REGULAR STRUCTURES OF LINES IN COMPLEX SPACES

by

Mahdad Khatirinejad Fard
B.Sc., Sharif University of Technology, 2000
M.Sc., Simon Fraser University, 2002

A THESIS SUBMITTED IN PARTIAL FULFILLMENT
OF THE REQUIREMENTS FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY
in the Department
of
Mathematics

SIMON FRASER UNIVERSITY
Fall 2008

APPROVAL

Name: Mahdad Khatirinejad Fard

Degree: Doctor of Philosophy

Title of thesis: Regular Structures of Lines in Complex Spaces

Examining Committee: Dr. Jonathan Jedwab
Chair

Dr. Petr Lisoněk
Senior Supervisor, Simon Fraser University

Dr. Luis Goddyn
Supervisory Committee, Simon Fraser University

Dr. Ladislav Stacho
Supervisory Committee, Simon Fraser University

Dr. Jason Bell
Internal Examiner, Simon Fraser University

Dr. Chris Godsil
External Examiner, University of Waterloo

Date Approved:

Abstract

We study the properties of regular structures of lines, such as equiangular sets of lines and mutually unbiased bases (MUBs) in a general setting that includes real, complex and quaternionic spaces. We formulate a common generalization of several results in real and complex spaces that also hold in the quaternionic space.

A set of lines is called equiangular if the angle between each pair is the same. A set of MUBs is a collection of orthonormal bases such that the angle between vectors from different bases is constant. Regular structures of lines have been studied in several fields such as digital communication, quantum computing, discrete mathematics and analysis.

Our new concept of a multipartite equiangular set of lines is a common generalization of equiangular lines and MUBs. We prove a bound on the size of such set of lines, which generalizes the well-known absolute upper bounds.

The existence of $d+1$ MUBs in $\mathbb{C}^d$ is only known for prime power dimensions. We study sets of $d+1$ MUBs that are the union of a standard basis and an orbit of the Weyl-Heisenberg group. As an example, we construct such MUBs in prime power dimensions. We also show connections between spherical 2-designs and other structures of lines.

Fiducial vectors have been widely used to construct large sets of equiangular lines. A complex vector is fiducial if its orbit under a Weyl-Heisenberg group is an equiangular set of d^2 lines. We give a new characterization of fiducial vectors, one that simplifies and significantly reduces the number of equations that must be solved to find a fiducial vector. We consider some possible classes of fiducial vectors and prove several nonexistence results. For example, using our new characterization we prove that the construction of fiducial vectors in small prime dimensions by Appleby (2005) essentially does not generalize.

Finally, we give some methods for constructing equiangular sets of lines in complex and quaternionic spaces. We also find numerical fiducial vectors with high precision in $\mathbb{C}^d, d \leq 21$.

To the memory of my grandma, Kobra Paswar (1914-2008)

"Once upon a time there was a sensible straight line who was hopelessly in love with a dot. 'You're the beginning and the end, the hub, the core and the quintessence,' he told her tenderly, but the frivolous dot wasn't a bit interested, for she only had eyes for a wild and unkempt squiggle who never seemed to have anything on his mind at all. All of the line's romantic dreams were in vain, until he discovered . . . angles! Now, with newfound self-expression, he can be anything he wants to be – a square, a triangle, a parallelogram .... And that's just the beginning!"

— *The Dot and the Line: A Romance in Lower Mathematics*, JUSTER NORTON, *1963*

Acknowledgments

The following figures deserve to be well-recognized. Why? Because, they are the ones behind the scene. The ones that had a share in bringing my dream to reality...

To Dr. Petr Lisoněk for being a kind, supportive and knowledgeable supervisor. I will not be able to thank you enough for bringing the thesis into its final shape and canceling various personal occasions. You are a great friend and thank you for your continual care.

Dr. Petr Lisoněk

To Dr. Luis Goddyn and Dr. Ladislav Stacho for various useful suggestions.

Dr. Luis Goddyn

Dr. Ladislav Stacho

To NSERC for generously providing me with the Canada Graduate Scholarship. I also thank MITACS, PIMS, IRMACS and the Department of Mathematics at SFU for all the support.

To Dr. Chris Godsil for traveling across the country to serve as my external examiner.

Dr. Chris Godsil

To Leyla for being a truly patient wife. It is not easy to be someone's wife whose work hours easily extends to midnight!

Leyla

To my mom and dad for teaching me how to love and how to live. It is impossible to express how proud I am to be your son.

Mom and Dad

To Mehrnoush for being a wonderful and lovely sister.

Mehrnoush

To Ksusha for not letting me give up, $\lim_{t\to 2.5^-} \mathcal{HR} = \infty$.

Ksusha

Contents

List of Tables

List of Figures

Chapter 1

Introduction

A line in a vector space is a one-dimensional subspace. Each line may be represented by a unit vector spanning that line and we will often identify a set of lines with a set of unit vectors that span these lines. The cosine of the angle between two lines is the absolute value of the inner product of the two vectors that represent the lines. A set of lines is called *equiangular* if the angle between each pair is the same. A set of *mutually unbiased bases (MUBs)* is a collection of orthonormal bases such that the angle between vectors from different bases is constant. Finding large sets of lines with few angles between the pairs is generally a difficult problem. Regular structures of lines, in particular equiangular sets of lines, have been studied (under various names) in several fields such as discrete geometry, combinatorics, harmonic analysis, frame theory, the theory of communication sequences, coding theory and quantum information theory. Unfortunately, due to the usage of different terminology and the lack of communication between these groups, many results have been rediscovered independently. In this section, we will give a brief overview of the development of regular structures of lines in the last 60 years.

1.1 Historical Background

In 1948, Haantjes [43] initiated the investigations of equiangular sets of lines in real spaces, using the elliptic geometry terminology. In particular, he proved that the 6 main diagonals of the icosahedron are equiangular and no bigger equiangular set of lines exists in $\mathbb{R}^3$ as well as in $\mathbb{R}^4$ (see Figure 1.1). His work was carried on for many years by his student, Johan Jacob Seidel (1919–2001). In 1966 van Lint and Seidel [78] made more contributions

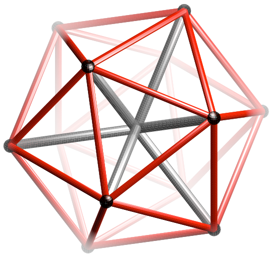

Figure 1.1: The six main diagonals of the icosahedron are equiangular.

on equiangular sets of lines in real spaces and proved that the maximum number of such lines in $\mathbb{R}^5, \mathbb{R}^6$ and $\mathbb{R}^7$ is $10, 16$ and at least 28, respectively. Later, they proved that the maximum number of such lines in $\mathbb{R}^7$ is 28. They also gave an upper bound, known as the relative bound, on the size of an equiangular set of lines with a predetermined angle. In 1970s, Seidel and others published important papers on this topic and also gave several characterizations of equiangular sets of lines in real spaces in terms of switching classes of graphs and regular two-graphs. They also constructed such sets of lines using strong and strongly regular graphs, projective and affine planes and residual Steiner triple systems (a block design obtained from a Steiner triple system by discarding all the triples that contain a fixed element). We refer the reader to "Geometry and Combinatorics, Selected Works of J. J. Seidel" [71] for a collection of papers on this topic.

One of the fundamental pieces of work on equiangular sets of lines in real spaces is the work of Lemmens and Seidel [59]. This paper is a great survey on equiangular sets of lines in real spaces. Using the point-line incidence matrix of a projective plane, they proved that, roughly speaking, there are equiangular sets of $d^{3/2}$ lines in $\mathbb{R}^d$. They also determined the maximum cardinality of a set of lines in $\mathbb{R}^d$ where the absolute value of the inner product of each pair is $1/3$. In general, the size of an equiangular set of lines in a d-dimensional real (as well as complex and quaternionic) space is $O(d^2)$ (see Theorem 2.8). In 2000, de Caen [26] gave a construction of equiangular sets of $2(d+1)^2/9$ lines in $\mathbb{R}^d$ when $d = 3 \cdot 2^{2t-1} - 1, t \in \mathbb{N}$. This is the only known construction in which the number of lines is quadratic in the dimension. As a result, this construction gives equiangular sets of $\Theta(d^2)$ lines in $\mathbb{R}^d$ for all d and solves the problem in real (as well as complex and quaternionic) spaces asymptotically. Another fundamental article is the work of Delsarte, Goethals, and Seidel [28] on spherical codes and designs. They explore the connections with spherical geometry and harmonic analysis.

The birth of equiangular sets of lines in complex spaces happened in another article of Delsarte, Goethals, and Seidel [27], where they derived bounds on the cardinality of sets of lines having a prescribed number of angles. In particular, they proved that the maximum cardinality of an equiangular set of lines in $\mathbb{C}^d$ is d^2. They also claimed that this upper bound is realized for $d = 2$ and $d = 3$ without giving any details (they refer the reader to Mitchell [61] and Coxeter [23] for more details). It is also mentioned in their paper that sets of lines with few angles that achieve a certain bound sometimes provide a combinatorial setting for interesting simple groups. In 1981, Hoggar [45] found a quaternionic 4-polytope, derived from a group generated by reflections. Using a computer calculation he showed that the vertices of the polytope give rise to an equiangular set of 64 lines in $\mathbb{C}^8$. Seventeen years later, he verified his calculations by hand in a short note [46]. Using difference sets, König [58] constructed an equiangular set of $d^2 - d + 1$ lines in $\mathbb{C}^d$ with the largest possible angle when $d - 1$ is prime. Later, Xia, Zhou, and Giannakis [84] noticed that König's construction works whenever $d - 1$ is a prime power.

After the work of Delsarte, Goethals, and Seidel [27], there seems to be no major progress on the problem of finding equiangular sets of lines in complex spaces until Zauner [85] introduced the problem in the quantum information theory setting in his PhD thesis in 1999. He conjectured that equiangular sets of d^2 lines exist for every dimension d as an orbit of a line under a group isomorphic to $\mathbb{Z}_d \times \mathbb{Z}_d$. We will precisely describe this method in Section 1.6. Zauner gave an explicit construction of such orbits for every $d \leq 5$. Since then the problem has attracted a great deal of attention among the quantum information theorists and it has been widely conjectured that for every d, equiangular sets of d^2 lines in $\mathbb{C}^d$ exist. In 2003, Renes, Blume-Kohout, Scott and Caves [66] gave some support for Zauner's conjecture by finding numerical solutions for $d \leq 45$. It may be argued however that their numerical solutions, which are floating point numbers with only 10 decimal digits, are not strong evidence to support the conjecture. They also found all $\mathbb{Z}_d \times \mathbb{Z}_d$-orbits of equiangular sets of lines in $\mathbb{C}^d$ for $d \leq 4$ and gave the number of such non-isomorphic orbits of equiangular sets of lines for $d \leq 7$ based on numerical methods. In 2005, Appleby [4] gave an explicit construction of $\mathbb{Z}_d \times \mathbb{Z}_d$-orbits of equiangular sets of lines for dimensions 7 and 19. Even though it is not obvious that the given constructions are indeed equiangular sets of lines, none of the mentioned articles [66, 4] provide a proof. We will investigate these constructions in more details in Chapter 3 and provide concise proofs.

Another interesting regular structure of lines is a set of mutually unbiased bases (MUBs), a union of orthonormal bases in which only 2 angles occur. It can be proved that there are at most $d+1$ MUBs in $\mathbb{C}^d$. A set of $d+1$ MUBs in $\mathbb{C}^d$ is called a complete set of MUBs. In 1980, Alltop [2] was the first to find complete sets of MUBs in every prime dimension and discussed their usefulness in communication sequences. A year later, Ivanovic [50] independently found complete sets of MUBs in all prime dimensions in the context of quantum applications. In 1989, Wootters and Fields [83] extended Alltop's construction to complete sets of MUBs in all prime power dimensions. Regardless of the appearance of hundreds of articles on MUBs and their applications, however, up to this date, the existence of $d+1$ MUBs in $\mathbb{C}^d$ for any non-prime power d is unknown. To name a few such articles, we refer to Klappenecker and Rötteler [54, 55], Grassl [41], Bengtsson et al. [12], Klimov et al. [57], and Aschbacher et al. [6].

Many authors have also investigated the connections between MUBs and other combinatorial objects. For example, Calderbank, Cameron, Kantor, and Seidel [17] constructed complete sets of MUBs using symplectic spreads and Kerdock codes; Bandyopadhyay, Boykin, Roychowdhury, and Vatan [8] constructed complete sets of MUBs using the eigenvectors of the Weyl-Heisenberg group; and Boykin, Sitharam, Tiep, and Wocjan [16] showed an important connection between MUBs and orthogonal decompositions of Lie algebras into Cartan subalgebras. Recently, Shparlinski and Winterhof [74] constructed approximate complete sets of MUBs in many non-prime power dimensions based on finite fields and also elliptic curves. Prior to that article, Klappenecker et al. [56] also constructed several approximate complete sets of MUBs. They relaxed the definition of MUBs in several different ways. Real MUBs may not be as interesting as the complex MUBs as there are at most 3 MUBs in most dimensions (see Boykin, Sitharam, Tarifi, and Wocjan [15]).

Spherical designs are another example of regular structure of lines. Recall that each line may be presented by a unit vector or equivalently a point on the unit sphere. Let S^{d-1} denote the unit sphere in $\mathbb{R}^d$. A spherical t-design is a finite set $\mathcal{L}$ of points on S^{d-1} such that the average value of any homogenous polynomial f of degree at most t on $\mathcal{L}$ is equal to the average value of f on the entire sphere S^{d-1}. If t is the largest integer for which $\mathcal{L}$ is a t-design, it is said that $\mathcal{L}$ approximates the sphere with strength t. An interesting example is a truncated icosahedron, the football, which approximates S^2 with strength 5 [39]. The football comprises 12 regular pentagonal faces (the black faces on the football) and 20 regular hexagonal faces (the white faces on the football). It has 60 vertices and 90 edges (see Figure 1.2). In 1981, Goethals and Seidel [39] noted that the football

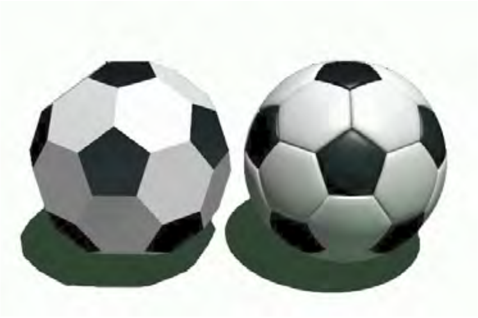

Figure 1.2: The football.

does not give the best approximation of the sphere among truncated icosahedrons. They showed that there exists another truncated icosahedron (whose faces are regular pentagons and non-regular hexagons) that approximates S^2 with strength 9. Generally, given d and t it is a difficult problem to find a spherical t-design on S^{d-1} with a small number of points. In 1984, Seymour and Zaslavsky [73] proved that given t and d there exists a number $N(d,t)$ such that for every $n \geq N(d,t)$ there exists a spherical t-design of n points on S^{d-1}.

It can be shown [81] that any spherical t-design $\mathcal{L}$ minimizes the t-energy defined by $E_t(\mathcal{L}) = \sum_{\mathbf{v},\mathbf{w}\in\mathcal{L}} |\langle \mathbf{v}, \mathbf{w}\rangle|^{2t}$ but the converse is generally not true. Recently, Cohn and Kumar [20] considered a broader class of energies. They noted that many of the previously known configurations of points on $S^{d-1} \subset \mathbb{R}^d$ that minimize a certain energy function, in fact, minimize a far broader class of energies. One of their main results is that any spherical $(2m-1)$-design in $\mathbb{R}^d$ in which only m distinct inner products occur between the pairs minimizes any potential energy

$$\sum_{\mathbf{v},\mathbf{w}\in\mathcal{L},\mathbf{v}\neq\mathbf{w}} f\left(|\mathbf{v}-\mathbf{w}|^2\right),$$

where $f : (0,4] \to [0,\infty)$ is a C^∞ mapping that is completely monotonic, i.e. $(-1)^k f^{(k)}(x) \geq 0$ for all $x \in (0,4]$ and $k \geq 0$. Note that for any two distinct points $\mathbf{v},\mathbf{w} \in S^{d-1}$, we have $0 < |\mathbf{v}-\mathbf{w}|^2 \leq (|\mathbf{v}|+|\mathbf{w}|)^2 \leq 4$. An interesting example of such configuration is the set of points (together with their antipodal points) on the unit sphere in $\mathbb{R}^{23}$ obtained from the equiangular set of $\binom{23+1}{2} = 276$ lines in $\mathbb{R}^{23}$ (see [38] for a thorough description of this set). This is a set of 552 points on the 23-dimensional unit sphere that is a spherical 5-design in which only three inner products occur: $-1, \pm 1/5$. Other intriguing examples are: the minimal vectors in the E_8 root lattice, a spherical 7-design consisting of 240 points on the unit sphere in $\mathbb{R}^8$ so that only 4 inner products occur between the pairs; and the minimal vectors in the Leech lattice, a set of 196560 points on the unit sphere in $\mathbb{R}^{24}$ that is a spherical 11-design with 6 inner products occurring between the pairs. In another recent paper, Ballinger et al. [7] report on massive computer experiments to find potential energy minimizing sets of points on the unit sphere.

A special case of spherical designs that have been widely studied are spherical 1-designs. In the frame theory, spherical 1-designs are called tight frames with a different, yet equivalent, definition. A set of vectors C in any inner product space V is a frame if there exist constants $A, B > 0$ such that $A\langle \mathbf{w}, \mathbf{w}\rangle \leq \sum_{\mathbf{v}\in C} |\langle \mathbf{v}, \mathbf{w}\rangle|^2 \leq B\langle \mathbf{w}, \mathbf{w}\rangle$ holds for all $\mathbf{w} \in V$. The set C is a tight frame if $A = B$ in the definition or equivalently $\sum_{\mathbf{v}\in C} \mathbf{v}\mathbf{v}^* = A\mathbf{I}$ (see Lemma 2.30). The vertices of the five Platonic solids and the football (Figure 1.2) are examples of tight frames in $\mathbb{R}^3$. As Benedetto and Fickus [11] mention, frames are interesting objects because they provide decompositions in applications such as signal processing where bases could be costly and tight frames are valuable to ensure fast convergence of such decompositions (see [11] for more details). Frame theory, initiated by Duffin and Schaeffer [29] in 1952, is a fundamental concept in non-harmonic Fourier series, signal processing, signal detection, image processing, data compression, sampling theory, and many other applications. One of the innovative papers in this field is the work of Daubechies, Grossmann and Meyer [25] in 1986 where they showed the role of the theory of frames in signal processing. Equiangular (tight) frames have also been considered by various authors. The relative bound is an upper bound on the cardinality of an equiangular set of lines in terms of the dimension and the common angle. In Section 2.2.2, we will see that an equiangular tight frame is equivalent to an equiangular set of lines that meets the relative bound. Recently, Karla [51] studied equiangular cyclic frames. Also, Tropp [77] and Sustik et al. [76] derived some necessary number theoretic restrictions on n and d for which an equiangular tight frame of size n in $\mathbb{R}^d$ or $\mathbb{C}^d$ exists. Zauner [85] proved the existence of an equiangular tight frame with $2d$ elements in $\mathbb{C}^d$, when d is a power of 2 or $d-1$ is a prime power. Renes [65] proved the existence of equiangular tight frames of size $2d-1$ in $\mathbb{C}^d$ and in $\mathbb{C}^{d-1}$, when d is a power of 2 or $2d-1$ is a prime power that is congruent to 3 modulo 4. For a thorough survey on frame theory, see Casazza [18].

1.2 Outline of the Thesis

In the rest of this chapter, we present the material that is used throughout this thesis. In particular, we investigate the required linear algebra over the quaternions. We refer the reader to Ebbinghaus et al. [30] and Hungerford [47] for more details.

In Chapter 2, we study the properties of equiangular sets of lines and mutually unbiased bases (MUBs) in a general setting that includes real, complex and quaternionic spaces. We formulate a common generalization of several results in real and complex spaces that also hold in the quaternionic space. In Section 2.1, we introduce the new notion of *multipartite equiangular set of lines* which is a common generalization of an equiangular set of lines and a set of mutually unbiased bases. We prove a bound (Theorem 2.3) on the size of such set of lines, which generalizes the well-known absolute upper bounds. All of these generalizations are new. In particular, to the best of our knowledge, no contribution on the quaternionic case was made prior to this work. The existence of $d+1$ MUBs in $\mathbb{C}^d$ is only known for prime power dimensions. We study sets of $d+1$ MUBs that are the union of a standard basis and an orbit of the (generalized) Weyl-Heisenberg group. We present a characterization of such sets of MUBs (Theorem 2.54 and Theorem 2.57). As an example, we construct such sets of MUBs in prime power dimensions, and classify them for $d \leq 5$. In Section 2.4, we show connections between spherical 2-designs and other structures of lines. In particular, we show how one may search for a tight equiangular set of n lines in $\mathbb{C}^d$ for every $d \leq n \leq d^2$ by minimizing a certain objective function (Theorem 2.71).

A complex vector is fiducial if its orbit under a Weyl-Heisenberg group of order d^3 represents an equiangular set of d^2 lines (see Section 1.6 for the details). Several authors (primarily physicists) have used fiducial vectors to construct large sets of equiangular lines. In Chapter 3, we thoroughly study fiducial vectors. We give a new characterization of fiducial vectors (Theorem 3.3). This result significantly reduces the number of equations that must be solved to find a fiducial vector. In the rest of Chapter 3, we consider some possible classes of fiducial vectors and use our characterization to prove several nonexistence results. For example, we prove that the construction of fiducial vectors in small prime dimensions by Appleby [4] does not generalize to other prime dimensions except for possibly a set with relative density zero in the set of primes that are congruent to 3 modulo 4 (Theorem 3.11).

Finally, we give some methods for constructing equiangular sets of lines in complex and quaternionic spaces. In particular, we show how to construct equiangular sets of lines using the well-studied conference and Hadamard matrices (Section 4.3) and how the Hopf mapping (well-known in homotopy theory) can be applied to construct equiangular sets of lines in the quaternionic space $\mathbb{H}^2$ (Section 4.4.3).

1.3 Composition Algebras

In order to work with structures of lines in a general setting that includes real, complex and quaternionic spaces, we briefly study composition algebras and present Hurwitz's classical theorem in this section.

Definition 1.1. *A vector space V over $\mathbb{R}$ equipped with a multiplication $V \times V \to V$, $(x, y) \mapsto xy$ is said to be an* algebra over $\mathbb{R}$ *or an* $\mathbb{R}$-algebra *if the two distributive laws*

$$(\alpha x + \beta y)z = \alpha(xz) + \beta(yz), \qquad z(\alpha x + \beta y) = \alpha(zx) + \beta(zy)$$

hold for all $\alpha, \beta \in \mathbb{R}$ and all $x, y, z \in V$. In particular, the relations $\alpha(xy) = (\alpha x)y = x(\alpha y)$ are always valid.

If the associative law $x(yz) = (xy)z$ holds for all $x, y, z \in V$, then the algebra is said to be *associative*; if the commutative law $xy = yx$ holds for all $x, y \in V$, then we speak of a *algebra!commutative*. Under these definitions an $\mathbb{R}$-algebra is, in general, neither associative nor commutative. An element $e \in V$ is called an *identity element* of the algebra, if $xe = ex = x$ for all $x \in V$. If such an element exists, then it is unique and is denoted by 1_V. The dimension of the $\mathbb{R}$-vector space V is called the *dimension of an algebra* and is denoted by $\dim_{\mathbb{R}} V$.

Example 1.2. Two $\mathbb{R}$-algebras are presented in this example.

(a) The $\mathbb{R}$-vector space of all real (complex) numbers is a 1- (respectively 2-) dimensional, associative and commutative $\mathbb{R}$-algebra with an identity element.

(b) For $n > 1$, the $\mathbb{R}$-vector space of all real (complex) $n \times n$ matrices is an n^2- (respectively $2n^2$-) dimensional, associative and non-commutative $\mathbb{R}$-algebra with an identity element.

Definition 1.3. *An $\mathbb{R}$-algebra $V \neq \{0\}$ with an identity element is called a* composition algebra *if it is equipped with a norm $|\,| : V \to \mathbb{R}$ satisfying $|xy| = |x|\,|y|$ for all x and y in V.*

Remark. Generally, in the definition of a composition algebra, the existence of an identity element is not assumed. Since we only work with composition algebras that have an identity element, we have assumed its existence in Definition 1.3.

An algebra V is a *division algebra* if $xy \neq 0$ for all x and y in $V \setminus \{0\}$. Since $|x| > 0$ for any $x \in V \setminus \{0\}$, it follows that a composition algebra is always a division algebra. A composition algebra is sometimes called a *normed division algebra*.

While the definition allows composition algebras to be infinite-dimensional, this, in fact, does not occur. In 1898, Hurwitz [48] proved that there are only four composition algebras. This is a classical result that may be found in various articles and books (for example see [22, page 72]).

Theorem 1.4. (Hurwitz) *The only composition algebras (up to isomorphism) are the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, the quaternions $\mathbb{H}$, and the octonions $\mathbb{O}$.*

Here, we look at these four composition algebras in more detail:

(a) **The real numbers:** The vector space of all real numbers $\mathbb{R}$ is a commutative associative composition algebra with the ordinary absolute value function as its norm.

(b) **The complex numbers:** Let $\mathbb{C} = \mathbb{R}(i)$, where $i^2 = -1$. That is, every element in $\mathbb{C}$ is of the form $a + bi$, where $a, b \in \mathbb{R}$. The *conjugate* of an element $x = a + bi \in \mathbb{C}$ is $\overline{x} = a - bi$. The mapping $|\,| : \mathbb{C} \to \mathbb{R}$ given by $|x| = (\overline{x}x)^{1/2} = \left(a^2 + b^2\right)^{1/2}$ defines a norm on $\mathbb{C}$. The real part of x is a and it is denoted by $\Re(x)$. Also, note that $\{1, i\}$ is a basis for the $\mathbb{R}$-vector space $\mathbb{C}$. The complex numbers $\mathbb{C}$ form a commutative and associative composition algebra.

(c) **The quaternions:** Let $\mathbb{H}$ be the set of elements of the form $a + bj$ or $a_1 + a_2 i + a_3 j + a_4 ij$, where $i^2 = j^2 = -1$, $ij = -ji$, $a, b \in \mathbb{C}$ and $a_1, a_2, a_3, a_4 \in \mathbb{R}$. The sum and product of two elements $a + bj$ and $a' + b'j$ is defined by $(a + a') + (b + b')j$ and $(aa' - bb') + (ab' + a'b)j$, respectively. The conjugate of an element $x = a_1 + a_2 i + a_3 j + a_4 ij \in \mathbb{H}$ is $\overline{x} = a_1 - a_2 i - a_3 j - a_4 ij$, the mapping $|\,| : \mathbb{H} \to \mathbb{R}$ given by $|x| = (\overline{x}x)^{1/2} = \left(\sum_{i=1}^{4} a_i^2\right)^{1/2}$ defines a norm for $\mathbb{H}$, the real part of x is a_1 and it is denoted by $\Re(x)$, and $\{1, i, j, ij\}$ is a basis for the $\mathbb{R}$-vector space $\mathbb{H}$. Every non-zero $x \in \mathbb{H}$ has a multiplicative inverse, namely $x^{-1} = \overline{x}/|x|^2$, such that $xx^{-1} = x^{-1}x = 1$. The quaternions $\mathbb{H}$ form a non-commutative and associative composition algebra.

(d) **The octonions:** Let $\mathbb{O}$ be the set of elements of the form $a+bk$ or $a_1+a_2j+a_3k+a_4jk$ or $b_1+b_2i+b_3j+b_4ij+b_5k+b_6ki+b_7kj+b_8k(ij)$, where $i^2=j^2=k^2=-1$, $ij=-ji$, $ik=-ki$, $kj=-jk$, $i(jk)=-(ij)k$, $j(ki)=-(jk)i$, $k(ij)=-(ki)j$, $a,b\in\mathbb{H}$, $a_1,a_2,a_3,a_4\in\mathbb{C}$, and $b_1,\dots,b_8\in\mathbb{R}$. The sum and product of two elements $a+bk$ and $a'+b'k$ is defined by $(a+a')+(b+b')k$ and $(aa'-bb')+(ab'+a'b)k$, respectively. The conjugate of an element $x=b_1+b_2i+\cdots+b_8k(ij)\in\mathbb{O}$ is $\overline{x}=b_1-b_2i-\cdots-b_8k(ij)$, the mapping $|\,|:\mathbb{O}\to\mathbb{R}$ given by $|x|=(\overline{x}x)^{1/2}=\left(\sum_{i=1}^{8}b_i^2\right)^{1/2}$ defines a norm on $\mathbb{O}$, the real part of x is b_1 and is denoted by $\Re(x)$, and $\{1,i,j,ij,k,ki,kj,k(ij)\}$ is a basis for the $\mathbb{R}$-vector space $\mathbb{O}$. The octonions $\mathbb{O}$ form an 8-dimensional non-commutative and non-associative composition algebra.

We have the following useful identities that are easy to prove (for example see [30]).

Lemma 1.5. *For any x and y in a composition algebra, we have*

$$\Re(xy)=\Re(yx),\qquad \overline{x\,y}=\overline{y}\,\overline{x},\qquad x\,\overline{x}=\overline{x}\,x=|x|^2.$$

Definition 1.6. *Throughout this thesis, $\mathbb{A}$ denotes an associative composition algebra. That is, $\mathbb{A}$ stands for $\mathbb{R},\mathbb{C}$ or $\mathbb{H}$.*

By $\dim_{\mathbb{R}}\mathbb{A}$ we mean the dimension of $\mathbb{A}$ as an $\mathbb{R}$-vector space. Notice that $\dim_{\mathbb{R}}\mathbb{R}=1$, $\dim_{\mathbb{R}}\mathbb{C}=2$, and $\dim_{\mathbb{R}}\mathbb{H}=4$.

1.4 Linear Algebra

In this section, we review the basics of the linear algebra over the reals and the complex numbers and carefully generalize them to the linear algebra over the quaternions. We were not able to find a solid reference that specifically concentrates on the linear algebra over the quaternions. Nevertheless, Hungerford [47] contains most of the results that we need. For the sake of completeness, we will also provide a proof whenever it is essential.

Notice that $\mathbb{R}^d$ and $\mathbb{C}^d$ are d-dimensional vector spaces over $\mathbb{R}$ and $\mathbb{C}$, respectively. Much of the linear algebra which works for $\mathbb{C}$ can be generalized to the quaternions $\mathbb{H}$. However, some care must be taken since $\mathbb{H}$ is not commutative. Notice that $\mathbb{H}$ has all of the properties of a field except commutativity and it is therefore a division ring. Therefore, to be precise, we should talk about $\mathbb{H}$-modules rather than $\mathbb{H}$-vector spaces.

Definition 1.7. *Let $\mathbb{A}$ be an associative composition algebra. A* (right) $\mathbb{A}$-module *is an additive abelian group M together with a mapping $M \times \mathbb{A} \to M$, $(m, q) \mapsto mq$ such that for all $q, q' \in \mathbb{A}$ and $m, m' \in M$:*

(i) $(m + m')q = mq + m'q,$ (ii) $m(q + q') = mq + mq',$

(iii) $(mq)q' = m(qq'),$ (iv) $m1_{\mathbb{A}} = m.$

Notice that $\mathbb{R}$-modules and $\mathbb{C}$-modules are just the familiar vector spaces over $\mathbb{R}$ and $\mathbb{C}$, respectively. In Hungerford [47, Chapter IV, p. 169] R-modules over a division ring R are called R-vector spaces. This is because the usual facts on independent sets and spanning sets in vector spaces are valid for modules over division rings. We follow the terminology and results given in Hungerford [47, Chapter IV], however we will use the term "$\mathbb{A}$-module" rather than "$\mathbb{A}$-vector space" to emphasize the difference.

