\} \\ \bar{b}_4^1 = \{22 & 23 & 24 & 25 & 26 & 27 & 28\} \\ \bar{b}_3^1 = \{29 & 30 & 31 & 32 & 33 & 34 & 35\} \\ \bar{b}_2^1 = \{36 & 37 & 38 & 39 & 40 & 41 & 42\} \\ \bar{b}_1^1 = \{43 & 44 & 45 & 46 & 47 & 48 & 49\} \end{bmatrix}, \bar{P}_2 = \begin{bmatrix} \bar{b}_7^2 = \{1 & 9 & 17 & 25 & 33 & 41 & 49\} \\ \bar{b}_6^2 = \{2 & 10 & 18 & 26 & 34 & 42 & 43\} \\ \bar{b}_5^2 = \{3 & 11 & 19 & 27 & 35 & 36 & 44\} \\ \bar{b}_4^2 = \{4 & 12 & 20 & 28 & 29 & 37 & 45\} \\ \bar{b}_3^2 = \{5 & 13 & 21 & 22 & 30 & 38 & 46\} \\ \bar{b}_2^2 = \{6 & 14 & 15 & 23 & 31 & 39 & 47\} \\ \bar{b}_1^2 = \{7 & 8 & 16 & 24 & 32 & 40 & 48\} \end{bmatrix},$$

$$\bar{P}_3 = \begin{bmatrix} \bar{b}_7^3 = \{1 & 10 & 19 & 28 & 30 & 39 & 48\} \\ \bar{b}_6^3 = \{2 & 11 & 20 & 22 & 31 & 40 & 49\} \\ \bar{b}_5^3 = \{3 & 12 & 21 & 23 & 32 & 41 & 43\} \\ \bar{b}_4^3 = \{4 & 13 & 15 & 24 & 33 & 42 & 44\} \\ \bar{b}_3^3 = \{5 & 14 & 16 & 25 & 34 & 36 & 45\} \\ \bar{b}_2^3 = \{6 & 8 & 17 & 26 & 35 & 37 & 46\} \\ \bar{b}_1^3 = \{7 & 9 & 18 & 27 & 29 & 38 & 47\} \end{bmatrix}, \bar{P}_4 = \begin{bmatrix} \bar{b}_7^4 = \{1 & 11 & 21 & 24 & 34 & 37 & 47\} \\ \bar{b}_6^4 = \{2 & 12 & 15 & 25 & 35 & 38 & 48\} \\ \bar{b}_5^4 = \{3 & 13 & 16 & 26 & 29 & 39 & 49\} \\ \bar{b}_4^4 = \{4 & 14 & 17 & 27 & 30 & 40 & 43\} \\ \bar{b}_3^4 = \{5 & 8 & 18 & 28 & 31 & 41 & 44\} \\ \bar{b}_2^4 = \{6 & 9 & 19 & 22 & 32 & 42 & 45\} \\ \bar{b}_1^4 = \{7 & 10 & 20 & 23 & 33 & 36 & 46\} \end{bmatrix},$$

$$\bar{P}_5 = \begin{bmatrix} \bar{b}_7^5 = \{1 & 12 & 16 & 27 & 31 & 42 & 46\} \\ \bar{b}_6^5 = \{2 & 13 & 17 & 28 & 32 & 36 & 47\} \\ \bar{b}_5^5 = \{3 & 14 & 18 & 22 & 33 & 37 & 48\} \\ \bar{b}_4^5 = \{4 & 8 & 19 & 23 & 34 & 38 & 49\} \\ \bar{b}_3^5 = \{5 & 9 & 20 & 24 & 35 & 39 & 43\} \\ \bar{b}_2^5 = \{6 & 10 & 21 & 25 & 29 & 40 & 44\} \\ \bar{b}_1^5 = \{7 & 11 & 15 & 26 & 30 & 41 & 45\} \end{bmatrix}, \bar{P}_6 = \begin{bmatrix} \bar{b}_7^6 = \{1 & 13 & 18 & 23 & 35 & 40 & 45\} \\ \bar{b}_6^6 = \{2 & 14 & 19 & 24 & 29 & 41 & 46\} \\ \bar{b}_5^6 = \{3 & 8 & 20 & 25 & 30 & 42 & 47\} \\ \bar{b}_4^6 = \{4 & 9 & 21 & 26 & 31 & 36 & 48\} \\ \bar{b}_3^6 = \{5 & 10 & 15 & 27 & 32 & 37 & 49\} \\ \bar{b}_2^6 = \{6 & 11 & 16 & 28 & 33 & 38 & 43\} \\ \bar{b}_1^6 = \{7 & 12 & 17 & 22 & 34 & 39 & 44\} \end{bmatrix},$$

$$\bar{P}_7 = \begin{bmatrix} \bar{b}_7^7 = \{1 & 14 & 20 & 26 & 32 & 38 & 44\} \\ \bar{b}_6^7 = \{2 & 8 & 21 & 27 & 33 & 39 & 45\} \\ \bar{b}_5^7 = \{3 & 9 & 15 & 28 & 34 & 40 & 46\} \\ \bar{b}_4^7 = \{4 & 10 & 16 & 22 & 35 & 41 & 47\} \\ \bar{b}_3^7 = \{5 & 11 & 17 & 23 & 29 & 42 & 48\} \\ \bar{b}_2^7 = \{6 & 12 & 18 & 24 & 30 & 36 & 49\} \\ \bar{b}_1^7 = \{7 & 13 & 19 & 25 & 31 & 37 & 43\} \end{bmatrix}, \bar{P}_8 = \begin{bmatrix} \bar{b}_7^8 = \{1 & 8 & 15 & 22 & 29 & 36 & 43\} \\ \bar{b}_6^8 = \{2 & 9 & 16 & 23 & 30 & 37 & 44\} \\ \bar{b}_5^8 = \{3 & 10 & 17 & 24 & 31 & 38 & 45\} \\ \bar{b}_4^8 = \{4 & 11 & 18 & 25 & 32 & 39 & 46\} \\ \bar{b}_3^8 = \{5 & 12 & 19 & 26 & 33 & 40 & 47\} \\ \bar{b}_2^8 = \{6 & 13 & 20 & 27 & 34 & 41 & 48\} \\ \bar{b}_1^8 = \{7 & 14 & 21 & 28 & 35 & 42 & 49\} \end{bmatrix},$$

In order to construct RBD(X, A), where $|X| = (q-e)(q-f) = (7-2)(7-1) = 30$ such that $\mu = 1$, do the following.

1. Choose any $e(=2)$ many blocks from $\bar{P}_1$. Let these blocks be $\bar{b}_1^1$ and $\bar{b}_2^1$. Let $S_1 = \bar{b}_1^1 \cup \bar{b}_2^1 = \{36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49\}$.

2. Choose another $f(=1)$ many block from $\bar{P}_1$. Let it be $\bar{b}^1_3$. Now choose any $(q-e)=5$ elements from each of the f blocks. Let these be $S_2=\{31,32,33,34,35\}$. Set $S=S_1\cup S_2=\{31,32,33,34,35,36,37,38,39,40,41,42, 43,44,45,46,47,48,49\}$ (indicated in red).

3. Remove the elements of the set S from the RBD $(\bar{X},\bar{A})$. Call the resulting combinatorial design a new RBD (X,A), where $|X|=30$ and $A=\{P_1,P_2,P_3,P_4,P_5,P_6,P_7,P_8\}$, presented as below.

$$P_1=\begin{bmatrix} b^1_7=\{1 & 2 & 3 & 4 & 5 & 6 & 7\} \\ b^1_6=\{8 & 9 & 10 & 11 & 12 & 13 & 14\} \\ b^1_5=\{15 & 16 & 17 & 18 & 19 & 20 & 21\} \\ b^1_4=\{22 & 23 & 24 & 25 & 26 & 27 & 28\} \\ b^1_3=\{29 & 30\} & & & & & \end{bmatrix}, P_2=\begin{bmatrix} b^2_7=\{1 & 9 & 17 & 25\} & \\ b^2_6=\{2 & 10 & 18 & 26\} & \\ b^2_5=\{3 & 11 & 19 & 27\} & \\ b^2_4=\{4 & 12 & 20 & 28 & 29\} \\ b^2_3=\{5 & 13 & 21 & 22 & 30\} \\ b^2_2=\{6 & 14 & 15 & 23\} & \\ b^2_1=\{7 & 8 & 16 & 24\} & \end{bmatrix},$$

$$P_3=\begin{bmatrix} b^3_7=\{1 & 10 & 19 & 28 & 30\} \\ b^3_6=\{2 & 11 & 20 & 22\} & \\ b^3_5=\{3 & 12 & 21 & 23\} & \\ b^3_4=\{4 & 13 & 15 & 24\} & \\ b^3_3=\{5 & 14 & 16 & 25\} & \\ b^3_2=\{6 & 8 & 17 & 26\} & \\ b^3_1=\{7 & 9 & 18 & 27 & 29\} \end{bmatrix}, P_4=\begin{bmatrix} b^4_7=\{1 & 11 & 21 & 24\} & \\ b^4_6=\{2 & 12 & 15 & 25\} & \\ b^4_5=\{3 & 13 & 16 & 26 & 29\} \\ b^4_4=\{4 & 14 & 17 & 27 & 30\} \\ b^4_3=\{5 & 8 & 18 & 28\} & \\ b^4_2=\{6 & 9 & 19 & 22\} & \\ b^4_1=\{7 & 10 & 20 & 23\} & \end{bmatrix},$$

$$P_5=\begin{bmatrix} b^5_7=\{1 & 12 & 16 & 27\} & \\ b^5_6=\{2 & 13 & 17 & 28\} & \\ b^5_5=\{3 & 14 & 18 & 22\} & \\ b^5_4=\{4 & 8 & 19 & 23\} & \\ b^5_3=\{5 & 9 & 20 & 24\} & \\ b^5_2=\{6 & 10 & 21 & 25 & 29\} \\ b^5_1=\{7 & 11 & 15 & 26 & 30\} \end{bmatrix}, P_6=\begin{bmatrix} b^6_7=\{1 & 13 & 18 & 23\} & \\ b^6_6=\{2 & 14 & 19 & 24 & 29\} \\ b^6_5=\{3 & 8 & 20 & 25 & 30\} \\ b^6_4=\{4 & 9 & 21 & 26\} & \\ b^6_3=\{5 & 10 & 15 & 27\} & \\ b^6_2=\{6 & 11 & 16 & 28\} & \\ b^6_1=\{7 & 12 & 17 & 22\} & \end{bmatrix},$$

$$P_7=\begin{bmatrix} b^7_7=\{1 & 14 & 20 & 26\} & \\ b^7_6=\{2 & 8 & 21 & 27\} & \\ b^7_5=\{3 & 9 & 15 & 28\} & \\ b^7_4=\{4 & 10 & 16 & 22\} & \\ b^7_3=\{5 & 11 & 17 & 23 & 29\} \\ b^7_2=\{6 & 12 & 18 & 24 & 30\} \\ b^7_1=\{7 & 13 & 19 & 25\} & \end{bmatrix}, P_8=\begin{bmatrix} b^8_7=\{1 & 8 & 15 & 22 & 29\} \\ b^8_6=\{2 & 9 & 16 & 23 & 30\} \\ b^8_5=\{3 & 10 & 17 & 24\} & \\ b^8_4=\{4 & 11 & 18 & 25\} & \\ b^8_3=\{5 & 12 & 19 & 26\} & \\ b^8_2=\{6 & 13 & 20 & 27\} & \\ \bar{b}^8_1=\{7 & 14 & 21 & 28\} & \end{bmatrix},$$

Note that here all the blocks are not of the same size, but any two blocks from different parallel classes have at most 1 element in common, i.e., $\mu = 1$. Except for the blocks of parallel class P_1, the blocks of the remaining parallel classes have sizes in the set $\{q-(e+f), q-(e+f)+1, \ldots, q-e\} = \{4,5\}$. Thus, we discard the Parallel class P_1. The remaining parallel classes form the required resolvable design, which we call RBD(X, A). Let us formalize the algorithm for the general case. Let $d = k \times s = (q-e)(q-f)$, with $0 < f \leq e < q$.

Construction 6.4.1. Let q be a prime power, construct $(q^2, q, 1)$-ARBIBD. Call this design $(\bar{X}, \bar{A})$ with $\bar{X} = \{1, 2, \ldots, q^2\}$ and $|\bar{A}| = q(q+1)$ many blocks, each block is of constant size q. It will have $r = q+1$ many parallel classes, call them $\left\{\bar{P}_1, \bar{P}_2, \ldots, \bar{P}_{q+1}\right\}$, each parallel class having q many blocks of constant size q. Between any two blocks from different parallel classes, exactly one element will be common, i.e., $|\bar{b}_i^l \cap \bar{b}_j^m| = 1$, $\forall\, l \neq m$.

1. Given $e \geq f$, choose $e(\geq 0)$ many blocks from $\bar{P}_1 = \left\{\bar{b}_1^1, \bar{b}_2^1, \ldots, \bar{b}_h^1\right\}$. Let $S_1 = \bar{b}_1^1 \cup \bar{b}_2^1 \cup \ldots \cup \bar{b}_h^1$. Therefore, $|S_1| = e \times q$.

2. From $\left\{\bar{b}_{e+1}^1, \bar{b}_{e+2}^1, \ldots, \bar{b}_{e+f}^1\right\}$ blocks of $\bar{P}_1$, choose any $(q-e)$ number of elements from each of them. Let S_2 be the union of all these elements. Therefore, $|S_2| = f \times (q-e)$. Let $S = S_1 \cup S_2$.

3. Remove the elements of set S from RBD $(\bar{X}, \bar{A})$ and remove parallel class $\bar{P}_1$ from $\bar{A}$. Call the resulting design RBD(X, A).

We claim that RBD(X, A) satisfies $|X| = (q-e)(q-f)$ and A consists of $q+1$ many parallel classes having different block sizes, such that blocks from different parallel classes have at most one element in common, i.e., $|b_i^l \cap b_j^m| \leq 1$ for all $l \neq m$, implying $\mu = 1$. We formalize this in the following lemma.

Lemma 6.4.1. *Let $d = (q-e)(q-f)$ for $f, e \in \mathbb{N}$ with $0 < f \leq e \leq q$ where q is some prime power. Then one can construct an RBD(X, A), with $|X| = d$ having block sizes from the set of integers $\{(q-e-f), (q-e-f+1), \ldots, (q-e)\}$ with $\mu = 1$, and having q many parallel classes.*

Proof. Refer to Construction 6.4.1 above. Here RBD$(\bar{X}, \bar{A})$ is an ARBIBD with $|\bar{X}| = q^2$, having a constant block size q. Note that any pair of blocks from different parallel classes have exactly one element in common, i.e., $|\bar{b}_i^l \cap \bar{b}_j^m| = 1$, $\forall\, l \neq m$. The number of elements in the set $|S| = |S_1 \cup S_2| = |S_1| + |S_2| = eq + f(q-e) < q^2$, which is a proper subset of $\bar{X}$. These elements are removed from all the parallel classes of RBD$(\bar{X}, \bar{A})$. Hence, the resulting design RBD(X, A) is such that $|X| = q^2 - eq - f(q-e) = (q-e)(q-f) = d$, having the same number of parallel classes as in $\bar{A} \setminus P_1$, which is q. The number of elements common between any two blocks from different parallel classes would be at most 1, i.e., $|b_i^l \cap b_j^m| \leq 1$, $\forall\, l \neq m$.