In the rest of this thesis, it turns out to be most convenient to define $\mathbb{A}$-modules as *right* modules (i.e. applying the scalar multiplication from the right), as we already stated in Definition 1.7. From now on, "$\mathbb{A}$-module" means "right $\mathbb{A}$-module". The choice of a right scalar multiplication will become more apparent once we define linear mappings (see Definition 1.9) and also when we define the notion of inner product (see Definition 1.14).

We generally consider a vector as a column vector and use $\mathbf{v}^T$ and $\mathbf{v}^*$ to denote the transpose and conjugate transpose of a vector $\mathbf{v}$, respectively. The following proposition follows immediately from Definition 1.7.

Proposition 1.8. *For a given integer $d \geq 1$ and an associative composition algebra $\mathbb{A}$, the set of all mappings from $\{0, \ldots, d-1\}$ to $\mathbb{A}$, denoted $\mathbb{A}^d$, represented by*

$$\mathbb{A}^d = \{(x_0, \ldots, x_{d-1})^T : x_i \in \mathbb{A}\},$$

together with the standard vector addition and the action of the scalars given by

$$(x_0, \ldots, x_{d-1})^T q = (x_0 q, \ldots, x_{d-1} q)^T$$

for any vector $(x_0, \ldots, x_{d-1})^T \in \mathbb{A}^d$ and any scalar $q \in \mathbb{A}$, is an $\mathbb{A}$-module.

Let M be an $\mathbb{A}$-module. An $\mathbb{A}$-*submodule* N of M is an additive subgroup of M such that $mq \in N$ for all $m \in N$ and $q \in \mathbb{A}$. Note that N itself is an $\mathbb{A}$-module. A subset X of an $\mathbb{A}$-module M is *linearly independent* provided that for every $m_1, \ldots, m_k \in X$ and

$q_1, \ldots, q_k \in \mathbb{A}$, we have $\sum_i m_i q_i = 0$ only if $q_1 = \cdots = q_k = 0$. A subset $\{m_1, \ldots, m_k\}$ of M *spans* M if every element of M can be written as $\sum_i m_i q_i$ for some $q_1, \ldots, q_k \in \mathbb{A}$. A *basis* for M is a linearly independent set that spans M. Every $\mathbb{A}$-module has a basis and more generally every linearly independent subset of an $\mathbb{A}$-module M is contained in a basis of M [47, Theorem 2.4]. Any two bases of M have the same cardinality and therefore any $\mathbb{A}$-module with a basis of size d is isomorphic to $\mathbb{A}^d$ [47, Theorem 2.7]. The size of any basis of an $\mathbb{A}$-module M is called the *dimension* of M and is denoted by $\dim_{\mathbb{A}} M$ (in module theory, this is usually called the rank of M, but due to the potential confusion with the rank of a matrix that will be often used in this thesis, we will avoid this terminology).

Since $\mathbb{O}$ is neither commutative nor associative we will not touch the space $\mathbb{O}^d$, even though it would be an interesting subject by itself. Various properties of sets of lines in real or complex spaces that have been studied in literature are in fact true in $\mathbb{H}^d$. Therefore, wherever possible, we present the results for $\mathbb{A}^d$, where $\mathbb{A}$ is an associative composition algebra. However, the main emphasis of this thesis is on complex spaces.

We generally assume $n \geq d \geq 2$ are integers and mostly work with n vectors in $\mathbb{A}^d$. We use $\mathbb{Z}_d$ to denote the ring of integers modulo d. If the indices of the coordinates of a vector $\mathbf{z} \in \mathbb{A}^d$ are not specified, then we are indexing the coordinates by $\mathbb{Z}_d$. That is, we consider $\mathbb{A}^d$ as the set of all mappings from $\mathbb{Z}_d$ to $\mathbb{A}$. When there is no confusion, we will write (z_j) instead of $(z_j)_{j \in \mathbb{Z}_d}$ to represent $\mathbf{z} \in \mathbb{A}^d$. The standard basis for $\mathbb{A}^d$ is denoted by $\{\mathbf{e}_j : j \in \mathbb{Z}_d\}$, where $(\mathbf{e}_j)_i = 1$ if $i = j$ and $(\mathbf{e}_j)_i = 0$ otherwise. Let δ_{ij} denote the Kronecker delta, that is $\delta_{ij} = 1$ if $i = j$ and $\delta_{ij} = 0$ otherwise. The $d \times d$ identity matrix and all-ones matrix are denoted by $\mathbf{I}_d$ and $\mathbf{J}_d$, respectively. The $d_1 \times d_2$ all-ones matrix is denoted by $\mathbf{J}_{d_1,d_2}$. The all-zeroes and all-ones vector of dimension d are denoted by $\mathbf{0}_d$ and $\mathbf{1}_d$, respetively. Whenever there is no confusion, the index d may be dropped.

Definition 1.9. *Let M and $\hat{M}$ be two $\mathbb{S}$-modules, where $\mathbb{S}$ is any associative composition algebra. An* $\mathbb{S}$-homomorphism *or* $\mathbb{S}$-linear mapping *$A : M \to \hat{M}$ is a mapping that satsfies $A(x + y) = A(x) + A(y)$ and $A(xq) = A(x)q$ for all $x, y \in M$ and $q \in \mathbb{S}$.*

Remark. Any $\mathbb{S}$-linear mapping from M to $\hat{M}$ can be represented by a $\hat{d} \times d$ matrix over $\mathbb{S}$ acting via matrix multiplication on the left, where M and $\hat{M}$ are $\mathbb{S}$-modules of dimensions d and $\hat{d}$, respectively (see Hungerford [47, p. 329]).

Let $\mathbb{S} \subseteq \mathbb{A}$ be two associative composition algebras such that $\mathbb{S} = \mathbb{R}$ or $\mathbb{S} = \mathbb{A}$. By restricting the mapping $M \times \mathbb{A} \to M$ to $M \times \mathbb{S} \to M$ in Definition 1.7, any $\mathbb{A}$-module

M may be considered as an $\mathbb{S}$-module. For example, we may consider $\mathbb{A}^{d'}$ as an $\mathbb{S}$-module of dimension $d' \cdot \dim_{\mathbb{S}} \mathbb{A}$. This is because if $\mathbb{S} = \mathbb{R}$, then we may replace each of the d' coordinates of a vector in $\mathbb{A}^{d'}$ with $\dim_{\mathbb{R}} \mathbb{A}$ real coordinates.

Now, consider $\mathbb{S}^d$ and $\mathbb{A}^{d'}$ as two $\mathbb{S}$-modules of dimensions d and $\hat{d} = d' \cdot \dim_{\mathbb{S}} \mathbb{A}$, respectively. Any $d' \times d$ matrix $\mathbf{A}$ with entries in $\mathbb{A}$ defines an $\mathbb{S}$-linear mapping from $\mathbb{S}^d$ to $\mathbb{A}^{d'}$ by mapping $\mathbf{v} \in \mathbb{S}^d$ to $\mathbf{A}\mathbf{v} \in \mathbb{A}^{d'}$. Notice that $\mathbf{A}$ can be represented as a $\hat{d} \times d$ matrix with entries in $\mathbb{S}$. For any $d' \times d$ matrix $\mathbf{A}$ with entries in $\mathbb{A}$, the *kernel* or *nullspace* of $\mathbf{A}$ over $\mathbb{S}$ is $\operatorname{Ker}_{\mathbb{S}}(\mathbf{A}) = \{\mathbf{v} \in \mathbb{S}^d : \mathbf{A}\mathbf{v} = \mathbf{0}\} \subseteq \mathbb{S}^d$ and the *image* or *range* or *column space* of $\mathbf{A}$ over $\mathbb{S}$ is $\operatorname{Im}_{\mathbb{S}}(\mathbf{A}) = \{\mathbf{A}\mathbf{v} : \mathbf{v} \in \mathbb{S}^d\} \subseteq \mathbb{A}^{d'}$. See Hungerford [47, Corollary 2.14] for a proof of the following lemma.

Lemma 1.10. *For any $d' \times d$ matrix $\mathbf{A}$ with entries in $\mathbb{A}$, the sets $\operatorname{Ker}_{\mathbb{S}}(\mathbf{A})$ and $\operatorname{Im}_{\mathbb{S}}(\mathbf{A})$ are $\mathbb{S}$-submodules of $\mathbb{S}^d$ and $\mathbb{A}^{d'}$, respectively, and*

$$\dim_{\mathbb{S}} \operatorname{Ker}_{\mathbb{S}}(\mathbf{A}) + \dim_{\mathbb{S}} \operatorname{Im}_{\mathbb{S}}(\mathbf{A}) = d.$$

One may similarly define the row space of $\mathbf{A}$ and it can be shown that the dimension of the row space is equal to $\dim_{\mathbb{S}} \operatorname{Im}_{\mathbb{S}}(\mathbf{A})$, the dimension of the column space of $\mathbf{A}$ (see Hungerford [47, Chapter VII, Corollary 2.5]).

Definition 1.11. *The $\mathbb{S}$-rank of a matrix $\mathbf{A}$ with entries in $\mathbb{A}$, denoted $\operatorname{rank}_{\mathbb{S}}(\mathbf{A})$, is defined by $\dim_{\mathbb{S}} \operatorname{Im}_{\mathbb{S}}(\mathbf{A})$.*

It is a classical fact that $\operatorname{rank}_{\mathbb{R}}(\mathbf{A})$ for any matrix $\mathbf{A}$ with real entries is equal to the number of non-zero eigenvalues of $\mathbf{A}$. Recall that $\overline{x}$ denotes the conjugate of an element $x \in \mathbb{A}$. Let $\mathbf{A}^T$ denote the transpose of a matrix $\mathbf{A}$. The conjugate transpose of a matrix $\mathbf{A}$ with entries in $\mathbb{A}$ is denoted by $\mathbf{A}^*$. For any $m \times n$ matrix $\mathbf{A}$ and $n \times p$ matrix $\mathbf{B}$, by Lemma 1.5, we have $(\mathbf{AB})^* = \mathbf{B}^*\mathbf{A}^*$. We say that matrix $\mathbf{A}$ with entries in $\mathbb{A}$ is *Hermitian* if $\mathbf{A}^* = \mathbf{A}$.

Theorem 1.12. *The set of all $d \times d$ Hermitian matrices with entries in $\mathbb{A}$ is an $\mathbb{R}$-vector space of dimension $d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$.*

Proof. For every $d \times d$ Hermitian matrix, each entry on the diagonal must be real (d free parameters) and each of the $\binom{d}{2}$ upper diagonal entries determines the corresponding lower diagonal entry ($\binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$ free parameters). □

Definition 1.13. *We will denote the $\mathbb{R}$-vector space of $d \times d$ Hermitian matrices with entries in $\mathbb{A}$ by $\mathcal{HM}_d(\mathbb{A})$.*

Definition 1.14. *The inner product of two vectors $\mathbf{v}, \mathbf{w} \in \mathbb{A}^d$ is defined by*

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

The inner product has the following properties:

$$\overline{\langle \mathbf{v}, \mathbf{w} \rangle} = \langle \mathbf{w}, \mathbf{v} \rangle, \qquad \langle \mathbf{v}q, \mathbf{w} \rangle = \overline{q} \langle \mathbf{v}, \mathbf{w} \rangle, \qquad \langle \mathbf{v}, \mathbf{w}q \rangle = \langle \mathbf{v}, \mathbf{w} \rangle q,$$

where $\mathbf{v}, \mathbf{w} \in \mathbb{A}^d$ and $q \in \mathbb{A}$. Also $\langle \mathbf{v}, \mathbf{v} \rangle$ is a positive real number for any $\mathbf{v} \neq \mathbf{0}$. The *norm* of a vector $\mathbf{v} \in \mathbb{A}^d$ is defined by $|\mathbf{v}| = \langle \mathbf{v}, \mathbf{v} \rangle^{1/2}$. For any $q \in \mathbb{A}$ and $\mathbf{v} \in \mathbb{A}^d$, we have $|\mathbf{v}q| = |\mathbf{v}||q|$. This is because $|\mathbf{v}q| = \langle \mathbf{v}q, \mathbf{v}q \rangle^{1/2} = (\overline{q} \langle \mathbf{v}, \mathbf{v} \rangle q)^{1/2} = (\langle \mathbf{v}, \mathbf{v} \rangle \overline{q} q)^{1/2} = |\mathbf{v}||q|$. Thus every non-zero vector $\mathbf{v} \in \mathbb{A}^d$ can be normalized to a vector of norm 1 by multiplying by $1/|\mathbf{v}| \in \mathbb{A}$. A *unit vector* is a vector with norm 1.

A set of vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ in $\mathbb{A}^d$ is called *orthonormal* if $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \delta_{ij}$ for all i and j. It is easy to see that any orthonormal set is linearly independent. Thus, an orthonormal set of size d is a basis for $\mathbb{A}^d$ and is called an *orthonormal basis*. The familiar Gram-Schmidt process for $\mathbb{R}^d$ and $\mathbb{C}^d$, also holds in $\mathbb{H}^d$ [32, Theorem 4.3]. For the sake of completeness, we give a proof.

Proposition 1.15. *Suppose $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is an orthonormal set in $\mathbb{A}^d$. Then there exist $\mathbf{v}_{k+1}, \ldots, \mathbf{v}_d \in \mathbb{A}^d$ such that $\{\mathbf{v}_1, \ldots, \mathbf{v}_d\}$ is an orthonormal basis for $\mathbb{A}^d$.*

Proof. We prove it by induction on ℓ, where $k \leq \ell \leq d$. Suppose $B = \{\mathbf{v}_1, \ldots, \mathbf{v}_\ell\}$ is an orthonormal set in $\mathbb{A}^d$. If B spans $\mathbb{A}^d$, then $\ell = d$ and we are done. Otherwise, choose a $\mathbf{w}$ that is not in the span of B. Define the unit vector $\mathbf{v}_{\ell+1} = \hat{\mathbf{v}}_{\ell+1} |\hat{\mathbf{v}}_{\ell+1}|^{-1}$, where

$$\hat{\mathbf{v}}_{\ell+1} = \mathbf{w} - \sum_{i=1}^{\ell} \mathbf{v}_i \langle \mathbf{v}_i, \mathbf{w} \rangle \neq \mathbf{0}.$$

For $1 \leq j \leq \ell$, we have $\langle \mathbf{v}_j, \mathbf{v}_{\ell+1} \rangle = 0$. This is because $\langle \mathbf{v}_j, \mathbf{v}_{\ell+1} \rangle = \langle \mathbf{v}_j, \hat{\mathbf{v}}_{\ell+1} \rangle |\hat{\mathbf{v}}_{\ell+1}|^{-1}$ and

$$\langle \mathbf{v}_j, \hat{\mathbf{v}}_{\ell+1} \rangle = \langle \mathbf{v}_j, \mathbf{w} \rangle - \langle \mathbf{v}_j, \sum_{i=1}^{\ell} \mathbf{v}_i \langle \mathbf{v}_i, \mathbf{w} \rangle \rangle = \langle \mathbf{v}_j, \mathbf{w} \rangle - \sum_{i=1}^{\ell} \langle \mathbf{v}_j, \mathbf{v}_i \rangle \langle \mathbf{v}_i, \mathbf{w} \rangle = 0.$$

□

Definition 1.16. *A $d \times d$ matrix $\mathbf{U}$ with entries in $\mathbb{A}$ is* unitary *if $\mathbf{U}\mathbf{U}^* = \mathbf{U}^*\mathbf{U} = \mathbf{I}_d$.*

Since $\mathbf{AB} = \mathbf{I}_d$ implies $\mathbf{BA} = \mathbf{I}_d$ (see [31, Theorem 2.24] or [86, Proposition 4.1]), either one of the equations $\mathbf{U}\mathbf{U}^* = \mathbf{I}_d$ or $\mathbf{U}^*\mathbf{U} = \mathbf{I}_d$ suffices for $\mathbf{U}$ to be unitary. Also, one may easily prove that $\mathbf{U}$ is unitary if and only if it preserves the inner product, that is $\langle \mathbf{Uv}, \mathbf{Uw} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle$ for all $\mathbf{v}, \mathbf{w} \in \mathbb{A}^d$ (one direction is easy and to prove the other direction note that $\langle \mathbf{U}\mathbf{e}_i, \mathbf{U}\mathbf{e}_j \rangle = \langle \mathbf{e}_i, \mathbf{e}_j \rangle = \delta_{ij}$). Note that the rows of $\mathbf{U}$ form an orthonormal basis.

A matrix $\mathbf{A}$ is *positive semi-definite* if $\mathbf{A}$ is Hermitian and $\langle \mathbf{v}, \mathbf{Av} \rangle \geq 0$ for all $\mathbf{v} \in \mathbb{A}^d$. Note that $\langle \mathbf{v}, \mathbf{Av} \rangle = \mathbf{v}^*\mathbf{Av} = \mathbf{v}^*\mathbf{A}^*\mathbf{v} = \langle \mathbf{Av}, \mathbf{v} \rangle = \overline{\langle \mathbf{v}, \mathbf{Av} \rangle}$ for any Hermitian matrix $\mathbf{A}$ and $\mathbf{v} \in \mathbb{A}^d$. Therefore $\langle \mathbf{v}, \mathbf{Av} \rangle \in \mathbb{R}$.

Lemma 1.17. *Let $\mathbf{A}$ be a $d \times d$ matrix with entries in $\mathbb{A}$ such that $\langle \mathbf{v}, \mathbf{Av} \rangle = 0$ for all $\mathbf{v} \in \mathbb{A}^d$. If $\mathbb{A} = \mathbb{R}$, then $\mathbf{A}^T = -\mathbf{A}$. If $\mathbb{A} \neq \mathbb{R}$, then $\mathbf{A} = \mathbf{0}$.*

Proof. For every $1 \leq k \leq l \leq d$, write the equation $\langle \mathbf{v}, \mathbf{Av} \rangle = \mathbf{v}^*\mathbf{Av} = 0$ for $\mathbf{v} = \mathbf{e}_k + \mathbf{e}_l$. Since $\mathbf{e}_k{}^*\mathbf{A}\mathbf{e}_k = \mathbf{e}_l{}^*\mathbf{A}\mathbf{e}_l = 0$, it follows that $\mathbf{A}_{kl} = \mathbf{e}_k{}^*\mathbf{A}\mathbf{e}_l = -\mathbf{e}_l{}^*\mathbf{A}\mathbf{e}_k = -\mathbf{A}_{lk}$. That is $\mathbf{A}^T = -\mathbf{A}$. If $\mathbb{A} \neq \mathbb{R}$, write the equation $\langle \mathbf{v}, \mathbf{Av} \rangle = 0$ for $\mathbf{v} = \mathbf{e}_k + \mathbf{e}_l i$. Again, since $\mathbf{e}_k{}^*\mathbf{A}\mathbf{e}_k = (\mathbf{e}_l i)^*\mathbf{A}(\mathbf{e}_l i) = 0$, we get $\mathbf{A}_{kl} i = \mathbf{e}_k{}^*\mathbf{A}(\mathbf{e}_l i) = -(\mathbf{e}_l i)^*\mathbf{A}\mathbf{e}_k = i\mathbf{A}_{lk} = -i\mathbf{A}_{kl}$. Hence, if $\mathbf{A}_{kl} = a_1 + a_2 i + a_3 j + a_4 ij$ with $a_1, a_2, a_3, a_4 \in \mathbb{R}$, then $a_1 = a_2 = 0$. Similarly, by writing the equation $\langle \mathbf{v}, \mathbf{Av} \rangle = 0$ for $\mathbf{v} = \mathbf{e}_k + \mathbf{e}_l j$ and $\mathbf{v} = \mathbf{e}_k + \mathbf{e}_l ij$, respectively, we get $a_1 = a_3 = 0$ and $a_1 = a_4 = 0$. Thus $\mathbf{A}_{kl} = 0$. □

Since $\mathbf{A}^T = -\mathbf{A}$ and $\mathbf{A}^T = \mathbf{A}$ imply $\mathbf{A} = \mathbf{0}$, we immediately get the following.

Corollary 1.18. *Let $\mathbf{A}$ be a $d \times d$ Hermitian matrix with entries in $\mathbb{A}$ such that $\langle \mathbf{v}, \mathbf{Av} \rangle = 0$ for all $\mathbf{v} \in \mathbb{A}^d$. Then $\mathbf{A} = \mathbf{0}$.*

The *trace* of a square matrix $\mathbf{A}$ is the sum of the entries on its diagonal and is denoted by $\mathrm{Tr}\,(\mathbf{A})$. The *Kronecker product* or *tensor product* of an $m \times n$ matrix $\mathbf{A} = (a_{ij})$ and a $p \times q$ matrix $\mathbf{B}$ is the $mp \times nq$ matrix defined by

$$\mathbf{A} \otimes \mathbf{B} = \begin{pmatrix} a_{11}\mathbf{B} & \cdots & a_{1n}\mathbf{B} \\ \vdots & \ddots & \vdots \\ a_{m1}\mathbf{B} & \cdots & a_{mn}\mathbf{B} \end{pmatrix}.$$

We write $\mathbf{A}^{\otimes t}$ to denote $\overbrace{\mathbf{A} \otimes \cdots \otimes \mathbf{A}}^{t}$. For any $\mathbf{v}_1, \mathbf{v}_2, \mathbf{w}_1, \mathbf{w}_2 \in \mathbb{C}^d$, we have

$$\langle \mathbf{v}_1 \otimes \mathbf{v}_2, \mathbf{w}_1 \otimes \mathbf{w}_2 \rangle = \sum_{i,j} \overline{(\mathbf{v}_1)_i (\mathbf{v}_2)_j} (\mathbf{w}_1)_i (\mathbf{w}_2)_j = \langle \mathbf{v}_1, \mathbf{w}_1 \rangle \langle \mathbf{v}_2, \mathbf{w}_2 \rangle. \tag{1.4.1}$$

Therefore, for any $\mathbf{v}, \mathbf{w} \in \mathbb{C}^d$, we have

$$\langle \mathbf{v}^{\otimes t}, \mathbf{w}^{\otimes t} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle^t. \tag{1.4.2}$$

Note that the above identity is not true in $\mathbb{H}^d$. The *Hadamard product* or *Schur product* of any two $m \times n$ matrices $\mathbf{A} = (a_{ij})$ and $\mathbf{B} = (b_{ij})$ is the matrix

$$\mathbf{A} \circ \mathbf{B} = (a_{ij} b_{ij}).$$

1.5 Lines

Lines are the main objects of this thesis. In this section, we study two important matrices, the projection matrix and the Gram matrix, that are associated to a line and a set of lines, respectively. We also present several lemmas that will be mostly used in Chapter 2. After we introduce the concept of equiangular set of lines in Section 2.2, we will see further properties of the projection and Gram matrices in Section 2.2.4.

Let $\mathbb{A}$ denote an associative composition algebra. The span of a vector $\mathbf{v} \in \mathbb{A}^d \setminus \{\mathbf{0}\}$ is the set $[\mathbf{v}] = \{\mathbf{v}q : q \in \mathbb{A}\}$. This set is a submodule of $\mathbb{A}^d$ of dimension 1. The projective space $\mathbb{AP}^{d-1}$ is the set $\{[\mathbf{v}] : \mathbf{v} \in \mathbb{A}^d, \mathbf{v} \neq \mathbf{0}\}$.

Definition 1.19. *A* line *in $\mathbb{A}^d$ is an element in the projective space $\mathbb{AP}^{d-1}$, the set of one-dimensional submodules of $\mathbb{A}^d$.*

Each element in $\mathbb{AP}^{d-1}$ can be represented by a vector $\mathbf{u}$ in $\mathbb{A}^d$ with norm 1. Recall that such a vector is called a unit vector. Note that such a representation is not unique since any unit vector $\mathbf{u}\lambda$ with $|\lambda| = 1\,(\lambda \in \mathbb{A})$ represents the same line. In this thesis, we only work with the unit vectors in $\mathbb{A}^d$ to represent a line, and we mostly work with lines which lie in a complex space $\mathbb{C}^d$, unless stated otherwise. The cosine of the angle between the lines spanned by unit vectors $\mathbf{v}, \mathbf{w} \in \mathbb{A}^d$ is defined as $|\langle \mathbf{v}, \mathbf{w} \rangle|$, the absolute value of their inner product.

Definition 1.20. *For a non-zero unit vector $\mathbf{v} \in \mathbb{A}^d$, the* projection *onto the line spanned by $\mathbf{v}$ is a linear mapping denoted by $\mathbf{P_v}$ and given by the matrix $\mathbf{P_v} = \mathbf{v}\mathbf{v}^*$.*

Note that the above definition is well-defined. This is because, by Lemma 1.5, we have $\mathbf{P}_{\mathbf{v}\lambda} = (\mathbf{v}\lambda)(\mathbf{v}\lambda)^* = \mathbf{v}|\lambda|^2\mathbf{v}^* = \mathbf{P_v}$ for any $\lambda \in \mathbb{A}$ with $|\lambda| = 1$. Thus, the projection onto a line is independent of the choice of the unit vector spanning that line. In the following lemma, we show that the projection matrix of a non-zero unit vector is a Hermitian matrix with rank 1 and trace 1.

Lemma 1.21. *For any non-zero unit vector* $\mathbf{v} \in \mathbb{A}^d$*, we have*

$$\text{(i)}\, \mathbf{P}_{\mathbf{v}}^2 = \mathbf{P}_{\mathbf{v}}, \qquad \text{(ii)}\, \mathbf{P}_{\mathbf{v}}^* = \mathbf{P}_{\mathbf{v}}, \qquad \text{(iii)}\, \mathrm{rank}_{\mathbb{A}}(\mathbf{P}_{\mathbf{v}}) = 1, \qquad \text{(iv)}\, \mathrm{Tr}\,(\mathbf{P}_{\mathbf{v}}) = 1.$$

Proof. The first two properties are easy to see. To prove (iii), notice that $\mathbf{P}_{\mathbf{v}}\mathbf{w} = \mathbf{0}$ if and only if $\mathbf{v}^*\mathbf{w} = \langle \mathbf{v}, \mathbf{w}\rangle = 0$. To see the forward direction, note that $\mathbf{P}_{\mathbf{v}}\mathbf{w} = \mathbf{0}$ implies $|\mathbf{v}^*\mathbf{w}|^2 = \mathbf{w}^*\mathbf{v}\mathbf{v}^*\mathbf{w} = \mathbf{w}^*\mathbf{P}_{\mathbf{v}}\mathbf{w} = 0$ and therefore $\mathbf{v}^*\mathbf{w} = 0$. The other direction is trivial. Now, since $\dim_{\mathbb{A}}\{\mathbf{w} \in \mathbb{A}^d : \langle \mathbf{v}, \mathbf{w}\rangle = 0\} = d - 1$, using Lemma 1.10, we get $\mathrm{rank}_{\mathbb{A}}(\mathbf{P}_{\mathbf{v}}) = 1$. Finally, we have $\mathrm{Tr}\,(\mathbf{P}_{\mathbf{v}}) = \sum_{k=1}^d (\mathbf{v}\mathbf{v}^*)_{kk} = \sum_{k=1}^d \mathbf{v}_k\overline{\mathbf{v}_k} = \sum_{k=1}^d \overline{\mathbf{v}_k}\mathbf{v}_k = \langle \mathbf{v}, \mathbf{v}\rangle = 1$. □

Lemma 1.22. *Let* $\mathbf{V}$ *be a* $d \times n$ *matrix with entries in* $\mathbb{A}$*. Then*

$$\sum_{i=1}^n \mathbf{P}_{\mathbf{v}_i} = \mathbf{V}\mathbf{V}^*,$$

where $\mathbf{v}_i$ *is the* i*-th column of* $\mathbf{V}$*.*

Proof. We may write $\mathbf{V} = \sum_i \mathbf{v}_i {\mathbf{e}_i}^*$, where $\{\mathbf{e}_1, \ldots \mathbf{e}_n\}$ is the standard basis for $\mathbb{A}^n$. Since ${\mathbf{e}_i}^*\mathbf{e}_j = \delta_{ij}$, we have $\mathbf{V}\mathbf{V}^* = \sum_{i,j} \mathbf{v}_i{\mathbf{e}_i}^*\mathbf{e}_j{\mathbf{v}_j}^* = \sum_i \mathbf{v}_i{\mathbf{v}_i}^* = \sum_i \mathbf{P}_{\mathbf{v}_i}$. □

The following lemma is crucial in proving the absolute and relative upper bound on the size of an equiangular set of lines (Theorem 2.3 and Theorem 2.13).

Lemma 1.23. *For all* $\mathbf{v}, \mathbf{w} \in \mathbb{A}^d$*, we have* $\Re(\mathrm{Tr}\,(\mathbf{P}_{\mathbf{v}}\mathbf{P}_{\mathbf{w}})) = |\langle \mathbf{v}, \mathbf{w}\rangle|^2$.

Proof. We have

$$\mathrm{Tr}\,(\mathbf{P}_{\mathbf{v}}\mathbf{P}_{\mathbf{w}}) = \sum_{k=1}^d (\mathbf{v}\mathbf{v}^*\mathbf{w}\mathbf{w}^*)_{kk} = \sum_{k=1}^d (\mathbf{v}\langle \mathbf{v}, \mathbf{w}\rangle\mathbf{w}^*)_{kk} = \sum_{k=1}^d \mathbf{v}_k\langle \mathbf{v}, \mathbf{w}\rangle\overline{\mathbf{w}_k}.$$

Since $\Re(ab) = \Re(ba)$ for any $a, b \in \mathbb{A}$, we get

$$\begin{aligned}
\Re\left(\sum_{k=1}^d \mathbf{v}_k\langle \mathbf{v}, \mathbf{w}\rangle\overline{\mathbf{w}_k}\right) &= \sum_{k=1}^d \Re(\mathbf{v}_k\langle \mathbf{v}, \mathbf{w}\rangle\overline{\mathbf{w}_k}) = \sum_{k=1}^d \Re\left(\langle \mathbf{v}, \mathbf{w}\rangle\overline{\mathbf{w}_k}\mathbf{v}_k\right) \\
&= \Re\left(\sum_{k=1}^d \langle \mathbf{v}, \mathbf{w}\rangle\overline{\mathbf{w}_k}\mathbf{v}_k\right) \\
&= \Re(\langle \mathbf{v}, \mathbf{w}\rangle\langle \mathbf{w}, \mathbf{v}\rangle) = \Re\left(|\langle \mathbf{v}, \mathbf{w}\rangle|^2\right) = |\langle \mathbf{v}, \mathbf{w}\rangle|^2.
\end{aligned}$$

□

Remark. If $\mathbf{v}, \mathbf{w} \in \mathbb{R}^d$ or $\mathbf{v}, \mathbf{w} \in \mathbb{C}^d$, then we simply have $\operatorname{Tr}(\mathbf{P}_{\mathbf{v}}\mathbf{P}_{\mathbf{w}}) = |\langle \mathbf{v}, \mathbf{w} \rangle|^2$.

Analogous to the the previous lemma, we have the following.