To obtain the sizes of the blocks in $\mathrm{RBD}(X, A)$, note that S_1 contains all elements from e number of blocks of $\bar{P}_1$. Hence, S_1 would have at least e elements in common with all the blocks of the remaining parallel classes. Thus, removal of the elements in S_1 from the parallel classes $\bar{P}_l, l \geq 2$ will remove at least e elements from each block of $\bar{P}_l$, which implies $|\bar{b}_i^l \setminus S_1| = q - e$. Further, S_2 contains $q - e$ elements from f many blocks of $\bar{P}_1$. Thus, the blocks in $\bar{P}_2, \bar{P}_3, \ldots, \bar{P}_{q+1}$ will have at most f elements in common with S_2. Consequently, after the removal of all the elements in S from the parallel class $\bar{P}_l$, the block size $|b_i^l|$, $l \geq 2$ will be at maximum $(q - e)$ and minimum $(q - e - f)$. However, the blocks in parallel class P_1 will be of sizes q or e and have a total of $(q - e)$ blocks, which we discard. □

Now, the $\mathrm{RBD}(X, A)$ can be used to construct AMUBs. Since the number of parallel classes in $\mathrm{RBD}(X, A)$ is q, and as per Theorem 6.3.1, we will obtain q many β-AMUBs. Although $\mu = 1$ here, the block sizes are not constant, hence Δ will consist of more than two elements, and thus it will not satisfy the criteria of APMUB, even though $\beta = 1 + \mathcal{O}(d^{-\lambda})$, where $\lambda = \frac{1}{2}$. For this situation, to characterize AMUB, we define the following.

Definition 6.4.2. *For $d = (q - e)(q - f)$, where $e \geq f$ and let $\theta_1 = \frac{1}{\sqrt{q-e-f}}, \theta_2 = \frac{1}{\sqrt{q-e-f+1}}, \ldots, \theta_{f+1} = \frac{1}{\sqrt{q-e}}$, then define $\Delta_2 = \{\theta_i\theta_j\} \cup \{0\}$ where $i, j = 1, 2, \ldots, (f + 1)$.*

Note that $|\Delta_2| = \binom{f+1}{2} + (f + 1) + 1 = \frac{(f+1)(f+2)}{2} + 1 = \mathcal{O}(f^2)$. Again, as in the case of Δ_1, here also the number of elements in Δ_2 is only dependent on the value of f and is proportional to the square of it. We now state and prove the result on β-AMUBs, using such $\mathrm{RBD}(X, A)$ as follows

Corollary 6.4.2. *Let $d = (q - e)(q - f)$ with q be some prime-power, $0 < f \leq e$ and $0 < (e + f) \leq \frac{3}{2}\sqrt{d}$ where $e, f \in \mathbb{N}$ then there exist at least q many β-AMUBs, with $\Delta \subseteq \Delta_2$, $\beta = \frac{\sqrt{d}}{q-(e+f)} = 1 + \frac{e+f}{2\sqrt{d}} + \mathcal{O}(d^{-1}) \leq 2$ and $1 - \frac{q-e}{d} \leq \epsilon \leq 1 - \frac{1}{q}$.*

Proof. Consider the $\mathrm{RBD}(X, A)$ from Construction 6.4.1, where $|X| = (q - e)(q - f)$ with $f \leq e$. The block sizes of $\mathrm{RBD}(X, A)$ are from the set $\{(q-e-f), (q-e-f+1), \ldots, (q-e)\}$ as given in Lemma 6.4.1. Using the Hadamard matrices of the order of block sizes, we get q many Orthonormal Basis. Thus, the normalizing factors of Hadamard matrices of different order would be from set $\left\{\frac{1}{\sqrt{q-(e+f)}}, \frac{1}{\sqrt{q-(e+f)+1}}, \ldots, \frac{1}{\sqrt{q-e}}\right\}$. Let's denote this set by $S_\theta = \{\theta_1, \theta_2, \ldots, \theta_{f+1}\}$ where $\theta_1 = \frac{1}{\sqrt{q-(e+f)}}$, $\theta_2 = \frac{1}{\sqrt{q-(e+f)+1}}, \ldots, \theta_{f+1} = \frac{1}{\sqrt{q-e+f}}$. There will be $f + 1$ elements in the set. Since $\mu = 1$ for the $\mathrm{RBD}(X, A)$, we have $\left|\langle\psi_i^l|\psi_j^m\rangle\right| = \theta_i\theta_j$ or 0, where $|\psi_i^l\rangle$ and $|\psi_j^m\rangle$ are the vectors from two different orthonormal bases constructed using a parallel class of $\mathrm{RBD}(X, A)$, and $\theta_i, \theta_j \in S_\theta$. Thus, $\Delta \subseteq \Delta_2$.

Now, $\max\left\{\left|\langle\psi_i^l|\psi_j^m\rangle\right|\right\} = \max\{\theta_i\theta_j\} = \frac{1}{q-(e+f)}$ corresponding to the maximum value of $\theta_i = \theta_j = \frac{1}{\sqrt{q-(e+f)}}$. Thus, $\beta = \frac{\sqrt{d}}{q-(e+f)}$ hence if $\beta \leq c$, using $d = (q-e)(q-f)$ and solving for q in terms of d, we get $q = d^{\frac{1}{2}}(1 + \frac{(e-f)^2}{4d})^{\frac{1}{2}} + \frac{e+f}{2} \Rightarrow efc + (e+f)\sqrt{d} \leq \frac{c^2-1}{c}d$, which for $c = 2$ we get $\frac{2ef}{\sqrt{d}} + (e+f) \leq \frac{3}{2}\sqrt{d}$ hence $0 < (e+f) < \frac{3}{2}\sqrt{d}$. Note that for this condition, we have $\frac{e+f}{2\sqrt{d}} < \frac{3}{4} < 1$, thus the series expansion gives $\beta = 1 + \frac{e+f}{2\sqrt{d}} + \mathcal{O}(d^{-1}) \leq 2$.

To estimate the sparsity, refer to the Lemma 6.3.1, since there are q many blocks in each parallel class, the ϵ is bounded above by $1 - \frac{1}{q}$, and for lower bound, the maximum block size is $q - e$, thus Corollary 6.3.1 gives ϵ is bounded below by $1 - \frac{q-e}{d}$, hence

$$1 - \frac{q-e}{d} \leq \epsilon \leq 1 - \frac{1}{q}.$$

□

For example, for the case of RBD(X, A) with $d = 5 \times 6 = (7-2)(7-1) = 30$, implying $e = 2$ and $f = 1$ shown in the example above, when used for constructing the β-AMUBs, we get $\beta = \frac{\sqrt{30}}{4} = 1.37$ and the set $\Delta = \frac{1}{\sqrt{d}} \times \{\beta_i\}$, where $\beta_i = \{0, 0.76, 0.93, 1.04, 1.09, 1.20, 1.37\}$

The Corollary 6.4.1 and Corollary 6.4.2 together imply that for every composite $d = k \times s$ such that $|s - k| \leq \sqrt{d}$, then we can always construct $\mathcal{O}(\sqrt{d})$ many APMUB. We formally state and prove following

Lemma 6.4.2. *For any composite number, $d = k \times s$, $k \leq s$ with $2\delta = s - k \leq \sqrt{d}$, then there exist $\mathcal{O}(\sqrt{d}\ )$ many β-AMUBs where $\beta \leq 1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}(d^{-\lambda}) \leq 2$, $\lambda = \frac{1-\theta}{2} = 0.2375$ and $\epsilon = 1 - \mathcal{O}(d^{-\frac{1}{2}})$.*

Proof. Consider the prime number p nearest to $u\left(= \frac{k+s}{2}\right)$ but greater than u. From result on gap in prime [5], there will exist a prime number p in the interval $[u, u + \mathcal{O}(u^\theta)]$ where $\theta = 0.525$. Now let $v = p - u$, hence $v \leq \mathcal{O}(u^\theta)$. Consequently, $s = p - v + \delta$ and $k = p - v - \delta$ where $2\delta = s - k$. Now, if $v \leq \delta$, then it becomes the case of $d = (q-e)(q+f)$ where $q = p$, $e = v + \delta$ and $f = v - \delta$, in which case we get $p + 1$ many β-AMUBs with $\beta = 1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}(d^{-1}) \leq 2$. On the other hand if $v \geq \delta$, then it becomes the case of $d = (q-e)(q-f)$ where $q = p$, $e = v+\delta$, and $f = v-\delta$ in which case we get p many β-AMUBs with $\beta = 1 + \frac{e+f}{2\sqrt{d}} + \mathcal{O}(d^{-1})$. And as shown in Lemma 6.3.3, we have $\frac{e+f}{2} = \delta + f = \delta + \mathcal{O}(d^{\frac{\theta}{2}})$. Hence $\beta = 1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}(d^{-\lambda}) \leq 2$ where $\lambda = \frac{1-\theta}{2} = 0.2375$.

Thus, considering both the cases together, we get $p + 1$ or p many β-AMUBs with $\beta \leq 1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}(d^{-\lambda}) \leq 2$. Since for $d = (p-e)(p+f)$ or $d = (p-e)(p-f)$, with $e \geq f$, we have $d = p^2 - (e \pm f)p \mp ef \Rightarrow p = \mathcal{O}(\sqrt{d})$, hence number of β-AMUBs is $\mathcal{O}(\sqrt{d})$.

The sparsity ϵ is bounded from below by $1 - \frac{s}{d}$ and bounded from above by $1 - \frac{1}{q}$ hence $\epsilon = 1 - \mathcal{O}(d^{-\frac{1}{2}})$. □

Note that, the number of β-AMUBs will always be $\geq \lfloor d^{\frac{1}{2}} \rfloor$. It can also be verified that, if we assume the validity of Cramér Conjecture [33], the above result will hold, but now the asymptotic series for β for the case of $d = (q-e)(q-f)$ will be $\beta = 1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}((\log^2 d)d^{-\frac{1}{2}}) \leq 2$. Thus if δ is bounded then we have $\beta = 1 + \mathcal{O}(d^{-\frac{1}{2}})$.

Let us now focus on using RBD, having constant block sizes. Such RBD has the advantage of using a single Hadamard matrix for the entire construction. Hence, RBD(X, A) are more amenable for ARMUB construction. Whereas RBD(X, A) with non-constant block size, intersection number μ is generally small and easy to construct, but then different order Hadamard matrices are required for constructing AMUBs. And since real Hadamard matrix exist only of order 2 or multiple of 4, thus getting ARMUB using such RBD having variable block sizes may not be possible. But our experience has shown that in general, constructing RBD(X, A), having a large number of parallel classes, and having constant block size for all the parallel classes such that intersection number μ remains small and bounded are difficult to achieve. In this direction, we present a few constructions of AMUBs/ARMUBs through RBDs having constant block size.

6.4.2 Construction of β-AMUBs through RBDs having constant block size

In [68, Theorem 2], it is shown that for any composite dimension $d = k \times s$, $k \leq s$ such that $\sqrt{\frac{s}{k}} < 2$, one can construct at least $N(s) + 1$ APMUBs. Here, the key idea is the use of MOLS(s) for the construction of RBD(X, A), having $N(s) + 1$ many parallel classes with $\mu = 1$. This also enables us to construct ARMUB using the real Hadamard matrix of order k if it exists. However, if only the Hadamard matrix of order s exists and not k, then to construct ARMUBs, the RBD(X, A) should have block size s. Nevertheless, from [68, Lemma 2], we know that in such a situation, $\mu \geq 2$. Hence, the minimum value of μ would be 2 in such a situation. Also, if $N(k) > N(s)$ and we wish to use the MOLS(s) to get RBD with more number of parallel classes, then in such situation we would like to have RBD, with a block of size s.

Our following construction achieves the minimal possible value of $\mu = 2$ when block size $s < k < 2s$. We express $k = s + f$, $0 < f \leq s$. Let us demonstrate the construction by explicitly constructing RBD(X, A) with $|X| = 5(5 + 3) = 10$, here $q = 5$ and $f = 3$. As in [68, Section 5.1], 4- MOLS(5) was used to get RBD$(\bar{X}, \bar{A})$ having 6 parallel classes. Following the steps of [68, Construction 3] for $d = (q - e)q$, where

$e = q - f$, we will use this, to construct RBD($\widetilde{X}, \widetilde{A}$) with $|\widetilde{X}| = (5-2)5 = 15$. For this let, $\widetilde{X} = \{26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37, 38, 39, 40\}$. Now, we will combine this design of RBD($\bar{X}, \bar{A}$). We will get RBD(X, A), with elements numbered 1 to 40. Explicitly RBD($\widetilde{X}, \widetilde{A}$) with $|\widetilde{X}| = 5(5-2) = 15$ is as follows.

$$\widetilde{P}_1 = \begin{bmatrix} \widetilde{b}^1_5 = \{26 & 32 & 38\} \\ \widetilde{b}^1_4 = \{27 & 33 & 39\} \\ \widetilde{b}^1_3 = \{28 & 34 & 40\} \\ \widetilde{b}^1_2 = \{29 & 35 & 36\} \\ \widetilde{b}^1_1 = \{30 & 31 & 37\} \end{bmatrix}, \widetilde{P}_2 = \begin{bmatrix} \widetilde{b}^2_5 = \{26 & 33 & 40\} \\ \widetilde{b}^2_4 = \{27 & 34 & 36\} \\ \widetilde{b}^2_3 = \{28 & 35 & 37\} \\ \widetilde{b}^2_2 = \{29 & 31 & 38\} \\ \widetilde{b}^2_1 = \{30 & 32 & 39\} \end{bmatrix}, \widetilde{P}_3 = \begin{bmatrix} \acute{b}^3_5 = \{26 & 34 & 37\} \\ \acute{b}^3_4 = \{27 & 35 & 38\} \\ \widetilde{b}^3_3 = \{28 & 31 & 39\} \\ \widetilde{b}^3_2 = \{29 & 32 & 40\} \\ \widetilde{b}^3_1 = \{30 & 33 & 36\} \end{bmatrix},$$

$$\widetilde{P}_4 = \begin{bmatrix} \widetilde{b}^4_5 = \{26 & 35 & 39\} \\ \widetilde{b}^4_4 = \{27 & 31 & 40\} \\ \widetilde{b}^4_3 = \{28 & 32 & 36\} \\ \widetilde{b}^4_2 = \{29 & 33 & 37\} \\ \widetilde{b}^4_1 = \{30 & 34 & 38\} \end{bmatrix}, \widetilde{P}_5 = \begin{bmatrix} \widetilde{b}^5_5 = \{26 & 31 & 36\} \\ \widetilde{b}^5_4 = \{27 & 32 & 37\} \\ \widetilde{b}^5_3 = \{28 & 33 & 38\} \\ \widetilde{b}^5_2 = \{29 & 34 & 39\} \\ \widetilde{b}^5_1 = \{30 & 35 & 40\} \end{bmatrix},$$