Lemma 1.24. *Given $n \times n$ matrices $\mathbf{A}$ and $\mathbf{B}$ with entries in $\mathbb{A}$, we have $\Re(\operatorname{Tr}(\mathbf{AB})) = \Re(\operatorname{Tr}(\mathbf{BA}))$.*

Proof. We have

$$\Re(\operatorname{Tr}(\mathbf{AB})) = \Re\Big(\sum_{i=1}^{n}\sum_{j=1}^{n} \mathbf{A}_{i,j}\mathbf{B}_{j,i}\Big) = \sum_{i=1}^{n}\sum_{j=1}^{n} \Re(\mathbf{A}_{i,j}\mathbf{B}_{j,i}),$$

and

$$\Re(\operatorname{Tr}(\mathbf{BA})) = \Re\Big(\sum_{j=1}^{n}\sum_{i=1}^{n} \mathbf{B}_{j,i}\mathbf{A}_{i,j}\Big) = \sum_{j=1}^{n}\sum_{i=1}^{n} \Re(\mathbf{B}_{j,i}\mathbf{A}_{i,j}),$$

Since $\Re(ab) = \Re(ba)$ for any $a, b \in \mathbb{A}$, we get $\Re(\operatorname{Tr}(\mathbf{AB})) = \Re(\operatorname{Tr}(\mathbf{BA}))$. □

Here, we present another lemma that will be useful in Chapter 2.

Lemma 1.25. *Suppose $\mathbf{G}$ is an $n \times n$ matrix with entries in $\mathbb{A}$ such that $\mathbf{G}^2 = (n/d)\mathbf{G}$ and $\Re(\operatorname{Tr}(\mathbf{G})) = n$. Then $\operatorname{rank}_{\mathbb{A}}(\mathbf{G}) = d$.*

Proof. Let $\operatorname{rank}_{\mathbb{A}}(\mathbf{G}) = k$. Hence $\operatorname{Im}_{\mathbb{A}}(\mathbf{G})$ is isomorphic to $\mathbb{A}^k$. By Proposition 1.15, assume $\{\mathbf{v}_1, \ldots, \mathbf{v}_k\}$ is an orthonormal basis for $\operatorname{Im}_{\mathbb{A}}(\mathbf{G})$. Let $\mathbf{U}$ be the matrix whose columns are $\mathbf{v}_1, \ldots, \mathbf{v}_k$. Since $(\mathbf{G} - (n/d)\mathbf{I}_n)\mathbf{G} = \mathbf{0}$, we have $\operatorname{Im}_{\mathbb{A}}(\mathbf{G}) = \operatorname{Ker}_{\mathbb{A}}(\mathbf{G} - (n/d)\mathbf{I}_n)$. Hence $\mathbf{G}\mathbf{v}_i = (n/d)\mathbf{v}_i$ for $1 \le i \le k$, that is $\mathbf{GU} = (n/d)\mathbf{U}$. It follows that

$$\mathbf{U}^*\mathbf{G}\mathbf{U} = \frac{n}{d}\mathbf{U}^*\mathbf{U} = \frac{n}{d}\mathbf{I}_k.$$

By taking the real part of the trace of both sides and using Lemma 1.24, we get

$$n = \Re(\operatorname{Tr}(\mathbf{G})) = \Re(\operatorname{Tr}(\mathbf{U}\mathbf{U}^*\mathbf{G})) = \Re(\operatorname{Tr}(\mathbf{U}^*\mathbf{G}\mathbf{U})) = \Re\left(\operatorname{Tr}\left(\frac{n}{d}\mathbf{I}_k\right)\right) = \frac{n}{d} \cdot k.$$

Hence $d = k$. □

A Gram matrix of a set of vectors in a vector space equipped with an inner product is a very useful object. We will further discuss the properties of this matrix in Section 2.2.4. However, since we need its basic properties in the proof of Theorem 2.3, we briefly study its properties here.

Definition 1.26. *A Gram matrix of a set of vectors $\{\mathbf{v}_1, \dots, \mathbf{v}_n\}$ in $\mathbb{A}^d$ is defined by*

$$\mathbf{G} = (\langle \mathbf{v}_i, \mathbf{v}_j \rangle)_{1 \le i,j \le n}.$$

Since we work with column vectors, we may write

$$\mathbf{G} = \mathbf{V}^* \mathbf{V},$$

where $\mathbf{V}$ is the $d \times n$ matrix with the n vectors as its columns.

It follows that $\mathbf{G}^* = \mathbf{G}$ and $\langle \mathbf{z}, \mathbf{G}\mathbf{z} \rangle = \langle \mathbf{z}, \mathbf{V}^*\mathbf{V}\mathbf{z} \rangle = \langle \mathbf{V}\mathbf{z}, \mathbf{V}\mathbf{z} \rangle \ge 0$ for all $\mathbf{z} \in \mathbb{A}^n$. Thus $\mathbf{G}$ is a positive semi-definite matrix. The converse is known to be true when $\mathbb{A} = \mathbb{R}$ or $\mathbb{C}$. That is, if $\mathbf{A}$ is a positive semi-definite matrix with entries in $\mathbb{C}$ then there is a matrix $\mathbf{B}$ such that $\mathbf{A} = \mathbf{B}^*\mathbf{B}$ (for example see Godsil and Royle [37, Lemma 8.6.1]). The next theorem shows that for a general associative composition algebra $\mathbb{A}$ the converse is almost true.

Theorem 1.27. *Let $\mathbf{A}$ be a positive semi-definite matrix with entries in $\mathbb{A}$. Then there is a matrix $\mathbf{B}$ such that $\mathbf{A} = \mathbf{B}^2$. Furthermore, if $\mathbb{A} \in \{\mathbb{R}, \mathbb{C}\}$ or if $\mathbf{A}^2 = \alpha\mathbf{A}$ for some $\alpha \in \mathbb{R}$, then we may assume $\mathbf{B}$ is Hermitian.*

Proof. By the definition of a positive semi-definite matrix, $\mathbf{A}$ is Hermitian. Thus, there is a unitary matrix $\mathbf{U}$ such that $\mathbf{U}^*\mathbf{A}\mathbf{U} = \mathbf{D}$, where $\mathbf{D}$ is a diagonal matrix such that each entry of $\mathbf{D}$ is a complex number $a + bi$ with $a, b \ge 0$ (see [32, Theorem 3.3] for a proof). Hence there is a diagonal matrix $\mathbf{C}$ such that $\mathbf{C}^2 = \mathbf{D}$. Therefore $\mathbf{B} = \mathbf{U}\mathbf{C}\mathbf{U}^*$ has the desired property. If $\mathbb{A} = \mathbb{R}$ or $\mathbb{C}$, then it is well-known that the diagonal entries of $\mathbf{D}$ are real and therefore $\mathbf{C}^* = \mathbf{C}$. If $\mathbf{A}^2 = \alpha\mathbf{A}$, then $\mathbf{D}^2 - \alpha\mathbf{D} = \mathbf{U}^*(\mathbf{A}^2 - \alpha\mathbf{A})\mathbf{U} = \mathbf{0}$. Hence, every diagonal entry of $\mathbf{D}$ is either equal to 0 or α and therefore is real. Thus $\mathbf{C}^* = \mathbf{C}$ in this case as well. □

Lemma 1.28. *For any matrix $\mathbf{V}$ with entries in $\mathbb{A}$, we have* $\operatorname{rank}_{\mathbb{R}}(\mathbf{V}^*\mathbf{V}) = \operatorname{rank}_{\mathbb{R}}(\mathbf{V})$. *That is, the dimension of an $\mathbb{R}$-module is equal to the $\mathbb{R}$-rank of the Gram matrix of any set of vectors spanning that module.*

Proof. If $\mathbf{V}^*\mathbf{V}\mathbf{z} = \mathbf{0}$ then $\mathbf{z}^*\mathbf{V}^*\mathbf{V}\mathbf{z} = 0$, which can be written as $\langle \mathbf{V}\mathbf{z}, \mathbf{V}\mathbf{z} \rangle = 0$. This implies $\mathbf{V}\mathbf{z} = \mathbf{0}$. On the other hand, $\mathbf{V}\mathbf{z} = \mathbf{0}$ implies $\mathbf{V}^*\mathbf{V}\mathbf{z} = \mathbf{0}$. Hence $\operatorname{Ker}_{\mathbb{R}}(\mathbf{V}^*\mathbf{V}) = \operatorname{Ker}_{\mathbb{R}}(\mathbf{V})$ and the result follows from Lemma 1.10 and Definition 1.11. □

Corollary 1.29. *Let $\mathcal{M} = \{\mathbf{A}_1, \ldots, \mathbf{A}_n\}$ be a finite subset of the $\mathbb{R}$-vector space $\mathcal{HM}_d(\mathbb{A})$. Also, let $\mathbf{G}$ be a matrix such that $\mathbf{G}_{ij} = \sum_{kl} \overline{(\mathbf{A}_i)_{kl}}(\mathbf{A}_j)_{kl} = \mathrm{Tr}\left(\mathbf{A}_i{}^*\mathbf{A}_j\right)$. Then the dimension of the $\mathbb{R}$-subspace spanned by $\mathcal{M}$ is equal to* $\mathrm{rank}_{\mathbb{R}}(\mathbf{G})$.

Proof. Consider each $\mathbf{A}_i$ as a d^2-dimensional column vector and let $\mathbf{V}$ be the $d^2 \times n$ matrix whose i-th column is $\mathbf{A}_i$. Notice that $\mathbf{V}^*\mathbf{V} = \mathbf{G}$. By Lemma 1.28, we have $\dim_{\mathbb{R}}(\mathrm{span}(\mathcal{M})) = \mathrm{rank}_{\mathbb{R}}(\mathbf{V}) = \mathrm{rank}_{\mathbb{R}}(\mathbf{V}^*\mathbf{V}) = \mathrm{rank}_{\mathbb{R}}(\mathbf{G})$. □

One may also define a Gram matrix of a set of lines by considering the vectors representing the lines. A set $\mathcal{L}$ of n lines in $\mathbb{A}^d$ is sometimes presented by a $d \times n$ matrix $\mathbf{V}$ whose columns are n unit vectors in $\mathbb{A}^d$ representing $\mathcal{L}$. Notice that if $\mathcal{L}$ is a set of lines in $\mathbb{A}^d$, then its Gram matrix is not unique, as one may choose $\mathbf{u}\lambda$ with $|\lambda| = 1$ to represent the line spanned by $\mathbf{u} \in \mathbb{A}^d$. Also, recall that a unitary transformation is a linear mapping that preserves the inner product of two vectors. These facts motivate the following definition.

Definition 1.30. *We say that two sets of lines $\mathcal{L}$ and $\mathcal{L}'$ in $\mathbb{A}^d$ are* equivalent *if there exists a permutation matrix $\mathbf{P}$ and a diagonal unitary matrix $\mathbf{D}$ such that*

$$\mathbf{G}' = \mathbf{D}^{-1}\mathbf{P}^{-1}\mathbf{G}\mathbf{P}\mathbf{D}$$

where $\mathbf{G}$ and $\mathbf{G}'$ are Gram matrices of $\mathcal{L}$ and $\mathcal{L}'$, respectively.

Example 1.31. Let $\mathcal{L} = \{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$ be a set of lines in $\mathbb{A}^d$ with a Gram matrix $\mathbf{G}$. Let σ be any permutation of $\{1, \ldots, n\}$. Also, let $\{\lambda_1, \ldots, \lambda_n\} \subset \mathbb{A}$ be such that $|\lambda_i| = 1$ for all i. Then a Gram matrix of $\mathcal{L}' = \{[\mathbf{v}_{\sigma(1)}\lambda_1], \ldots, [\mathbf{v}_{\sigma(n)}\lambda_n]\}$ is given by $\mathbf{D}^{-1}\mathbf{P}^{-1}\mathbf{G}\mathbf{P}\mathbf{D}$ where $\mathbf{P}$ represents the permutation σ and $\mathbf{D}$ is the diagonal matrix with $\mathbf{D}_{ii} = \lambda_i$. This is because $\lambda_i^{-1}\langle \mathbf{v}_{\sigma(i)}, \mathbf{v}_{\sigma(j)}\rangle\lambda_j = \langle \mathbf{v}_{\sigma(i)}\lambda_i, \mathbf{v}_{\sigma(j)}\lambda_j\rangle$. Hence $\mathcal{L}'$ and $\mathcal{L}$ are equivalent sets of lines.

Example 1.32. Let $\mathcal{L} = \{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$ be a set of lines in $\mathbb{A}^d$ and let $\mathbf{U}$ be any $d \times d$ unitary matrix. Then $\mathcal{L}' = \{[\mathbf{U}\mathbf{v}_1], \ldots, [\mathbf{U}\mathbf{v}_n]\}$ and $\mathcal{L}$ have equal Gram matrices and therefore are equivalent sets of lines.

1.6 The Weyl-Heisenberg Group

Here, we give the definition of an important group that is used throughout the thesis and state its properties.

Let ω denote a primitive d-th root of unity in $\mathbb{C}$. The *Pauli matrices* for $\mathbb{Z}_d$ are defined by their action on the standard basis $\{\mathbf{e}_j : j \in \mathbb{Z}_d\}$ of $\mathbb{C}^d$ as follows:

$$\begin{aligned} \mathbf{X}: &\quad \mathbf{e}_j \mapsto \mathbf{e}_{j+1}, \\ \mathbf{Y}: &\quad \mathbf{e}_j \mapsto \omega^j \mathbf{e}_j. \end{aligned}$$

Since $\mathbf{X}^d = \mathbf{Y}^d = \mathbf{I}_d$, we may regard the exponent k in $\mathbf{X}^k$ and $\mathbf{Y}^k$ to be an element of $\mathbb{Z}_d$. Note that $\mathbf{X}^k$ maps $\mathbf{e}_j$ to $\mathbf{e}_{j+k}$ and $\mathbf{Y}^k$ maps $\mathbf{e}_j$ to $\omega^{jk}\mathbf{e}_j$.

Lemma 1.33. *The Pauli matrices* $\mathbf{X}$ *and* $\mathbf{Y}$ *for* $\mathbb{Z}_d$ *have the following properties.*

(i) $\mathbf{YX} = \omega\mathbf{XY}$,

(ii) $\mathbf{X}^r\mathbf{Y}^s$ *commutes with* $\mathbf{X}^{r'}\mathbf{Y}^{s'}$ *if and only if* $sr' = s'r$ *in* $\mathbb{Z}_d$,

(iii) $\mathrm{Tr}\,(\mathbf{X}^r\mathbf{Y}^s) = 0$ *for all* $r, s \in \mathbb{Z}_d$ *unless* $r = s = 0$.

Proof. For every $j \in \mathbb{Z}_d$ we have $\mathbf{YXe}_j = \mathbf{Ye}_{j+1} = \omega^{j+1}\mathbf{e}_{j+1} = \omega^{j+1}\mathbf{Xe}_j = \omega\mathbf{XYe}_j$. Therefore (i) holds. By applying (i) repeatedly we have $\mathbf{X}^r\mathbf{Y}^s\mathbf{X}^{r'}\mathbf{Y}^{s'} = \omega^{sr'}\mathbf{X}^{r+r'}\mathbf{Y}^{s+s'}$ and $\mathbf{X}^{r'}\mathbf{Y}^{s'}\mathbf{X}^r\mathbf{Y}^s = \omega^{s'r}\mathbf{X}^{r+r'}\mathbf{Y}^{s+s'}$. Hence $\mathbf{X}^r\mathbf{Y}^s$ and $\mathbf{X}^{r'}\mathbf{Y}^{s'}$ commute if and only if $\omega^{sr'} = \omega^{s'r}$ or equivalently $sr' = s'r$ in $\mathbb{Z}_d$. Finally $\mathrm{Tr}\,(\mathbf{X}^r\mathbf{Y}^s) = \sum_j \mathbf{e}_j{}^T\mathbf{X}^r\mathbf{Y}^s\mathbf{e}_j = \sum_j \omega^{sj}\mathbf{e}_j{}^T\mathbf{e}_{j+r} = 0$ unless $r = s = 0$. □

By Lemma 1.33, the group generated by the $d \times d$ matrices $\mathbf{X}$ and $\mathbf{Y}$, denoted $\mathrm{GP}(d)$, is

$$\mathrm{GP}(d) = \left\{\omega^i\mathbf{X}^j\mathbf{Y}^k : i, j, k \in \mathbb{Z}_d\right\}.$$

This group is usually called the *generalized Pauli group* or the *one-dimensional finite Weyl-Heisenberg group*. For any group G, let $\mathrm{Z}(G)$ denote its centre. Assume $\omega^i\mathbf{X}^j\mathbf{Y}^k \in \mathrm{Z}(\mathrm{GP}(d))$. Then $\mathbf{X}^j\mathbf{Y}^k$ must commute with $\mathbf{X}$. Therefore, by Lemma 1.33 (ii), we get $j \cdot 0 = k \cdot 1$, that is $k = 0$. Similarly, since $\mathbf{X}^j\mathbf{Y}^k$ must commute with $\mathbf{Y}$, we get $j = 0$. Hence $\mathrm{Z}(\mathrm{GP}(d))$=$\langle\omega\mathbf{I}_d\rangle = \{\omega^i\mathbf{I}_d : i \in \mathbb{Z}_d\}$. Define

$$\mathcal{H}_d = \mathrm{GP}(d)/(\mathrm{Z}(\mathrm{GP}(d)).$$

Observe that the quotient group $\mathcal{H}_d = \left\{\mathbf{X}^j\mathbf{Y}^k\langle\omega\mathbf{I}_d\rangle : j, k \in \mathbb{Z}_d\right\}$ is isomorphic to $\mathbb{Z}_d \times \mathbb{Z}_d$. The group $\mathcal{H}_d$ acts on $\mathbb{CP}^{d-1}$, where the action is given by $\left(\mathbf{X}^j\mathbf{Y}^k\langle\omega\mathbf{I}_d\rangle, [\mathbf{z}]\right) \mapsto \left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right]$. Therefore the orbit of an element $[\mathbf{z}] \in \mathbb{CP}^{d-1}$ is the set $\left\{\left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right] : j, k \in \mathbb{Z}_d\right\}$. To simplify the terminology, we refer the following set as the Weyl-Heisenberg orbit of a vector.

Definition 1.34. *The set* $\left\{\left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right] : j,k \in \mathbb{Z}_d\right\} \subset \mathbb{CP}^{d-1}$ *is called the* Weyl-Heisenberg orbit *of* $\mathbf{z} \in \mathbb{C}^d$.

We will discuss the Weyl-Heisenberg orbit and its connection to equiangular sets of lines in complex spaces in Chapter 3.

1.7 Applications

1.7.1 Real Lines

Equiangular lines in Euclidean spaces have mostly applications in designing geometrical objects that are optimal in some sense. For example, Mondal, Samanta, and Heath proved recently that the Voronoi tessellations of the real projective space generated by equiangular lines are congruent (see [62] for the details). They also mention that an equiangular set of lines forms the best n-point representation of an isotropically distributed one-dimensional subspace in terms of mutual information.

1.7.2 Complex Lines

As mentioned before, regular structures of complex lines, such as an equiangular set of lines and a set of mutually unbiased bases, have important applications in quantum information theory and signal processing. Like mutually unbiased bases, equiangular lines have been used in quantum cryptographic protocols (see Fuchs and Sasaki [34]) and in quantum tomography (see Caves, Fuchs, and Schack [19]). In this section, we briefly discuss some of these applications. Before proceeding, we give the basic of quantum mechanics terminology in a very simplified form. We warn the reader that the section on quantum mechanics and the applications following it are for illustration purposes. For more details on the fundamtental notions of quantum mechanics, see Kaye, Laflamme and Mosca [52] or Nielsen and Chuang [63, Chapter 2].

Quantum Mechanics

A *pure quantum state* is simply a line, represented by a vector $\mathbf{v}$ in a complex space $\mathbb{C}^d$. The *density matrix* of a state $\mathbf{v}$ is the projection matrix $\mathbf{P_v} = \mathbf{v}\mathbf{v}^*$. Generally a state $\mathbf{v}$ is represented by its density matrix. A *mixed state* is a collection of pure states $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$, where each $\mathbf{v}_i$ occurs with a certain probability, say p_i. We assume $\sum_i p_i = 1$. Any mixed state may be represented by a positive semidefinite Hermitian matrix with trace 1. Specifically, the mixed state $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is represented by $\sum_i p_i \mathbf{P}_{\mathbf{v}_i}$, the density matrix of a mixed state. This is because each $\mathbf{v}_i$ may be represented by the matrix $\mathbf{P}_{\mathbf{v}_i}$. Here are the postulates of quantum mechanics:

Postulate 1. *The state of any isolated physical system is described by a pure quantum state.*

To be precise, each isolated quantum mechanical system may be represented by a line in $\mathbb{C}^d$, i.e. the phase of the vector describing the system does not matter. Such a system is called a quantum mechanical d-level system. An example of a quantum mechanical two-level system is a single photon that can be found in one of two distinct paths. Another example is the presence/absence of a photon in a particular location or path. The state of either of these systems is described by a unit vector in $\mathbb{C}^2$.

Postulate 2. *The time-evolution in a quantum system is given by a unitary transformation.*

In other words, at any given time, the state of a system may be described in terms of the initial state of the system by a change of basis (which is given by a unitary matrix).

Postulate 3. *A quantum system may be measured using a set of measurement matrices.*

A *measurement* is a collection of matrices $\{\mathbf{M}_i\}_i$ such that $\sum_i \mathbf{M}_i^* \mathbf{M}_i = \mathbf{I}$. A *positive operator-valued measurement* (POVM) is a set of positive semi-definite matrices which sum to the identity matrix. Thus $\{\mathbf{M}_i^* \mathbf{M}_i : i = 1, \ldots, n\}$ is a POVM. If each $\mathbf{M}_i$ is a projection on a subspace, we call $\{\mathbf{M}_1, \ldots, \mathbf{M}_n\}$ a *projective measurement.*

Postulate 4. *Quantum systems are composed using tensor products.*

Quantum mechanics	Mathematics
(pure) state	line
mixed state	set of lines
density matrix	positive semi-definite matrix with trace 1
measurement	a (special) collection of matrices

Table 1.1: Quantum mechanics vs. mathematics vocabulary

Below, we briefly describe some of the connections of equiangular sets of lines and mutually unbiased bases with quantum mechanics as well as digital communication.

Quantum Fingerprinting

Suppose we have two public channels available: an expensive authenticated channel and a cheap unsecured channel. We would like to communicate over these channels in such a way that the receiver can authenticate the received messages with the highest possible probability. This is done by sending the message over the cheap channel and a small part of the message (called fingerprint) over the expensive channel. If the fingerprint matches to the appropriate part of the original message, the receiver would take the message to be authentic. Let F be the set of valid fingerprints that will be communicated. We may encode every message $a \in F$ with a pure quantum state $\mathbf{v}_a \in \mathbb{C}^d$. The probability of authenticating b instead of a is $|\langle \mathbf{v}_a, \mathbf{v}_b \rangle|$. Thus, the worst-case error probability is

$$P_{wce} := \max_{a \neq b \in F} |\langle \mathbf{v}_a, \mathbf{v}_b \rangle|.$$

Therefore the goal is to find sets of n pure quantum states in $\mathbb{C}^d$ which minimize the worst-case error probability. Such configurations are called *optimal Grassmannian packings* (see Conway, Hardin, and Sloane [21] and Strohmer and Heath [75]). They are also called 2-uniform (n, d)-frames (see Bodmann and Paulsen [14]). Let $|F| = n$. Welch [81] proved the bound

$$\max_{a \neq b \in F} |\langle \mathbf{v}_a, \mathbf{v}_b \rangle| \geq \sqrt{\frac{n-d}{d(n-1)}},$$

where equality occurs if and only if $n \leq d^2$ and $|\langle \mathbf{v}_a, \mathbf{v}_b \rangle| = \sqrt{(n-d)/(d(n-1))}$ for all distinct $a, b \in F$. That is $\{\mathbf{v}_a : a \in F\}$ is an equiangular set of lines meeting the relative bound. We will discuss the relative bound in Section 2.2.2. Also sets of mutually unbiased bases (MUBs) give optimal Grassmannian packings (see [83]). If d is a prime power, then $d+1$ MUBs exist and thus we have examples of optimal Grassmannian packings with $n = d^2 + d$. For more details on quantum fingerprinting, see for example Scott, Walgate, and Sanders [70].

Quantum Tomography

Tomography is a technique for displaying a representation of a cross section through a human body or other solid object using X-rays or ultrasound. In Greek, *tomos* means slice or section. Quantum tomography or quantum state tomography is the process of reconstructing the mixed quantum state (or equivalently the density matrix) of a particle or particles through a series of measurements in different bases: Suppose we have an unknown mixed quantum state or equivalently a $\rho \in \mathbb{C}^{d\times d}$ such that $\rho^* = \rho$ and $\mathrm{Tr}\,(\rho) = 1$. Thus ρ is specified by $d^2 - 1$ free parameters. Any orthonormal basis $\mathcal{B}$ for $\mathbb{C}^d$ gives a measurement $\{M_{\mathbf{v}} = \mathbf{v}\mathbf{v}^* : \mathbf{v} \in \mathcal{B}\}$. Assume that ρ is in state $\mathbf{v}$ with probability $p_{\mathbf{v}}$, where $\mathbf{v} \in \mathcal{B}$. Therefore $\rho = \sum_{\mathbf{v}\in\mathcal{B}} p_{\mathbf{v}} M_{\mathbf{v}}$ so that $\sum_{\mathbf{v}\in\mathcal{B}} p_{\mathbf{v}} = 1$. We may specify the unknown probabilities by $d-1$ free parameters. Hence, at least $(d^2-1)/(d-1) = d+1$ different measurements are required to determine ρ completely from measurement statistics. By measuring ρ in each basis a finite number of times, we find the probabilities $p_{\mathbf{v}}$ (approximately) with some possible error. This error is minimized when the bases are unbiased. Therefore, mutually unbiased bases are the optimal measurements in terms of statistical error.

Since ρ is specified by $d^2 - 1$ free parameters, using the measurement arising from an equiangular set of d^2 lines in $\mathbb{C}^d$, we may completely reconstruct ρ. In quantum information theory community, an equiangular set of d^2 lines in $\mathbb{C}^d$ is called a *symmetric informationally complete positive operator valued measurement (SIC-POVM).*

Code Division Multiple Access (CDMA)

A multiple access method allows several terminals connected to the same channel to share its capacity and communicate over it. A code division multiple access (CDMA) is a method exploited by several radio communication technologies. For more information on CDMA, see for example [40]. In signal processing community, a *Maximum-Welch-bound-equality (MWBE) codebook* with parameters (n, d) is a set $\mathcal{L}$ of n lines in $\mathbb{C}^d$ such that

$$I_{\max}(\mathcal{L}) := \max_{\mathbf{v}\neq\mathbf{w}\in\mathcal{L}} |\langle \mathbf{v}, \mathbf{w}\rangle| = \sqrt{\frac{n-d}{d(n-1)}}.$$

Note that $I_{\max}$ is the same quantity as P_{wce} that we saw in the section on quantum fingerprinting. As seen before, given an arbitrary set of n lines $\mathcal{L}$ in $\mathbb{C}^d$ we have $I_{\max}(\mathcal{L}) \geq \sqrt{\frac{n-d}{d(n-1)}}$ and equality occurs if and only if $n \leq d^2$ and $|\langle \mathbf{v}, \mathbf{w}\rangle| = \sqrt{\frac{n-d}{d(n-1)}}$ for every distinct $\mathbf{v}, \mathbf{w} \in \mathcal{L}$, i.e $\mathcal{L}$ is an equiangular set of n lines in $\mathbb{C}^d$ meeting the relative bound. If $n = d^2 + d$, the quantity $I_{\max}(\mathcal{L})$ is minimized when $\mathcal{L}$ is represented by a set of mutually unbiased bases (MUBs). One of the advantages of MUBs over MWBE codebooks in $\mathbb{C}^d$ is that when only d users are active, there is no inter-user interference. MWBE codebooks are used in direct spread CDMA systems to distinguish among the signals of different users. Sarwate [69] gives a well rounded treatment of MWBE codebooks.

Chapter 2

Regular Structures of Lines

One of the most challenging problems in algebraic combinatorics is finding large sets of lines with few angles between the pairs. This includes the problems of finding equiangular sets of lines and sets of mutually unbiased bases. In this chapter, we work on these two problems. For the purpose of completeness, in many places in this chapter, we state the results in a general setting that includes real, complex and quaternionic spaces. In the last section, we give an overview of spherical designs. This will provide us with a tool to search for large sets of lines with few angles between the pairs.

2.1 Multipartite Equiangular Sets of Lines

Here we introduce a new notion, which we call a multipartite equiangular set of lines. The main motivation is to provide a common framework for considering equiangular sets of lines and mutually unbiased bases (MUBs), which will be discussed in the next sections. The new object is a common generalization of equiangular set of lines and MUBs. Let $\mathbb{A}$ denote an associative composition algebra. Recall that a line in $\mathbb{A}^d$ is an element in the projective space $\mathbb{AP}^{d-1}$, which can be represented by a unit vector $\mathbf{u} \in \mathbb{A}^d$. Also recall that the cosine of the angle between the lines spanned by unit vectors $\mathbf{v}, \mathbf{w} \in \mathbb{A}^d$ is defined as $|\langle \mathbf{v}, \mathbf{w} \rangle|$.

Definition 2.1. *Given integers $n \geq 1$, $k \geq 1$ and $d \geq 2$, a set of n lines in $\mathbb{A}^d$ is called an (n, k, d)-*multipartite equiangular set of lines *or (n, k, d)-*MEL *in short, if it can be partitioned into k sets $\mathcal{L}_1, \ldots, \mathcal{L}_k$ with $|\mathcal{L}_i| = n/k$ such that for all i and j and for every distinct $[\mathbf{v}] \in \mathcal{L}_i$*

and $[\mathbf{w}] \in \mathcal{L}_j$*, we have*

$$|\langle \mathbf{v}, \mathbf{w} \rangle|^2 = \alpha_{ij},$$

for some constants $\alpha_{ij} \in \mathbb{R}$*.*

Example 2.2. Equiangular sets of n lines in $\mathbb{A}^d$ are the $(n, 1, d)$-MELs. We will discuss these sets in Section 2.2. Mutually unbiased bases (MUBs) are examples of (kd, k, d)-MELs with $\alpha_{ii} = 0$ and $\alpha_{ij} = \alpha$ for some constant α and every $i \neq j$. We will look at MUBs in Section 2.3. Notice that any set of n lines in $\mathbb{A}^d$ is trivially an (n, n, d)-MEL.

In the following theorem, we find an upper bound on n, the cardinality of an (n, k, d)-multipartite equiangular set of lines. This theorem is a generalization of the well-known absolute upper bound on the size of an equiangular set of lines in $\mathbb{A}^d$ (see Theorem 2.8) and also the upper bound on the number of MUBs in $\mathbb{A}^d$ (see Theorem 2.34). Also a generalization of the following theorem (see Theorem 2.6) implies that there are at most $\binom{d}{2} \dim_{\mathbb{R}} \mathbb{A} + 1$ flat equiangular lines in $\mathbb{A}^d$ (see Theorem 4.8). Recall that $\mathcal{HM}_d(\mathbb{A})$ denotes the $\mathbb{R}$-vector space of $d \times d$ Hermitian matrices with entries in $\mathbb{A}$. Also recall that $\dim_{\mathbb{R}}(\mathcal{HM}_d(\mathbb{A})) = d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$ (see Theorem 1.12). In the case of multipartite equiangular set of lines, the following theorem clearly gives a better bound than the Delsarte, Goethals and Seidel bound [27].