Note that, any two blocks from different parallel class of RBD($\widetilde{X}, \widetilde{A}$) has at most one point in common. Now taking corresponding block wise union of RBD($\widetilde{X}, \widetilde{A}$) with RBD($\bar{X}, \bar{A}$), i.e., $b^i_j = \bar{b}^i_j \cup \widetilde{b}^i_j$. Ignore any one of the parallel class of RBD($\bar{X}, \bar{A}$). The resulting RBD(X, A) is given as follows.

$$P_1 = \begin{bmatrix} b^1_5 = \{1 & 7 & 13 & 19 & 25 & 26 & 32 & 38\} \\ b^1_4 = \{2 & 8 & 14 & 20 & 21 & 27 & 33 & 39\} \\ b^1_3 = \{3 & 9 & 15 & 16 & 22 & 28 & 34 & 40\} \\ b^1_2 = \{4 & 10 & 11 & 17 & 23 & 29 & 35 & 36\} \\ b^1_1 = \{5 & 6 & 12 & 18 & 24 & 30 & 31 & 37\} \end{bmatrix}, P_2 = \begin{bmatrix} \check{b}^2_5 = \{1 & 8 & 15 & 17 & 24 & 26 & 33 & 40\} \\ b^2_4 = \{2 & 9 & 11 & 18 & 25 & 27 & 34 & 36\} \\ b^2_3 = \{3 & 10 & 12 & 19 & 21 & 28 & 35 & 37\} \\ b^2_2 = \{4 & 6 & 13 & 20 & 22 & 29 & 31 & 38\} \\ b^2_1 = \{5 & 7 & 14 & 16 & 23 & 30 & 32 & 39\} \end{bmatrix},$$

$$P_3 = \begin{bmatrix} b^3_5 = \{1 & 9 & 12 & 20 & 23 & 26 & 34 & 37\} \\ b^3_4 = \{2 & 10 & 13 & 16 & 24 & 27 & 35 & 38\} \\ b^3_3 = \{3 & 6 & 14 & 17 & 25 & 28 & 31 & 39\} \\ b^3_2 = \{4 & 7 & 15 & 18 & 21 & 29 & 32 & 40\} \\ b^3_1 = \{5 & 8 & 11 & 19 & 22 & 30 & 33 & 36\} \end{bmatrix}, P_4 = \begin{bmatrix} b^4_5 = \{1 & 10 & 14 & 18 & 22 & 26 & 35 & 39\} \\ b^4_4 = \{2 & 6 & 15 & 19 & 23 & 27 & 31 & 40\} \\ b^4_3 = \{3 & 7 & 11 & 20 & 24 & 28 & 32 & 36\} \\ b^4_2 = \{4 & 8 & 12 & 16 & 25 & 29 & 33 & 37\} \\ b^4_1 = \{5 & 9 & 13 & 17 & 21 & 30 & 34 & 38\} \end{bmatrix},$$

$$P_5 = \begin{bmatrix} b^5_5 = \{1 & 6 & 11 & 16 & 21 & 26 & 31 & 36\} \\ \check{b}^5_4 = \{2 & 7 & 12 & 17 & 22 & 27 & 32 & 37\} \\ b^5_3 = \{3 & 8 & 13 & 18 & 23 & 28 & 33 & 38\} \\ b^5_2 = \{4 & 9 & 14 & 19 & 24 & 29 & 34 & 39\} \\ b^5_1 = \{5 & 10 & 15 & 20 & 25 & 30 & 35 & 40\} \end{bmatrix}.$$

It can be seen that in the above RBD(X, A), any two blocks from different parallel class have either one or two points in common. X consist of points from 1 to 40, and $A = \{P_1 \cup P_2 \cup P_3 \cup P_4 \cup P_5\}$. The technique is more formally explained for the general case in the following Construction.

Construction 6.4.2. Let $d = k \times s = (s + f)s$, with $0 < f \leq s$

1. Using [68, Construction 1], construct an $RBD(\bar{X}, \bar{A})$ using w-MOLS(s). The resulting RBD$(\bar{X}, \bar{A})$ has $\bar{X} = \{1, 2, \ldots, s^2\}$ and $|A| = s(N(s) + 2)$ many blocks. It will have $r = N(s) + 2$ many parallel classes, namely $\left\{\bar{P}_1, \bar{P}_2, \ldots, \bar{P}_{N(s)}, \bar{P}_0, \bar{P}_\infty\right\}$, each having s many blocks of constant size s. The blocks of the parallel class $\bar{P}_l$ are denoted by $\bar{b}^l_i, i = 1, 2, \ldots, s$. Between any two blocks from different parallel class, have exactly one point in common i.e., $|\bar{b}^l_i \cap \bar{b}^m_j| = 1$, $\forall\, l \neq m$.
2. Pick any parallel class, say $\bar{P}_1$. Remove $(s - f)$ many blocks from it and let $S = \left\{b^1_1 \cup b^1_2 \cup \ldots \cup b^1_{(s-f)}\right\}$.
3. Remove all the points of S from $\bar{X}$ i.e., $\bar{X} \setminus S$ and also remove the points of S from all the blocks of parallel classes $\left\{\bar{P}_2, \bar{P}_3, \ldots, \bar{P}_{s+1}\right\}$. Let the resulting parallel classes be called as $\left\{\widetilde{P}_2, \widetilde{P}_3, \ldots, \widetilde{P}_{q+1}\right\}$ i.e., $\widetilde{P}_i = \bar{P}_i \setminus S$.
4. Discard the parallel class $\bar{P}_1$.
5. Construct another $RBD(X, A)$ having elements from $(\bar{X}, \bar{A})$. Then $|X| = s^2$ and $|A| = s(N(s) + 2)$ blocks with $r = N(s) + 2$ many parallel classes $\{P_1, P_2, \ldots, P_r\}$.
6. Discard any one parallel class from A_1, say P_1.
7. Form a new design (X, A) where $X = \tilde{X} \cup X$, $A = \{P_2, P_3, \ldots, P_r\}$ where $P_l = P_l + \widetilde{P}_l$. Then (X, A) is the required RBD.

We claim that the above design (X, A) is an RBD such that $|X| = s(s + f)$ and A consists of $N(s) + 1$ many parallel classes, $A = \{P_2, \ldots, P_r\}$, each parallel class have s many blocks, $P_l = \left\{b^l_1, b^l_2, \ldots, b^l_s\right\}$ for $l = 2, 3, \ldots, r$, each of size $(s + f)$ i.e., $|b^l_i| = (s + f)$, for all $i \in \{1, 2, \ldots, s\}$ and $l \in \{2, 3, \ldots, r\}$, such that blocks from different parallel classes have at most two points in common, i.e., $1 \leq |b^l_i \cap b^m_j| \leq 2$, $\forall\, i \neq j$. We formalize this using the following lemma.

Lemma 6.4.3. *Let $d = (s + f)s$ with $0 < f \leq s$, then one can construct an RBD(X, A), with $|X| = d$ having constant block size of $(s + f)$ with $\mu = 2$ and having $N(s) + 1$ many parallel classes, where $N(s)$ is the number of $MOLS(s)$.*

Proof. Refer to Construction 6.4.2. Since any pair of blocks from different parallel classes is of size s and has exactly one point in common in RBD$(\bar{X}, \bar{A})$, i.e., $|\bar{b}_i^l \cap \bar{b}_j^m| = 1, \forall\, l \neq m$, removing the elements of $S = \left\{\bar{b}_1^1 \cup \bar{b}_2^1 \cup \ldots \cup \bar{b}_{s-f}^1\right\}$ from the entire design will remove exactly $(s-f)$ elements from each block $\bar{b}_t^l$, $l \neq 1$. Hence, the blocks $\tilde{b}_t^l = \bar{b}_t^l \setminus S$ will be of constant size $|\tilde{b}_i^l| = f$ and $|\tilde{b}_i^l \cap \tilde{b}_j^m| \leq 1, \forall\, l \neq m$.

On the other hand, in an RBD(X, A), any pair of blocks from different parallel classes is of size s and has exactly one point in common, i.e., $|b_i^l \cap b_j^m| = 1, \forall\, l \neq m$. Since the design (X, A), where $X = \tilde{X} \cup \bar{X}$, $A = \{P_2, P_3, \ldots, P_r\}$, and $P_l = P_l + \widetilde{P}_l$, is a direct union of the blocks for $\bar{A}$ and $\tilde{A}$, it will have either one point or two points in common between blocks of different parallel classes. □

Now using such RBD, we can construct β-AMUBs with the following characteristics.

Theorem 6.4.1. *If $d = s(s+f)$, with $s, f \in \mathbb{N}$ and $f \leq s$, then one can construct $N(s)+1$ many approximate MUBs with $\beta = 2\sqrt{\frac{s}{s+f}} = 2 - \frac{f}{\sqrt{d}} + \mathcal{O}(d^{-1}) \leq 2$ and sparsity $\epsilon = 1 - \frac{1}{s}$. If there exist a real Hadamard matrix of order $(s+f)$, then one can construct $N(s)+1$ many approximate real MUBs (ARMUBs) with the same β and ϵ. Furthermore, $\Delta = \left\{0, \frac{\beta_o}{\sqrt{d}}, \frac{2\beta_o}{\sqrt{d}}\right\}$ where $\frac{1}{\sqrt{2}} \leq \beta_o = 1 - \frac{f}{2\sqrt{d}} + \mathcal{O}(d^{-1}) < 1$.*

Proof. Following the Construction 6.4.2, we construct an RBD(X, A) with $|X| = d = (s+f)s$. The block size is $(s+f)$, and the number of parallel classes is $N(s)+1$. Since the intersection number $\mu = 2$, we have $\beta = \frac{2\sqrt{d}}{s+f} = 2\sqrt{\frac{s}{s+f}} < 2$. The result follows from the construction of β-AMUBs in [65] and Theorem 6.3.2. The minimum possible β in this situation is when $f = s$, for which $\beta \leq \sqrt{2}$. The asymptotic variation of the parameters in terms of d is given by $\beta = 2 - \frac{f}{\sqrt{d}} + \mathcal{O}(d^{-1})$. However, here, β converges to 2. The sparsity is given by $\epsilon = 1 - \frac{s+f}{d} = 1 - \frac{1}{s}$. Using the real Hadamard matrix of order $(s+f)$, we obtain the ARMUBs with the same β and ϵ. However, the set Δ, which contains all the different values of the absolute value of dot product $|\langle\psi_i^l|\psi_j^m\rangle|$ of vectors $|\psi_i^l\rangle$ and $|\psi_j^m\rangle$ from different bases, is restricted to set $\left\{0, \frac{1}{s+f}, \frac{2}{s+f}\right\}$. Hence, $\Delta = \left\{0, \frac{\beta_o}{\sqrt{d}}, \frac{2\beta_o}{\sqrt{d}}\right\}$ where $\beta_o = \sqrt{\frac{s}{s+f}}$ hence $\frac{1}{\sqrt{2}} \leq \beta_o = 1 - \frac{f}{2\sqrt{d}} + \mathcal{O}(d^{-1}) < 1$, where the lower bound correspond to the situation when $f = s$. □

When $s = q$, some power of a prime number, there is well-known method of construction of affine resolvable $(q^2, q, 1)$-BIBD which is an RBD. In this regard, we have the following immediate corollary.

Corollary 6.4.3. *If $d = q(q+f)$, where q is some power of a prime and $q, f \in \mathbb{N}$ such that $f \leq q$, then we can construct q many AMUBs with $\beta = 2\sqrt{\frac{q}{q+f}} = 2 - \frac{f}{\sqrt{d}} + \mathcal{O}(d^{-1})$. Moreover, if there exist a real Hadamard matrix of order $(q+f)$, one can construct q many approximate real MUBs (ARMUBs) with the same parameters.*

The proof of this corollary follows directly from the fact that $N(q) = q - 1$. For example, the RBD(X, A) constructed above having 5 parallel classes, can be converted into 5 orthonormal bases, which gives $\beta = 2\sqrt{\frac{5}{8}} = 1.58 < 2$ and $\epsilon = 1 - \frac{1}{5} = 0.8$.

The corollary above is a generalization of the result for $d = q(q+1)$ [65, Theorem 4] to $q(q+f)$, having a similar parameter, $\beta = 2 - \mathcal{O}(d)$. In fact, the result of [65, Theorem 4] is a particular case of our present result, where the block size is larger than the number of blocks, with $e = 0, f = 1$, and $\mu = 2$. There are $q+1$ many parallel classes in an RBD, each having a constant block size of $(q+1)$. In that case, $\beta = 2\sqrt{\frac{q}{q+1}} = 2 - \mathcal{O}(\frac{1}{\sqrt{d}})$, which is the same as [65, Theorem 4]. Once again, we would like to point out that these are not APMUBs but provide results of the same quality in terms of absolute inner product values as [65], but over a larger class. In order to obtain APMUBs, we must have $\mu = 1$.

The above Theorem 6.4.1 and [68, Theorem 2], together give the following important corollary, which enables us to construct β-ARMUBs, such that $\beta < 2$, for every $d = k \times s$, $k \leq s$ such that $s - k < \sqrt{d}$ and there exist a real Hadamard matrix of order k or s. The quality of the constructed β-ARMUB depends on the factors of d and $|s - k|$.

Corollary 6.4.4. *Let $d = k \times s$, with $|s - k| < \sqrt{d}$. If a real Hadamard matrix of order k exists, then one can construct $N(s) + 1$ many β-ARMUB, with sparsity $\epsilon = 1 - \frac{1}{k}$. If $k < s$ then $\beta = \sqrt{\frac{s}{k}} = 1 + \frac{\delta}{\sqrt{d}} + \mathcal{O}(\frac{\delta^2}{d}) < 2$, and if $k > s$ then $\beta = 2\sqrt{\frac{s}{k}} = 2 - \frac{\delta}{\sqrt{d}} + \mathcal{O}(\frac{\delta^2}{d}) < 2$, where $2\delta = |s - k|$. And if $k = s$, then $\beta = 1$*

Proof. When we have a Hadamard matrix of order k, and if $k < s$ then we employ the construction corresponding to $d = (s-e)s$, [68, Construction 3], with $k = s - e$, which will result into $N(s) + 1$ many β-AMUBs, with $\beta = \sqrt{\frac{s}{k}}$ and $\epsilon = 1 - \frac{1}{s}$ as stated in [68, Theorem 2]. On the other hand when $k > s$ then we will employee above Construction 6.4.2 for $d = s(s+f)$ to construct $N(s)+1$ many β-AMUBs with $\beta = 2\sqrt{\frac{s}{s+f}} = 2 - \frac{\delta}{\sqrt{d}} + \mathcal{O}(\frac{\delta^2}{d}) < 2$. □

The quality of the constructed AMUBs for $d = k \times s$ depends on $\delta = |s - k| < \sqrt{d}$, and the smaller the δ, the closer β becomes to 1. However, note that the number of AMUBs is only of the order of $N(k)$ or $N(s)$, which is generally small. Nevertheless note that $N(w) \to \infty$ as $w \to \infty$ whereas the number or real MUBs for most of the non square dimension is either 2 or 3.