Theorem 2.3. *For any* (n, k, d)*-multipartite equiangular set of lines in* $\mathbb{A}^d$*, we have*

$$n \leq d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A} + k - 1.$$

Proof. Suppose $\{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$ is an (n, k, d)-MEL. Let $\mathcal{M} = \{\mathbf{v}_i {\mathbf{v}_i}^* : 1 \leq i \leq n\} \subset \mathcal{HM}_d(\mathbb{A})$ be the set of projection matrices of $\mathbf{v}_i$'s. Consider the matrix $\mathbf{G}$ defined by $\mathbf{G}_{i,j} = \operatorname{Tr}\left(\mathbf{v}_i \mathbf{v}_i^* \mathbf{v}_j \mathbf{v}_j^*\right)$. By Lemma 1.23, we have $\Re(\mathbf{G}_{i,j}) = |\langle \mathbf{v}_i, \mathbf{v}_j \rangle|^2$. Let $m = n/k$. Recall that $\mathbf{J}_m$ denotes the $m \times m$ all-ones matrix and $\mathbf{I}_m$ denotes the $m \times m$ identity matrix. By the definition of multipartite equiangular set of lines, the real part of the entries of $\mathbf{G}$ is equal to

$$\Re(\mathbf{G}) = \begin{pmatrix} (1-\alpha_{11})\mathbf{I}_m + \alpha_{11}\mathbf{J}_m & \alpha_{12}\mathbf{J}_m & \cdots & \alpha_{1k}\mathbf{J}_m \\ \alpha_{21}\mathbf{J}_m & (1-\alpha_{22})\mathbf{I}_m + \alpha_{22}\mathbf{J}_m & \cdots & \alpha_{2k}\mathbf{J}_m \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{k1}\mathbf{J}_m & \alpha_{k2}\mathbf{J}_m & \cdots & (1-\alpha_{kk})\mathbf{I}_m + \alpha_{kk}\mathbf{J}_m \end{pmatrix}.$$

For any $i \in \{1, \ldots, n\} \setminus \{rm : 1 \leq r \leq k\}$, let $r \in \{1, \ldots, k\}$ be such that $(r-1)m < i < rm$. The vector $\mathbf{e}_{i+1} - \mathbf{e}_i$ is an eigenvector of $\Re(\mathbf{G})$ with eigenvalue $1 - \alpha_{rr}$. Since $\alpha_{rr} \neq 1$ for all r, these vectors account for $k(m-1) = n-k$ nonzero eigenvalues with sum equal to

$$\sum_{r=1}^{k}(m-1)(1-\alpha_{rr}) = k(m-1) - (m-1)\sum_{r=1}^{k}\alpha_{rr} = n-k-(m-1)\sum_{r=1}^{k}\alpha_{rr}.$$

Since $\operatorname{Tr}(\Re(\mathbf{G})) = n$, it follows that the sum of the remaining k eigenvalues is equal to $k + (m-1)\sum_{r=1}^{k}\alpha_{rr} > 0$. Thus there exists at least one other nonzero eigenvalue. It follows that $\operatorname{rank}_{\mathbb{R}}(\mathbf{G}) \geq \operatorname{rank}_{\mathbb{R}}(\Re(\mathbf{G})) \geq n-k+1$. On the other hand $\mathcal{M}$ is a subset of the $\mathbb{R}$-vector space $\mathcal{HM}_d(\mathbb{A})$ which has dimension $d + \binom{d}{2}\dim_{\mathbb{R}}\mathbb{A}$. Now, by Corollary 1.29, the dimension of the $\mathbb{R}$-subspace spanned by $\mathcal{M}$ is equal to $\operatorname{rank}_{\mathbb{R}}(\mathbf{G})$. Hence

$$n-k+1 \leq \operatorname{rank}_{\mathbb{R}}(\mathbf{G}) = \dim_{\mathbb{R}}(\operatorname{span}(\mathcal{M})) \leq d + \binom{d}{2}\dim_{\mathbb{R}}\mathbb{A}.$$

□

Corollary 2.4. *For every $(n,1,d)$-multipartite equiangular set $\mathcal{L}$ of lines in $\mathbb{A}^d$ with $n = d + \binom{d}{2}\dim_{\mathbb{R}}\mathbb{A}$, the set $\{\mathbf{v}\mathbf{v}^* : [\mathbf{v}] \in \mathcal{L}\}$ forms a basis for $\mathcal{HM}_d(\mathbb{A})$.*

Proof. Substituting $k = 1$ in the last inequality in the proof of Theorem 2.3, we have

$$n \leq \dim_{\mathbb{R}}(\operatorname{span}(\mathcal{M})) \leq d + \binom{d}{2}\dim_{\mathbb{R}}\mathbb{A},$$

where $\mathcal{M} = \{\mathbf{v}\mathbf{v}^* : [\mathbf{v}] \in \mathcal{L}\} \subset \mathcal{HM}_d(\mathbb{A})$. Since $\dim_{\mathbb{R}}\mathcal{HM}_d(\mathbb{A}) = d + \binom{d}{2}\dim_{\mathbb{R}}\mathbb{A} = n$, the set $\mathcal{M}$ must be a basis for the $\mathbb{R}$-vector space $\mathcal{HM}_d(\mathbb{A})$. □

The definition of an (n,k,d)-MEL can be generalized so that the sets $\mathcal{L}_i$ in Definition 2.1 do not necessarily have the same size.

Definition 2.5. *Given integers $k \geq 1$, $d \geq 2$ and a multiset $\mathbf{n} = \{n_1; \ldots; n_k\}$ of positive integers, a set of $\sum_{i=1}^{k} n_i$ lines in $\mathbb{A}^d$ is called an $(\mathbf{n},k,d)$-*multipartite equiangular set of lines *if it can be partitioned into k sets $\mathcal{L}_1, \ldots, \mathcal{L}_k$ with $|\mathcal{L}_i| = n_i$ such that for all i and j and for every distinct $[\mathbf{v}] \in \mathcal{L}_i$ and $[\mathbf{w}] \in \mathcal{L}_j$, we have*

$$|\langle \mathbf{v}, \mathbf{w} \rangle|^2 = \alpha_{ij},$$

for some constants $\alpha_{ij} \in \mathbb{R}$.

With a similar argument as in the proof of Theorem 2.3 one can prove the following generalization.

Theorem 2.6. *For any $(\{n_1; \ldots; n_k\}, k, d)$-multipartite equiangular set of lines in $\mathbb{A}^d$, we have*

$$\sum_{i=1}^{k} n_i \leq d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A} + k - 1.$$

2.2 Equiangular Set of Lines

Definition 2.7. *A set of lines in $\mathbb{A}^d$ spanned by unit vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ is* equiangular *if there exists a constant α such that $|\langle \mathbf{v}_i, \mathbf{v}_j \rangle| = \alpha$ for every $1 \leq i < j \leq n$.*

As mentioned in Example 2.2, an equiangular set of lines is simply a MEL with $k = 1$.

2.2.1 The Absolute Bound

In this section, we derive a bound on the size of an equiangular set of lines in $\mathbb{A}^d$ that is only dependent on d. The following theorem is a known result, especially when $\mathbb{A} = \mathbb{R}$ or $\mathbb{C}$. It is a special case of Theorem 2.3 when $k = 1$.

Theorem 2.8. *An equiangular set of lines in $\mathbb{A}^d$ has size at most $d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$.*

The above bound on the size of an equiangular set of lines in $\mathbb{A}^d$ is known as the *absolute bound*. As an immediate corollary, since $\dim_{\mathbb{R}} \mathbb{R} = 1$, we get the following bound for the real space.

Corollary 2.9. *An equiangular set of lines in $\mathbb{R}^d$ has size at most $\binom{d+1}{2}$.*

It is proved that an equiangular set of $\binom{d+1}{2}$ lines $\mathbb{R}^d$ may only exist if $d = 2, 3$ or $d + 2$ is a square of an odd integer and a construction of such sets is only known for $d = 2, 3, 7, 23$ (for example, see Godsil and Royle [37]). Recently, it was proved that an equiangular set of $\binom{48}{2}$ lines in $\mathbb{R}^{47}$ does not exist [9].

Since $\dim_{\mathbb{R}} \mathbb{C} = 2$, using Theorem 2.3, we get the following bound for the complex space.

Corollary 2.10. *An equiangular set of lines in $\mathbb{C}^d$ has size at most d^2.*

In contrast to the real case, it is widely believed (mostly by physicists) that an equiangular set of d^2 lines in $\mathbb{C}^d$ always exists [85, 4, 66, 42, 33]. If an equiangular set of d^2 lines in $\mathbb{C}^d$

exists then we must have $\alpha = 1/\sqrt{d+1}$ (see Corollary 2.17). To the best of our knowledge, the existence of equiangular sets of d^2 lines are claimed in [85, 46, 66, 4, 41, 42] for $d \leq 10$ and $d \in \{12, 19\}$. In addition, it is claimed in [33] (with reference to private communication with Markus Grassl) that such sets also exist for $d \in \{11, 13, 15\}$. In most of these papers, the proof that such given sets are equiangular is not published, as it may generally require pages of tedious algebra to give a complete proof. Nevertheless, the problem is still open for a general d:

Problem 2.11. For any integer $d \geq 2$, does there exist an equiangular set of d^2 lines in $\mathbb{C}^d$?

Since $\dim_{\mathbb{R}} \mathbb{H} = 4$, using Theorem 2.3, we get the following bound for the quaternionic space.

Corollary 2.12. *An equiangular set of lines in $\mathbb{H}^d$ has size at most $2d^2 - d$.*

Examples of such lines are even harder to find. In Chapter 4, we will give an explicit construction of an equiangular set of 6 lines in $\mathbb{H}^2$.

2.2.2 The Relative Bound

In this section, we derive a second bound on the size of an equiangular set of lines. This bound depends both on d and the cosine of the common angle. The following theorem is known as the *relative bound* and is proved in various contexts. The proof is a replicate of Godsil and Royle [37, Lemma 11.4.1] generalized to an arbitrary $\mathbb{A}^d$, where $\mathbb{A}$ is an associative composition algebra.

Theorem 2.13. *If there is an equiangular set of n lines in $\mathbb{A}^d$ with the cosine of the common angle equal to α and $d\alpha^2 < 1$, then*

$$n \leq \frac{d - d\alpha^2}{1 - d\alpha^2},$$

or equivalently

$$\alpha \geq \sqrt{\frac{n-d}{d(n-1)}}.$$

Let the n lines be represented by $\mathbf{v}_1, \ldots, \mathbf{v}_n$, and for every $1 \leq i \leq n$, let $\mathbf{P}_{\mathbf{v}_i} = \mathbf{v}_i \mathbf{v}_i^*$ denote the projection onto the line spanned by $\mathbf{v}_i$. Then equality holds if and only if

$$\sum_{i=1}^{n} \mathbf{P}_{\mathbf{v}_i} = \frac{n}{d} \mathbf{I}_d.$$

Proof. Let $\mathbf{S} = \sum_{i=1}^{n} \mathbf{P}_{\mathbf{v}_i}$. Consider $\mathbf{B} = \mathbf{S} - (n/d)\mathbf{I}_d$. Using Lemma 1.23, we have

$$\begin{aligned}
\Re\left(\operatorname{Tr}\left(\mathbf{B}^2\right)\right) &= \Re\left(\operatorname{Tr}\left(\mathbf{S}^2 - \frac{2n}{d}\mathbf{S} + \frac{n^2}{d^2}\mathbf{I}_d\right)\right) \\
&= \sum_{i,j} \Re\left(\operatorname{Tr}\left(\mathbf{P}_{\mathbf{v}_i}\mathbf{P}_{\mathbf{v}_j}\right)\right) - \frac{2n}{d}\sum_{i} \Re\left(\operatorname{Tr}\left(\mathbf{P}_{\mathbf{v}_i}\right)\right) + \frac{n^2}{d^2} \cdot d \\
&= \sum_{i,j} |\langle \mathbf{v}_i, \mathbf{v}_j \rangle|^2 - \frac{2n}{d}\sum_{i} 1 + \frac{n^2}{d} \\
&= \left(n + n(n-1)\alpha^2\right) - \frac{n^2}{d} = \frac{n}{d}\left(d - d\alpha^2 - n(1 - d\alpha^2)\right).
\end{aligned}$$

Since $\mathbf{B}$ is a Hermitian matrix, the result follows from the fact that $\Re\left(\operatorname{Tr}\left(\mathbf{B}^2\right)\right) = \operatorname{Tr}\left(\mathbf{B}^2\right) = \operatorname{Tr}\left(\mathbf{B}\mathbf{B}^*\right) = \sum_{i,j} |\mathbf{B}_{ij}|^2 \geq 0$ and equality holds if and only $\mathbf{B} = \mathbf{0}$. □

In Section 2.2.4, we will define frames as well as tight frames and discuss their relationship with equiangular sets of lines. For the time being, we would like to emphasize that any set of vectors representing a set of lines that meet the relative bound, i.e. satisfy the equality condition in Theorem 2.13, is called a tight frame:

Definition 2.14. *A* tight frame *is a set of unit vectors* $\mathbf{v}_1, \ldots, \mathbf{v}_n$ *in* $\mathbb{A}^d$ *for which*

$$\sum_{i=1}^{n} \mathbf{P}_{\mathbf{v}_i} = \frac{n}{d}\mathbf{I}_d.$$

Here $\mathbf{P}_{\mathbf{v}_i} = \mathbf{v}_i{\mathbf{v}_i}^*$ *is the matrix of the projection onto the line spanned by* $\mathbf{v}_i$.

Hence, any equiangular set of lines that meet the relative bound in Theorem 2.13 is called a *tight equiangular set of lines.*

Lemma 2.15. *If* $\{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$ *is an equiangular set of lines in* $\mathbb{A}^d$ *with the cosine of the common angle equal to* α*, then the following are equivalent.*

(i) $\alpha = \sqrt{\dfrac{n-d}{d(n-1)}}$,

(ii) $\sum_{i=1}^{n} \mathbf{P}_{\mathbf{v}_i} = \dfrac{n}{d}\mathbf{I}_d$,

(iii) $\mathbf{I}_d$ *is an* $\mathbb{R}$*-linear combination of* $\mathbf{P}_{\mathbf{v}_1}, \ldots, \mathbf{P}_{\mathbf{v}_n}$,

where $\mathbf{P}_{\mathbf{v}_i} = \mathbf{v}_i{\mathbf{v}_i}^*$ *for* $1 \leq i \leq n$.

Proof. We only need to prove (iii) implies (ii). Write $\mathbf{I}_d = \sum_i c_i \mathbf{P}_{\mathbf{v}_i}$ for some scalars $c_1, \ldots, c_n \in \mathbb{R}$. By taking trace from both sides, and using Lemma 1.21, we get $d = \sum_i c_i$. By multiplying both sides by a fixed $\mathbf{P}_{\mathbf{v}_j}$ and then taking trace, we get $\mathrm{Tr}\left(\mathbf{P}_{\mathbf{v}_j}\right) = \sum_i c_i \mathrm{Tr}\left(\mathbf{P}_{\mathbf{v}_i}\mathbf{P}_{\mathbf{v}_j}\right)$. Hence $1 = \Re(\mathrm{Tr}\left(\mathbf{P}_{\mathbf{v}_j}\right)) = \sum_i c_i \Re(\mathrm{Tr}\left(\mathbf{P}_{\mathbf{v}_i}\mathbf{P}_{\mathbf{v}_j}\right)) = \sum_i c_i |\langle \mathbf{v}_i, \mathbf{v}_j \rangle|^2$, by Lemma 1.21 and Lemma 1.23. Thus, $1 = (1-\alpha^2)c_j + \alpha^2 \sum_i c_i = (1-\alpha^2)c_j + \alpha^2 d$. It follows that all c_j's must be equal and since they add up to d they must be equal to d/n. □

Corollary 2.16. *Suppose we have an equiangular set of $d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$ lines in $\mathbb{A}^d$ with the cosine of the common angle equal to α, then*

$$\alpha = \frac{1}{\sqrt{d + \dfrac{2}{\dim_{\mathbb{R}} \mathbb{A}}}}.$$

Proof. It follows from Corollary 2.4 that the existence of an equiangular set of $d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$ lines in $\mathbb{A}^d$ implies their projection matrices form a basis for the $\mathbb{R}$-vector space $\mathcal{HM}_d(\mathbb{A})$. In particular, $\mathbf{I}_d$ is an $\mathbb{R}$-linear combination of these projection matrices. The result follows from Lemma 2.15 by substituting $n = d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$. □

Corollary 2.17. *The cosine of the common angle of an equiangular set of d^2 lines in $\mathbb{C}^d$ is equal to $\frac{1}{\sqrt{d+1}}$.*

2.2.3 A Lower Bound via Duality

In his PhD dissertation, Zauner [85, Chapter 2.2] uses the notion of coherent duality (Kohärente Dualität) in $\mathbb{C}^d$ to derive a lower bound on the number of lines in a tight equiangular set. By taking an insight from his work, which is written in German, and generalizing it to an arbitrary $\mathbb{A}^d$, where $\mathbb{A}$ is an associative composition algebra, we present the notion of duality in this section and derive an analogous lower bound. Before we do so, we would like to reiterate that the familiar Gram-Schmidt process for $\mathbb{R}^d$ and $\mathbb{C}^d$, also holds in $\mathbb{H}^d$ (see Proposition 1.15).

Given a tight equiangular set $\mathcal{L} = \{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$ of n lines in $\mathbb{A}^d$, recall that $\mathbf{V}$ is the $d \times n$ matrix where the i-th column is equal to $\mathbf{v}_i$. By Lemma 1.22 and Theorem 2.13, we have

$$\mathbf{V}\mathbf{V}^* = \sum_i \mathbf{v}_i {\mathbf{v}_i}^* = \frac{n}{d}\mathbf{I}_d.$$

Thus the rows of the matrix $\sqrt{d/n}\mathbf{V}$, say $\mathbf{u}_1, \ldots, \mathbf{u}_d$, are $d \leq n$ orthonormal vectors in $\mathbb{A}^n$. By Proposition 1.15, we may extend $\{\mathbf{u}_1, \ldots, \mathbf{u}_d\}$ to an orthonormal basis of $\mathbb{A}^n$ by adding vectors $\mathbf{u}_{d+1}, \ldots, \mathbf{u}_n$. Let $\mathbf{U}$ be the $n \times n$ matrix with rows $\mathbf{u}_1, \ldots, \mathbf{u}_d, \mathbf{u}_{d+1}, \ldots, \mathbf{u}_n$. The columns of $\mathbf{U}$ may be written as $\sqrt{d/n}(\mathbf{v}_i, \mathbf{w}_i) \in \mathbb{A}^d \times \mathbb{A}^{n-d}$, $i = 1, \ldots, n$. We have $\mathbf{U}\mathbf{U}^* = \mathbf{I}$, i.e. $\mathbf{U}$ is a unitary matrix. Therefore $\mathbf{U}^*\mathbf{U} = \mathbf{I}$ or equivalently, $\langle \mathbf{v}_i, \mathbf{v}_j \rangle + \langle \mathbf{w}_i, \mathbf{w}_j \rangle = (n/d)\delta_{ij}$ for every $i, j \in \{1, \ldots, n\}$. It follows that

$$|\langle \mathbf{w}_i, \mathbf{w}_j \rangle| = \begin{cases} \dfrac{n-d}{d} & \text{for } i = j, \\ |\langle \mathbf{v}_i, \mathbf{v}_j \rangle| & \text{for } i \neq j. \end{cases}$$

By letting $d^* = n - d$ and considering $|\langle \mathbf{v}_i, \mathbf{v}_j \rangle|^2 = \dfrac{n-d}{d(n-1)}$ for $i \neq j$, we get

$$|\langle \sqrt{d/d^*}\mathbf{w}_i, \sqrt{d/d^*}\mathbf{w}_j \rangle|^2 = \frac{d^2}{(n-d)^2}|\langle \mathbf{w}_i, \mathbf{w}_j \rangle|^2 = \begin{cases} 1 & \text{for } i = j, \\ \dfrac{n-d^*}{d^*(n-1)} & \text{for } i \neq j. \end{cases}$$

Therefore $\mathcal{L}^* = \left\{[\sqrt{d/d^*}\mathbf{w}_1], \ldots, [\sqrt{d/d^*}\mathbf{w}_n]\right\}$ is a tight equiangular set of n lines in $\mathbb{A}^{d^*}$. Notice that we require $d^* > 1$, and consequently $n > d + 1$, since otherwise $\frac{n-d^*}{d^*(n-1)} = 1$ and all the elements in $\mathcal{L}^*$ would be scalar multiples of each other. The set $\mathcal{L}^*$ is called a *dual* of the set $\mathcal{L}$, and we have the following useful theorem.

Theorem 2.18. *Let $n > d + 1 > 2$ be integers. Then there exists a tight equiangular set of n lines in $\mathbb{A}^d$ if and only if there exists a tight equiangular set of n lines in $\mathbb{A}^{n-d}$.*

As a corollary, we have the following lower bound on the size of a tight equiangular set of lines in any given dimension.

Corollary 2.19. *If there exists a tight equiangular set of $n > d + 1 > 2$ lines in $\mathbb{A}^d$, then*

$$n \geq d + \frac{1 + \sqrt{\dfrac{8d}{\dim_{\mathbb{R}} \mathbb{A}} + 1}}{2}.$$

Proof. Since the maximum possible number of lines in an equiangular set of lines in $\mathbb{A}^d$ is $d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A}$, using Theorem 2.18 we must have

$$n \leq (n - d) + \binom{n-d}{2} \dim_{\mathbb{R}} \mathbb{A}.$$

Solving the above inequality for n yields the desired result. □

Corollary 2.20. *Let $k \geq 2$ be an integer. Then there exists no tight equiangular set of $d+k$ lines in $\mathbb{A}^d$ for $d > \binom{k}{2} \dim_{\mathbb{R}} \mathbb{A}$.*

Proof. If such a set exists, Theorem 2.18 implies the existence of a tight equiangular set of $d+k$ lines in $\mathbb{A}^k$. Thus, we must have $d+k \leq k + \binom{k}{2} \dim_{\mathbb{R}} \mathbb{A}$. □

2.2.4 The Gram and the Frame Matrices

In Section 1.5, we established the definition of two important matrices associated to a set of lines and briefly studied their properties. Restricted to equiangular set of lines, we investigate further properties of these matrices. Recall from Definition 1.26 that the Gram matrix of a set C of n vectors in $\mathbb{A}^d$ is the matrix $\mathbf{G} = \mathbf{V}^*\mathbf{V}$, where $\mathbf{V}$ is the $d \times n$ matrix with the elements of C as its columns. The (i,j)-entry of $\mathbf{G}$ is the inner product of the i-th and j-th vector in C.

Lemma 2.21. *Suppose $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ is a tight frame in $\mathbb{A}^d$. Let $\mathbf{g}_i$ denote the i-th column of its corresponding Gram matrix. Then*

$$\langle \sqrt{\frac{d}{n}}\mathbf{g}_i, \sqrt{\frac{d}{n}}\mathbf{g}_j \rangle = \langle \mathbf{v}_i, \mathbf{v}_j \rangle$$

for every i and j.

Proof. We have

$$\begin{aligned} \langle \mathbf{g}_i, \mathbf{g}_j \rangle &= \sum_{k=1}^{d} (\mathbf{g}_i)_k^* (\mathbf{g}_j)_k = \sum_{k=1}^{d} \langle \mathbf{v}_i, \mathbf{v}_k \rangle \langle \mathbf{v}_k, \mathbf{v}_j \rangle \\ &= \mathbf{v}_i{}^* (\sum_{k=1}^{n} \mathbf{P}_{\mathbf{v}_k}) \mathbf{v}_j = \frac{n}{d} \langle \mathbf{v}_i, \mathbf{v}_j \rangle. \end{aligned}$$

□

Recall that a Gram matrix of a set of lines $\mathcal{L}$ is the Gram matrix of a set of vectors that represent $\mathcal{L}$ and therefore is not unique.

Corollary 2.22. *Suppose $\mathcal{L}$ is a tight equiangular set of n lines in $\mathbb{A}^d$. Let $\mathcal{L}'$ be the set of columns of a Gram matrix of $\mathcal{L}$, normalized by $\sqrt{d/n}$. Then $\mathcal{L}'$ is equivalent to $\mathcal{L}$. In particular, $\mathcal{L}'$ is also a tight equiangular set of n lines embeddable in $\mathbb{A}^d$.*

Proof. Let $\mathbf{G}$ be a Gram matrix of $\mathcal{L}$. Since $\dim_{\mathbb{A}} \operatorname{Im}_{\mathbb{A}}(\mathbf{G}) = \operatorname{rank}_{\mathbb{A}}(\mathbf{G}) \leq d$, the set $\mathcal{L}'$ is embeddable in $\mathbb{A}^d$. The result follows from Lemma 2.21. □

Definition 2.23. *Given a set C of n unit vectors in $\mathbb{A}^d$, let $\mathbf{V}$ be a $d \times n$ matrix with the elements of C as its columns. Then*

$$\mathbf{S} = \mathbf{V}\mathbf{V}^*$$

is called a frame matrix *of the vectors in C.*

It follows that $\mathbf{S}^* = \mathbf{S}$ and $\langle \mathbf{z}, \mathbf{S}\mathbf{z} \rangle = \langle \mathbf{z}, \mathbf{V}\mathbf{V}^*\mathbf{z} \rangle = \langle \mathbf{V}^*\mathbf{z}, \mathbf{V}^*\mathbf{z} \rangle \geq 0$ for all $\mathbf{z} \in \mathbb{A}^d$. Thus $\mathbf{S}$ is a positive semi-definite matrix.

One may also define a frame matrix of a set of lines by considering the vectors representing the lines. In contrast to the Gram matrix, notice that the frame matrix of a set of lines is unique. This is because, by Lemma 1.22, $\mathbf{S} = \sum_{\mathbf{v} \in C} \mathbf{v}\mathbf{v}^*$ and if $[\mathbf{v}] = [\mathbf{v}']$, i.e. $\mathbf{v}$ and $\mathbf{v}'$ represent the same line, then $\mathbf{v}\mathbf{v}^* = \mathbf{v}'\mathbf{v}'^*$, as we discussed in the comments following Definition 1.20. Recall from Definition 2.14 that a tight frame is a set of unit vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in \mathbb{A}^d$ for which $\sum_{i=1}^{n} \mathbf{P}_{\mathbf{v}_i} = (n/d)\mathbf{I}_d$, where $\mathbf{P}_{\mathbf{v}} = \mathbf{v}\mathbf{v}^*$. Due to the uniqueness of the frame matrix, we may extend the definition of a tight frame to a set of lines:

Definition 2.24. *A set of lines $\{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$ in $\mathbb{A}^d$ is called* tight *if $\sum_{i=1}^{n} \mathbf{v}_i {\mathbf{v}_i}^* = (n/d)\mathbf{I}_d$.*

Lemma 2.25. *Let $\mathbf{V}$ be a $d \times n$ matrix with entries in $\mathbb{A}$ such that $\operatorname{rank}_{\mathbb{A}}(\mathbf{V}) = d$. Then the frame matrix of the columns of $\mathbf{V}$ is an invertible matrix.*

Proof. Let $\mathbf{S} = \mathbf{V}\mathbf{V}^*$ be the frame matrix of the columns of $\mathbf{V}$. Suppose $\mathbf{v} \in \operatorname{Ker}_{\mathbb{A}}(\mathbf{S})$. Then $\langle \mathbf{V}^*\mathbf{v}, \mathbf{V}^*\mathbf{v} \rangle = \mathbf{v}^*\mathbf{V}\mathbf{V}^*\mathbf{v} = \mathbf{v}^*\mathbf{S}\mathbf{v} = 0$. Therefore $\mathbf{V}^*\mathbf{v} = \mathbf{0}$, that is $\mathbf{v} \in \operatorname{Ker}_{\mathbb{A}}(\mathbf{V}^*)$. It follows that $\operatorname{Ker}_{\mathbb{A}}(\mathbf{S}) \subseteq \operatorname{Ker}_{\mathbb{A}}(\mathbf{V}^*)$ and therefore $\dim_{\mathbb{A}} \operatorname{Ker}_{\mathbb{A}}(\mathbf{S}) \leq \dim_{\mathbb{A}} \operatorname{Ker}_{\mathbb{A}}(\mathbf{V}^*)$. Recall that the dimensions of the row space and the column space of a matrix are both equal to the dimension of the row space of the conjugate transpose of that matrix [47, Chapter VII, Corollary 2.5]). Lemma 1.10 implies that

$$\operatorname{rank}_{\mathbb{A}}(\mathbf{S}) = \dim_{\mathbb{A}} \operatorname{Im}_{\mathbb{A}}(\mathbf{S}) \geq \dim_{\mathbb{A}} \operatorname{Im}_{\mathbb{A}}(\mathbf{V}^*) = \dim_{\mathbb{A}} \operatorname{Im}_{\mathbb{A}}(\mathbf{V}) = \operatorname{rank}_{\mathbb{A}}(\mathbf{V}) = d.$$

Since $\mathbf{S}$ is a $d \times d$ matrix, we have $\operatorname{rank}_{\mathbb{A}}(\mathbf{S}) = d$. Thus $\mathbf{e}_1, \ldots, \mathbf{e}_d$ are in $\operatorname{Im}_{\mathbb{A}}(\mathbf{S})$ and therefore there is a matrix $\mathbf{S}^{-1}$ such that $\mathbf{S}\mathbf{S}^{-1} = \mathbf{I}_d$. It follows that $\mathbf{S}^{-1}\mathbf{S} = \mathbf{I}_d$ (see [31, Theorem 2.24] or [86, Proposition 4.1]) and therefore $\mathbf{S}$ is invertible. □

The following lemma is a variation of Lemma 1.28 that is needed in this section.

Lemma 2.26. *Fix* $\mathbb{A} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$*. For a given matrix* $\mathbf{V}$ *with entries in* $\mathbb{A}$*, we have* $\operatorname{rank}_{\mathbb{A}}(\mathbf{V}^*\mathbf{V}) = \operatorname{rank}_{\mathbb{A}}(\mathbf{V})$*. That is, the dimension of an* $\mathbb{A}$*-module is equal to the* $\mathbb{A}$*-rank of the Gram matrix of any set of vectors spanning that module.*

Proof. If $\mathbf{V}^*\mathbf{V}\mathbf{z} = \mathbf{0}$ then $\mathbf{z}^*\mathbf{V}^*\mathbf{V}\mathbf{z} = 0$, which can be written as $\langle \mathbf{V}\mathbf{z}, \mathbf{V}\mathbf{z}\rangle = 0$. This implies $\mathbf{V}\mathbf{z} = \mathbf{0}$. On the other hand, $\mathbf{V}\mathbf{z} = \mathbf{0}$ implies $\mathbf{V}^*\mathbf{V}\mathbf{z} = \mathbf{0}$. Hence $\operatorname{Ker}_{\mathbb{A}}(\mathbf{V}^*\mathbf{V}) = \operatorname{Ker}_{\mathbb{A}}(\mathbf{V})$ and the result follows from Lemma 1.10 and Definition 1.11. □

A result similar to the following theorem appears in [35, Lemma 6.1] which only deals with real numbers. The proof of the non-obvious direction seems to be new.

Theorem 2.27. *Let* $\mathbf{V}$ *be any* $d \times n$ *matrix with entries in* $\mathbb{A}$ *whose columns are unit vectors. Let* $\mathbf{S} = \mathbf{V}\mathbf{V}^*$ *and* $\mathbf{G} = \mathbf{V}^*\mathbf{V}$*. Then the set of columns of* $\mathbf{V}$ *is a tight frame, i.e.* $\mathbf{S} = (n/d)\mathbf{I}_d$*, if and only if*

$$\mathbf{G}^2 = \frac{n}{d}\mathbf{G}.$$

Proof. Suppose $\mathbf{S} = (n/d)\mathbf{I}_d$. We have $\mathbf{V}\mathbf{V}^* = \sum_{[\mathbf{v}]\in\mathcal{L}} \mathbf{P}_{\mathbf{v}} = (n/d)\mathbf{I}_d$. Hence $\mathbf{G}^2 = \mathbf{V}^*\mathbf{V}\mathbf{V}^*\mathbf{V} = (n/d)\mathbf{G}$. To prove the converse, assume $\mathbf{G}^2 = (n/d)\mathbf{G}$. Hence $\mathbf{V}\mathbf{G}^2\mathbf{V}^* = (n/d)\mathbf{V}\mathbf{G}\mathbf{V}^*$. Since $\mathbf{G} = \mathbf{V}^*\mathbf{V}$, it follows that $\mathbf{S}^2(\mathbf{S} - (n/d)\mathbf{I}_d) = \mathbf{0}$. The columns of $\mathbf{V}$ are unit vectors. Hence each diagonal entry of $\mathbf{G}$ is equal to 1 and therefore $\operatorname{Tr}(\mathbf{G}) = n$. Thus, by Lemma 1.28 and Lemma 1.25, we get $\operatorname{rank}_{\mathbb{A}}(\mathbf{V}) = \operatorname{rank}_{\mathbb{A}}(\mathbf{G}) = d$. Now, Lemma 2.25 implies that the matrix $\mathbf{S}$ is invertible. Therefore $\mathbf{S} - (n/d)\mathbf{I}_d = \mathbf{0}$. □

As a consequence, we have the following useful criterion to check whether a matrix is a Gram matrix of a tight equiangular set of n lines in $\mathbb{A}^d$.

Corollary 2.28. *An* $n \times n$ *Hermitian matrix* $\mathbf{G}$ *is a Gram matrix of a tight equiangular set of* n *lines in* $\mathbb{A}^d$ *if and only if* $\mathbf{G} \circ \mathbf{G}^T = \mathbf{I}_n + (n-d)/d(n-1)(\mathbf{J}_n - \mathbf{I}_n)$ *and* $\mathbf{G}^2 = (n/d)\mathbf{G}$*.*

Proof. Let $\mathcal{L} = \{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$, and notice that if $\mathbf{G}$ is a Gram matrix of $\mathcal{L}$ then $(\mathbf{G}\circ\mathbf{G}^T)_{ij} = \langle \mathbf{v}_i, \mathbf{v}_j\rangle\langle \mathbf{v}_j, \mathbf{v}_i\rangle = |\langle \mathbf{v}_i, \mathbf{v}_j\rangle|^2$. Now, if $\mathbf{G}$ is a Gram matrix of a tight equiangular set of n lines in $\mathbb{A}^d$ then $|\langle \mathbf{v}_i, \mathbf{v}_j\rangle|^2 = (n-d)/d(n-1)$ and $\mathbf{S} = (n/d)\mathbf{I}_d$, by Theorem 2.13. Therefore $\mathbf{G}^2 = (n/d)\mathbf{G}$, by Theorem 2.27. To prove the converse, since $\mathbf{G}^*\mathbf{G} = \mathbf{G}^2 = (n/d)\mathbf{G}$ and $\operatorname{Tr}(\mathbf{G}) = n$, it follows from Lemma 1.25 that $\operatorname{rank}_{\mathbb{A}}(\mathbf{G}) = d$. We also have

$$\langle \mathbf{v}, \mathbf{G}\mathbf{v}\rangle = (d/n)\langle \mathbf{v}, \mathbf{G}^*\mathbf{G}\mathbf{v}\rangle = (d/n)\langle \mathbf{G}\mathbf{v}, \mathbf{G}\mathbf{v}\rangle \geq 0$$

for any $\mathbf{v}$. Therefore $\mathbf{G}$ is a positive semi-definite matrix. By Theorem 1.27, there is a matrix $\mathbf{B}$ such that $\mathbf{G} = \mathbf{B}^*\mathbf{B}$. Hence $\operatorname{rank}_{\mathbb{A}}(\mathbf{B}) = \operatorname{rank}_{\mathbb{A}}(\mathbf{G}) = d$, by Lemma 1.28. Therefore the columns of $\mathbf{B}$ span a d-dimensional submodule of $\mathbb{A}^n$ and are therefore embedable in $\mathbb{A}^d$. Also, by Theorem 2.27, we have $\mathbf{B}\mathbf{B}^* = (n/d)\mathbf{I}_d$. It follows that set of columns of $\mathbf{B}$ is a tight equiangular set of n lines in $\mathbb{A}^d$. □

Example 2.29 (Sustik and Tropp [77])**.** Here is an example of a Gram matrix $\mathbf{G}$ of a tight equiangular set of 9 lines in $\mathbb{C}^3$. Let $\omega = e^{\pi i/3}$ and define $\mathbf{G} = \mathbf{I}_9 + (1/2)\mathbf{W}$, where

$$\mathbf{W} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & \overline{\omega} & \overline{\omega} & \overline{\omega} & -1 & \omega & \omega & \omega \\ 1 & \omega & 0 & \overline{\omega} & \omega & \overline{\omega} & \overline{\omega} & -1 & \omega \\ 1 & \omega & \omega & 0 & \overline{\omega} & \overline{\omega} & \omega & \overline{\omega} & -1 \\ 1 & \omega & \overline{\omega} & \omega & 0 & \overline{\omega} & -1 & \omega & \overline{\omega} \\ 1 & -1 & \omega & \omega & \omega & 0 & \overline{\omega} & \overline{\omega} & \overline{\omega} \\ 1 & \overline{\omega} & \omega & \overline{\omega} & -1 & \omega & 0 & \overline{\omega} & \omega \\ 1 & \overline{\omega} & -1 & \omega & \overline{\omega} & \omega & \omega & 0 & \overline{\omega} \\ 1 & \overline{\omega} & \overline{\omega} & -1 & \omega & \omega & \overline{\omega} & \omega & 0 \end{pmatrix}.$$

The interesting feature of the matrix $\mathbf{G}$ is that all of the off-diagonal entries are of the form $(1/2)x$, where x is a sixth root of unity. One may use Corollary 2.28 to check that $\mathbf{G}$ is in fact a Gram matrix of a tight equiangular set of 9 lines in $\mathbb{C}^3$. This example is due to Sustik and appears in Tropp [77].

As a side note we would like to mention that frame theory is a fundamental concept in signal processing, image processing, data compression, sampling theory, and many other applications. Frame theory was initiated by Duffin and Schaeffer [29]. A set of vectors C in $\mathbb{A}^d$ is called a *frame* (not necessarily a tight frame) for $\mathbb{A}^d$ if there exist constants $A, B > 0$ such that

$$A\langle \mathbf{w}, \mathbf{w}\rangle \leq \sum_{\mathbf{v}\in C} |\langle \mathbf{w}, \mathbf{v}\rangle|^2 \leq B\langle \mathbf{w}, \mathbf{w}\rangle$$

for all $\mathbf{w} \in \mathbb{A}^d$. It is not hard to see that if C is a finite set that spans $\mathbb{A}^d$ then such A and B always exist. If $A = B$ then it is called a *tight frame*. It is not hard to see that when $|C|$ is finite, this definition coincides with Definition 2.14. It must also be the case that for tight frames $A = n/d$, where $n = |C|$. The following observation is known for $\mathbb{R}^d$ and $\mathbb{C}^d$. For the purpose of completeness, we give a proof for $\mathbb{A}^d$.

Lemma 2.30. *For any set of unit vectors $\{\mathbf{v}_1, \ldots, \mathbf{v}_n\}$ in $\mathbb{A}^d$, the following are equivalent.*

(i) *There exists a constant A such that $\sum_{i=1}^n |\langle \mathbf{w}, \mathbf{v}_i\rangle|^2 = A\langle \mathbf{w}, \mathbf{w}\rangle$ for all $\mathbf{w} \in \mathbb{A}^d$.*

(ii) $\sum_{i=1}^n \mathbf{P}_{\mathbf{v}_i} = (n/d)\mathbf{I}_d$, *where $\mathbf{P}_\mathbf{v} = \mathbf{v}\mathbf{v}^*$.*

Proof. Let $\mathbf{S} = \sum_{i=1}^n \mathbf{P}_{\mathbf{v}_i}$ and consider $\mathbf{B} = \mathbf{S} - A\mathbf{I}_d$. Assume (i) holds. Then $\mathbf{B}$ is a Hermitian matrix and $\mathbf{w}^*\mathbf{B}\mathbf{w} = 0$ for all $\mathbf{w} \in \mathbb{A}^d$. By Corollary 1.18, we get $\mathbf{B} = \mathbf{0}$ or equivalently $\mathbf{S} = A\mathbf{I}_d$. We also have $Ad = \mathrm{Tr}\,(A\mathbf{I}_d) = \mathrm{Tr}\,(\mathbf{S}) = \sum_{i=1}^n \mathrm{Tr}\,(\mathbf{P}_{\mathbf{v}_i}) = n$, by Lemma 1.21. Hence $A = n/d$. To prove the converse multiply both sides of $\sum_{i=1}^n \mathbf{P}_{\mathbf{v}_i} = (n/d)\mathbf{I}_d$ by $\mathbf{w}^*$ from the left and by $\mathbf{w}$ from the right. We get

$$\sum_{i=1}^n |\langle \mathbf{w}, \mathbf{v}_i\rangle|^2 = \sum_{i=1}^n \mathbf{w}^*\mathbf{v}_i{\mathbf{v}_i}^*\mathbf{w} = (n/d)\langle \mathbf{w}, \mathbf{w}\rangle.$$

□

Another object equivalent to a tight frame is a spherical 1-design. This is discussed in Section 2.4. Recall from Lemma 2.25 that the frame matrix $\mathbf{S}$ of any set of vectors in $\mathbb{A}^d$ that span $\mathbb{A}^d$ is invertible. Since $\mathbf{S}$ is a positive semi-definite matrix, so is $\mathbf{S}^{-1}$. This is because $(\mathbf{S}^{-1})^* = (\mathbf{S}^*)^{-1} = \mathbf{S}^{-1}$ and $\langle \mathbf{v}, \mathbf{S}^{-1}\mathbf{v}\rangle = \langle \mathbf{S}^{-1}\mathbf{v}, \mathbf{S}(\mathbf{S}^{-1}\mathbf{v})\rangle \geq 0$. Hence by Theorem 1.27, there is a matrix, denoted $\mathbf{S}^{-1/2}$, such that $(\mathbf{S}^{-1/2})^2 = \mathbf{S}^{-1}$ and we may assume $\mathbf{S}^{-1/2}$ is Hermitian if we work over $\mathbb{R}$ or $\mathbb{C}$.

Note that any frame for $\mathbb{R}^d$ or $\mathbb{C}^d$ may be converted to a tight frame as follows. Consider the matrix $\hat{\mathbf{V}} = \sqrt{n/d}\,\mathbf{S}^{-1/2}\,\mathbf{V}$ and let $\hat{C}$ denote the set of column vectors of $\hat{\mathbf{V}}$. We have

$$\begin{aligned}\hat{\mathbf{V}}\hat{\mathbf{V}}^* = (n/d)\mathbf{S}^{-1/2}\mathbf{V}\mathbf{V}^*(\mathbf{S}^{-1/2})^* &= (n/d)\mathbf{S}^{-1/2}\mathbf{S}(\mathbf{S}^{-1/2})^* \\ &= (n/d)\mathbf{S}^{-1/2}(\mathbf{S}^{-1/2})^{-2}\mathbf{S}^{-1/2} = (n/d)\mathbf{I}_d.\end{aligned}$$

Thus $\hat{\mathbf{V}}$ is a tight frame. However, note that if $\mathcal{L}$ is an equiangular frame then $\hat{\mathcal{L}}$ is not necessarily equiangular. For a thorough survey on this subject, see Casazza [18]. Also see Benedetto and Fickus [11].

2.3 Mutually Unbiased Bases

Here we study another regular structure of lines, represented by a union of orthonormal bases in which only 2 angles occur. We give an upper bound on the size of such a set in $\mathbb{A}^d$, where $\mathbb{A}$ is an associative composition algebra. Then we only work with complex spaces and briefly study the known properties of such sets. We explore the possible connection between such sets and other known combinatorial objects such as orthogonal arrays. Finally, we propose a new idea for constructing such sets based on the orbit of a complex vector, called an MUB-fiducial vector, under a Weyl-Heisenberg group. We also give a characterization on the existence of such MUB-fiducial vectors.

Definition 2.31. *Let $\mathcal{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_k\}$ be a collection of k orthonormal bases in $\mathbb{A}^d$ such that for every $i \neq j$ and $\mathbf{v} \in \mathcal{B}_i$ and $\mathbf{w} \in \mathcal{B}_j$ we have $|\langle \mathbf{v}, \mathbf{w} \rangle| = \alpha$ for some constant α. Such a collection of vectors is called a set of k* mutually unbiased bases (MUBs) *in $\mathbb{A}^d$.*

Recall that a $d \times d$ matrix $\mathbf{U}$ is unitary if $\mathbf{U}^*\mathbf{U} = \mathbf{I}_d$ or equivalently if the mapping $\mathbf{v} \mapsto \mathbf{U}\mathbf{v}$ preserves the inner product. By applying a unitary transformation we may always assume that $\mathcal{B}_1$ is the standard basis. Therefore the absolute value of every coordinate of every vector in $\mathcal{B}_j$, where $j \geq 2$, must be α. Since each vector in $\mathcal{B}_j$ is a unit vector, we must have $\alpha = 1/\sqrt{d}$.

A matrix is *flat* (or α-flat) if all the entries have the same absolute value (say α). By writing the vectors of each orthonormal basis as columns of a unitary matrix, we get the following definition which is equivalent to Definition 2.31.

Definition 2.32. *Let $\mathcal{B} = \{\mathbf{B}_1, \ldots, \mathbf{B}_k\}$ be a collection of k $d \times d$ unitary matrices with entries in $\mathbb{A}$ such that for every $i \neq j$, the matrix $\mathbf{B}_i^*\mathbf{B}_j$ is α-flat for some constant α. Such a collection of matrices is called a* set of k MUBs.

As before, we may assume $\mathbf{B}_1 = \mathbf{I}$.

Example 2.33. Here is a set of 3 MUBs in $\mathbb{C}^2$:

$$\left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1+i}{2} & \frac{-1+i}{2} \end{pmatrix}, \begin{pmatrix} \frac{1+i}{2} & \frac{-1+i}{2} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix} \right\}.$$

As mentioned in Example 2.2, the set of lines spanned by the unit vectors of a set of MUBs is an example of a (kd, k, d)-multipartite equiangular set of lines with $\alpha_{ii} = 0$ and $\alpha_{ij} = \alpha$ for some constant α and every $i \neq j$. Therefore, we get the following upper bound on the number of MUBs in $\mathbb{A}^d$.

Theorem 2.34. *For any collection of k MUBs in $\mathbb{A}^d$, we have $k \leq \dfrac{\dim_{\mathbb{R}} \mathbb{A}}{2} d + 1$.*

Proof. By Theorem 2.3, we have $kd \leq d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A} + k - 1$. Solving for k yields the result. □

For the rest of this chapter, we will only focus on complex spaces.

2.3.1 Abelian Subspace Decomposition

In [8], Bandyopadhyay, Boykin, Roychowdhury and Vatan developed an interesting equivalence between mutually unbiased bases and commuting bases of orthogonal unitary matrices. Our main purpose in this section is to investigate this equivalence further. Then, we use their formulation to explore the possible connection between mutually unbiased bases and other known combinatorial objects. As an example, in Proposition 2.45, we see why establishing a possible link between mutually unbiased bases and orthogonal arrays is possibly a difficult task.

Let $M_d(\mathbb{C})$ denote the d^2-dimensional $\mathbb{C}$-vector space of all $d \times d$ matrices with entries in $\mathbb{C}$. This vector space is equipped with the standard inner product $\langle \mathbf{A}, \mathbf{B} \rangle = \operatorname{Tr}(\mathbf{A}^* \mathbf{B}) = \sum_{i,j} \overline{\mathbf{A}_{ij}} \mathbf{B}_{ij}$. By $\operatorname{span}_{\mathbb{C}}(\{\mathbf{A}_1, \ldots, \mathbf{A}_k\})$ or $\operatorname{span}_{\mathbb{C}}(\mathbf{A}_1, \ldots, \mathbf{A}_k)$ we mean the subspace of $M_d(\mathbb{C})$ spanned by the matrices $\mathbf{A}_1, \ldots, \mathbf{A}_k$. The following is classical result in linear algebra. For example, see Hoffman and Kunze [44] for a proof.

Lemma 2.35. *Let $\{\mathbf{A}_1, \ldots, \mathbf{A}_k\}$ be a set of complex matrices such that $\mathbf{A}_i \mathbf{A}_i^* = \mathbf{A}_i^* \mathbf{A}_i$ and $\mathbf{A}_i \mathbf{A}_j = \mathbf{A}_j \mathbf{A}_i$ for every $i \neq j$. Then there exists a unitary matrix $\mathbf{U}$ such that $\mathbf{U} \mathbf{A}_i \mathbf{U}^*$ is a diagonal matrix for every i.*

A subspace W of $M_d(\mathbb{C})$ is said to be *abelian* if $\mathbf{AB} = \mathbf{BA}$ for all $\mathbf{A}, \mathbf{B} \in W$. Note that W is abelian if and only if any basis of W is a set of pairwise commuting matrices. A matrix $\mathbf{A}$ is *traceless* if $\operatorname{Tr}(\mathbf{A}) = 0$.

Definition 2.36. *We call any $(d-1)$-dimensional abelian subspace of $M_d(\mathbb{C})$* nice *if it has an orthogonal basis consisting of traceless unitary matrices. Such a basis is called a* nice *basis.*

Definition 2.37. *Let $\{\mathcal{M}_1, \ldots, \mathcal{M}_k\}$ be a collection of k nice bases in $M_d(\mathbb{C})$ such that for every $i \neq j$ and $\mathbf{A} \in \mathcal{M}_i$ and $\mathbf{B} \in \mathcal{M}_j$ we have $\langle \mathbf{A}, \mathbf{B} \rangle = 0$. We call such a collection of bases a set of k* mutually orthogonal nice bases *(MONB) in $\mathbb{C}^d$.*

Example 2.38. Let $\mathbf{X}$ and $\mathbf{Y}$ be the $d \times d$ Pauli matrices defined in Section 1.6. By Lemma 1.33, $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3\}$ is a set of 3 MONBs in $\mathbb{C}^d$, where

$$\begin{aligned}\mathcal{M}_1 &= \{\mathbf{Y}, \ldots, \mathbf{Y}^{d-1}\},\\ \mathcal{M}_2 &= \{\mathbf{X}, \ldots, \mathbf{X}^{d-1}\},\\ \mathcal{M}_3 &= \{\mathbf{XY}, \ldots, \mathbf{X}^{d-1}\mathbf{Y}^{d-1}\}.\end{aligned}$$

The following theorem shows that the existence of MUBs is equivalent to the existence of MONBs. This result is originally due to Bandyopadhyay et. al [8]. For the sake of completeness, we include the main steps of the proof.

Theorem 2.39. [8] *There exist k MUBs in $\mathbb{C}^d$ if and only if there exist k MONBs in $\mathbb{C}^d$.*

Proof. For any orthonormal basis $\mathcal{B} = \{\mathbf{v}_0, \ldots, \mathbf{v}_{d-1}\}$ of $\mathbb{C}^d$, define $\phi(\mathcal{B}) = \{\mathbf{A}_1, \ldots, \mathbf{A}_{d-1}\}$ where

$$\mathbf{A}_k = \sum_{t=0}^{d-1} \omega^{kt} \mathbf{v}_t \mathbf{v}_t^*.$$

It is straightforward to show that if $\{\mathcal{B}_1, \ldots, \mathcal{B}_k\}$ is a collection of k MUBs in $\mathbb{C}^d$ then $\{\phi(\mathcal{B}_1), \ldots, \phi(\mathcal{B}_k)\}$ is a collection of k MONBs in $\mathbb{C}^d$.

To prove the converse, let $\mathcal{M} = \{\mathbf{A}_1, \ldots, \mathbf{A}_{d-1}\}$ be a nice basis in $M_d(\mathbb{C})$. Let $\psi(\mathcal{M}) = \{\mathbf{v}_0, \ldots, \mathbf{v}_{d-1}\}$ be the orthonormal basis such that each $\mathbf{A}_j$ is a diagonal matrix with respect to this basis. Such a basis exists due to Lemma 2.35. Again, it is easy to show that if $\{\mathcal{M}_1, \ldots, \mathcal{M}_k\}$ is a collection of k MONBs in $\mathbb{C}^d$ then $\{\psi(\mathcal{M}_1), \ldots, \psi(\mathcal{M}_k)\}$ is a collection of k MUBs in $\mathbb{C}^d$. □

The following lemma is new.

Lemma 2.40. *Let W be a nice subspace of $M_d(\mathbb{C})$. Then there exists a unitary matrix $\mathbf{U}$ such that*

$$W = \{\mathbf{U}^*\mathbf{D}\mathbf{U} : \mathbf{D} \textit{ is diagonal}, \operatorname{Tr}(\mathbf{D}) = 0\}.$$

Proof. Let $\{\mathbf{A}_1, \ldots, \mathbf{A}_{d-1}\}$ be a nice basis of W consisting of commuting traceless unitary matrices. By Lemma 2.35, there exists a unitary matrix $\mathbf{U}$ such that for every i, the matrix $\mathbf{U}\mathbf{A}_i\mathbf{U}^* = \mathbf{D}_i$ is diagonal. For every i, we have $\operatorname{Tr}(\mathbf{D}_i) = \operatorname{Tr}(\mathbf{A}_i) = 0$. Since $\mathbf{A}_i = \mathbf{U}^*\mathbf{D}_i\mathbf{U}$ and any linear combination of traceless diagonal matrices is a traceless diagonal matrix, it follows that

$$W \subseteq \{\mathbf{U}^*\mathbf{D}\mathbf{U} : \mathbf{D} \text{ is diagonal}, \operatorname{Tr}(\mathbf{D}) = 0\}.$$

Let $\mathbf{D}_0 = \mathbf{I}$. For every i, let $\mathbf{v}_i \in \mathbb{C}^d$ be the vector corresponding to the diagonal of $\mathbf{D}_i$. Note that $\mathbf{v}_0$ is the all-ones vector. We have $\langle \mathbf{v}_i, \mathbf{v}_j \rangle = \langle \mathbf{D}_i, \mathbf{D}_j \rangle = \langle \mathbf{A}_i, \mathbf{A}_j \rangle = 0$ for every $0 \leq i < j \leq d-1$. Thus $\{\mathbf{v}_0, \ldots, \mathbf{v}_{d-1}\}$ is an orthogonal basis for $\mathbb{C}^d$. Given any diagonal matrix $\mathbf{D}$ with $\mathrm{Tr}\,(\mathbf{D}) = 0$, let $\mathbf{v}$ be the vector corresponding to its diagonal. Then $\langle \mathbf{v}, \mathbf{v}_0 \rangle = 0$. Hence $\mathbf{v} \in \mathrm{span}_{\mathbb{C}}\,(\mathbf{v}_1, \ldots, \mathbf{v}_{d-1})$ and therefore $\mathbf{D} \in \mathrm{span}_{\mathbb{C}}\,(\mathbf{D}_1, \ldots, \mathbf{D}_{d-1})$. This implies that $\mathbf{U}^*\mathbf{D}\mathbf{U} \in W$. □

In the following new lemma we show that every nice subspace has a nice basis consisting of powers of a unitary matrix.

Lemma 2.41. *Any nice subspace of $M_d(\mathbb{C})$ has an orthogonal basis of the form*

$$\{\mathbf{A}, \mathbf{A}^2, \ldots, \mathbf{A}^{d-1}\}$$

where $\mathbf{A}$ is a unitary matrix such that $\mathrm{Tr}\,(\mathbf{A}^s) = 0$ for $1 \leq s \leq d-1$ and $\mathbf{A}^d = \mathbf{I}_d$.

Proof. Let $\mathbf{Y}$ be the diagonal Pauli matrix, that is $\mathbf{Y}_{ij} = \delta_{ij}\omega^i$ where ω is a primitive d-th root of unity. We have $\mathrm{Tr}\,(\mathbf{Y}^s) = \sum_{i=0}^{d-1} \omega^{si} = 0$ for every $1 \leq s \leq d-1$. Also, $\mathbf{Y}$ is a unitary matrix and $\mathbf{Y}^d = \mathbf{I}_d$. Any $d \times d$ diagonal matrix with entries in $\mathbb{C}$ can be written as a $\mathbb{C}$-linear combination of the matrices $\mathbf{Y}, \ldots, \mathbf{Y}^{d-1}, \mathbf{Y}^d = \mathbf{I}_d$. To see this, let $\mathbf{v}_s$ be the vector corresponding to the diagonal of $\mathbf{Y}^s$. Then the matrix whose columns are $\mathbf{v}_1, \ldots, \mathbf{v}_d$ is a Vandermonde matrix and is therefore invertible. By Lemma 2.40, any nice subspace of $M_d(\mathbb{C})$ is of the form $\{\mathbf{U}^*\mathbf{D}\mathbf{U} : \mathbf{D} \text{ is diagonal}, \mathrm{Tr}\,(\mathbf{D}) = 0\}$ for some unitary matrix $\mathbf{U}$. Hence, the matrix $\mathbf{A} = \mathbf{U}^*\mathbf{Y}\mathbf{U}$ has the desired properties.

□

It is interesting to note that there are several combinatorial objects that have similar properties to MUBs and it would be quite intriguing to know whether their existence is equivalent to the existence of MUBs. One of these combinatorial objects is an orthogonal array.

An *orthogonal array* $OA(k, d)$ is a $k \times d^2$ array with entries from $\{1, \ldots, d\}$ having the property that in any two rows, each (ordered) pair of symbols from $\{1, \ldots, d\}$ occurs exactly once. There are several objects, such as $k-2$ mutually orthogonal Latin squares (MOLS) of order d, that are equivalent to an orthogonal array $OA(k, d)$ (see [1]). As a reminder, a *Latin square* of order d is a $d \times d$ matrix with entries from the set $\{1, \ldots, d\}$, such that each row and each column is a permutation on $\{1, \ldots, d\}$. Two Latin squares L and L' of order d are *orthogonal* if $\{(L_{ij}, L'_{ij}) : 1 \leq i,j \leq d\} = \{(i,j) : 1 \leq i,j \leq d\}$. For a given d, we denote the maximum k for which an $OA(k,d)$ exists by $N_{OA}(d)$. Note that by the above remark, $N_{MOLS}(d) = N_{OA}(d) - 2$, where $N_{MOLS}(d)$ denotes the maximum number of Latin squares in a set of MOLS of order d.

Definition 2.42. *For a given integer $d \geq 2$, the maximum number of bases in a set of mutually unbiased bases of $\mathbb{C}^d$ is denoted by $N(d)$.*

The following theorem is a collection of known results on $N(d)$.

Theorem 2.43. *Let $d \geq 2$ be an integer. The function $N(d)$ has the following properties.*

(a) $N(d) \leq d + 1$.

(b) $N(p^r) = p^r + 1$ *for any prime p and $r \geq 1$.*

(c) $N(mn) \geq \min\{N(m), N(n)\}$ *for all $m, n \geq 2$.*

(d) $N(d) \geq p^r + 1$, *where p is the smallest prime divisor of d and $p^r | d$. In particular, $N(d) \geq 3$ for all d and $N(d) \geq 4$ for all odd d.*

(e) $N(d^2) \geq N_{OA}(d)$.

Proof. Part (a) follows immediately from Theorem 2.34, since $\dim_{\mathbb{R}} \mathbb{C} = 2$. To prove part (b) for $r = 1$, let $\mathcal{M}_{-1} = \{\mathbf{Y}, \ldots, \mathbf{Y}^{p-1}\}$ and $\mathcal{M}_j = \{\mathbf{X}\mathbf{Y}^j, \ldots, \mathbf{X}^{p-1}\mathbf{Y}^{j(p-1)}\}$ for every $0 \leq\ j \leq\ p-1$, where $\mathbf{X}$ and $\mathbf{Y}$ are the Pauli matrices for $\mathbb{Z}_p$. Since $\mathrm{Tr}\,(\mathbf{X}^r\mathbf{Y}^s) = 0$ (unless $r = s = 0$) and $\mathbf{Y}\mathbf{X} = \omega\mathbf{X}\mathbf{Y}$, it follows that $\{\mathcal{M}_j : -1 \leq j \leq p-1\}$ is a collection of $p+1$ MONBs and therefore $N(p) \geq p+1$, by Theorem 2.39. Part (a) implies $N(p) = p+1$. The reader may find a proof for $r > 1$ in Wootters and Fields [83] or Bandyopadhyay et. al [8]. We will give an independent proof for $r > 1$ in Section 2.3.5 when $p \neq 2, 3$. For part (c), let $k = \min\{N(m), N(n)\}$. For any $B \subseteq \mathbb{C}^m$ and $B' \subseteq \mathbb{C}^n$, let $B \otimes B' = \{\mathbf{v} \otimes \mathbf{v}' : \mathbf{v} \in\ B, \mathbf{v}' \in B'\}$. If $\mathcal{B} = \{\mathcal{B}_1, \ldots, \mathcal{B}_{N(m)}\}$ is a set of $N(m)$ MUBs in $\mathbb{C}^m$ and $\mathcal{B}' = \{\mathcal{B}'_1, \ldots, \mathcal{B}'_{N(n)}\}$ is a set of $N(n)$ MUBs in $\mathbb{C}^n$ then $\mathcal{B} = \{\mathcal{B}_1 \otimes \mathcal{B}'_1, \ldots, \mathcal{B}_k \otimes \mathcal{B}'_k\}$ is a set of k MUBS is in $\mathbb{C}^{mn}$. This is because, by equation (1.4.1),

$$|\langle \mathbf{v} \otimes \mathbf{v}', \mathbf{w} \otimes \mathbf{w}' \rangle|^2 = |\langle \mathbf{v}, \mathbf{w} \rangle|^2 |\langle \mathbf{v}', \mathbf{w}' \rangle|^2 = \begin{cases} \dfrac{1}{mn} & \text{if } |\langle \mathbf{v}, \mathbf{w} \rangle| = \dfrac{1}{m} \text{ and } |\langle \mathbf{v}', \mathbf{w}' \rangle| = \dfrac{1}{n}, \\ 0 & \text{if } |\langle \mathbf{v}, \mathbf{w} \rangle| = 0 \text{ or } |\langle \mathbf{v}', \mathbf{w}' \rangle| = 0. \end{cases}$$

Part (d) follows immediately from parts (b) and (c). One may prove $N(d) \geq 3$ directly as follows. Let

$$\begin{aligned}\mathcal{M}_{-1} &= \{\mathbf{Y}, \ldots, \mathbf{Y}^{d-1}\},\\ \mathcal{M}_0 &= \{\mathbf{X}, \ldots, \mathbf{X}^{d-1}\},\\ \mathcal{M}_1 &= \{\mathbf{XY}, \ldots, \mathbf{X}^{d-1}\mathbf{Y}^{d-1}\}.\end{aligned}$$

Then $\{\mathcal{M}_{-1}, \mathcal{M}_0, \mathcal{M}_1\}$ is a set of 3 MONBs in $\mathbb{C}^d$ and apply Theorem 2.39. Similarly, if d is odd, let $\mathcal{M}_2 = \{\mathbf{XY}^2, \ldots, \mathbf{X}^{d-1}\mathbf{Y}^{2(d-1)}\}$. Then $\{\mathcal{M}_{-1}, \mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2\}$ is a set of 4 MONBs in $\mathbb{C}^d$ and apply Theorem 2.39 to get $N(d) \geq 4$. Note that $\mathcal{M}_0$ and $\mathcal{M}_2$ are disjoint if and only if d is odd. This is because $\{(r, 2r) : r \in \mathbb{Z}_d \setminus \{0\}\} \cap \{(r, 0) : r \in \mathbb{Z}_d \setminus \{0\}\} = \emptyset$ if and only if d is odd. Part (e) is proved by Wocjan and Beth [82]. □

Remark. The function $N_{OA}(d)$ satisfies the same conditions as $N(d)$ does in Theorem 2.43. In fact, we know much more about the function $N_{OA}(d)$ and it would be interesting to know whether $N(d)$ also satisfies all of the known properties of $N_{OA}(d)$. As an example, it is proved that $N_{OA}(d) \geq 4$, $d \neq 2, 6$ (see [79, Theorem 22.7]). It is also proved that for every $d \geq 2$, if there exists an $OA(d, d)$ then it can be extended to an $OA(d+1, d)$ (see [79, page 287]). Equivalently, if there exist $d-2$ MOLS of order d then there exist $d-1$ MOLS of order d. The proof of this result is rather easy, however proving a similar result for $N(d)$ seems to be out of reach at the moment. One may ask the following questions.