6.5 Discussion and comparison with existing results on AMUBs

We have shown that for a composite $d = k \times s$, if $|s - k| < \sqrt{d}$, then RBD can be used to constructed $\geq \sqrt{d}$ many very sparse β-AMUBs, with $\beta \leq 2$ for all such composite d. This is to be compared with the fact that corresponding to such composite $d = k \times s = p_1^{n_1}\, p_2^{n_2}\, \ldots\, p_m^{n_m}$, number of MUB possible is $p_r^{n_r} + 1$ where $p_r^{n_r}$ is $\min\{p_1^{n_1}, p_2^{n_2}, \ldots, p_m^{n_m}\}$. Thus number of β-AMUBs will always be greater than MUBs for such composite d.

In order to construct AMUBs, for a such composite d, we express $d = (q - e)(q + f)$ or $(q - e)(q - f)$, where $q \geq \frac{|s+k|}{2}$ is some prime-power closest to $\frac{|s+k|}{2}$. Then, we construct an RBD, whose block sizes are $\mathcal{O}(\sqrt{d})$, with $\mu = 1$. The most important parameter which control the quality of AMUBs, measured by closeness of β to 1, is $\frac{|s-k|}{2}$. The order of set Δ, which consist of different possible values of $|\langle \psi_i^l | \psi_j^m \rangle|$, where $|\psi_i^l\rangle$ and $|\psi_j^m\rangle$ are basis vectors from different bases is $\mathcal{O}(f^2)$. Hence for small f, we get only a few different values of $|\langle \psi_i^l | \psi_j^m \rangle|$. For the case of $d = (q - e)(q + f)$, the $0 \leq f \leq \delta$ and for the case of $d = (q - e)(q - f)$ the $0 \leq f = \mathcal{O}(d^{\frac{\theta}{2}})$. Thus smaller the δ, the β will be closer to 1 and $|\Delta|$ will be small. And when $\delta = 0$ i.e., $d = q^2$, we get $q + 1$ many MUBs. For example for $d = 6 \times 10$ we can construct 10 β-AMUBs with $\beta = 1.29$ where as for same d we have only 4 MUBs. And for $d = 6 \times 7$ we can construct 8 β-AMUBs with $\beta = 1.08$ where as for same d we have only 3 MUBs. Note that smaller the δ, closer is the β to 1

The RBD having constant block size is particularly useful for constructing β-ARMUBs. We have shown that for a composite $d = k \times s$ with $|s - k| < \sqrt{d}$, such that a real Hadamard matrix of order k or s is available, then we can construct $N(s) + 1$ or $N(k) + 1$ many β-ARMUBs with $\beta < 2$ respectively. For example for $d = 4 \times 7$ we can construct 7 β-ARMUBs with $\beta = 1.32$ where as only 2 real MUBs exist [18, Table 1] in this case. Consider for $d = 7 \times 12$ we can construct 7 β-ARMUBs with $\beta = 1.527$ where as only 2 real MUBs exist in this case as well [18, Table 1].

Here we generalize the result for $d = q(q + 1)$ of Chapter 4 to $q(q + f)$ in Corollary 6.4.3 having a similar form of $\beta = 2 - \mathcal{O}(d^{-\frac{1}{2}})$. We also improve the number of β-AMUBs for the case of $(q - e)(q + f)$ where previously only $\lfloor \frac{q-e}{f} \rfloor + 1$ many β-AMUBs could be constructed. However, now q many β-AMUBs could be constructed with same $\beta = 1 + \mathcal{O}(d^{-\frac{1}{2}})$, but now $|\Delta|$ increased from 2 to $\mathcal{O}(f^2)$ as in Definition 6.4.1. In fact, we generalized the case for $d = (q - e)(q + f), 0 < f \leq e$ for the construction of β-AMUBs to include the case for $d = (q - e)(q \pm f)$. Thus, for situation like $d = 9 \times 10$ or $d = 13 \times 15$ etc., we cannot construct APMUBs, but can construct β-AMUBs by expressing these d in the form of $(q - e)(q - f)$ for suitable e and f. However, this generalization comes at the expense of increasing $|\Delta|$ to $|\Delta_1|$ (Definition 6.4.1) or to $|\Delta_2|$ (Definition 6.4.2), as opposed to the previous scenario of

APMUBs where $|\Delta| = 2$.

We make the following observation applicable to various construction of β-AMUBs here, highlighting common characteristics of AMUBs constructed using RBD(X, A).

1. One of the critical parameters of RBD(X, A) is the intersection number, denoted as μ, which is the maximum number of elements common between any pair of blocks from different parallel classes. Note that, as each parallel class contains all the points of X, a block in a parallel class is bound to have at least one point in common with some block of a different parallel class, and therefore $\mu \geq 1$. A lower value of μ is desirable for a lower value of β.

2. In general, using RBD(X, A), with $|X| = d = k \times s$ a composite number, we can obtain good quality β-AMUBs (ARMUBs) if $\delta = \frac{|s-k|}{2}$ is small. In fact, the smaller the value of δ, the better the quality of the AMUBs. For large values, we get poor-quality AMUBs (ARMUBs). .

3. The other critical parameter is the block size of RBD(X, A). The block sizes should be around $\sqrt{d}$ to obtain good quality AMUB(ARMUBs). Closer the block size to $\sqrt{d}$, closer the value of β to 1.

4. In general, for composite d with small δ and a resolvable design having a block size $\mathcal{O}(\sqrt{d})$ with small μ, the β of the constructed AMUBs is of the form $\beta = \mu(1 \pm \frac{\delta}{\sqrt{d}} + \mathcal{O}(d^{-1}))$. In such a situation, generally, we get $\mathcal{O}(\sqrt{d})$ many AMUBs.

5. For ARMUBs, a Hadamard matrix corresponding to the block sizes of the parallel class should exist. Thus, RBD with block sizes equal to the order of some Hadamard Matrix is sufficient to construct ARMUBs. However, since the real Hadamard matrix exists only for order 2 or orders multiple of 4, it is easier to construct ARMUBs with RBD having a constant block size, a multiple of 4.

6. Sparsity (ϵ) of the constructed AMUBs depends on the block sizes. The larger the block size, the smaller the sparsity, and vice versa.

7. The set of all the different absolute values of the dot product of basis vectors of AMUBs, denoted by $|\Delta|$, is dependent on the number of different block sizes of RBD. The more different sizes of blocks in RBD, the larger the size of $|\Delta|$. Hence, RBD having a constant block size is desirable to get a smaller size of the set $|\Delta|$. Furthermore, $|\Delta|$ is also dependent on the value of μ. The larger the value, the larger the size of $|\Delta|$. Hence, a smaller intersection number in RBD is also desirable to get a smaller size of the set $|\Delta|$.

The best result, applicable for most of the dimensions, for β-AMUBs is based on the elliptic curve construction, [86, Theorem 2] where the construction gave p^{t-1}, $t \geq 2$ where p is a prime such that $\sqrt{n} - 1 \leq \sqrt{p} \leq \sqrt{n} + 1$.

$$|\langle \psi_i^l | \psi_j^m \rangle| \leq \frac{2t + \mathcal{O}(d^{-\frac{1}{2}})}{\sqrt{d}} = \mathcal{O}(d^{-\frac{1}{2}}) \Rightarrow \beta = 2t + \mathcal{O}(d^{-\frac{1}{2}}).$$

Here the smallest value of $\beta = 4 + \mathcal{O}(d^{-\frac{1}{2}}) > 4$, corresponding to $t = 1$. However, here we could provide a construction where $\beta \leq 2$. Thus the β is closer to one in all our construction than this. On the other hand, we obtain only $\mathcal{O}(\sqrt{d})$ many AMUBs, whereas [86, Theorem 2] can provide $\mathcal{O}(d)$ many AMUBs. The other generic construction of AMUBs applicable for all d is of Klappenecker et al. [61] where they gave construction of AMUBs that has $\beta = \mathcal{O}(d^{\frac{1}{4}})$ [61, Theorem 11] or the construction of AMUBs based on the finite field [86, Theorem 1] where $\beta = \mathcal{O}(\sqrt{\log d})$. Thus in all the known construction of AMUBs for a generic d, the β constructed using RBD is much closer to 1 than the other known construction. In fact here $\beta \to 1$ for larger d where as for other it blows up without any bound or tends to a larger values.

In case of certain specific kinds of d, as per our survey, only for $d = q - 1$, where q is some power of prime, there are d or $d + 1$ AMUBs [61, 96] where $\beta = 1 + \mathcal{O}(d^{-\lambda})$ for $\lambda > 0$. The other known case of the β of this form, for $d = q(q - 1)$, the number of AMUBs is $\mathcal{O}(\sqrt{d})$, and for $d = \phi(n)$, the number of AMUBs is equal to the smallest prime division of n, which is always less than $\sqrt{n}$ when n is not a prime number [91]. At the same time, we have shown that for all composite $d = k \times s$ when $|s - k| < d^{\frac{1}{2}}$ then we will get more than $\sqrt{d}$ many AMUBs with $\beta = 1 + \mathcal{O}(d^{-\lambda})$ for $\lambda > 0$. Thus, we can effectively construct such AMUBs for a large set of integer d. Further, we are also able to construct ARMUBs with $\beta = 1 + \mathcal{O}(d^{-\lambda})$ or with $\beta = 1 - \mathcal{O}(d^{-\lambda}) < 2$ for such d whenever real Hadamard matrix of order k or order s is available. Moreover, all these AMUBs are very sparse where in general the sparsity $\epsilon = 1 - \mathcal{O}(d^{-\frac{1}{2}})$ for both complex and real cases.

6.6 Conclusion

In this chapter, our study suggests that constructing RBD(X, A), having a large number of parallel classes, and having constant block size for all the parallel classes such that block sizes remain near $\mathcal{O}(\sqrt{d})$ as well as the intersection number μ remains small, are not easy to achieve. In general we start with RBD(X, A) with $\mathcal{O}(\sqrt{d})$ many parallel classes, having $\mu = 1$ or 2. We intend to work on constructing RBD(X, A)'s, having larger order of parallel classes, keeping μ small and block sizes near $\mathcal{O}(\sqrt{d})$. Our results show that such RBD(X, A) will enable one to construct even larger number of AMUBs, without compromising the inner product value. Further, if the condition $|s-k| < \sqrt{d}$ can be released, it will be applicable for all the d's. Certain informal observations suggest that this condition is not very restrictive, and the ratio of integers, which satisfy this condition to the total numbers less than certain finite large integer, is almost one. Nevertheless, there are infinitely many integers that do not satisfy this condition, and hence effort in the direction to dispense with this condition may be worthwhile.

Chapter 7

A Heuristic Framework to search for Approximate MUBs

We have explained throughout this thesis that as optimal number of MUBs may not always be available for different composite dimensions, Approximate MUBs (AMUBs) might be studied through different techniques. In this chapter, we deviate from the earlier chapters where combinatorial structures are exploited and take a different heuristic based approach to obtain AMUBs with significantly good parameters. Given a non-prime dimension d, we note the closest prime $d' > d$ and form $d'+1$ MUBs through the existing methods. Then our proposed idea is (i) to apply basis reduction techniques (that are well studied in Machine Learning literature) in obtaining the initial solutions, and finally (ii) to exploit the steepest ascent kind of search to achieve further improved results. The efficacy of our technique is shown through construction of AMUBs in dimensions $d = 6, 10, 46$ from $d' = 7, 11$ and 47 respectively. Our technique provides a novel framework in construction of AMUBs that can be refined in a case-specific manner. From a more generic view, this approach considers approximately solving a challenging (where efficient deterministic algorithms are not known) mathematical problem in discrete domain through state-of-the-art heuristic ideas.

7.1 Introduction

Combinatorial constructions (as in the previous chapters) and algebraic as well as search based techniques (see [81] and the references therein) are trending in AMUB literature. However, the strategies have their respective limitations too. The combinatorial constructions work on dimensions of certain kinds, and the computations for the rich but restricted class of unitary transformations explored in [81] are not applicable for higher dimensions. Thus, in this chapter, we explore alternative heuristics to construct AMUBs in any dimension with good computational efficiency.

We propose a generic approach in constructing AMUBs through dimension reduction, using Singular Value Decomposition (SVD) as the primary and initial component of our algorithm. Given an arbitrary dimension d, we start from d', the closest prime power larger than d. As the construction for $(d'+1)$ MUBs exist for prime power d', we apply dimension reduction to those MUBs to obtain a potential collection of AMUBs in dimension d. Finally, a heuristic search on this collection produces $(d+1)$ AMUBs in the d-dimensional Hilbert space $\mathbb{C}^d$. This approach works for any dimension d, and is quite efficient for higher dimensional spaces. Although SVD is quite prominent for its dimensionality-related applications in mathematics and machine learning [82], to the best of our knowledge, such an SVD-based dimension reduction technique has never been studied for constructions of AMUB. For a more detailed background, let us refer to Section 7.1.1, where we present the two measures used in this chapter to determine the closeness of AMUBs to MUBs. We also briefly explain the basics of dimension reduction using Singular Value Decomposition (SVD) here.

Let us now formally propose the framework. We devise two strategies for dimension reduction using the general idea of SVD – *merged* and *non-merged*. We treat the reduced bases obtained from the SVD routine as our initial solution set for prospective AMUBs, which will further be subjected to a steepest ascent kind of heuristic search, as proposed in [81]. It is thus natural that for $d = 6$, we do not obtain results as good as in [81], as the algebraic structure is not used at all. However, our results for $d = 6$ is encouraging and only slightly weaker than that of [81], though we relax the restrictions related to the parameterization and proceed with a general class of bases. More important is that, our proposed technique can be adapted easily in case of higher dimensions to construct more number of AMUBs exceeding the lower bound on MUBs. These we present in details in Section 7.2. The algorithm is presented in two parts – 'Creation of Bases' and 'Choice of Bases'. We also highlight the heuristic search technique in [81], as we subject the reduced bases obtained from our dimension reduction step to this search routine.

It is generally accepted that to construct large number of MUBs in $\mathbb{C}^d$, where $d = 2 \bmod 4$ is quite difficult and in such dimensions using known construction methods for prime powers, we get only 3 MUBs. Hence we implement our techniques for dimensions of the form $d = 2p$, where p is a Sophie Germain prime [38] (that is, both p and $2p+1$ are primes), as large number of MUBs are available in dimension $d' = d + 1 = 2p + 1$. In particular we consider the dimensions $d = 6, 10, 46$, where our proposed strategy yields AMUBs with good parameters. Section 7.3 describes the experimental results. Section 7.4 concludes the chapter by summarizing our contribution in the domain of AMUB constructions, and by indicating the scope for further generalization of our framework to higher-dimensional Hilbert spaces. Note that our results are not the best ones (see [32] and the references therein) for the small dimensions like six or ten. However, the existing results for small dimensions are case specific and there is no clear evidence that such techniques are scalable to very large dimensions.