Problem 2.44. For every $d \neq 2, 6$, is it true that $N(d) \geq 4$? For every $d \geq 2$, is it true that any set of d MUBs in $\mathbb{C}^d$ can be extended to a set of $d+1$ MUBs in $\mathbb{C}^d$? Is it true that $N(d) = N_{OA}(d)$?

According to the following proposition, it could be challenging to prove or disprove that a set of 3 MUBs in $\mathbb{C}^3$ can be extended to a set of 4 MUBs in $\mathbb{C}^3$. The following proposition is new.

Proposition 2.45. *The following are equivalent.*

(i) *Any set of* 3 *MUBs in* $\mathbb{C}^3$ *can be extended to a set of* 4 *MUBs in* $\mathbb{C}^3$.

(ii) *Let* $\mathbf{A}$ *and* $\mathbf{B}$ *be unitary* 3×3 *matrices such that* $\mathbf{A}^3 = \mathbf{B}^3 = \mathbf{I}_3$, $\mathbf{AB}$ *and* $\mathbf{BA}$ *commute and* $\operatorname{Tr}\left(\mathbf{A}^i\mathbf{B}^j\right) = 0$ *unless* $i = j = 0$. *Then* $(\mathbf{AB})^3 = \mathbf{I}_3$.

Proof. (i)⇒(ii) Let $\mathbf{A}$ and $\mathbf{B}$ be as given in (ii). Then $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3\}$ is a collection of 3 MONBs in $\mathbb{C}^3$, where $\mathcal{M}_1 = \{\mathbf{A}, \mathbf{A}^2\}$ and $\mathcal{M}_2 = \{\mathbf{B}, \mathbf{B}^2\}$ and $\mathcal{M}_3 = \{\mathbf{AB}, \mathbf{A}^2\mathbf{B}^2\}$. By Theorem 2.39, the existence of k MONBs is equivalent to the existence of k MUBs. Therefore, by (i), there exists an $\mathcal{M}_4$ such that $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3, \mathcal{M}_4\}$ is an MONB in $\mathbb{C}^3$. Now, if $\mathbf{AB}^2 \in \operatorname{span}_{\mathbb{C}}(\mathcal{M}_1)$, then $\mathbf{AB}^2 = c_1\mathbf{A} + c_2\mathbf{A}^2$ for some $c_1, c_2 \in \mathbb{C}$. Since $\mathbf{A}^3 = \mathbf{I}_3$, by multiplying both sides of this equation by $\mathbf{A}^2$ from the left, we get $\mathbf{B}^2 = c_1\mathbf{I}_3 + c_2\mathbf{A}$. It follows that $0 = \operatorname{Tr}\left(\mathbf{B}^2\right) = c_1\operatorname{Tr}(\mathbf{I}_3) + c_2\operatorname{Tr}(\mathbf{A}) = 3c_1$. Hence $\mathbf{B}^2$ is a scalar multiple of $\mathbf{A}$, that is $\mathbf{0} \neq \mathbf{B} \in \mathcal{M}_1 \cap \mathcal{M}_2$, which is a contradiction. Hence $\mathbf{AB}^2 \notin \operatorname{span}_{\mathbb{C}}(\mathcal{M}_1)$. By applying a similar technique, we may show that $\mathbf{AB}^2, \mathbf{A}^2\mathbf{B} \notin \operatorname{span}_{\mathbb{C}}(\mathcal{M}_i)$ for $i = 1, 2, 3$. This means that $\mathbf{AB}^2, \mathbf{A}^2\mathbf{B} \in \mathcal{M}_4$. Since $\mathcal{M}_4$ is abelian, we have $(\mathbf{AB}^2)(\mathbf{A}^2\mathbf{B}) = (\mathbf{A}^2\mathbf{B})(\mathbf{AB}^2)$ or equivalently $\mathbf{B}^2\mathbf{A}^2 = (\mathbf{AB})^2$. Multiply both sides by $\mathbf{AB}$ from the left to get $(\mathbf{AB})^3 = \mathbf{I}_3$.

(ii)⇒(i) Suppose there exists a set of 3 MUBs in $\mathbb{C}^3$. By Theorem 2.39 there exist 3 MONBs, say $\mathcal{M}_1, \mathcal{M}_2$, and $\mathcal{M}_3$, in $\mathbb{C}^3$. By Lemma 2.41, we may assume $\mathcal{M}_1 = \{\mathbf{A}, \mathbf{A}^2\}$ and $\mathcal{M}_2 = \{\mathbf{B}, \mathbf{B}^2\}$ for some unitary 3×3 matrices $\mathbf{A}$ and $\mathbf{B}$ such that $\mathbf{A}^3 = \mathbf{B}^3 = \mathbf{I}_3$ and $\operatorname{Tr}\left(\mathbf{A}^i\mathbf{B}^j\right) = 0$ unless $i = j = 0$. Hence $\mathbf{AB}, \mathbf{AB}^2, \mathbf{A}^2\mathbf{B}, \mathbf{A}^2\mathbf{B}^2 \notin \operatorname{span}_{\mathbb{C}}(\mathcal{M}_1) \cup \operatorname{span}_{\mathbb{C}}(\mathcal{M}_2)$. This is because these four matrices are orthogonal to the matrices spanning $\mathcal{M}_1$ and $\mathcal{M}_2$. By symmetry, we may assume $\mathbf{AB} \in \mathcal{M}_3$. Now, we consider two cases. Case 1: If $\mathbf{A}^2\mathbf{B} \in \mathcal{M}_3$, since $\operatorname{span}_{\mathbb{C}}(\mathcal{M}_3)$ is abelian, then $(\mathbf{AB})(\mathbf{A}^2\mathbf{B}) = (\mathbf{A}^2\mathbf{B})(\mathbf{AB})$ which simplifies to $\mathbf{AB} = \mathbf{BA}$. Thus $\mathbf{AB}^2$ and $\mathbf{A}^2\mathbf{B}^2$ commute and therefore by letting $\mathcal{M}_4 = \{\mathbf{AB}^2, \mathbf{A}^2\mathbf{B}^2\}$, we get a set of 4 MONBs $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3, \mathcal{M}_4\}$ in $\mathbb{C}^3$. Case 2: If $\mathbf{A}^2\mathbf{B}^2 \in \mathcal{M}_3$, since $\operatorname{span}_{\mathbb{C}}(\mathcal{M}_3)$ is abelian, then $(\mathbf{AB})(\mathbf{A}^2\mathbf{B}^2) = (\mathbf{A}^2\mathbf{B}^2)(\mathbf{AB})$ which simplifies to $(\mathbf{BA})(\mathbf{AB}) = (\mathbf{AB})(\mathbf{BA})$. Therefore, by (ii), we have $(\mathbf{AB})^3 = \mathbf{I}_3$. Hence

$$(\mathbf{AB}^2)(\mathbf{A}^2\mathbf{B}) = \mathbf{AB}^2\mathbf{A}^2(\mathbf{AB})^3\mathbf{B} = \mathbf{A}(\mathbf{AB})^2\mathbf{B} = (\mathbf{A}^2\mathbf{B})(\mathbf{AB}^2).$$

Thus $\mathbf{AB}^2$ and $\mathbf{A}^2\mathbf{B}$ commute. Therefore $\{\mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_3, \mathcal{M}_4\}$ is a set of 4 MONBs in $\mathbb{C}^3$ with $\mathcal{M}_4 = \{\mathbf{AB}^2, \mathbf{A}^2\mathbf{B}\}$. In either case, by Theorem 2.39, we get 4 MUBs in $\mathbb{C}^3$. □

Conjecture 2.46. *Any set of d MUBs in $\mathbb{C}^d$ can be extended to a set of $d+1$ MUBs in $\mathbb{C}^d$.*

We will give a new proof of the fact that for any prime power q, there exist $q+1$ MUBs in $\mathbb{C}^q$. Before we do so, we first study the zero-sum sets on the unit complex circle. Zero-sum sets are useful in classifying the special MUBs, that will be introduced in Section 2.3.3, in small dimensions. They are also of an independent interest.

2.3.2 Zero-sum Sets of Points on the Unit Complex Circle

For a given integer $n \geq 2$, consider the n n-th roots of unity. Their sum is zero.

Definition 2.47. *We say that a finite subset $S \subset \mathbb{C}$ is* zero-sum *if the sum of its elements is zero and $|s| = 1$ for each $s \in S$.*

Can we find other arrangements of zero-sum set of n points? If so, can we classify them? Of course, rotating a zero-sum set yields another zero-sum set. Therefore, for simplicity, we can always assume that the complex number $z = 1$ is in the zero-sum set. Such a zero-sum set will be called *normalized.* Also, the union of any two zero-sum sets is again a zero-sum set. Hence we only consider *indecomposable* zero-sum sets, that is zero-sum sets that cannot be written as the union of two non-empty zero-sum sets.

Question 2.48. How could we arrange n points on the unit complex circle so that their sum is zero? Find all normalized indecomposable zero-sum sets of n points.

In this section, we answer the above question for $n \leq 5$. In the next section, we will use these results to classify all mutually unbiased bases in $\mathbb{C}^d$ with $d \leq 5$ that arise from a Weyl-Heisenberg orbit. Any point $z \neq -1$ on the unit complex circle may be presented by

$$z(t) = \frac{1-t^2}{1+t^2} + \frac{2t}{1+t^2}i,$$

where $t \in \mathbb{R}$. Note that for any point $e^{i\theta}$ on the unit circle, t is the tangent of $\theta/2$. Antipodal pairs of points on the unit complex circle sum to zero. Therefore $\{-1, 1\}$ is the only normalized zero-sum set of 2 points. The following theorem shows that there is a unique normalized zero-sum set of 3 points.

Theorem 2.49. *Let ω be a primitive third root of unity. The set $\{1, \omega, \omega^2\}$ is the unique normalized zero-sum set of 3 points.*

Proof. Let $\{1, x, y\}$ be a zero-sum set. Clearly $x \neq -1$, thus let $x = z(t)$ for some $t \in \mathbb{R}$. Since $1 + x = -y$ is on the unit circle, it follows that

$$\left(1 + \frac{1-t^2}{1+t^2}\right)^2 + \left(0 + \frac{2t}{1+t^2}\right)^2 = 1,$$

which simplifies to $t^2 - 3 = 0$. Thus $t = \pm\sqrt{3}$. That is, $x = e^{i\theta}$ with $\tan(\theta/2) = \pm\sqrt{3}$ or equivalently $\theta = \pm 2\pi/3$. □

Any zero-sum set of 4 points is the union of two antipodal pairs of points on the unit complex circle. This is proved in the following theorem.

Theorem 2.50. *There is no indecomposable zero-sum set of* 4 *points.*

Proof. Let $\{1, x, y, u\}$ be a normalized zero-sum set of 4 points. We may assume $x \neq -1$ and $y \neq -1$. Write $x = z(t)$ and $y = z(s)$ for some $t, s \in \mathbb{R}$. Since $1 + x + y = -u$ is on the unit circle, it follows that

$$\left(1 + \frac{1-t^2}{1+t^2} + \frac{1-s^2}{1+s^2}\right)^2 + \left(0 + \frac{2t}{1+t^2} + \frac{2s}{1+s^2}\right)^2 = 1,$$

which simplifies to $ts = -1$. By writing $x = e^{i\theta}$ and $y = e^{i\theta'}$, we have $\tan(\theta/2)\tan(\theta'/2) = -1$, or equivalently $|\theta/2 - \theta'/2| = \pi/2$. Hence, x and y are an antipodal pair of points. This means $x + y = 0$ and therefore $u = -1$. Thus $\{1, x, y, u\}$ is decomposable. □

One may see that there are infinitely many indecomposable normalized zero-sum sets of 5 points (we will not prove this, but one may imply this from Theorem 2.52). However, we are only interested in those zero-sum sets in which the product of the elements is equal to 1.

Definition 2.51. *We say that a finite subset $S \subset \mathbb{C}$ is* one-product *if the product of its elements is equal to one and $|s| = 1$ for each $s \in S$.*

We are able to characterize indecomposable normalized zero-sum one-product sets of 5 points.

Theorem 2.52. *Any indecomposable normalized zero-sum one-product set of* 5 *points is of the form $\{1, x, \overline{x}, y, \overline{y}\}$ with $\Re(x + y) = -1/2$ and $-1/4 < \Re(x) < 1/2$.*

Proof. Let $S = \{1, x, y, u, v\}$ be a normalized zero-sum one-product set of 5 points. Since S is indecomposable, we may assume $x, y, u, v \neq -1$. Write $x = z(t), y = z(s), u = z(p)$ and $v = z(q)$ for some distinct $t, s, p, q \in \mathbb{R} \setminus \{0\}$. Since $1 + x + y + u + v = 0$, we have

$$\begin{aligned} 1 + \frac{1-t^2}{1+t^2} + \frac{1-s^2}{1+s^2} + \frac{1-p^2}{1+p^2} + \frac{1-q^2}{1+q^2} &= 0, \\ 0 + \frac{2t}{1+t^2} + \frac{2s}{1+s^2} + \frac{2p}{1+p^2} + \frac{2q}{1+q^2} &= 0, \end{aligned}$$

which may be rewritten as

$$\frac{2(1-ts)(1+st)}{(1+t^2)(1+s^2)} + \frac{2(1-pq)(1+pq)}{(1+p^2)(1+q^2)} = -1, \qquad (2.3.1)$$

$$\frac{(s+t)(1+st)}{(1+t^2)(1+s^2)} + \frac{(p+q)(1+pq)}{(1+p^2)(1+q^2)} = 0. \qquad (2.3.2)$$

Since $xyuv = 1$, the sum of the arguments of x, y, u and v is an integer multiple of 2π. Therefore the tangent of the sum of the halves of the arguments of x and y is the negative of the tangent of the sum of the halves of the arguments of u and v, that is

$$\frac{s+t}{1-st} = -\frac{p+q}{1-pq}. \tag{2.3.3}$$

Substituting $1-pq = -(p+q)(1-st)/(s+t)$ in equation (2.3.1) and multiplying both sides by $s+t$, we get

$$\frac{(s+t)(1+ts)}{(1+t^2)(1+s^2)} - \frac{(p+q)(1+pq)}{(1+p^2)(1+q^2)} = -\frac{(s+t)}{2(1-st)}. \tag{2.3.4}$$

By adding equations (2.3.4) and (2.3.2), we have

$$\frac{(s+t)(1+st)}{(1+t^2)(1+s^2)} = -\frac{(s+t)}{4(1-st)},$$

which can be rewritten as

$$(s+t)\left(s^2+t^2-3s^2t^2+5\right) = 0. \tag{2.3.5}$$

Similarly, by subtracting equations (2.3.4) and (2.3.2), we get

$$(p+q)\left(p^2+q^2-3p^2q^2+5\right) = 0. \tag{2.3.6}$$

All of the above arguments were applied to the pair $\{\{s,t\},\{p,q\}\}$. Since all of the above identities are symmetric in s, t, p and q, it follows that all of the mentioned equalities also hold for the pairs $\{\{s,p\},\{t,q\}\}$ and $\{\{s,q\},\{t,p\}\}$, that is $(s+p)\left(s^2+p^2-3s^2p^2+5\right) = 0$, $(s+p)/(1-sp) = -(t+q)/(1-tq)$ and so on. Recall that $x = z(s)$ and $u = z(p)$. Note that $s+p = 0$ if and only if $u = \overline{x}$. Also, by substituting $s^2 = (1-\Re(x))/(1+\Re(x))$ and $t^2 = (1-\Re(y))/(1+\Re(y))$ in $s^2+t^2-3s^2t^2+5$, we observe that $\Re(x+y) = -1/2$ if and only of $s^2+t^2-3s^2t^2+5 = 0$.

Thus, if any two of the elements in $\{x, y, u, v\}$, say x and u, are conjugates then $s+p = 0$ and therefore $t+q = 0$ which means y and v are conjugates. Now, since $t \neq p$, it follows that $s+t \neq 0$ and therefore $s^2+t^2-3s^2t^2+5 = 0$ or equivalently, $\Re(x+y) = -1/2$. Since $x, y \neq -1$ and $\Re(x) = -1/2 - \Re(y)$ it follows that $-1 < \Re(x) < 1/2$. Also notice that $-1/4 < \Re(x) < 1/2$ if and only if $-1 < \Re(y) < 1/2$. Therefore, by symmetry, we may assume $-1/4 < \Re(x) < 1/2$.

If no two elements in $\{x, y, u, v\}$ are conjugates then $\pm s, \pm t, \pm p$ and $\pm q$ are all distinct and therefore $s^2+t^2-3s^2t^2+5 = 0, s^2+p^2-3s^2p^2+5 = 0$, and so on. This implies that

$\Re(x+y), \Re(x+u)$ and so on are all equal to $-1/2$. But then $\Re(y-u)=0$ and therefore $\Re(y)=\Re(u)=-1/4$. But then $\Re(x)=\Re(u)=-1/4$, which means not all of the x, y, u, v are distinct, a contradiction. □

2.3.3 MUBs Arising from the Weyl-Heisenberg Orbit

As mentioned in Chapter 1, there have been several approaches [2, 50, 83, 8, 54] in constructing MUBs. Here, we propose a new method for constructing MUBs.

Recall that unitary transformations preserve the inner product, therefore by applying an appropriate unitary transformation on any complete set $\{\mathcal{B}_0, \mathcal{B}_1, \ldots, \mathcal{B}_d\}$ of MUBs in $\mathbb{C}^d$, we may assume that $\mathcal{B}_d$ is the standard basis. In this section, we consider sets of MUBs for which $\cup_{i=0}^{d-1}\mathcal{B}_i$ is a Weyl-Heisenberg orbit. To the best of our knowledge, this is a new approach in constructing MUBs (the only other known idea [8] that uses the Weyl-Heisenberg group to construct MUBs is considering the eigenvectors of the Pauli matrices). We give a characterization theorem for the existence of such MUBs. Using this characterization, we show that such MUBs always exist for every prime dimension p. The existence of $p+1$ MUBs for any prime p is already known. We will also show that by considering a generalized Weyl-Heisenberg orbit, such MUBs also exist for a prime power dimension $p^m, m \geq 1, p \neq 2, 3$. The construction of p^m+1 MUBs in $\mathbb{C}^{p^m}$ due to Klappenecker and Rötteler [54] is essentially an example of such MUBs.

Definition 2.53. *We say that a vector* $\mathbf{z} \in \mathbb{C}^d$ *is* $\mathbb{Z}_d$-MUB-fiducial *if* $\{\mathcal{B}_0, \ldots, \mathcal{B}_{d-1}\}$ *together with the standard basis form a complete set of mutually unbiased bases, where* $\mathcal{B}_i = \left\{\mathbf{X}^i\mathbf{Y}^j\mathbf{z} \,:\, j \in \mathbb{Z}_d\right\}$, $0 \leq i \leq d-1$.

Note that if $\mathbf{z} = (z_j)$ is a $\mathbb{Z}_d$-MUB-fiducial vector in $\mathbb{C}^d$ then we must have $|z_j| = 1/\sqrt{d}$ for every $j \in \mathbb{Z}_d$. We also have

$$\langle \mathbf{X}^i\mathbf{Y}^j\mathbf{z}, \mathbf{X}^i\mathbf{Y}^{j'}\mathbf{z}\rangle = \langle \mathbf{Y}^j\mathbf{z}, \mathbf{Y}^{j'}\mathbf{z}\rangle = \sum_{k\in\mathbb{Z}_d} |z_k|^2\omega^{k(j'-j)} = \delta_{jj'}.$$

Thus, each $\mathcal{B}_i$ is an orthonormal basis by the definition.

Theorem 2.54. *A vector* $\mathbf{z} = (z_j) \in \mathbb{C}^d$ *with* $|z_j| = 1/\sqrt{d}$ *is* $\mathbb{Z}_d$*-MUB-fiducial if and only if for every* $s, t \in \mathbb{Z}_d$ *with* $0 < s \leq t \leq \lfloor d/2 \rfloor$*, the following holds:*

$$f_{s,t}(\mathbf{z}) := \sum_{j\in\mathbb{Z}_d} z_j\overline{z}_{j+s}\overline{z}_{j+t}z_{j+s+t} = 0.$$

Proof. Fix $s \in \mathbb{Z}_d \setminus \{0\}$. For every $k \in \mathbb{Z}_d$ we have $\mathbf{X}^{-s}\mathbf{Y}^k\mathbf{z} = (z_{j+s}\omega^{k(j+s)})$. Thus $\mathbf{z}^*\mathbf{X}^{-s}\mathbf{Y}^k\mathbf{z} = \sum_{j\in\mathbb{Z}_d} \overline{z}_j z_{j+s}\omega^{k(j+s)}$. This implies that

$$\begin{aligned}
|\mathbf{z}^*\mathbf{X}^{-s}\mathbf{Y}^k\mathbf{z}|^2 &= \left(\sum_{j\in\mathbb{Z}_d} z_j\overline{z}_{j+s}\omega^{-k(j+s)}\right)\left(\sum_{j'\in\mathbb{Z}_d} \overline{z}_{j'}z_{j'+s}\omega^{k(j'+s)}\right)\\
&= \sum_{j,j'\in\mathbb{Z}_d} z_j\overline{z}_{j+s}\overline{z}_{j'}z_{j'+s}\omega^{k(j'-j)}\\
&= \sum_{t\in\mathbb{Z}_d}\sum_{j\in\mathbb{Z}_d} z_j\overline{z}_{j+s}\overline{z}_{j+t}z_{j+t+s}\omega^{kt}\\
&= f_s\left(w^k\right),
\end{aligned}$$

where $f_s(x) = \sum_{t=0}^{d-1} f_{s,t}(\mathbf{z})x^t$. It follows that the vector $\mathbf{z}$ with $|z_j| = 1/\sqrt{d}$ is $\mathbb{Z}_d$-MUB-fiducial if and only if $f_s\left(\omega^k\right) = 1/d$ for every $s \in \mathbb{Z}_d \setminus \{0\}$ and $k \in \mathbb{Z}_d$. This means that $f_s(x) - 1/d$ vanishes on $\{x \in \mathbb{C} : x^d = 1\}$. Since $f_s(x) - 1/d$ is a polynomial of degree at most $d-1$, this is equivalent to the fact that $f_s(x) - 1/d$ is identically equal to zero. That is $f_{s,t}(\mathbf{z}) = 0$ when $s, t \in \mathbb{Z}_d \setminus \{0\}$ (note that $f_{s,0}(\mathbf{z}) = 1/d$ for any $\mathbf{z} = (z_j)_{j\in\mathbb{Z}_d}$ with $z_j = 1/\sqrt{d}$). Since $f_{s,t}(\mathbf{z}) = f_{t,s}(\mathbf{z})$ and

$$f_{s,-t}(\mathbf{z}) = \sum_{j\in\mathbb{Z}_d} z_j\overline{z}_{j+s}\overline{z}_{j-t}z_{j+s-t} = \sum_{j\in\mathbb{Z}_d} z_{j+t}\overline{z}_{j+t+s}\overline{z}_j z_{j+s} = \overline{f_{s,t}(\mathbf{z})},$$

we may assume $0 < s \le t \le \lfloor d/2 \rfloor$. □

When $d = q$ is a prime power, we may index the coordinates of a vector in $\mathbb{C}^q$ with $\mathbb{F}_q$, the finite field with q elements, rather than $\mathbb{Z}_q$. Equivalently, we may think of $\mathbb{C}^q$ as the set of all mappings from $\mathbb{F}_q$ to $\mathbb{C}$. Let p be prime and $q = p^m, m \ge 1$. The mapping $\mathrm{Tr}: \mathbb{F}_q \to \mathbb{F}_p$ defined by $\mathrm{Tr}\,(x) = \sum_{i=0}^{m-1} x^{p^i}$ is called the *absolute trace mapping.* It is easy to see that Tr is a p^{m-1}-to-1 $\mathbb{F}_p$-linear mapping. Let ω denote a primitive p-th root of unity in $\mathbb{C}$. The *Pauli matrices* for $\mathbb{F}_q$ are defined by their action on the standard basis $\{\mathbf{e}_x : x \in \mathbb{F}_q\}$ as follows:

$$\begin{aligned}
\mathbf{X}(s): &\quad \mathbf{e}_x \mapsto \mathbf{e}_{x+s},\\
\mathbf{Y}(s): &\quad \mathbf{e}_x \mapsto \omega^{\mathrm{Tr}(sx)}\mathbf{e}_x,
\end{aligned}$$

where $s \in \mathbb{F}_q$. Note that $\mathbf{X}(s)^p = \mathbf{Y}(s)^p = \mathbf{I}_q$.

Definition 2.55. *The set* $\{\mathbf{X}(s)\mathbf{Y}(k)\mathbf{z} : s, k \in \mathbb{F}_q\} \subset \mathbb{C}^q$ *is called the* generalized Weyl-Heisenberg orbit *of* $\mathbf{z} \in \mathbb{C}^q$*.*

For prime p, we may identify $\mathbb{F}_p$ with $\mathbb{Z}_p$ and therefore the generalized Weyl-Heisenberg orbit of a vector $\mathbf{z} \in \mathbb{C}^p$ is the same as the Weyl-Heisenberg orbit of $\mathbf{z}$.

Definition 2.56. *We say that a vector $\mathbf{z} \in \mathbb{C}^q$ is* $\mathbb{F}_q$-MUB-fiducial *if $\{\mathcal{B}_s : s \in \mathbb{F}_q\}$ together with the standard basis form a complete set of mutually unbiased bases, where $\mathcal{B}_s = \{\mathbf{X}(s)\mathbf{Y}(k)\mathbf{z} : k \in \mathbb{F}_q\}$, $s \in \mathbb{F}_q$.*

As before, if $\mathbf{z}$ is an $\mathbb{F}_q$-MUB-fiducial vector in $\mathbb{C}^q$ then we must have $|z_j| = 1/\sqrt{q}$ for every $j \in \mathbb{F}_q$. We also have

$$\langle \mathbf{X}(s)\mathbf{Y}(k)\mathbf{z}, \mathbf{X}(s)\mathbf{Y}(k')\mathbf{z}\rangle = \langle \mathbf{Y}(k)\mathbf{z}, \mathbf{Y}(k')\mathbf{z}\rangle = \sum_{t\in\mathbb{F}_q} |z_t|^2 \omega^{\mathrm{Tr}(t(k'-k))} = \delta_{kk'}.$$

Thus, each $\mathcal{B}_s$ is an orthonormal basis by the definition. The proof of the following theorem is similar to the proof of Theorem 2.54, but requires more algebraic techniques. Before we give a proof, we state the preliminary tools. Consider the multiplicative groups $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ and $\mathbb{F}_p^* = \mathbb{F}_p \setminus \{0\}$. Let $\mathbb{F}_{q:p} \subset \mathbb{F}_q$ denote a set of coset representatives of $\mathbb{F}_p^*$ in $\mathbb{F}_q^*$. That is, every element in $x \in \mathbb{F}_q^*$ may be uniquely expressed as ya for some $y \in \mathbb{F}_{q:p}$ and $a \in \mathbb{F}_p$. For every $k \in \mathbb{F}_q$ and $a \in \mathbb{F}_p$, define

$$T(k,a) = \{t \in \mathbb{F}_q^* : \mathrm{Tr}\,(kt) = a\}.$$

Since Tr is an $\mathbb{F}_p$-linear mapping, $\mathrm{Tr}\left(c^{-1}kt\right) = c^{-1}\mathrm{Tr}\,(kt)$ for every $c \in \mathbb{F}_p^*$ and therefore $T(c^{-1}k, a) = T(k, ac)$.

Theorem 2.57. *A vector $\mathbf{z} = (z_j)_{j\in\mathbb{F}_q} \in \mathbb{C}^q$ with $|z_j| = 1/\sqrt{q}$ is $\mathbb{F}_q$-MUB-fiducial if and only if for every $(s,\ell,a) \in \mathbb{F}_q^* \times \mathbb{F}_{q:p} \times \mathbb{F}_p$ we have*

$$\sum_{t\in T(\ell,a)} f_{s,t}(\mathbf{z}) = 0,$$

where $f_{s,t}(\mathbf{z}) = \sum_{j\in\mathbb{F}_q} z_j \overline{z}_{j+s} \overline{z}_{j+t} z_{j+s+t}$.

Proof. Fix $(s,k) \in \mathbb{F}_q^* \times \mathbb{F}_q$. We have $\mathbf{X}(-s)\mathbf{Y}(k)\mathbf{z} = (z_{j+s}\omega^{\mathrm{Tr}(k(j+s))})$. Thus $\mathbf{z}^*\mathbf{X}(-s)\mathbf{Y}(k)\mathbf{z} = \sum_{j\in\mathbb{F}_q} \overline{z}_j z_{j+s} \omega^{\mathrm{Tr}(k(j+s))}$. This implies that

$$\begin{aligned}
|\mathbf{z}^*\mathbf{X}(-s)\mathbf{Y}(k)\mathbf{z}|^2 &= \left(\sum_{j\in\mathbb{F}_q} z_j \overline{z}_{j+s} \omega^{-\mathrm{Tr}(k(j+s))}\right)\left(\sum_{j'\in\mathbb{F}_q} \overline{z}_{j'} z_{j'+s} \omega^{\mathrm{Tr}(k(j'+s))}\right) \\
&= \sum_{j,j'\in\mathbb{F}_q} z_j \overline{z}_{j+s} \overline{z}_{j'} z_{j'+s} \omega^{\mathrm{Tr}(k(j'-j))} \\
&= \sum_{t\in\mathbb{F}_q}\sum_{j\in\mathbb{F}_q} z_j \overline{z}_{j+s} \overline{z}_{j+t} z_{j+t+s} \omega^{\mathrm{Tr}(kt)} = \sum_{t\in\mathbb{F}_q} f_{s,t}(\mathbf{z})\omega^{\mathrm{Tr}(kt)}.
\end{aligned}$$

Since $f_{s,0}(\mathbf{z}) = 1/q$ for any vector $\mathbf{z}$ with $|z_j| = 1/\sqrt{q}$, we get

$$|\mathbf{z}^*\mathbf{X}(-s)\mathbf{Y}(k)\mathbf{z}|^2 = \begin{cases} 1/q + \sum_{a\in\mathbb{F}_p}\sum_{t\in T(k,a)} f_{s,t}(\mathbf{z})\omega^a = 1/q + g_{s,k}(\omega) & \text{if } k \neq 0, \\ 1/q + \sum_{t\in\mathbb{F}_q^*} f_{s,t}(\mathbf{z}) = 1/q + g_{s,1}(1) & \text{if } k = 0, \end{cases}$$

where $g_{s,k}(x) = \sum_{a\in\mathbb{F}_p} F_{s,k,a}(\mathbf{z})x^a$ and $F_{s,k,a}(\mathbf{z}) = \sum_{t\in T(k,a)} f_{s,t}(\mathbf{z})$. It follows that the vector $\mathbf{z}$ with $|z_j| = 1/\sqrt{q}$ is $\mathbb{F}_q$-MUB-fiducial if and only if $g_{s,1}(1) = 0$ and $g_{s,k}(\omega) = 0$ for every $s, k \in \mathbb{F}_q^*$. For any $c \in \mathbb{F}_p^*$, we have

$$F_{s,kc,a}(\mathbf{z}) = \sum_{t\in T(kc,a)} f_{s,t}(\mathbf{z}) = \sum_{t\in T(k,ac^{-1})} f_{s,t}(\mathbf{z}) = F_{s,k,ac^{-1}}(\mathbf{z}).$$

Therefore

$$g_{s,kc}(x) = \sum_{a\in\mathbb{F}_p} F_{s,kc,a}(\mathbf{z})x^a = \sum_{a\in\mathbb{F}_p} F_{s,k,ac^{-1}}(\mathbf{z})x^a = \sum_{a\in\mathbb{F}_p} F_{s,k,a}(\mathbf{z})x^{ac} = g_{s,k}(x^c).$$

Therefore the condition "$g_{s,k}(\omega) = 0$ for every $s, k \in \mathbb{F}_q^*$" is equivalent to "$g_{s,\ell}(\omega^c) = 0$ for every $(s,\ell,c) \in \mathbb{F}_q^* \times \mathbb{F}_{q:p} \times \mathbb{F}_p^*$". Also note that $g_{s,k}(1) = g_{s,1}(1)$ for every $s, k \in \mathbb{F}_q^*$. As a result, a vector $\mathbf{z}$ with $|z_j| = 1/\sqrt{q}$ is $\mathbb{F}_q$-MUB-fiducial if and only if $g_{s,\ell}(\omega^c) = 0$ for every $(s,\ell,c) \in \mathbb{F}_q^* \times \mathbb{F}_{q:p} \times \mathbb{F}_p$. This means that $g_{s,\ell}(x)$, which is a polynomial of degree at most $p-1$, vanishes on $\{x \in \mathbb{C} : x^p = 1\}$. Equivalently, $g_{s,\ell}(x)$ is identically equal to zero. That is, $\sum_{t\in T(\ell,a)} f_{s,t}(\mathbf{z}) = 0$ for every $(s,\ell,a) \in \mathbb{F}_q^* \times \mathbb{F}_{q:p} \times \mathbb{F}_p$. □

2.3.4 Classification for $d \leq 5$

In this section, we will classify all $\mathbb{Z}_d$-MUB-fiducial vectors in $\mathbb{C}^d$ for $d \leq 5$. Since for any $\mathbb{Z}_d$-MUB-fiducial vector $\mathbf{z}$ and $\theta \in \mathbb{R}$, the vector $e^{i\theta}\mathbf{z}$ is also a $\mathbb{Z}_d$-MUB-fiducial vector, we will always assume that the coordinate corresponding to $j = 0$ of any $\mathbb{Z}_d$-MUB-fiducial vector $\mathbf{z} = (z_j)_{j\in\mathbb{Z}_d}$ has argument equal to zero, that is $z_0 = 1/\sqrt{d}$. Such a $\mathbb{Z}_d$-MUB-fiducial vector is said to be *normalized*.

Theorem 2.58. *A vector $\mathbf{z} = \frac{1}{\sqrt{2}}(1,\alpha)^T \in \mathbb{C}^2$ is a normalized $\mathbb{Z}_2$-MUB-fiducial vector if and only if $\alpha^4 = -1$, i.e. $\alpha \in \{e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4}\}$.*

Proof. Using Theorem 2.54, $\mathbf{z}$ is a $\mathbb{Z}_2$-MUB-fiducial vector in $\mathbb{C}^2$ if and only if $\alpha^2 + \overline{\alpha}^2 = 0$ and $|\alpha| = 1$, which is equivalent to $\alpha^4 = -1$. □

Notice that Example 2.33 was established by taking $\alpha = e^{\pi i/4}$ in Theorem 2.58.

Theorem 2.59. *A vector* $\mathbf{z} = \frac{1}{\sqrt{3}}(1, \alpha, \beta)^T \in \mathbb{C}^3$ *is a normalized* $\mathbb{Z}_3$*-MUB-fiducial vector if and only if* $\{\alpha^3, \beta^3\} = \{e^{2\pi i/3}, e^{4\pi i/3}\}$.

Proof. Using Theorem 2.54, $\mathbf{z}$ is a $\mathbb{Z}_3$-MUB-fiducial vector in $\mathbb{C}^3$ if and only if $\overline{\alpha}^2\beta + \alpha\overline{\beta}^2 + \beta\alpha = 0$ and $|\alpha| = 1$ and $|\beta| = 1$. Dividing by $\alpha\beta$, we may rewrite this as $1 + 1/\alpha^3 + 1/\beta^3 = 0$ with $|\alpha| = 1$ and $|\beta| = 1$. This means that $\{1, 1/\alpha^3, 1/\beta^3\}$ is a normalized zero-sum set of 3 points on the unit complex circle. By Theorem 2.49, $\{1, 1/\alpha^3, 1/\beta^3\}$ must be the set of third roots of unity. Hence $\{\alpha^3, \beta^3\} = \{e^{2\pi i/3}, e^{4\pi i/3}\}$. □

Theorem 2.60. *There exists no* $\mathbb{Z}_4$*-MUB-fiducial vector in* $\mathbb{C}^4$.

Proof. Towards a contradiction, assume $\mathbf{z} = \frac{1}{2}(1, \alpha, \beta, \gamma)^T \in \mathbb{C}^4$ with $|\alpha| = |\beta| = |\gamma| = 1$ is a normalized $\mathbb{Z}_4$-MUB-fiducial vector. By letting $s = t = 1$ in Theorem 2.54, we get

$$0 = \frac{\beta}{\alpha^2} + \frac{\alpha\gamma}{\beta^2} + \frac{\beta}{\gamma^2} + \alpha\gamma = \frac{\beta}{\alpha^2\gamma^2}\left(\alpha^2 + \gamma^2\right) + \frac{\alpha\gamma}{\beta^2}\left(\beta^2 + 1\right).$$

Similarly, by letting $s = 1$ and $t = 2$ in Theorem 2.54, we get

$$0 = \frac{\gamma}{\alpha\beta} + \frac{\alpha}{\beta\gamma} + \frac{\alpha\beta}{\gamma} + \frac{\beta\gamma}{\alpha} = \frac{\left(\alpha^2 + \gamma^2\right)\left(\beta^2 + 1\right)}{\alpha\beta\gamma}.$$

The above identities imply that $\beta^2 + 1 = 0$ and $\alpha^2 + \gamma^2 = 0$. But then by considering $s = t = 2$ in Theorem 2.54, we have $f_{2,2}(\mathbf{z}) = \beta^2 + 1/\beta^2 + (\alpha/\gamma)^2 + (\gamma/\alpha)^2 = -4 \neq 0$, which is a contradiction. □

Theorem 2.61. *A vector* $\mathbf{z} = \frac{1}{\sqrt{5}}(1, \alpha, \beta, \gamma, \delta)^T \in \mathbb{C}^5$ *is a normalized* $\mathbb{Z}_5$*-MUB-fiducial vector if and only if* $\alpha = \omega^a, \beta = \omega^b, \gamma = \omega^c$ *and* $\delta = \omega^d$ *with* $a + b + c + d \equiv 0 \pmod 5$*, where* $\omega = e^{2\pi i/5}$.

Proof. By Theorem 2.54, $\mathbf{z}$ is a $\mathbb{Z}_5$-MUB-fiducial vector if and only if $|\alpha| = |\beta| = |\gamma| = |\delta| = 1$ and $(z, w, t, u) = (\alpha, \beta, \gamma, \delta)$ is a solution of

$$\begin{aligned}
f_{1,1}(\mathbf{z}) = \frac{w}{z^2} + \frac{zt}{w^2} + \frac{wu}{t^2} + \frac{t}{u^2} + zu &= 0, \\
f_{1,2}(\mathbf{z}) = \frac{t}{zw} + \frac{zu}{wt} + \frac{w}{tu} + \frac{zt}{u} + \frac{wu}{z} &= 0, \\
f_{2,2}(\mathbf{z}) = \frac{u}{w^2} + \frac{z}{t^2} + \frac{zw}{u^2} + wt + \frac{ut}{z^2} &= 0.
\end{aligned}$$

By dividing the above equations by zu, wu/z and wt, respectively, we get

$$\begin{aligned}\frac{w}{z^3u}+\frac{t}{w^2u}+\frac{w}{zt^2}+\frac{t}{u^3z}+1 &= 0, && (2.3.7)\\ \frac{t}{w^2u}+\frac{z^2}{w^2t}+\frac{z}{tu^2}+\frac{z^2t}{wu^2}+1 &= 0, && (2.3.8)\\ \frac{u}{w^3t}+\frac{z}{wt^3}+\frac{z}{u^2t}+1+\frac{u}{z^2w} &= 0. && (2.3.9)\end{aligned}$$

By considering equation (2.3.7), since $\frac{w}{z^3u}\cdot\frac{t}{w^2u}\cdot\frac{w}{zt^2}\cdot\frac{t}{u^3z}\cdot 1 = 1$, Theorem 2.52 implies that one of the following three cases occurs:

Case I. $\frac{w}{z^3u}\cdot\frac{t}{w^2u}=1$ and $\frac{w}{zt^2}\cdot\frac{t}{u^3z}=1$.

We have $t = z^3wu^2 = z^{-2}wu^{-3}$. Hence $z^5u^5 = 1$. Let $I = \langle f_{1,1}(\mathbf{z}), f_{1,2}(\mathbf{z}), f_{2,2}(\mathbf{z}), z^5u^5 - 1, t - z^3wu^2\rangle$. Using a computer algebra system, such as MAPLE ™, we may find the Gröbner basis of I with respect to any ordering is $\{1\}$ and therefore there is no solution in this case.

Case II. $\frac{w}{z^3u}\cdot\frac{w}{zt^2}=1$ and $\frac{t}{w^2u}\cdot\frac{t}{u^3z}=1$.

We have $z^4t^2u = w^2$ and $zw^2u^4 = t^2$. By letting $I = \langle f_{1,1}(\mathbf{z}), f_{1,2}(\mathbf{z}), f_{2,2}(\mathbf{z}), z^4t^2u - w^2, zw^2u^4 - t^2\rangle$, we may find that the Gröbner basis of I with respect to the pure lexicographic monomial order induced by $z > w > t > u$ is $\{z^2, w^2, t^2, u^2\}$. Hence $(z, w, t, u) = (\alpha, \beta, \gamma, \delta)$ is a desired solution if and only if $\alpha = \beta = \gamma = \delta = 0$, which is a contradiction to $|\alpha| = |\beta| = |\gamma| = |\delta| = 1$.

Case III. $\frac{w}{z^3u}\cdot\frac{t}{u^3z}=1$ and $\frac{t}{w^2u}\cdot\frac{w}{zt^2}=1$.

We get $wt = z^4u^4$ and $zwtu = 1$. Let $I = \langle f_{1,1}(\mathbf{z}), f_{1,2}(\mathbf{z}), f_{2,2}(\mathbf{z}), wt - z^4u^4, zwtu - 1\rangle$. By computing the Gröbner bases of I with respect to the pure lexicographic monomial orders induced by $z > w > t > u$ and $u > t > w > z$, it follows that if $(z, w, t, u) = (\alpha, \beta, \gamma, \delta)$ is a desired solution then $\alpha^5 = \beta^5 = \gamma^5 = \delta^5 = 1$. Thus, by letting $(z, w, t, u) = \left(\omega^a, \omega^b, \omega^c, \omega^d\right)$

with $a+b+c+d \equiv 0 \pmod 5$ (which is equivalent to $zwtu = 1$), we find that

$$\begin{aligned} f_{1,1}(\mathbf{z}) &= \omega^{b-2a} + \omega^{a+c-2b} + \omega^{b+d-2c} + \omega^{c-2d} + \omega^{a+d} \\ &= \omega^{a+d}\left(\omega^{-3a+b-d} + \omega^{-2b+c-d} + \omega^{-a+b-2c} + \omega^{-a+c-3d} + 1\right) \\ &= \omega^{a+d}\left(\omega^{2(-a+b-2c)} + \omega^{-(-a+b-2c)} + \omega^{-a+b-2c} + \omega^{-2(-a+b-2c)} + 1\right) \\ &= 0, \end{aligned}$$

and

$$\begin{aligned} f_{1,2}(\mathbf{z}) &= \omega^{-a-b+c} + \omega^{a+d-b-c} + \omega^{b-c-d} + \omega^{a+d-c} + \omega^{b+d-a} \\ &= \omega^{b+d-a}\left(\omega^{a-b+2c} + \omega^{2(a-b+2c)} + \omega^{-2(a-b+2c)} + \omega^{-(a-b+2c)} + 1\right) \\ &= 0, \end{aligned}$$

and similarly $f_{2,2}(\mathbf{z}) = 0$. This completes the proof.

□

2.3.5 A Construction for Prime Powers

Recall that for any integer $d \geq 2$, the set $\{\mathbf{X}^i\mathbf{Y}^j\mathbf{z} : i, j \in \mathbb{Z}_d\} \subset \mathbb{C}^d$ is the Weyl-Heisenberg orbit of $\mathbf{z} \in \mathbb{C}^d$. Also for any prime power q, the set $\{\mathbf{X}(a)\mathbf{Y}(b)\mathbf{z} : a, b \in \mathbb{F}_q\} \subset \mathbb{C}^q$ is the generalized Weyl-Heisenberg orbit of $\mathbf{z} \in \mathbb{C}^q$. When q is prime, these two orbits are exactly the same. The following theorem shows the existence of $q+1$ MUBs in $\mathbb{C}^q$ when q is a prime power other than powers of 2 and 3. This theorem is new, however the construction of the MUBs that results from this theorem is equivalent to the construction of the MUBs due to Klappenecker and Rötteler [54].

Theorem 2.62. *Let $p \geq 5$ be a prime number, $q = p^m$ for some $m \geq 1$, and $\omega = e^{2\pi i/p}$. Then*

$$\mathbf{z} = \frac{1}{\sqrt{q}}\left(\omega^{\mathrm{Tr}\left(x^3\right)}\right)_{x \in GF(q)}$$

is an $\mathbb{F}_q$-MUB-fiducial vector in $\mathbb{C}^q$.

Proof. For every $s, t \in \mathbb{F}_q^*$, let $f_{s,t}(\mathbf{z})$ be as defined in Theorem 2.57. Since

$$x^3 - (x+s)^3 - (x+t)^3 + (x+s+t)^3 = 6stx + 3st(s+t)$$

and Tr is a linear mapping, we get

$$\begin{aligned} f_{s,t}(\mathbf{z}) &= q^{-2} \sum_{x \in GF(q)} \omega^{\mathrm{Tr}\left(x^3\right) - \mathrm{Tr}\left((x+s)^3\right) - \mathrm{Tr}\left((x+t)^3\right) + \mathrm{Tr}\left((x+s+t)^3\right)} \\ &= q^{-2} \omega^{\mathrm{Tr}(3st(s+t))} \sum_{x \in GF(q)} \omega^{\mathrm{Tr}(6stx)}. \end{aligned}$$

Since the characteristic of the field $\mathbb{F}_q$ is neither 2 nor 3, we have $6 \neq 0$. Hence the mapping $x \mapsto \mathrm{Tr}\,(6stx)$ is a p^{m-1}-to-1 mapping from $\mathbb{F}_q$ to $\mathbb{F}_p$. Therefore $f_{s,t}(\mathbf{z}) = q^{-2} \omega^{\mathrm{Tr}(3st(s+t))} p^{m-1} \sum_{j \in \mathbb{Z}_p} \omega^j = 0$. The result follows from Theorem 2.57. □

The observation that for prime powers $q = p^m$ with $p \neq 2, 3$, there exist $q + 1$ MUBs, as we already mentioned, has been known since 1980. We would like to emphasize that the above theorem provides a construction of such complete set of MUBs that is a union of a standard basis and an orbit of a (generalized) Weyl-Heisenberg group.

As a side note, we would like to mention that Theorem 2.62 implies the following well-known result in analytic number theory:

Corollary 2.63 (Quadratic Gauss Sum for Primes)**.** *Let p be a prime and $\omega = e^{2\pi i/p}$. For any $a \in \mathbb{Z}_p \setminus \{0\}$, we have*

$$\Big| \sum_{j \in \mathbb{Z}_p} \omega^{aj^2} \Big| = \sqrt{p}.$$

Proof. The proof for $p = 2$ and $p = 3$ is straightforward. Let us assume $p \geq 5$. Let $\mathbf{z}$ be as in Theorem 2.62 with $q = p$. Note that in $\mathrm{GF}(p)$, we have $\mathrm{Tr}\,(x) = x$. Let $r \in \mathbb{Z}_p \setminus \{0\}$ be such that $3r = a$. By Theorem 2.62, we get $|\langle \mathbf{z}, \mathbf{X}^{-r}\mathbf{z} \rangle| = 1/\sqrt{p}$. On the other hand, since $|\omega^{r^3/4}| = 1$ and $\{j + r/2 : j \in \mathbb{Z}_p\} = \mathbb{Z}_p$, we have

$$|\langle \mathbf{z}, \mathbf{X}^{-r}\mathbf{z} \rangle| = p^{-1} \Big| \sum_{j \in \mathbb{Z}_p} \omega^{(j+r)^3 - j^3} \Big| = p^{-1} \Big| \omega^{\frac{r^3}{4}} \sum_{j \in \mathbb{Z}_p} \omega^{3r\left(j + \frac{r}{2}\right)^2} \Big| = p^{-1} \Big| \sum_{j \in \mathbb{Z}_p} \omega^{aj^2} \Big|.$$

□

2.4 Spherical 2-Designs

Spherical designs are another example of regular structure of lines that have been studied in various fields including frame theory, digital communication and quantum information theory. In this section, we give a brief survey on spherical designs. We also discuss their connection with (tight) equiangular set of lines and mutually unbiased bases. As an intriguing instance, we give a numerical example of a tight equiangular set of 169 lines in $\mathbb{C}^{13}$ that we obtained by using this connection. Some of the observations are new.

Let μ be the unique measure on $\mathbb{CP}^{d-1}$ which is invariant under unitary transformations and normalized so that $\int_{\mathbb{CP}^{d-1}} d\mu(\mathbf{z}) = 1$. Let $t, \ell \geq 1$ be integers. Denote $Hom(t, \ell)$ the set of polynomials in $\mathbb{C}[x_0, \ldots, x_{d-1}, y_0, \ldots, y_{d-1}]$ that are homogenous of degree t in the variables $x_0, \ldots, x_{d-1}$ and homogenous of degree ℓ in the variables $y_0, \ldots, y_{d-1}$. To every $p \in Hom(t, \ell)$ we associate the mapping $p_o(\mathbf{z}) = p(\mathbf{z}, \mathbf{z}^*)$ for $\mathbf{z} \in \mathbb{C}^d$. Since p is homogeneous, we get

$$p_o(e^{i\theta}\mathbf{z}) = e^{i\theta(t-\ell)} p_o(\mathbf{z})$$

for each $\theta \in \mathbb{R}$. Therefore, p_o is a well-defined mapping on $\mathbb{CP}^{d-1}$ only if $t = \ell$. Define

$$Hom(t,t)_o = \{p_o : p \in Hom(t,t)\},$$

the set of homogenous polynomials in $z_0, \ldots, z_{d-1}, \overline{z}_0, \ldots, \overline{z}_{d-1}$ of degree at most t. For example, given a unit vector $\mathbf{w} \in \mathbb{C}^d$, the mapping $p_o(\mathbf{z}) = |\langle \mathbf{z}, \mathbf{w} \rangle|^{2t}$ is an element in $Hom(t,t)_o$. We refer the reader to [55] for further information.

Definition 2.64. *A set $\mathcal{L} \subset \mathbb{CP}^{d-1}$ is a* spherical t-design *if*

$$\int_{\mathbb{CP}^{d-1}} f(\mathbf{z}) d\mu(\mathbf{z}) = \frac{1}{|\mathcal{L}|} \sum_{[\mathbf{z}] \in \mathcal{L}} f(\mathbf{z})$$

for every $f \in Hom(t,t)_o$. That is, the average of f over $\mathbb{CP}^{d-1}$ is equal to its average over $\mathcal{L}$.

Notice that if $\mathcal{L}$ is a t-design then $\mathcal{L}$ is also a k-design for all $1 \leq k \leq t$. For a given set of lines $\mathcal{L}$ in $\mathbb{CP}^{d-1}$, we define the *t-energy* of $\mathcal{L}$ by

$$E_t(\mathcal{L}) = \sum_{[\mathbf{v}],[\mathbf{w}] \in \mathcal{L}} |\langle \mathbf{v}, \mathbf{w} \rangle|^{2t}.$$

Recall that for any $[\mathbf{v}], [\mathbf{w}] \in \mathbb{CP}^{d-1}$, the vector $\mathbf{v}^{\otimes t}$ denotes the tensor product of $\mathbf{v}$ with itself t times. Also, recall from (1.4.2) that $\langle \mathbf{v}^{\otimes t}, \mathbf{w}^{\otimes t} \rangle = \langle \mathbf{v}, \mathbf{w} \rangle^t$. The following lemma is known.

Lemma 2.65. [55] *For any $[\mathbf{w}] \in \mathbb{CP}^{d-1}$ and integer $t \geq 1$,*

$$\int_{\mathbb{CP}^{d-1}} |\langle \mathbf{z}, \mathbf{w} \rangle|^{2t} d\mu(\mathbf{z}) = \binom{d+t-1}{t}^{-1}.$$

Proof. Since μ is invariant under unitary transformations, we may assume $\mathbf{w} = \mathbf{e}_0$. The result follows from Rudin [68, Proposition 1.4.9]. □

The following inequality is known as Welch bound [81].

Theorem 2.66. [81] *For any set of $n \geq \binom{d+t-1}{t}$ lines $\mathcal{L} \subset \mathbb{CP}^{d-1}$, we have*

$$E_t(\mathcal{L}) \geq \frac{n^2}{\binom{d+t-1}{t}}.$$

Equality holds if and only if $\mathcal{L}$ is a t-design.

Proof. Let $\overline{\mathbf{v}}$ denote the conjugate of $\mathbf{v}$. Write $\mathbf{z}_1 = n^{-1}\sum_{[\mathbf{v}]\in\mathcal{L}}(\mathbf{v}^{\otimes t} \otimes \overline{\mathbf{v}}^{\otimes t})$ and $\mathbf{z}_2 = \int_{\mathbb{CP}^{d-1}} \mathbf{v}^{\otimes t} \otimes \overline{\mathbf{v}}^{\otimes t} d\mu(\mathbf{v})$. Since

$$\langle \mathbf{v}^{\otimes t} \otimes \overline{\mathbf{v}}^{\otimes t}, \mathbf{w}^{\otimes t} \otimes \overline{\mathbf{w}}^{\otimes t}\rangle = \langle \mathbf{v}, \mathbf{w}\rangle^t \langle \overline{\mathbf{v}}, \overline{\mathbf{w}}\rangle^t = |\langle \mathbf{v}, \mathbf{w}\rangle|^{2t},$$

using Lemma 2.65, we have

$$\begin{aligned}
\langle \mathbf{z}_1, \mathbf{z}_1\rangle &= n^{-2} \sum_{[\mathbf{v}],[\mathbf{w}]\in\mathcal{L}} |\langle \mathbf{v}, \mathbf{w}\rangle|^{2t}, \\
\langle \mathbf{z}_1, \mathbf{z}_2\rangle &= n^{-1} \sum_{[\mathbf{v}]\in\mathcal{L}} \int_{\mathbb{CP}^{d-1}} |\langle \mathbf{v}, \mathbf{w}\rangle|^{2t} d\mu(\mathbf{w}) = \binom{d+t-1}{t}^{-1}, \\
\langle \mathbf{z}_2, \mathbf{z}_2\rangle &= \iint_{\mathbb{CP}^{d-1}} |\langle \mathbf{v}, \mathbf{w}\rangle|^{2t} d\mu(\mathbf{v}) d\mu(\mathbf{w}) = \binom{d+t-1}{t}^{-1}.
\end{aligned}$$

Therefore $\langle \mathbf{z}_1 - \mathbf{z}_2, \mathbf{z}_1 - \mathbf{z}_2\rangle = n^{-2}\sum_{[\mathbf{v}],[\mathbf{w}]\in\mathcal{L}} |\langle \mathbf{v}, \mathbf{w}\rangle|^{2t} - \binom{d+t-1}{t}^{-1}$. The result follows from the fact that $\langle \mathbf{z}_1 - \mathbf{z}_2, \mathbf{z}_1 - \mathbf{z}_2\rangle \geq 0$ and equality holds if and only if $\mathbf{z}_1 = \mathbf{z}_2$. By the construction of $\mathbf{z}_1$ and $\mathbf{z}_2$, this is equivalent to $\int_{\mathbb{CP}^{d-1}} f(\mathbf{v}) = n^{-1}\sum_{[\mathbf{v}]\in\mathcal{L}} f(\mathbf{v})$ for all monomials (and hence for all polynomials, by linearity) $f \in Hom(t,t)_o$. Thus equality holds if and only if $\mathcal{L}$ is a t-design. □

Recall that a tight frame (Definition 2.14) and a tight set of lines (Definition 2.24) are equivalent objects. The following result has been recently observed by the frame theory community (see [11]) and is also known to quantum information theorists (see [66]).

Corollary 2.67. *Let $\mathcal{L} \subset \mathbb{CP}^{d-1}$ be a set of $n \geq d$ lines. Then $\mathcal{L}$ is tight if and only if it is a 1-design.*

Proof. Let $\mathbf{V}$ be a $d\times n$ matrix where the columns represent the n lines in $\mathcal{L}$. Let $\mathbf{G}=\mathbf{V}^*\mathbf{V}$ be a Gram matrix of $\mathcal{L}$ and $\mathbf{S}=\mathbf{V}\mathbf{V}^*$ be its frame matrix. Let the eigenvalues of $\mathbf{S}$ be $\lambda_1,\ldots,\lambda_d$. We have

$$\begin{aligned} E_1(\mathcal{L}) &= \sum_{[\mathbf{v}],[\mathbf{w}]\in\mathcal{L}} |\langle \mathbf{v},\mathbf{w}\rangle|^2 = \mathrm{Tr}\left(\mathbf{G}\mathbf{G}^*\right) = \mathrm{Tr}\left(\mathbf{G}^2\right) = \mathrm{Tr}\left(\mathbf{S}^2\right) = \sum_{i=1}^{d} {\lambda_i}^2 \\ &\geq \frac{1}{d}\left(\sum_{i=1}^{d}\lambda_i\right)^2 = \frac{1}{d}\mathrm{Tr}\left(\mathbf{S}\right)^2 = \frac{n^2}{d}. \end{aligned}$$

By Theorem 2.66, $\mathcal{L}$ is a 1-design if and only if $E_1(\mathcal{L})=n^2/d$. The above inequality implies that the latter is equivalent to $\lambda_1=\cdots=\lambda_d=n/d$ or equivalently $\mathbf{S}=(n/d)\mathbf{I}_d$ which is the definition of a tight set of lines. □

The following theorem is due to Renes et. al [66].

Theorem 2.68. [66] *An equiangular set of d^2 lines in $\mathbb{C}^d$ is a 2-design. Conversely, any 2-design of size d^2 is an equiangular set.*

Proof. If $\mathcal{L}$ is an equiangular set of $n=d^2$ lines in $\mathbb{C}^d$ then $|\langle\mathbf{v},\mathbf{w}\rangle|^2=1/(d+1)$ for every distinct $[\mathbf{v}],[\mathbf{w}]\in\mathcal{L}$. Hence $E_2(\mathcal{L})=n^2/\binom{d+1}{2}$. Theorem 2.66 implies that $\mathcal{L}$ is a 2-design. Conversely, if $\mathcal{L}$ is a 2-design with $n=d^2$ then $E_2(\mathcal{L})=n^2/\binom{d+1}{2}$ and $E_1(\mathcal{L})=n^2/d$. Therefore in the following inequality

$$\begin{aligned} \tfrac{d^2(d-1)}{d+1} = E_2(\mathcal{L})-n &= \sum_{\mathbf{v}\neq\mathbf{w}} |\langle\mathbf{v},\mathbf{w}\rangle|^4 \\ &\geq \tfrac{1}{n(n-1)}\left(\sum_{\mathbf{v}\neq\mathbf{w}}|\langle\mathbf{v},\mathbf{w}\rangle|^2\right)^2 = \tfrac{1}{n(n-1)}\left(E_1(\mathcal{L})-n\right)^2 = \tfrac{d^2(d-1)}{d+1}, \end{aligned}$$

equality holds. Therefore all of the $|\langle\mathbf{v},\mathbf{w}\rangle|$, when $\mathbf{v}\neq\mathbf{w}$, are equal. □

Corollary 2.69. *A set $\mathcal{L}\subset\mathbb{CP}^{d-1}$ of size d^2 is an equiangular set of lines if and only if*

$$E_2(\mathcal{L}) = \sum_{[\mathbf{v}],[\mathbf{w}]\in\mathcal{L}} |\langle\mathbf{v},\mathbf{w}\rangle|^4 = \frac{2d^3}{d+1}.$$

Proof. This is an immediate corollary of Theorem 2.68 and Theorem 2.66. □

The following observation is new.

Corollary 2.70. *A tight equiangular set of $n \geq \binom{d+1}{2}$ lines in $\mathbb{C}^d$ is a 2-design if and only if $n = d^2$.*

Proof. Let $\mathcal{L}$ be a tight equiangular set of n lines in $\mathbb{C}^d$. Then $|\langle \mathbf{v}, \mathbf{w} \rangle|^4 = (n-d)^2/(d(n-1))^2$ for all distinct $[\mathbf{v}], [\mathbf{w}] \in \mathcal{L}$. Since $n \leq d^2$, we have

$$E_2(\mathcal{L}) - \frac{n^2}{\binom{d+1}{2}} = \frac{n^2(d-1)(d^2-n)}{d^2(d+1)(n-1)} \geq 0,$$

and equality holds if and only if $n = d^2$. The result follows from Theorem 2.66. □

Even though tight equiangular sets of n lines in $\mathbb{C}^d$, with $\binom{d+1}{2} \leq n < d^2$, are not 2-designs, they are still the optimal solutions to the optimization problem described below. Notice that the following bound is weaker than the bound given in Theorem 2.66, but it holds for any set of lines of any size greater than or equal to d. The following theorem generalizes Theorem 2.68 and Corollary 2.69. To the best of our knowledge, this result is not documented in the literature.

Theorem 2.71. *For any set of $n \geq d$ lines $\mathcal{L} \subset \mathbb{CP}^{d-1}$, we have*

$$E_2(\mathcal{L}) \geq n + \frac{n(n-d)^2}{d^2(n-1)}.$$

Moreover, given $d \leq n \leq d^2$, a set $\mathcal{L}$ is a tight equiangular set of n lines in $\mathbb{C}^d$ if and only if

$$E_2(\mathcal{L}) = n + \frac{n(n-d)^2}{d^2(n-1)}.$$

Proof. By Theorem 2.66, we have $E_1(\mathcal{L}) \geq n^2/d$. Hence

$$\begin{aligned} E_2(\mathcal{L}) - n &= \sum_{\mathbf{v} \neq \mathbf{w}} |\langle \mathbf{v}, \mathbf{w} \rangle|^4 \\ &\geq \frac{1}{n(n-1)} \left(\sum_{\mathbf{v} \neq \mathbf{w}} |\langle \mathbf{v}, \mathbf{w} \rangle|^2 \right)^2 = \frac{1}{n(n-1)} \left(E_1(\mathcal{L}) - n \right)^2 \\ &\geq \frac{1}{n(n-1)} \left(\frac{n^2}{d} - n \right)^2 = \frac{n(n-d)^2}{d^2(n-1)}. \end{aligned}$$

Therefore, equality holds if and only if $|\langle \mathbf{v}, \mathbf{w} \rangle|^2$, when $\mathbf{v} \neq \mathbf{w}$, are all equal to $\frac{n-d}{d(n-1)}$. □

Recall from Definition 1.34 that the Weyl-Heisenberg orbit of a vector $\mathbf{z} \in \mathbb{C}^d$ is the set $\left\{\left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right] : j, k \in \mathbb{Z}_d\right\}$. If an equiangular set of d^2 lines is also the Weyl-Heisenberg orbit of a vector $\mathbf{z} \in \mathbb{C}^d$ then we may reduce the number of variables in the objective function in Theorem 2.71 from $O(d^3)$ to $O(d)$. This is an immediate corollary of Corollary 2.69.