In such a scenario, our method provides a generic technique for approximate solutions with significantly good parameters as noted from experiments. In fact, we did not see any heuristic methods to consider the dimension 46, that we put in experiment here.

7.1.1 Closeness Measures for AMUBs

We broadly use two measures to validate our results in terms of the *closeness* of AMUBs to MUBs: (i) Average Squared Distance (ASD) among the bases and (ii) maximum distance of $\langle a_i|b_j\rangle$ from $\frac{1}{\sqrt{d}}$, termed as Drift Measure.

$\overline{D^2}$ – **Average Squared Distance (ASD) between bases.**

To measure the quality of AMUBs generated by our algorithm, we use the concept of distance between two bases, following Bengtsson *et al.* [8], who used the distance between two bases as a yardstick to measure the unbiasedness, and Raynal *et al.* [81], who used a similar measure to determine the results of their proposed algorithms.

The squared distance between two orthonormal bases $\mathbf{A} = \{|a_1\rangle, \ldots, |a_d\rangle\}$ and $\mathbf{B} = \{|b_1\rangle, \ldots, |b_d\rangle\}$ of a d-dimensional Hilbert space $\mathbb{C}^d$ is defined as

$$D^2_{\mathbf{AB}} = 1 - \frac{1}{d-1}\sum_{i,j=1}^{d}\left(|\langle a_i|b_j\rangle|^2 - \frac{1}{d}\right)^2, \tag{7.1}$$

and for a set of k orthonormal bases in $\mathbb{C}^d$, the Average Squared Distance (ASD) between the $k(k-1)/2$ pairs of bases is defined as the average over all pairs:

$$\overline{D^2} = \frac{2}{k(k-1)}\sum_{\mathbf{A}<\mathbf{B}} D^2_{\mathbf{AB}}. \tag{7.2}$$

The value of ASD is maximum ($\overline{D^2} = 1$) for a perfect set of MUBs, that is, when $|\langle a_i|b_j\rangle| = \frac{1}{\sqrt{d}}$ for all $i, j = 1, \ldots, d$ and for all pairs of bases **A, B** in the set. Thus, deviation of $\overline{D^2}$ from one in Eq. (7.2) provides a measure of *closeness* for AMUBs.

S – **Maximum Distance of** $|\langle a_i|b_j\rangle|$ **from** $\frac{1}{\sqrt{d}}$**.**

Consider a set of m orthonormal bases in $\mathbb{C}^d$, where we choose pairs of bases $\mathbf{A} = \{|a_1\rangle, \ldots, |a_d\rangle\}$ and $\mathbf{B} = \{|b_1\rangle, \ldots, |b_d\rangle\}$ at a time. One may choose $\binom{m}{2}$ pairs of bases $\mathbf{A}, \mathbf{B}$, and for each pair $\mathbf{A}, \mathbf{B}$, one may compute d^2 inner products $|\langle a_i|b_j\rangle|$ for $i, j = 1, \ldots, d$.

We define the Drift Measure S as the maximum of absolute values of the distance $|\langle a_i|b_j\rangle| - 1/\sqrt{d}$ over all such choices of base pairs and inner products:

$$S = \max_{\mathbf{A},\mathbf{B}} \max_{i,j} ||\langle a_i|b_j\rangle| - 1/\sqrt{d}| \tag{7.3}$$

The value of Drift is minimum ($S = 0$) for a perfect set of MUBs, that is, when $|\langle a_i|b_j\rangle| = \frac{1}{\sqrt{d}}$ for all $i, j = 1, \ldots, d$ for all pairs of bases **A, B** in MUBs. Thus, deviation of S from 0 in Eq. (7.3) provides a measure of *closeness* for AMUBs. In order to understand how is the maximum departure in the form of some $\frac{\alpha}{\sqrt{d}}$, we also refer to α such as

$$\alpha = \sqrt{d} \cdot S, \tag{7.4}$$

in the results section (Section 7.3).

In case of β-AMUBs, it can be easily shown that (for a detailed derivation, refer to [68]),

$$S = \frac{\beta - 1}{\sqrt{d}} \tag{7.5}$$

Therefore, we have,

$$\beta = \alpha + 1 \tag{7.6}$$

7.1.2 Dimension Reduction using SVD

The primary idea of generating AMUBs in our proposal revolves around the concept of dimension reduction. Several dimension reduction techniques are available in the literature [42, 57], where the main purpose of these algorithms is to reduce certain high-dimensional data to a suitable lower dimension, preserving the characteristics and properties of the data as much as possible. In case of dimension reduction in this initiative, we focus on Singular Value Decomposition (SVD).

The techniques related to SVD for real square matrices were proposed by Beltrami and Jordan and for complex matrices by Autonne (see [92] and references therein). The generic algorithm for SVD in case of rectangular matrices was proposed by Eckart and Young in the Autonne-Eckart-Young Theorem [40]. SVD decomposes a matrix of higher dimension into two unitary (orthogonal) matrices and a diagonal matrix containing the singular values. The singular values are ordered by their magnitudes (importance) in the data. The mathematical formulation of SVD is as follows.

Singular Value Decomposition.

Over $\mathbb{C}$, a matrix $\mathbf{A}^{p\times q}$ of rank $\rho(\mathbf{A}) = r$ can be decomposed as $\mathbf{A}^{p\times q} = \mathbf{U}^{p\times p}\ \mathbf{\Sigma}^{p\times q}\ \mathbf{V}^{q\times q}$, where $\mathbf{U}^{p\times p}$ and $\mathbf{V}^{q\times q}$ are unitary matrices, and $\mathbf{\Sigma}$ comprises of the r nonnegative real singular values of the matrix $\mathbf{A}$ along its diagonal as $\mathrm{Diag}(\sigma_1, \sigma_2, \ldots, \sigma_r)$ with $\sigma_1 \geq \sigma_2 \geq \ldots \geq \sigma_r \geq 0$, and with all other values equal to 0. The columns of $\mathbf{U}$ are called the left singular vectors of $\mathbf{A}$ and the columns of $\mathbf{V}$ are called the right singular vectors of $\mathbf{A}$. The *complete* Singular Value Decomposition (SVD) of the matrix $\mathbf{A}^{p\times q}$ can be expressed using the partitioning of matrices as follows.

$$\begin{array}{ccc} \mathbf{U}\quad (p\times p) & \mathbf{\Sigma}\quad (p\times q) & \mathbf{V}^T\quad (q\times q) \\ \left[\begin{array}{ccc|ccc} & & & & & \\ & & & & & \\ u_1 & \cdots & u_r & u_{r+1} & \cdots & u_p \\ & & & & & \\ & & & & & \end{array}\right] & \left[\begin{array}{ccc|ccc} \sigma_1 & & & & \vdots & \\ & \ddots & & \cdots & 0 & \cdots \\ & & \sigma_r & & \vdots & \\ \hline & \vdots & & & \vdots & \\ \cdots & 0 & \cdots & \cdots & 0 & \cdots \\ & \vdots & & & \vdots & \end{array}\right] & \left[\begin{array}{c} v_1^T \\ \vdots \\ v_r^T \\ \hline v_{r+1}^T \\ \vdots \\ v_q^T \end{array}\right] \end{array}$$

SVD in Our Proposal.

We intend to generate AMUBs in $\mathbb{C}^d$ by dimension reduction from $\mathbb{C}^{d'}$, where d' is the closest prime power larger than d. In this chapter, we provide examples where $d' = d+1$ is a prime, and $\frac{d}{2}$ is a prime too. To accomplish this, we reduce a $z \times d'$ matrix to a $z \times d$ matrix, where $z \in \mathbb{Z}^+$ varies depending on the choice of our algorithms. We perform SVD on the $z \times d'$ matrix to obtain $\mathbf{U}^{z\times z}$, $\mathbf{\Sigma}^{z\times d'}$ and $\mathbf{V}^{d'\times d'}$. Finally, to obtain the reduced matrix of order $z \times d$ for generating AMUBs, we take the product of $\mathbf{U}^{z\times z}$, the first d singular values from $\mathbf{\Sigma}$ and a sub-matrix of order $d \times d$ from $\mathbf{V}$. If consecutive singular values are identical, there would be various choices to construct reduced matrices. In such cases, we try to optimize choices through exhaustive or heuristic searches.

7.2 Construction of AMUBs

The algorithm proposed in this section for generating d-dimensional Approximate Mutually Unbiased Bases (AMUBs) is a combination of dimension reduction and then search techniques to obtain appropriate bases with maximum possible ASD and a small value of S, as defined in Section 7.1.1. In the first part, we prepare the suitable bases for AMUB selection through dimension reduction. In the second part, we search for the best set of AMUBs from the bases developed in the first part. Finally, we apply a gradient-ascent kind of heuristic search as in [81] on the available AMUBs to obtain further improved results.

7.2.1 Creation of Bases

We use SVD to reduce suitable bases from a higher prime power (or prime) dimension d' to the target composite dimension $d < d'$. There are two aspects that we investigate here. That is, we propose two techniques to apply SVD – *Merging technique* and *Non-Merging technique.* First let us explain the merging technique through Figure 7.1. Then the Algorithm 1 follows.

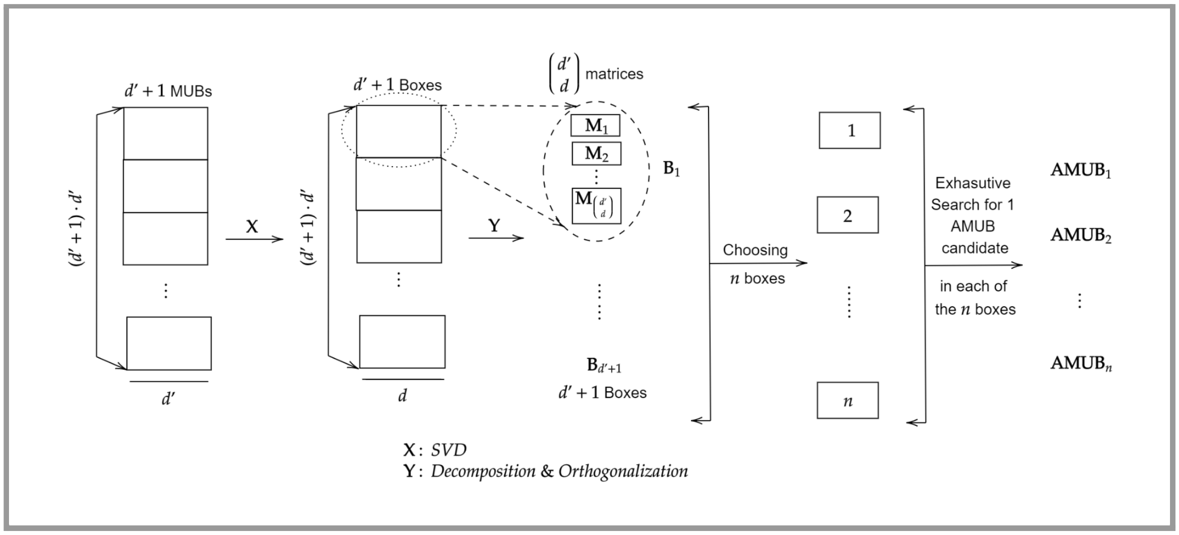

Figure 7.1: Merging technique: Schematic Representation

As one may note, corresponding to $d'+1$ many MUBs of dimension d', we naturally have each matrix with $d' \times d'$ entries. Thus, one can see that we have total $(d'+1) \cdot d'$ vectors here. Now the dimension will be reduced to d. Now we will consider all the $(d'+1) \cdot d'$ vectors for input to the SVD technique and then put them in different $d'+1$ buckets. Each bucket will contain d' many vectors. We will consider d vectors from those d' and orthogonalize them to have a basis. Thus, there will be several options of a basis from a bucket, and we will choose different buckets to obtain the bases corresponding to an AMUB. This will continue to obtain the best result. Naturally while considering $d' = 7$ and $d = 6$, such buckets can be searched exhaustively. However, the computational requirement becomes much higher and while running on a laptop, such exhaustive searches cannot be completed in reasonable time (say one hour) for $d' = 11, d = 10$. Thus, in these case exhaustive searches are not possible, and we go for only reasonable random samples of the complete possibilities. Nevertheless, one must note that given a powerful computational set-up, such exhaustive search is possible for even higher dimensions and the computational effort can be estimated beforehand.

```
Algorithm 1: Merging technique
  Data: Target dimension $d$
  Step 1 : Generate $d'+1$ many MUBs of dimension $d'$, where $d'$ is the next higher
    prime to $d$.
  Step 2 : Merge the bases as generated in Step 1 in a matrix of order
    $((d'+1)\cdot d')\times d'$.
  Step 3 : Implement the routine of SVD to reduce the dimension of the matrix
    formed in Step 2 to $((d'+1)\cdot d')\times d$.
  Step 4 : The matrix as developed in Step 3 is split into $d'+1$ many boxes, each
    containing a matrix of order $d'\times d$.
  Step 5 : In each box, decompose the matrix into $\binom{d'}{d}$ many matrices of order $d\times d$
    and then orthogonalize to form the possible candidates for AMUB selection.
```

In the second effort, we consider each $d'\times d'$ matrix separately and apply SVD on each of them to construct each bucket and provide the results.

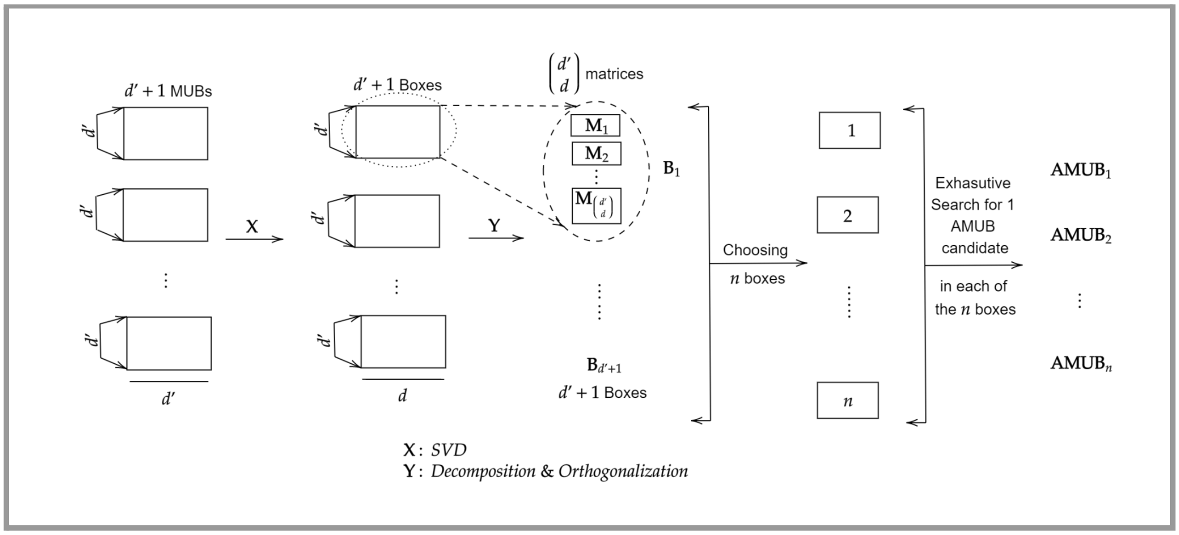

Figure 7.2: Non-Merging technique: Schematic Representation

As one can observe in Section 7.3, the results out of merging and non-merging techniques do not differ much. This needs further effort to study including investigating certain theoretical issues. In this technique (Non-Merged) of dimension reduction, the MUBs of dimension d' comes out to be unitary matrices. Hence, the SVD decomposition gives all the singular values as identity. Therefore, we always eliminate the last row and last column of the right singular matrix obtained from the decomposition and the corresponding singular value is made 0, post which an exhaustive search is performed as in the Merged technique and the dimension reduction proceeds as usual. We explain the non-merging technique in Figure 7.2 and then in Algorithm 2.

```
Algorithm 2: Non-Merging technique
  Data: Target dimension $d$
  Step 1 : Generate $d' + 1$ many MUBs of dimension $d'$, where $d'$ is the next higher
    prime to $d$.
  Step 2 : Instead of merging the bases as generated in Step 1, implement the routine
    of SVD directly to these $d' + 1$ bases to obtain $d' + 1$ many matrices of order $d' \times d$,
    and then arrange them into $d' + 1$ many boxes.
  Step 3 : In each box, decompose the the matrix into $\binom{d'}{d}$ many matrices of order
    $d \times d$ and then orthogonalize to form the possible candidates for AMUB selection.
```

Thus, from both of our techniques as illustrated above in Algorithms 1, 2, the idea of dimension reduction results in $d' + 1$ many boxes, each containing $\binom{d'}{d}$ bases of dimension d, and we thereby, proceed to our next step of choosing the appropriate bases.

7.2.2 Choice of Bases

The next component of our AMUB construction technique involves searching through the bases created and stored in $d'+1$ many boxes (as in Section 7.2.1) to obtain the set of required AMUBs, which will result in best possible measures (as defined in Section 7.1.1) used for the experimentation. In general, the search procedure used to create n many AMUBs of dimension d, as illustrated through the following algorithmic steps relates to an exhaustive combinatorial search procedure.

```
Algorithm 3: The Exhaustive Search Procedure
  Step 1 : Choose $n$ boxes from $d' + 1$ many boxes in $\binom{d'+1}{n}$ ways.

  Step 2 : From each of the chosen $n$ boxes, select a candidate base of dimension $d$ in
    $\binom{k}{1}$ ways, where $k = \binom{d'}{d}$.

  Step 3 : Then, determine the respective measures for the selected candidate bases
    as in Step 2.

  Step 4 : Choose the set of bases with the best possible results.
```

This exhaustive search procedure is implemented for dimensions $d = 6, 10$ for four AMUBs and only for $d = 6$ in the case of five MUBs. Mathematically, for n many AMUBs and a dimension d, that we obtain from a higher prime power dimension d', the exhaustive search complexity is $\binom{d'+1}{n} \cdot \left[\binom{\binom{d'}{d}}{1}\right]^n$. However, other than the cases mentioned above, we could not manage the exhaustive search in reasonable time in a simple laptop. However, the formula clearly provides the estimation of computational requirements in practice and can be achieved in a high end computational facility for even larger dimensions.

7.2.3 Further Heuristics

The set of AMUBs that we obtain from the above dimension reduction technique and search is again subjected to another gradient-ascent kind of heuristic for improved results. The heuristic search algorithm as given in [81] is tweaked and this is applied on the initial solutions (n AMUBs) obtained from Section 7.2.2. This is broadly a steepest-ascent search procedure, where the gradients are computed in each iteration and the set of n bases are altered accordingly keeping the property of orthonormality intact, thereby resulting in the set of AMUBs with optimal approximations. The algorithm is given as follows.

```
Algorithm 4: The Heuristic Search Algorithm
  Step 1 : The gradient $\{G_k : k = 1, 2, \ldots, n\}$ of the $k^{th}$ base is computed with
    respect to the remaining $n-1$ bases, where $G_k$ is given by,
      $$G_k = \frac{8}{n(n-1)(d-1)} Im\left[\sum_{l=1}^{n}\sum_{i,j=1}^{d}(|k_i\rangle\langle k_i|l_j\rangle\langle l_j|)^2\right]$$
  Step 2 : For the step size ($\epsilon$) of the algorithm, compute $\sigma_k$ corresponding to the $k^{th}$
    base such that, $\sigma_k = \epsilon G_k$ with a common $\epsilon > 0$.
  Step 3 : Implement a finite unitary change of the basis $k$, i.e., $|k_j\rangle \rightarrow V_k |k_j\rangle$, where
    $V_k = \mathbf{1} + i\sigma_k$ upto first order of $\sigma_k$.
  Step 4 : Finally, orthogonalize the set of $n$ bases $|k_j\rangle$, $j = 1, 2, \ldots, d$; $k = 1, 2, \ldots, n$.
```

We run the algorithm until all the components of the gradient vanishes.

7.3 Results & Numerical Study

In this section, we present the results obtained from the implementation of the dimension reduction algorithms (refer to Algorithms 1, 2 and 3). Further, we provide the results, when the AMUBs obtained from the dimension reduction algorithms are subjected to the heuristic search technique (refer to Algorithm 4). The values of the dimensions (d and d'), measures, i.e., maximum ASD ($\overline{D^2_{\max}}$) over all the iterations (refer to Equation 7.2) and the corresponding Drift Measure S (refer to Equation 7.3) and α (refer to Equation 7.4). We also highlight the complexity of our computations by reporting the number of iterations (denoted by $\#\mathbf{I}$). Note that, the initial solutions, i.e., the reduced bases obtained from the dimension reduction algorithms (Merging as well as Non-Merging techniques) are subjected to the heuristic search procedure for a fixed number of iterations ($\#\mathbf{I} = 20000$) for $d = 6, 10$ and ($\#\mathbf{I} = 1000$) for $d = 46$ and step size ($\epsilon = 0.500$). We also present the results corresponding to the heuristic search taking into account i) *maximization of ASD* ($\overline{D^2}$) and ii) *minimization of the Drift Measure* (S). Thereafter, we provide a comparative study of our results along with the results obtained from a combinatorial point of view as in [65, Corollary 1] and [86]. Some relevant observations are also noted in this section corresponding to the results obtained under our proposed framework.

First, we perform dimension reduction using the Merged technique (as in Algorithm 1). The results are presented (Table 7.1) for $n = 4$ and 5 sets of AMUBs in dimension 6, 10 and 46 respectively. Since the complexity for choosing bases for dimensions $10, 46$ is computationally expensive in certain cases, we randomly choose certain sets of boxes and search for the best results in them. That is the exhaustive search as in Algorithm 3 is not implemented in all the cases.

Table 7.1: Numerical Results for Merging technique: Algorithm 1

Number of Bases	$d' \to d$	$\overline{D^2_{\max}}$	S	α	$\#\mathbf{I}$
$n = 4$	$7 \to 6$	0.912	0.380	0.931	$\binom{8}{4}7^4$
	$11 \to 10$	0.936	0.405	1.281	$\binom{12}{4}11^4$
	$47 \to 46$	0.979	0.317	2.150	47^4
$n = 5$	$7 \to 6$	0.904	0.389	0.953	$\binom{8}{5}7^5$
	$11 \to 10$	0.928	0.388	1.227	11^5
	$47 \to 46$	0.979	0.350	2.374	47^5

Remark 7.3.1. *The computational results as presented in Table 7.1 suggests that, our proposed algorithm related to the Merging technique (Algorithm 1) successfully generates increased sets (*larger than the available bound*) of AMUBs with closer approximations to MUBs (with respect to $\overline{D^2}$).*

The resultant reduced sets of bases/AMUBs obtained from the Merging technique are further subjected to the Heuristic Search Algorithm, the results of which are provided below, both with respect to $\overline{D^2}$ and S in Tables 7.2 and 7.3 respectively.

Remark 7.3.2. *Few of the notable observations when the Heuristic Search is aimed at maximizing $\overline{D^2}$ under the Merging technique, are as follows,*

Table 7.2: Numerical Results for Heuristic Search (Algorithm 4) on the bases obtained from the Merged technique with respect to ASD ($\overline{D^2}$)

Number of Bases	$d' \to d$	$\overline{D^2_{\max}}$	S	α	# **I**	Step Size (ϵ)
$n = 4$	$7 \to 6$	0.971	0.383	0.938	10000	0.500
	$11 \to 10$	0.973	0.447	1.414	10000	0.500
	$47 \to 46$	0.982	0.366	2.482	1000	0.500
$n = 5$	$7 \to 6$	0.960	0.399	0.977	10000	0.500
	$11 \to 10$	0.930	0.369	1.167	10000	0.500
	$47 \to 46$	0.981	0.314	2.130	1000	0.500

- *For a fixed set of bases (n), as the dimension (d) increases, the average distance between the bases ($\overline{D^2}$) tends to increase.*

- *Now if the dimension (d) is kept fixed, the average distance between the bases seems to vary inversely with n.*

- *The value of α which normalizes the Drift Measure (S) is higher for larger dimensions (keeping n fixed) as well as for higher values of n (keeping d fixed).*

Table 7.3: Numerical Results for Heuristic Search (Algorithm 4) on the bases obtained from the Merged technique with respect to Drift Measure (S)

Number of Bases	$d' \to d$	$\overline{D^2_{\max}}$	S	α	# **I**	Step Size (ϵ)
$n = 4$	$7 \to 6$	0.931	0.325	0.797	10000	0.500
	$11 \to 10$	0.964	0.305	0.965	10000	0.500
	$47 \to 46$	0.977	0.320	2.174	1000	0.500
$n = 5$	$7 \to 6$	0.936	0.355	0.871	10000	0.500
	$11 \to 10$	0.917	0.332	1.050	10000	0.500
	$47 \to 46$	0.978	0.305	2.071	1000	0.500

Remark 7.3.3. *In case the heuristic search is aimed at minimizing the Drift Measure* (S) *under the Merging technique, we note the following.*

- *In view of the values of S (both in the cases when n and d are considered to be fixed) in Table 7.3, the pattern in which S varies is not definitive unlike $\overline{D^2}$.*
- *The behavior of α tends to be the same as mentioned in Note 7.3.2.*

Consequently in Tables 7.4, 7.5 and 7.6, we report the results for the same sets of operations, as in dimension reduction and subjecting the bases to the heuristic search routine, when performed with the Non-Merged sets of bases both with respect to the optimization routine followed in view of maximizing the average distance ($\overline{D^2}$) and the Drift (S). As mentioned earlier, to avoid the high complexity in choosing bases for sets of 4 and 5 AMUBs of dimension 46 and sets of 5 AMUBs of dimension 10, we have randomly chosen certain sets of boxes instead of performing an exhaustive search and reported the best results obtained in them.

Table 7.4: Numerical results for the Non-Merging technique: Algorithm 2

Number of Bases	$d' \to d$	$\overline{D^2_{\max}}$	S	α	# **I**
$n = 4$	$7 \to 6$	0.909	0.423	1.036	$\binom{8}{4}7^4$
	$11 \to 10$	0.933	0.448	1.417	$\binom{12}{4}11^4$
	$47 \to 46$	0.974	0.558	3.785	47^4
$n = 5$	$7 \to 6$	0.901	0.423	1.036	$\binom{8}{5}7^5$
	$11 \to 10$	0.916	0.520	1.644	11^5
	$47 \to 46$	0.975	0.447	3.032	47^5

Remark 7.3.4. *Observations as reported above in Table 7.4 shows that the proposed Non-Merging technique for generating AMUBs results into increased sets of bases (with respect to $\overline{D^2}$) providing close approximations to MUBs.*

Remark 7.3.5. *In reference to Tables 7.5 and 7.6, we note the following.*

- *Heuristic Search aimed at* maximization *of $\overline{D^2}$ (Table 7.5) under the Non-Merging technique leads to an increasing trend in the average distance between the bases both in the cases when i) d increases over a fixed value of n and ii) n increases over a fixed value of the dimension (d).*
- *When the Heuristic Search* minimizes *S (Table 7.6) under the Non-Merging technique does not show any definitive pattern in the values of the Drift Measure, whereas the values α increases with d.*

Table 7.5: Numerical results for Heuristic Search (Algorithm 4) on the Bases obtained from Non-Merged technique with respect to $\overline{D^2}$

Number of Bases	$d' \to d$	$\overline{D^2_{\max}}$	S	α	# **I**	Step Size (ϵ)
$n=4$	$7 \to 6$	0.972	0.404	0.989	10000	0.500
	$11 \to 10$	0.973	0.440	1.391	10000	0.500
	$47 \to 46$	0.982	0.600	4.069	1000	0.500
$n=5$	$7 \to 6$	0.959	0.399	0.977	10000	0.500
	$11 \to 10$	0.967	0.391	1.236	10000	0.500
	$47 \to 46$	0.983	0.451	3.059	1000	0.500

Table 7.6: Numerical results for Heuristic Search (Algorithm 4) on the Bases obtained from Non-Merged technique with respect to Drift Measure (S)

Number of Bases	$d' \to d$	$\overline{D^2_{\max}}$	S	α	# **I**	Step Size (ϵ)
$n=4$	$7 \to 6$	0.963	0.337	0.826	10000	0.500
	$11 \to 10$	0.926	0.303	0.958	10000	0.500
	$47 \to 46$	0.974	0.558	3.787	1000	0.500
$n=5$	$7 \to 6$	0.908	0.364	0.892	10000	0.500
	$11 \to 10$	0.917	0.338	1.070	10000	0.500
	$47 \to 46$	0.983	0.446	3.026	1000	0.500

Remark 7.3.6. *Some important observations related to the Merged and Non-Merged techniques of dimension reduction as well as the measures $\overline{D^2}$ and S are as follows.*

- *In reference to the results for the Merging and Non-Merging techniques presented above in Tables 7.1 and 7.4, we observe that, the initial solutions in case of the Merging technique provides more or less better results than the Non-Merging technique with respect to the value of $\overline{D^2}$ (*more closer to 1*) as well as the value of S (*comparatively lower*).*

- *It is also to be noted that, we are considering the efficacy of our results, i.e.,* closeness *of AMUBs to MUBs in terms of $\overline{D^2}$ as the heuristic search [81] deals with the optimization of $\overline{D^2}$, also we have extended the optimization (*minimization*) with respect to the Drift Measure S. Further we observe that in the Merging and Non-Merging techniques, achieving* simultaneous control *over both $\overline{D^2}$ and S seems to be quite difficult at this stage, i.e., as the value of $\overline{D^2}$ is being optimized (*closer to 1*) by the Heuristic Search, the value of S does not decrease. On the other hand, when the Heuristic Search aims at* minimizing *S, the value of $\overline{D^2}$ moves further away from* 1*, which is naturally expected from the respective definitions of the measures used.*

In the following Table 7.7, we present the results for dimensions $d = 6, 10$ and 46, where AMUBs have been constructed using a combinatorial technique. In reference to [65, Corollary 1], combinatorial construction for AMUBs is available for every even dimension with $k = 2$. For such construction, it can be shown that,

$$\overline{D^2} = \frac{d \cdot (k^2 - 1)}{k^2 \cdot (d - 1)}, \text{for } k = 2 \tag{7.7}$$

$$\Rightarrow \overline{D^2} = \frac{3}{4} \cdot \frac{d}{d-1} \tag{7.8}$$

It is to be noted that, the value of $\overline{D^2}$ is smaller in case of the combinatorial construction of AMUBs in comparison to the the construction algorithms proposed here for generating AMUBs. Observe that, $\overline{D^2} \to 1 - \frac{1}{k^2}$ asymptotically for large values of d. And in general for the dimensions under consideration, i.e., $d = 6, 10$ and 46, we have $\overline{D^2} \to \frac{3}{4} = 0.75 \ll$ all the values of $\overline{D^2}$ achieved using the above techniques. We should also mention that the theoretical result of [86] is not applicable for the small dimensions $d = 6, 10$. The bound for $d = 46$ is also worse than what we obtain by our technique.

Table 7.7: Numerical Results for AMUBs constructed using Combinatorial techniques [65, Corollary 1]

Number of Bases	d	$\overline{D^2}$	S	α
$n = 4, 5$	6	0.900	0.408	0.999
	10	0.833	0.316	0.999
	46	0.767	0.352	2.387

All the results above are computed in a laptop supported by `Apple M1 chip - 8 core CPU` and `8 GB of RAM`, using the open source `Python` programming language. We have implemented a multiprocessing technique using the `Python` function `multiprocessing.ProcessPool`, with 16 processes to speed up the process of choosing AMUBs in dimension reduction technique. Significant improvement over execution timings as well as number of iterations can be obtained if the program is executed on a GPU integrated environment. The SVD routine was performed using the `numpy.linalg.svd` function from the `Python` library `numpy`. In Algorithms 1, 2 and 4, we utilize the QR Decomposition routine for orthogonalizing the set of bases using the `numpy.linalg.qr` function from the `Python` library `numpy`. The relevant codes of the numerical experimentation and computations are present in the `GitHub Repository` [27].

7.4 Conclusion

In this chapter we have presented a broad framework for the construction of AMUBs. The initial approach is based on the widely used dimension reduction technique, namely the Singular Value Decomposition (SVD). This technique has been successfully exploited in different domains of the Machine Learning literature. The resulting approximate MUBs from this strategy are considered as initial solutions. Consequently, those are further subjected to a steepest ascent kind of heuristic search technique, as in [81], to obtain improved results. The novelty of our approach lies in the fact that the broad framework does not require any prior mathematical formulation and parameterization of the AMUBs to be generated. Observe that, the heuristic search has been implemented aiming to optimize the average distance between the bases ($\overline{D^2}$) [81] and further extended to an optimization of the drift measure (S). Hence, it is to be kept in mind that, this generic approach of computation and experimentation to generate AMUBs presented here can be efficiently used with the two available optimizations as and when required. As we note, these are only initial experimental results that can be improved with different kinds of refinements and even with this initial approach, we could obtain quite encouraging results.

Further, our prospective work will address another general experimentation of generating AMUBs for any dimension d. One may first consider the available MUBs for that dimension d, say k and then produce sets of $k+1$ AMUBs, where the $(k+1)$-th basis may be explored from the dimension reduction technique, i.e., which involves the reduction of dimension d' (next higher prime to d) to d. For example, consider dimension $d = 6 = 2 \cdot 3$, for which $k = 3$ MUBs are known to exist. To generate sets of $k+1 = 4$ AMUBs, we will take the 4-th AMUB from the bases created by the dimension reduction routine (reducing dimension from $d' = 7$ to $d = 6$). We may go for some steepest ascent kind of heuristic further. Similarly, for dimension $d = 12 = 2^2 \cdot 3$, one can obtain sets of $k + 1 = 5$ AMUBs from the $k = 4$ MUBs that are known to exist. The 5-th AMUB would be generated through dimension reduction (from $d' = 13$ to $d = 12$) and further search. Likewise, this approach can be extended to higher dimension, providing another generic framework in obtaining Approximate Mutually Unbiased Bases.

With this chapter, we conclude our technical contributions in this thesis. In the next chapter we will present the concluding remarks and explain the important open questions that might be interesting as future research directions.

Chapter 8

Concluding Remarks

Here we first summarize the contribution of the thesis and then list related open problems in this direction of research.

8.1 Summary of the thesis

In this dissertation we have studied several issues related to certain approximate versions of Mutually Unbiased Bases (MUBs). Chapter 1 presents a brief introduction and in Chapter 2, we provide an outline of existing research and show how our work fits in that framework. The next four chapters are contributory works of this thesis.

In Chapter 3, we present a construction method to obtain at most $(\sqrt{d}+1)$ many approximate MUBs for the dimension $d = q^2$, where q is any positive integer. For $q \equiv 0 \bmod 4$, we obtain Approximate Real MUBs (ARMUBs) under the assumption that a Hadamard matrix of order q exists. We also identify the inner product values between the vectors from two different bases. In particular, we show that for a prime x, and $d = (4x)^2$, we obtain $(\frac{\sqrt{d}}{4}+1)$ many ARMUBs such that for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| \leq \frac{4}{\sqrt{d}}$. This contribution of this chapter has been published in [67].

We work in the similar direction for improved and generalized techniques in Chapter 4. Various constructions exploiting involved combinatorial structures such as Resolvable Block Designs are studied in this chapter. We start with a generic construction idea to relate the RBDs with MUBs and Approximate Real MUBs. Our construction is such that the basis vectors have small number of non-zero co-ordinates. That is, the constructed bases are sparse. Specific parameters have been explored for which we could demonstrate new classes of approximate MUBs and provide improved results. For example, we identify a novel infinite family of $\lceil\sqrt{d}\rceil$ many ARMUBs for dimensions $d = q(q+1)$, where q is a prime power and

$q \equiv 3 \bmod 4$. Here, for any two vectors v_1, v_2 belonging to different bases, $|\langle v_1|v_2\rangle| < \frac{2}{\sqrt{d}}$. We also study other important scenario such as $d = sq^2$, where q is a prime power and $sq \equiv 0 \bmod 4$. The work of this chapter got published in [65].

Our final work in this direction is to formalize the definition of approximate MUBs with further restrictions. This is presented in Chapter 5. We introduce the nomenclature Almost Perfect MUBs (APMUBs), where the absolute value of inner product $|\langle v_1|v_2\rangle|$ is exactly two-valued, one being zero and the other $\leq \frac{1+\mathcal{O}(d^{-\lambda})}{\sqrt{d}}$, such that $\lambda > 0$ and the numerator $1+\mathcal{O}(d^{-\lambda}) \leq 2$. Here, the constructed vectors have the important feature that large number of its components are zero as in our earlier constructions. Further, each non-zero component is of equal magnitude. Here also, the techniques are mostly based on Resolvable Block Designs (RBDs). We first show that for a composite dimension $d = k \cdot s$, $k \leq s \leq 4k$, one can construct at least $N(s)+1$ many APMUBs, where $N(s)$ is the number of Mutually Orthogonal Latin Squares (MOLS) of order s. Then we also consider the cases when the component of the vectors are real, producing real APMUBs of similar order, whenever real Hadamard matrix of order k are available. Moreover, when $s = q$, a prime power, we have $N(q) = q - 1$. This provides a construction method of $q \sim \mathcal{O}(\sqrt{d})$ many APMUBs. The methodology is extended to composite dimension of the general form $d = (q-e)(q+f)$, $e, f \in \mathbb{N}$, with $0 \leq f \leq e$ and a prime power q. We have noted that such cases are at least as numerous as the prime numbers in the set of positive integers. These results are also related to construction of Bi-angular vectors. The APMUBs, so constructed in $\mathbb{C}^d$ or $\mathbb{R}^d$, present sets of Bi-angular vectors which are of the order of $\mathcal{O}(d^{3/2})$ in numbers (the known upper bound is $\mathcal{O}(d^2)$). All these results are available in [68].

Relaxing the strict criteria of APMUB we revisit the AMUBs in Chapter 6. Here we extend and generalize the ideas of Chapter 4, taking some ideas from Chapter 5. As in the previous two chapters the Resolvable Block Designs are exploited, but with much greater details. In this regard, we broadly categorize RBD(X, A) into two categories, one where all the parallel classes have a constant block size and another where they do not have a constant block size. The results provide various classes of AMUBs both in real and complex cases for composite dimensions, that are not prime power. These results are presented in [66].

While the deterministic combinatorial constructions are the prime contributions in this thesis, we also explored a heuristic framework to search Approximate MUBs with good parameters. This is presented in the final contributory chapter, namely Chapter 7. We obtain some interesting parameters when we compare them with the Approximate MUBs presented in Chapters 3, 4. In particular, these are not APMUBs as described in Chapter 7 that are of nice combinatorial structures. Instead of combinatorial techniques, certain heuristics are implemented and the experimental results from certain computer programs are reported. The basic idea is as follows. Given any non-prime dimension d, we first consider the closest prime $d' > d$ and construct $d'+1$ MUBs through the existing methods, such as [79, 60, 6]. Then we explore two techniques one after the other. First we apply basis reduction techniques from Machine Learning literature to generate the initial solutions. Then the steepest ascent kind of search strategy is used to improve the results. The experimental outcome is evaluated through construction of AMUBs for the dimensions $d = 6, 10, 46$ from the primes $d' = 7, 11$ and 47 respectively. Our technique here provides a generic framework in construction of Approximate MUBs heuristically, that is published in [28].

With this backdrop, let us now present a few problems that we find interesting for future research.

8.2 Future research directions

In this thesis we have contributed different results related to Approximate MUBs (AMUBs). Naturally the prime questions are:

- how to increase the numbers of such AMUBs,
- how to obtain such MUBs in different dimensions, i.e., we like to cover the space of positive integers as much as possible, and
- how to achieve the absolute value of the inner product between two vectors from two different AMUBs close to $\frac{1}{\sqrt{d}}$.

The results of Chapter 3 provides a method to obtain at most $(\sqrt{d} + 1)$ many approximate MUBs for the dimension $d = q^2$. That is, the further questions will be, how can we relax the square dimension, how to make the inner product value closer to $\frac{1}{\sqrt{d}}$ from $\frac{4}{\sqrt{d}}$ and how to increase the numbers beyond $\mathcal{O}(\sqrt{d})$. Further here the constraints are more as we are discussing about real vectors only. This is the reason more involved combinatorial structures like RBDs are exploited in Chapters 4, 5. In this direction, we have presented certain questions in Section 5.6.3. Increase in the number of parallel classes are always beneficial to have more approximate MUBs. That is why, further efforts are required in this direction. Considering $d = (q - e)(q + e)$, it seems that more than $r = \left\lfloor \frac{q}{e} \right\rfloor + 1$ many parallel classes can be explored. A detailed research in this direction and exploring related combinatorial objects will be important here. Additional questions are also there in the following cases:

- $d = q(q + f)$, RBD having block size q, with $q + f$ blocks in each parallel classes,
- $d = (q - e)(q + f),\ 0 < e < f$, RBD having block size $q - e$, with $q + f$ blocks in each parallel classes.

In these cases actually we depended on the bounds provided by the MOLS. Improving these further will be an important research area.

We consider different forms of d, mostly as product of two numbers. Now the question is, how to estimate the density of integers d, for which our method of RBD can give $\mathcal{O}(\sqrt{d})$ many APMUBs. We have shown the existence of APMUBs of $\mathcal{O}(\sqrt{d})$ for dimension d of the form $(q-e)(q+f)$ with $0 \leq f \leq e$ such that $0 \leq (f+4e) \leq 3q$. Note that number of APMUB as per Theorem 5.6.2 (and the following remark) is $\lfloor \frac{q-e}{f} \rfloor + 1 = \mathcal{O}(\sqrt{d})$ whenever f is bounded. Particularly when $f = 0$, we have $d = (q-e)q$ and $0 \leq e \leq \frac{3}{4}q$ then the number of APMUBs is $q = \mathcal{O}(\sqrt{d})$ for all such d. Basic analysis reveals that at least constant proportion of prime density ($\mathcal{O}(\frac{N}{\log N})$, for an integer of the order of N) may be covered in such cases. However, number theoretic techniques may be employed to obtain specific estimates, and that could be an interesting area to study.

Chapter 7 considers certain heuristics. However, the area of dimension reduction needs more involved studies. The dimension reduction techniques to obtain an orthonormal basis of dimension d from a higher dimension d' is by itself an interesting computational problem. Further, in the framework of approximate MUBs, one needs to restrict the absolute value of the inner product between two vectors from two different bases. Such basis reduction techniques with further restrictions may require further efforts by combining advanced tools from linear algebra and discrete algorithms.

Finally we like to conclude this thesis by again pointing out that there are several open problems in the domain of actually constructing the (exact) MUBs. While we have considered several approximate versions in this thesis, the original problems related to MUBs are still open even after significant efforts by researchers for half a century. Interested researchers may have a look at [39, 64] and the references therein for deeper information about these problems.

Bibliography

[1] 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`

[2] 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

[3] D. M. Appleby, I. Bengtsson, and H. B. Dang. *Galois unitaries, mutually unbiased bases, and mub-balanced states.* Quantum Information and Computation, 15(15-16): 1261–1294, 2014. doi: `https://doi.org/10.26421/QIC15.15-16-1`, arXiv: `https://arxiv.org/abs/1409.7987`

[4] K. T. Arasu and T. A. Gulliver. *Self-dual codes over F/sub p/ and weighing matrices.* IEEE Transactions on Information Theory, 47(5): 2051–2055, 2001. doi: `https://doi.org/10.1109/18.930940`

[5] R. C. Baker, G. Harman, and J. Pintz. *The difference between consecutive primes, II.* Proceedings of the London Mathematical Society, 83(3): 532–562, 2001. doi: `https://doi.org/10.1112/plms/83.3.532`

[6] 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

[7] 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

[8] 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

[9] 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.

[10] 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

[11] D. Best. *Biangular vectors*. MS thesis, Department of Mathematics and Computer Science University of Lethbridge, 2013. URL: https://core.ac.uk/download/pdf/185288092.pdf

[12] D. Best, H. Kharaghani, and H. Ramp. *Mutually unbiased weighing matrices*. Designs, Codes and Cryptography, 76(2): 237–256, 2015. doi: https://doi.org/10.1007/s10623-014-9944-6

[13] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory*. Vol. 1, 2nd ed., Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1999. doi: https://doi.org/10.1017/CBO9780511549533

[14] 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

[15] 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

[16] 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.

[17] 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.

[18] P. O. Boykin, M. Sitharam, M. Tarifi, and P. Wocjan. *Real Mutually Unbiased Bases.* 2005. arXiv: https://arxiv.org/abs/quant-ph/0502024, 2005.

[19] 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

[20] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. *$\mathbb{Z}_4$-kerdock codes, orthogonal spreads, and extremal Euclidean line-sets.* Proceedings of The London Mathematical Society, 75(2): 436–480, 1997. doi: https://doi.org/10.1112/S0024611597000403

[21] P. J. Cameron. *Hadamard and Conference Matrices.* 2018. URL: http://www-groups.mcs.st-andrews.ac.uk/~pjc/Summer18/conf.pdf.

[22] P. J. Cameron and J. J. Seidel. *Quadratic forms over $GF(2)$.* Indagationes Mathematicae (Proceedings), 76(1): 1–8, 1973. doi: https://doi.org/10.1016/1385-7258(73)90014-0

[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] P. G. Casazza, A. Farzannia, J. I. Haas, and T. T. Tran. *Toward the classification of biangular harmonic frames.* Applied and Computational Harmonic Analysis, 46(3): 544–568, 2019. doi: https://doi.org/10.1016/j.acha.2017.06.004

[25] P. G. Casazza, G. Kutyniok, and F. Philipp. *Introduction to finite frame theory.* In: P. G. Casazza, G. Kutyniok (eds.), Finite Frames - Theory and Applications, Applied and Numerical Harmonic Analysis, pp. 1–53, 2013. doi: https://doi.org/10.1007/978-0-8176-8373-3_1

[26] P. G. Casazza and R. G. Lynch. *A brief introduction to Hilbert space frame theory and its applications.* arXiv: https://arxiv.org/abs/1509.07347, 2016

[27] S. Chaudhury, A. Kumar, S. Maitra, S. Roy, and S. SenGupta. GitHub Repository for Codes - https://bit.ly/3KPS9jk, uploaded by S. Chaudhury, 2022.

[28] S. Chaudhury, A. Kumar, S. Maitra, S. Roy, and S. SenGupta. *A Heuristic Framework to Search for Approximate Mutually Unbiased Bases.* Cyber Security, Cryptology, and Machine Learning - 6th International Symposium, LNCS, 13301: 208–223, 2022. doi: https://doi.org/10.1007/978-3-031-07689-3_16

[29] 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`.

[30] 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`

[31] C. J. Colbourn and J. H. Dinitz. *Handbook of combinatorial designs*. Second Edition, CRC press, 2010. doi: `https://doi.org/10.1201/9781420010541`

[32] M. P. Colomer, L. Mortimer, I. Frérot, M. Farkas, and A. Acín. *Three Numerical Approaches to find Mutually Unbiased Bases using Bell Inequalities*. Quantum, 2022, 6, pp.778. doi: `https://doi.org/10.22331/q-2022-08-17-778`, arXiv : `https://arxiv.org/abs/2203.09429`, 2022

[33] H. Cramér. *On the order of magnitude of the difference between consecutive prime numbers*. Acta arithmetica, 2(1): 23–46, 1936.

[34] D. Crnković, R. Egan, B. G. Rodrigues, and A. Švob. *LCD codes from weighing matrices*. Applicable Algebra in Engineering, Communication and Computing, 32(2): 175–89, 2021. doi: `https://doi.org/10.1007/s00200-019-00409-8` arXiv: `https://arxiv.org/abs/1812.00368`, 2019

[35] P. Delsarte. *An Algebraic Approach to the Association Schemes of Coding Theory.* Thesis, Dissertation, Philips research reports, no. 10, 1973. URL: `https://books.google.co.in/books?id=zna0SgAACAAJ`.

[36] P. Delsarte, J. M. Goethals, and J. J. Seidel. *Bounds for systems of lines, and Jacobi polynomials*. Geometry and Combinatorics, pp. 193–207, 1991. doi: `https://doi.org/10.1016/B978-0-12-189420-7.50020-7`

[37] D. Ž. Djoković. *Hadamard matrices of order* 764 *exist.* Combinatorica, 28(4): 487–489, 2008. doi: `https://doi.org/10.1007/s00493-008-2384-z`

[38] H. Dubner. *Large Sophie Germain primes*. Math Comput. 65(213): 393–397, 1996. doi: `https://doi.org/10.1090/S0025-5718-96-00670-9`.

[39] 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`

[40] C. Eckart and G. Young. *A principal axis transformation for non-hermitian matrices.* Bulletin of the American Mathematical Society, 45(2): 118–121, 1939. doi: `https://doi.org/10.1090/S0002-9904-1939-06910-3`

[41] R. Egan. *A survey of complex generalized weighing matrices and a construction of quantum error-correcting codes.* arXiv: `https://arxiv.org/abs/2309.07522`

[42] I. K. Fodor. *A Survey of Dimension Reduction Techniques.* Technical report, Lawrence Livermore National Lab., CA (US), 2002.

[43] C. Godsil and A. Roy. *Equiangular lines, mutually unbiased bases, and spin models.* European Journal of Combinatorics, 30(1):246–262, 2009. doi: `https://doi.org/10.1016/j.ejc.2008.01.002`

[44] R. Gow. *Real mutually unbiased bases and representations of groups of odd order by real scaled Hadamard matrices of* 2*-power size.* arXiv: `https://arxiv.org/abs/1410.4059v2`, 2017

[45] 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

[46] H. Hanani. *On resolvable balanced incomplete block designs.* Journal of Combinatorial Theory, Series A, 17(3): 275–289, 1974. doi: `https://doi.org/10.1016/0097-3165(74)90093-4`.

[47] M. Harada and S. Suda. *On binary codes related to mutually quasi-unbiased weighing matrices.* Australasian Journal of Combinatorics, 66(1): 10–22, 2015. arXiv: `https://arxiv.org/abs/1504.03502`, 2016.

[48] A. Hedayat and W. D. Wallis. *Hadamard matrices and their applications.* Institute of Mathematical Statistics: Annals of Statistics, 6(6): 1184–1238, 1978. doi: `https://doi.org/10.1214/aos/1176344370`

[49] W. Holzmann, H. Kharaghani, and W. Orrick. *On the real unbiased Hadamard matrices.* Contemporary Mathematics, Combinatorics and Graphs, 531: 243–250, 2010.

[50] W. Holzmann, H. Kharaghani, and S. Suda. *Mutually unbiased biangular vectors and association schemes.* Algebraic Design Theory and Hadamard Matrices, 133: 149–157, 2015. doi: `https://doi.org/10.1007/978-3-319-17729-8_12`.

[51] W. C. Huffman and V. Pless. *Fundamentals of Error-Correcting Codes.* Cambridge University Press, 2003. doi: `https://doi.org/10.1017/CBO9780511807077`

[52] 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

[53] J. John, K. Russell, E. Williams, and D. Whitaker. *Theory & methods: Resolvable designs with unequal block sizes.* Australian & New Zealand Journal of Statistics, 41(1): 111–116, 1999. doi: https://doi.org/10.1111/1467-842X.00065

[54] D. Jungnickel and V. D. Tonchev. *Perfect codes and balanced generalized weighing matrices.* Finite Fields and Their Applications, 5(3): 294–300, 1999. doi: https://doi.org/10.1006/ffta.1999.0252

[55] D. Jungnickel and V. D. Tonchev. *Perfect codes and balanced generalized weighing matrices, II.* Finite Fields and Their Applications, 8(2): 155–165, 2002. doi: https://doi.org/10.1016/S1571-0653(04)00162-3

[56] S. Kageyama. *Resolvability of Block Designs.* The Annals of Statistics, 4(3): 655–661, 1976. doi: https://doi.org/10.1214/aos/1176343475.

[57] D. Kalman. *A Singularly Valuable Decomposition: The SVD of a Matrix.* The College Mathematics Journal, 27(1), 2–23, 1996. doi: https://doi.org/10.1080/07468342.1996.11973744

[58] H. Kharaghani and B. T. Rezaie. *A Hadamard Matrix of Order 428.* Journal of Combinatorial Designs, 13(6): 435–440, 2005. doi: https://doi.org/10.1002/jcd.20043

[59] H. Kharaghani and S. Suda. *Unbiased orthogonal designs.* Designs, Codes and Cryptography, 86(7): 1573–1588, 2018. doi: https://doi.org/10.1007/s10623-017-0414-9

[60] 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

[61] 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

[62] C. Koukouvinos and J. Seberry. *Weighing matrices and their applications.* Journal of Statistical planning and inference, 62(1): 91–101, 1997. doi: https://doi.org/10.1016/S0378-3758(96)00172-3

[63] A. Kourbatov. *Upper bounds for prime gaps related to Firoozbakht's conjecture*. Journal of Integer Sequences, Vol. 18, 2015. arXiv: `https://arxiv.org/abs/1506.03042`, 2019.

[64] O. Krueger and R. F. Werner. *Some Open Problems in Quantum Information Theory.* arXiv `https://arxiv.org/abs/quant-ph/0504166`, 2005

[65] 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`

[66] A. Kumar and S. Maitra. *Further Constructions of AMUBs for Non-prime Power Composite Dimensions*. Preprint. arXiv: `https://arxiv.org/abs/2402.04231`, 2024.

[67] 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`

[68] A. Kumar. S. Maitra and S. Roy. *Almost Perfect Mutually Unbiased Bases that are Sparse*. Preprint. arXiv: `https://arxiv.org/abs/2402.03964`, 2024.

[69] A. LeClair. *An asymptotic upper bound on prime gaps*. arXiv: `https://arxiv.org/abs/1506.03359`, 2015.

[70] 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`

[71] J. Li and K. Feng. *Constructions on approximately mutually unbiased bases by galois rings*. Journal of Systems Science and Complexity, 28(6): 1440–1448, 2015. doi: `https://doi.org/10.1007/s11424-015-3262-6`

[72] M. Magsino and D. G. Mixon. *Biangular Gabor frames and Zauner's conjecture*. In proceeding of Wavelets and Sparsity XVIII, 11138: 111381G. International Society for Optics and Photonics, SPIE, 2019. doi: `https://doi.org/10.1117/12.2529671`

[73] G. Mikhail and S. Ferenc. *Biangular Lines Revisited*. Discrete & Computational Geometry, 66(3): 1113–1142, 2021. doi: `https://doi.org/10.1007/s00454-021-00276-6`

[74] H. Nozaki and S. Suda. *Weighing matrices and spherical codes*. Journal of algebraic Combinatorics, 42: 283–291, 2015 doi: `https://doi.org/10.1007/s10801-015-0581-6` arXiv: `https://arxiv.org/abs/1309.3892`, 2014

[75] R. E. A. C. Paley. *On orthogonal Matrices.* Journal of Mathematics and Physics, 12(1–4): 311–320, 1933. doi: https://doi.org/10.1002/sapm1933121311.

[76] T. Paterek, B. Dakić, and Č. Brukner. *Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models.* Physical Review A, 79(1): 012109, 2009. doi: https://doi.org/10.1103/PhysRevA.79.012109, arXiv: https://arxiv.org/abs/0804.2193, 2009

[77] 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

[78] H. D. Patterson and E. R. Williams. *A new class of resolvable incomplete block designs.* Biometrika, 63(1): 83–92, 1976. doi: https://doi.org/10.1093/biomet/63.1.83

[79] A. O. Pittenger and M. H. Rubin. *Mutually Unbiased Bases, Generalized Spin Matrices and Separability.* Linear Algebra and its Applications, 390: 255–278, 2004. doi: https://doi.org/10.1016/j.laa.2004.04.025 arXiv: https://arxiv.org/abs/quant-ph/0308142, 2004

[80] D. K. Raychaudhuri and R. M. Wilson. *The existence of resolvable block designs.* A survey of Combinatorial Theory, PP. 361–375. Elsevier, 1973. doi: https://doi.org/10.1016/B978-0-7204-2262-7.50035-1

[81] P. Raynal, X. Lu, and B. Englert. *Mutually unbiased bases in six dimensions: The four most distant bases.* Phys.Rev. 83, 062303, 2011. doi: https://doi.org/10.1103/PhysRevA.83.062303

[82] R. A. Sadek. *SVD Based Image Processing Applications: State of The Art, Contributions and Research Challenges.* International Journal of Advanced Computer Science and Applications, 3(7), 2012. doi: https://doi.org/10.14569/IJACSA.2012.030703 arXiv: https://arxiv.org/abs/1211.7102, 2012

[83] M. Saniga and M. Planat. *Hjelmslev geometry of mutually unbiased bases.* Journal of Physics A: Mathematical and General, 39(2): 435, 2005. doi: https://dx.doi.org/10.1088/0305-4470/39/2/013

[84] 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

[85] 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`

[86] 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`

[87] S. S. Shrikhande. *Affine resolvable balanced incomplete block designs: a survey.* Aequationes Mathematicae, 14(3): 251–269, 1976. doi: `https://doi.org/10.1007/BF01835977`

[88] S. Shrikhande and D. Raghavarao. *Affine α-resolvable incomplete block designs*. Contributions to statistics, Elsevier, pp. 471–480, 1965. doi: `https://doi.org/10.1016/B978-1-4832-3160-0.50034-8`

[89] J. H. Silverman and J. T. Tate. *Rational Points on Elliptic Curves*. Springer, 2015. doi: `https://doi.org/10.1007/978-3-319-18588-0`

[90] N. K. Sinha. *On a new property of primes that leads to a generalization of Cramér's conjecture.* arXiv: `https://arxiv.org/abs/1010.1399`, 2010.

[91] N. Sripaisan and Y. Meemark. *Approximately mutually unbiased bases by frobenius rings*. Journal of Systems Science and Complexity, 33(4): 1244–1251, 2020. doi: `https://doi.org/10.1007/s11424-020-8251-8`

[92] G. W. Stewart. *On the early history of the singular value decomposition.* SIAM Review, 35(4): 551-566, 1993. doi: `https://doi.org/10.1137/1035134`

[93] D. R. Stinson. *Combinatorial designs: constructions and analysis.* Springer Science & Business Media, 2007.

[94] F. Szöllősi. *Construction classification and parametrization of complex Hadamard matrices*. ProQuest Dissertations And Theses; Thesis (Ph.D.)–The University of Wisconsin - Madison, 2011. arXiv: `https://arxiv.org/abs/1110.5590`, 2011

[95] The Online Encyclopedia of Integer Sequences. *Primes p such that* $2p-1$ *is also Prime.* URL: `http://oeis.org/A005382`

[96] G. Wang, M. Y. Niu, and F. W. Fu. *Two new constructions of approximately mutually unbiased bases.* International Journal of Quantum Information, 16(4): 1850038, 2018. doi: `https://doi.org/10.1142/S0219749918500387`

[97] 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

[98] 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

[99] 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

[100] W. K. Wootters. *Quantum measurements and finite geometry.* Foundations of Physics, 36(1): 112–126, 2006. doi: https://doi.org/10.1007/s10701-005-9008-x arXiv: https://arxiv.org/abs/quant-ph/0406032, 2004

[101] 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

[102] 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