Corollary 2.72. *For a given $\mathbf{z} \in \mathbb{C}^d$, the set $\left\{\left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right] : j, k \in \mathbb{Z}_d\right\}$ is an equiangular set of d^2 lines if and only if*

$$\sum_{i,j=0}^{d-1} |\langle \mathbf{z}, \mathbf{X}^i\mathbf{Y}^j\mathbf{z}\rangle|^4 = \frac{2d}{d+1}.$$

Using the `Minimize` command in Maple ™ we have found such vectors $\mathbf{z} \in \mathbb{C}^d$ with high precision up to dimension $d = 21$. Such a vector $\mathbf{z}$ is called a fiducial vector and is throughly discussed in Chapter 3. Using the `PSLQ` algorithm, which is built-in in Maple ™, we have found the minimal polynomial of each coordinate of many of these fiducial vectors. Let $z = re^{i\theta}$ be one of the coordinates of a fiducial vector in $\mathbb{C}^d$. We observed empirically that the degree of the minimal polynomial of z grows exponentially in d. However, the minimal polynomials of r and $\tan\theta$ grow linearly in d. Specifically, the minimal polynomial of r has only even terms, thus one may consider the minimal polynomial of r^2. We also observed that certain integer multiples of r^2 (depending on d) have minimal polynomials with significantly smaller coefficients. Analogously, the minimal polynomial of $\tan\theta$ has also even terms and is 'almost' reciprocal.

Example 2.73. Using Corollary 2.72, we observed that there are six non-equivalent (up to phase shift, conjugation, rotation, and reflection) fiducial vectors in $\mathbb{C}^8$. Here is an example of a minimal polynomial of $12r^2$, where r is the absolute value of the first coordinate of one of the six fiducial vectors in $\mathbb{C}^8$:

$$\begin{gathered} x^{16} - 32\,x^{15} + 468\,x^{14} - 4128\,x^{13} + 24462\,x^{12} - 103088\,x^{11} \\ +320288\,x^{10} - 751328\,x^9 + 1343683\,x^8 - 1813296\,x^7 + 1789664\,x^6 \\ -1240160\,x^5 + 597150\,x^4 - 229520\,x^3 + 91580\,x^2 - 29792\,x + 4049. \end{gathered}$$

Here is the same polynomial for the second coordinate:

$$x^2 - 3x + 1.$$

In fact, the minimal polynomial of each of the other coordinates is one of the above. Here is the minimal polynomial of $\tan^2\theta$, where θ is the argument of one of the coordinates of one of the six fiducial vectors in $\mathbb{C}^8$:

$$x^8 - 408x^7 + 7752x^6 - 48168x^5 + 124578x^4 - 144504x^3 + 69768x^2 - 11016x + 81.$$

You may observe that the coefficient of $x^i, (i = 0, \ldots, 4)$ is equal to the coefficient of x^{8-i} times 3^{4-i}.

Example 2.74. Here is one of the intriguing examples of a numerical fiducial vector that we have found in $\mathbb{C}^{13}$. Let

$$\begin{aligned}
r_0 &= 0.41639853560612059231342885948408030331982133602243146906 75... \\
r_1 = r_3 = r_9 &= 0.08973318891027385718805855508724363337452297833588295660 22... \\
r_2 = r_5 = r_6 &= 0.20739482701870860527464855998835934495057759643705423553 71... \\
r_4 = r_{10} = r_{12} &= 0.19954300470062551439915188974915550637270348828872899771 71... \\
r_7 = r_8 = r_{11} &= 0.42971542869354670663348599593982721514457336745459471451 19...
\end{aligned}$$

and

$$\begin{aligned}
t_0 &= 0 \\
t_1 = t_3 + 8 = t_9 - 2 &= 4.02186834054336278123895829672554019456748575121629 97... \\
t_2 = t_5 + 4 = t_6 - 4 &= 3.84157862535396359948068047917255648590733925229161 84... \\
t_4 = t_{10} + 1 = t_{12} + 3 &= -1.09128661596191010362387365521927573236863049448246... \\
t_7 = t_8 = t_{11} - 2 &= 1.67366986623323989545134157003254034474526176211815 24...
\end{aligned}$$

Then $\mathbf{z} = \left(r_j e^{2\pi i t_j/13}\right) \in \mathbb{C}^{13}$ satisfies $||\langle \mathbf{X}^j \mathbf{Y}^k \mathbf{z}, \mathbf{z} \rangle|^2 - 1/14| \leq 10^{-30}$. Notice that $r_{3j} = r_j$ and $t_{3j} - t_j \in \mathbb{Z}$ for all $j \in \mathbb{Z}_{13}$.

Chapter 3

Fiducial Vectors

In this chapter, we study the properties of the equiangular sets of lines that form an orbit under the action of the Weyl-Heisenberg group on $\mathbb{CP}^{d-1}$. It is widely believed by physicists [85, 4, 66, 42, 33] that for every dimension d such an orbit exists. A vector whose Weyl-Heisenberg orbit produces an equiangular set of lines is called a *fiducial* vector. We will consider several types of fiducial vectors such as *almost flat*, *argument Legendre*, and *real Legendre*. We will also explore the fiducial vectors where the absolute values of their coordinates take only 2 different values. The argument Legendre fiducial vectors are almost flat and are discussed by Appleby [4] in specific dimensions. Since the real Legendre fiducial vectors have very similar properties to the argument Legendre ones and also all of the coordinates of such vectors have the same argument, we have also investigated this class of fiducial vectors. We will also prove that there is no fiducial vector for which the absolute values of the coordinates form a periodic sequence. Throughout this chapter, some nontrivial properties of the Legendre symbol are used several times in the proof of the theorems. We refer the reader to Section 3.6 for more details.

All of the results in this chapter, except the cited ones, are new and are published in [53].

3.1 The Characterizing Identities

In Theorem 3.3, we give a new characterization of fiducial vectors, one that simplifies and significantly reduces the number of equations that must be solved to find a fiducial vector. This theorem is new and is extremely useful when proving the rest of the results obtained in this chapter.

Recall that the *Pauli matrices* for $\mathbb{Z}_d$ are defined by their action on the standard basis $\{\mathbf{e}_j : j \in \mathbb{Z}_d\}$ of $\mathbb{C}^d$ as follows:

$$\begin{aligned} \mathbf{X}: &\quad \mathbf{e}_j \mapsto \mathbf{e}_{j+1}, \\ \mathbf{Y}: &\quad \mathbf{e}_j \mapsto \omega^j \mathbf{e}_j, \end{aligned}$$

where $\omega = e^{2\pi i/d}$. Almost all of the known constructions of maximum equiangular sets of lines are Weyl-Heisenberg orbits. That is, they are of the form $\left\{\left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right] : j,k \in \mathbb{Z}_d\right\} \subset \mathbb{CP}^{d-1}$ for some $\mathbf{z} \in \mathbb{C}^d$ (To the best of our knowledge, the only known exceptions are the sets of 36 lines in $\mathbb{C}^6$ and 64 lines in $\mathbb{C}^8$ constructed by Grassl [42] and the set of 64 lines in $\mathbb{C}^8$ constructed by Hoggar [46]; Hoggar uses the group $\mathbb{Z}_2^3$ instead of $\mathbb{Z}_8$). Recall from comments prior to Definition 1.34 that the quotient group $\mathcal{H}_d = \{\mathbf{X}^j\mathbf{Y}^k\langle\omega\mathbf{I}_d\rangle : j,k \in \mathbb{Z}_d\}$ acts on $\mathbb{CP}^{d-1}$, however to simplify the terminology we refer to the set $\left\{\left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right] : j,k \in \mathbb{Z}_d\right\} \subset \mathbb{CP}^{d-1}$ as the Weyl-Heisenberg orbit of $\mathbf{z} \in \mathbb{C}^d$.

Definition 3.1. *A unit vector* $\mathbf{z} \in \mathbb{C}^d$ *is called* fiducial *if* $\left\{\left[\mathbf{X}^j\mathbf{Y}^k\mathbf{z}\right] : j,k \in \mathbb{Z}_d\right\} \subset \mathbb{CP}^{d-1}$ *is an equiangular set of lines.*

It is widely believed that for every d there exists a fiducial vector in $\mathbb{C}^d$ (for example see [85, 4, 66, 42, 33]). As an abstract object, the equiangular set of d^2 lines in $\mathbb{C}^d$ has been discussed in different contexts. For example, in quantum information theory it is a *symmetric informationally complete positive operator valued measurement (SIC-POVM)*, which is composed of d^2 rank-one operators all of whose operator inner products are equal. In the quantum information theory community, there has been notable interest to construct such SIC-POVMs in every dimension and most of the focus has been on SIC-POVMs which are invariant under the Weyl-Heisenberg group (i.e. the SIC-POVMs that arise from fiducial vectors). As we briefly discussed in Section 1.7, equiangular lines have several applications to quantum information such as quantum fingerprinting [70], quantum tomography [19] and quantum cryptographic protocols [34]. They also play a role in the Bayesian formulation of the quantum mechanics [19, 34] where they make nice standard quantum measurements. Equiangular lines have also been studied in the context of spherical codes and designs [28].

One of the interesting properties of an equiangular set of lines of the form $\{[\mathbf{gz}] : \mathbf{g} \in G\}$ is that with certain assumptions on G, instead of checking the equality of $\binom{|G|}{2}$ inner products, one may only need to check $|G|$ of them.

Lemma 3.2. *Let G be a set of $d \times d$ complex matrices such that $\mathbf{I}_d \in G$ and for every $\mathbf{A}, \mathbf{B} \in G$ we have $\mathbf{A}^* \in G$ and $\lambda\mathbf{AB} \in G$ for some $\lambda \in \mathbb{C}$ with $|\lambda| = 1$. Let $\mathbf{z} \in \mathbb{C}^d$ be a unit vector. Then $\{[\mathbf{gz}] : \mathbf{g} \in G\}$ is an equiangular set of lines if and only if $|\mathbf{z}^*\mathbf{gz}| = c$ for every $\mathbf{g} \in G \setminus \{\mathbf{I}_d\}$. Here c is the cosine of the common angle between the lines.*

Note that since $\mathcal{H}_d$, introduced above, is a group, the set $\{\mathbf{X}^j\mathbf{Y}^k : j, k \in \mathbb{Z}_d\}$ is closed under matrix multiplication up to a scalar factor of absolute value 1. It is also closed under the conjugate transpose operator and contains the identity matrix.

For a given dimension d, by definition, a fiducial vector may be viewed as a solution of a system of multivariate polynomials in $z_0, \ldots, z_{d-1}, \overline{z_0}, \ldots, \overline{z}_{d-1}$ over the field $\mathbb{Q}(\omega)$. The following theorem shows that one need only consider $\mathbb{Q}$ instead of $\mathbb{Q}(\omega)$ and it gives a different characterization of fiducial vectors. The following theorem is new.

Theorem 3.3. *A vector $\mathbf{z} = (z_j) \in \mathbb{C}^d$ is fiducial if and only if for every $(s, t) \in \mathbb{Z}_d \times \mathbb{Z}_d$ with $0 \leq s \leq t \leq \lfloor d/2 \rfloor$ the following identities hold:*

$$f_{s,t}\left(\mathbf{z}\right) := \sum_{j \in \mathbb{Z}_d} z_j \overline{z}_{j+s} \overline{z}_{j+t} z_{j+s+t} = \frac{\delta_{s0} + \delta_{t0}}{d+1}.$$

Proof. For every $k \in \mathbb{Z}_d$ we have $\mathbf{X}^{-s}\mathbf{Y}^k\mathbf{z} = (z_{j+s}\omega^{k(j+s)})$. Thus, we get $\mathbf{z}^*\mathbf{X}^{-s}\mathbf{Y}^k\mathbf{z} = \sum_{j \in \mathbb{Z}_d} \overline{z}_j z_{j+s}\omega^{k(j+s)}$. This implies that

$$\begin{aligned}
|\mathbf{z}^*\mathbf{X}^{-s}\mathbf{Y}^k\mathbf{z}|^2 &= \left(\sum_{j \in \mathbb{Z}_d} z_j \overline{z}_{j+s}\omega^{-k(j+s)}\right)\left(\sum_{j' \in \mathbb{Z}_d} \overline{z}_{j'} z_{j'+s}\omega^{k(j'+s)}\right) \\
&= \sum_{j,j' \in \mathbb{Z}_d} z_j \overline{z}_{j+s} \overline{z}_{j'} z_{j'+s}\omega^{k(j'-j)} \\
&= \sum_{t \in \mathbb{Z}_d} \sum_{j \in \mathbb{Z}_d} z_j \overline{z}_{j+s} \overline{z}_{j+t} z_{j+t+s}\omega^{kt} \\
&= f_s\left(w^k\right),
\end{aligned}$$

where $f_s(x) = \sum_{t=0}^{d-1} f_{s,t}(\mathbf{z})x^t$. It follows that the vector $\mathbf{z}$ is fiducial if and only if

$$f_s\left(\omega^k\right) = \begin{cases} 1 & \text{for } (s,k) = (0,0), \\ \\ \frac{1}{d+1} & \text{for } (s,k) \neq (0,0). \end{cases} \tag{3.1.1}$$

Let $\Omega_d = \{x \in \mathbb{C} : x^d = 1\}$. For $s = 0$, the above identity holds if and only if $f_0(x) - 1/(d+1)$ vanishes on $\Omega_d \backslash \{1\}$ and $f_0(1) = 1$, that is $\sum_{t \in \mathbb{Z}_d} f_{0,t}(\mathbf{z}) = 1$. For every $s \neq 0$, identity (3.1.1) holds if and only if $f_s(x)-1/(d+1)$ vanishes on Ω_d. Since $f_s(x)-1/(d+1)$ is a polynomial of degree at most $d-1$, this is equivalent to the the fact that $f_s(x)$ is identically equal to zero. That is $f_{s,t}(\mathbf{z})=0$ when $t \neq 0$, and $f_{s,0}(\mathbf{z})=1/(d+1)$. By combining the above cases, we get the desired result. Since $f_{s,t}(\mathbf{z})=f_{t,s}(\mathbf{z})=\overline{f_{s,-t}(\mathbf{z})}$, we may assume $0<s\leq t\leq \lfloor d/2\rfloor$. □

Remark. We have noted that the above theorem has also been rediscovered independently in [5], a few months after the original submission of [53].

By letting $t=0$ in Theorem 3.3, we get the following necessary conditions for a vector to be fiducial.

Corollary 3.4. *Let $\mathbf{z}=(r_je^{i\theta_j})$, where $r_j\in\mathbb{R}$ and $\theta_j\in[0,2\pi)$, be a fiducial vector in $\mathbb{C}^d$. Then the following identities hold:*

$$\sum_{j\in\mathbb{Z}_d} r_j^2 r_{j+s}^2 = \frac{1+\delta_{s0}}{d+1}. \tag{3.1.2}$$

Remark. Note that Corollary 3.4 gives a necessary condition (only using the absolute values of the coordinates) on whether a vector is fiducial.

A note on equiangular vectors. A set of vectors in $\mathbb{R}^d$ is called equiangular if the inner product between every two distinct vectors in the set is a constant. Note the difference between equiangular vectors and equiangular lines where we require the absolute value of the inner products to be a constant. Now, assume that $\mathbf{z}=(r_je^{i\theta_j})$, where $r_j\in\mathbb{R}$ and $\theta_j\in[0,2\pi)$, is a fiducial vector in $\mathbb{C}^d$. Also, let $\mathbf{v}=\left(\sqrt{\frac{d+1}{2}r_j^2}\right)$. Then, using Corollary 3.4, one may observe that $S=\{\mathbf{X},\mathbf{X}\mathbf{v},\ldots,\mathbf{X}^{d-1}\mathbf{v}\}$ is a set of d equiangular vectors on the unit sphere in $\mathbb{R}^d$ with common angle 60°. Note that the set S is unique up to a unitary transformation $\mathbf{Q}$. This is because the matrix whose set of columns is S can be decomposed to $\mathbf{QR}$, where $\mathbf{Q}$ is a unitary and $\mathbf{R}$ is an upper triangular matrix.

3.2 Almost Flat Fiducial Vectors

In this section, we consider fiducial vectors in which the coordinates take exactly two distinct absolute values. This is a generalization of a known result that is discussed below.

A vector in $\mathbb{C}^d$ is called *flat* if all its coordinates have the same absolute value. It is proved [36] that there are at most d^2-d+1 flat equiangular lines in $\mathbb{C}^d$ (and there are exactly $d^2 - d + 1$ such lines when $d - 1$ is a prime power). We will discuss this in more detail in Section 4.2. In particular, no flat fiducial vectors exist (this can also be concluded easily from Corollary 3.4). To take it one step further, we say a vector is *almost flat* if it is flat except for one coordinate. Appleby [4] constructed fiducial vectors in dimensions 7 and 19 which are almost flat. Using an eigenvalue argument, Roy [67] proved that for almost flat fiducial vectors in $\mathbb{C}^d$, the absolute values of the coordinates are determined in terms of d. We provide an alternative proof of this fact here.

Theorem 3.5. [67] *Let* $\mathbf{z}$ *be a fiducial vector in* $\mathbb{C}^d$ *such that one coordinate of* $\mathbf{z}$ *has absolute value* b*, and all other coordinates have absolute value* a*. Then*

$$a^2 = \frac{1 \mp 1/\sqrt{d+1}}{d}, \quad b^2 = \frac{1 \pm (d-1)/\sqrt{d+1}}{d}.$$

Proof. Since $\mathbf{z}$ is a unit vector, we have $b^2 + (d-1)a^2 = 1$. By letting $s = 0$ in Corollary 3.4, we get $b^4 + (d-1)a^4 = 2/(d+1)$. Solving for a^2 and b^2, we get the stated values. □

Remark. Note that $(a^2, b^2) = ((1 + 1/\sqrt{d+1})/d, (1 - (d-1)/\sqrt{d+1})/d)$ is only possible for $d \leq 3$, since we must have $a^2, b^2 \geq 0$.

In fact, we can prove a stronger result. Namely, the existence of a cyclic difference set in $\mathbb{Z}_d$ is a necessary condition for the existence of fiducial vectors in which the coordinates take exactly two distinct absolute values. Before stating the result, recall that a (d, k, λ)-*cyclic difference set* is a set $D = \{\alpha_1, \ldots, \alpha_k\} \subseteq \mathbb{Z}_d$ such that each element in $\mathbb{Z}_d \setminus \{0\}$ can be represented as a difference $\alpha_i - \alpha_j$ in exactly λ different ways (see for example [13] and [10]). The following theorem is new.

Theorem 3.6. *Let* $a \neq b$ *be real numbers and* k, d *be integers such that* $0 < k \leq d/2$*. Let* $\mathbf{z} = (z_j) \in \mathbb{C}^d$ *be a fiducial vector such that* k *coordinates of* $\mathbf{z}$ *have absolute value* b*, and all other coordinates have absolute value* a*. Let* $D = \{j \in \mathbb{Z}_d : |z_j| = b\}$*. Then*

$$a^2 = \frac{1}{d}\left(1 \mp \sqrt{\frac{k(d-1)}{(d+1)(d-k)}}\right), \quad b^2 = \frac{1}{d}\left(1 \pm \sqrt{\frac{(d-k)(d-1)}{k(d+1)}}\right),$$

and D *forms a* (d, k, λ)*-cyclic difference set in* $\mathbb{Z}_d$*. In particular,* $d - 1$ *must divide* $k(k-1)$*.*

Proof. By letting $s = 0$ in Corollary 3.4 and the fact that $\mathbf{z}$ is a unit vector, it follows that

$$kb^2 + (d-k)a^2 = 1, \quad kb^4 + (d-k)a^4 = 2/(d+1).$$

It is easy to see that if $k = 0$ then no a and b exist. Thus $k \geq 1$. Solving for a^2 and b^2, we get

$$a^2 = \frac{1}{d}\left(1 \mp \sqrt{\frac{k(d-1)}{(d+1)(d-k)}}\right), \qquad b^2 = \frac{1}{d}\left(1 \pm \sqrt{\frac{(d-k)(d-1)}{k(d+1)}}\right).$$

Hence

$$(a^2 - b^2)^2 = \frac{d-1}{d^2(d+1)}\left(\frac{k}{d-k} + \frac{d-k}{k} + 2\right) = \frac{d-1}{(d+1)(d-k)k}. \tag{3.2.1}$$

Let $N_s(x, y) = |\{i \in \mathbb{Z}_d : |z_i| = x, |z_{i+s}| = y\}|$. Since there are k coordinates that have absolute value b and $d - k$ coordinates that have absolute value a, we have

$$N_s(b, b) + N_s(b, a) = \quad k \quad = N_s(b, b) + N_s(a, b). \tag{3.2.2}$$

$$N_s(a, a) + N_s(a, b) = \quad d - k \quad = N_s(a, a) + N_s(b, a). \tag{3.2.3}$$

On the other hand, by Corollary 3.4 we have

$$N_s(a, a)a^4 + N_s(b, b)b^4 + (N_s(a, b) + N_s(b, a))a^2b^2 = \frac{1}{d+1}$$

for every $s \in \mathbb{Z}_d \setminus \{0\}$. Thus, by using identities (3.2.2) and (3.2.3), this can be rewritten as $(N_s(b, b) - k)(a^2 - b^2)^2 = -1/(d + 1)$. Substituting identity (3.2.1) implies that

$$N_s(b, b) = k - \frac{(d-k)k}{d-1} = \frac{k(k-1)}{d-1} := \lambda$$

is independent of s. By definition of D and $N_s(b, b)$, this means that every $s \in \mathbb{Z}_d \setminus \{0\}$ can be represented as a difference of two distinct elements of D in exactly λ different ways. □

Note that Theorem 3.5 is a special case ($k = 1$) of Theorem 3.6.

Remark. Note that the condition $(a^2, b^2) = ((1 + \sqrt{k(d-1)/(d+1)/(d-k)})/d, (1 - \sqrt{(d-k)(d-1)/(d+1)/k})/d)$ is only possible for $d \leq 2k + 1$.

3.3 Argument Legendre Fiducial Vectors

One of the main results of this section is Theorem 3.11, where we prove that the construction of fiducial vectors in the specific dimensions 7 and 19 by Appleby [4] essentially does not generalize. Inspired by his constructions, we introduce the argument Legendre fiducial vectors.

Let p denote a prime number. For every $j \in \mathbb{Z}_p$ let $\left(\frac{j}{p}\right)$ denote the Legendre symbol, that is $\left(\frac{j}{p}\right)$ is 0 (respectively 1 or -1) if $j = 0$ (respectively if j is a quadratic or a non-quadratic residue). The *resultant* of two polynomials $P(x) = A\prod_{i=1}^{n}(x - \alpha_i)$ and $Q(x) = B\prod_{i=1}^{m}(x - \beta_i)$ in $\mathbb{C}[x]$ is defined to be the

$$\operatorname{Res}(P, Q) = A^m B^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

In particular, $P(x)$ and $Q(x)$ have a common root if and only if $\operatorname{Res}(P, Q) = 0$.

Definition 3.7. *We say a fiducial vector* $\mathbf{z} = (z_j) \in \mathbb{C}^p$ *is* argument Legendre (AL) *if there exist* $a, b, \theta \in \mathbb{R}$ *such that*

$$z_j = \begin{cases} b & \textit{if } j = 0, \\ ae^{i\left(\frac{j}{p}\right)\theta} & \textit{if } j \neq 0. \end{cases}$$

Note that AL fiducial vectors are almost flat. Thus, by Theorem 3.5 and its succeeding remark, if $p > 3$ then we must have $a^2 = (1 - 1/\sqrt{p+1})/p$ and $b^2 = (1 + (p-1)/\sqrt{p+1})/p$. In fact, if an AL fiducial vector exists in $\mathbb{C}^p$, $p \equiv 3 \pmod 4$, then the value of θ is also determined in terms of p (see Proposition 3.9 below). The case $p \equiv 1 \pmod 4$ is more complicated and the value of θ is restricted to only four values. This is mainly because Lemma 3.17 (iii), Lemma 3.18 and Lemma 3.19, which are essential in our calculations, only hold when p is congruent to 3 modulo 4 and there seems to be no analogous formulation for primes that are congruent to 1 modulo 4.

Proposition 3.8. *Let* $p \equiv 1 \pmod 4$. *If* $\mathbf{z} \in \mathbb{C}^p$ *is an AL fiducial vector with parameters* (a, b, θ) *then* $c = \cos\theta$ *satisfies*

$$\left(-2\,c^2 + 4\,\psi\,c - 6\,\psi^2 + \psi^4 + 1\right)\left(-2\,c^2 + 4\,\psi\,c - 2\,\psi^2 + \psi^4 - 3\right) = 0,$$

where $\psi = \sqrt{2 + \sqrt{p+1}}$.

Proof. Let $\delta = \sqrt{p+1}$. Hence $\psi = \sqrt{\delta + 2}$. By Theorem 3.5, we have $a = 1/\sqrt{\delta(\delta+1)}$ and $b = \psi/\sqrt{\delta(\delta+1)}$. By definition, we must have $|\sum_{j\in\mathbb{Z}_p} z_j\overline{z}_{j+1}|^2 = 1/(p+1)$. Since $\left(\frac{-1}{p}\right) = 1$, using Lemma 3.18, we may rewrite this as

$$\begin{aligned}\frac{1}{p+1} &= \left|z_0\overline{z}_1 + z_{-1}\overline{z}_0 + \sum_{j\in\mathbb{Z}_p\setminus\{0,-1\}} z_j\overline{z}_{j+1}\right|^2\\ &= \left|ab\Big(e^{-i\theta}+e^{i\theta}\Big) + a^2\left(\sum_{j\in\mathbb{Z}_p\setminus\{0,-1\}} e^{i\left(\left(\frac{j}{p}\right)-\left(\frac{j+1}{p}\right)\right)\theta}\right)\right|^2\\ &= \left|2ab\cos\theta + a^2\left(\frac{1}{2}(p-3)+\frac{1}{4}\left(p-1\right)e^{2i\theta}+\frac{1}{4}\left(p-1\right)e^{-2i\theta}\right)\right|^2\\ &= \left(2abc+\frac{a^2}{2}\left(p-4+2c^2\right)\right)^2.\end{aligned}$$

By making the above substitutions for a, b, p, and δ and factoring out the non-zero terms, the previous expression can be written as

$$\left(-2\,c^2+4\,\psi\,c-6\,\psi^2+\psi^4+1\right)\left(-2\,c^2+4\,\psi\,c-2\,\psi^2+\psi^4-3\right)=0.$$

□

Proposition 3.8 shows that when $p \equiv 1 \pmod 4$ the value of θ in an AL fiducial vector is restricted to only four values, as mentioned above. However, when $p \equiv 3 \pmod 4$, the value of θ is determined in terms of p. For the rest of this section, we will only work with primes that are congruent to 3 modulo 4.

Proposition 3.9. *Let $p > 3$ such that $p \equiv 3 \pmod 4$. If $\mathbf{z} \in \mathbb{C}^p$ is an AL fiducial vector with parameters (a, b, θ) then*

$$\theta = \begin{cases}\cos^{-1}(1/\sqrt{2+\sqrt{p+1}}) & \text{for } p \equiv 3 \pmod 8,\\ \cos^{-1}(-\sqrt{\frac{2+\sqrt{p+1}}{p+1}}) & \text{for } p \equiv 7 \pmod 8.\end{cases} \tag{3.3.1}$$

Proof. Let $c = \cos\theta$, $\delta = \sqrt{p+1}$, and $\psi = \sqrt{\delta+2}$. By Theorem 3.5, we have $a = 1/\sqrt{\delta(\delta+1)}$ and $b = \psi/\sqrt{\delta(\delta+1)}$. By definition, we must have $|\sum_{j\in\mathbb{Z}_p} z_j\overline{z}_{j+1}|^2 = 1/(p+1)$. Using Lemma 3.18 and Lemma 3.19, we may rewrite this as

$$(2bc+(p-1)ac^2-a)^2+4(1-c^2)(b-ac)^2 = 1/a^2(p+1). \tag{3.3.2}$$

By making the above substitutions for a, b, p, and δ and factoring out the non-zero terms, the previous expression can be written as

$$P(c) := (\psi c-1)\left((\psi^2-2)c+\psi\right)\left((\psi^2-2)(\psi^2-4)c^2+2\psi c+\psi^2-6\right)=0. \tag{3.3.3}$$

Let $f_{s,t}(\mathbf{z})$ be as defined in Theorem 3.3. Using Lemma 3.19 and Lemma 3.20, we get

$$f_{1,-1}(\mathbf{z}) = \begin{cases} a^4(p-3)c^2(2c^2-1) + 2a^3b(4c^3-3c) + a^2b^2 & \text{for } p \equiv 3 \pmod 8 \\ a^4c^2(p(2c^2-1)+2c^2-5) + 2a^3bc + a^2b^2 & \text{for } p \equiv 7 \pmod 8 \end{cases}$$

Note that $f_{1,-1}(\mathbf{z}) = 0$ by Theorem 3.3. As before, both polynomials on the right hand side can be factored in $\mathbb{R}[\psi]$. After factoring out the non-zero terms, we get the following: If $p \equiv 3 \pmod 8$ then

$$Q_1(c) := (\psi c - 1)\left(2(\psi^2-4)c^3 + 2\psi c^2 - (\psi^2-6)c - \psi\right) = 0. \tag{3.3.4}$$

The only common root of the equations (3.3.3) and (3.3.4) is $c = 1/\psi$. This is because the resultant of $P(c)/(\psi c - 1)$ and $Q_1(c)/(\psi c - 1)$ is equal to

$$8\psi^3(\psi-1)^2(\psi+1)^2(\psi-2)^2(\psi+2)^2 \neq 0,$$

since $\psi > 2$. Therefore $\theta = \cos^{-1}\left(1/\sqrt{2+\sqrt{p+1}}\right)$, as desired. If $p \equiv 7 \pmod 8$ then

$$Q_2(c) := \left((\psi^2-2)c+\psi\right)\left(2(\psi^2-2)c^3 - 2\psi c^2 - (\psi^2-4)c + \psi\right) = 0. \tag{3.3.5}$$

Again, since the resultant of $P(c)/\left((\psi^2-2)c+\psi\right)$ and $Q_2(c)/\left((\psi^2-2)c+\psi\right)$ is

$$-8\,(\psi-1)^2\,(\psi+1)^2\,\left(\psi^2-6\right)\left(\psi^2-2\right)^5 \neq 0,$$

it follows that the only common root of the equations (3.3.3) and (3.3.5) is $c = -\psi/(\psi^2-2)$ and therefore we must have $\theta = \cos^{-1}\left(-\sqrt{\frac{2+\sqrt{p+1}}{p+1}}\right)$ in this case. □

Remark. For $p > 19$ the quadratic factor in equation (3.3.3) is always positive. Therefore equation (3.3.3) simplifies to $(\psi c - 1)\left((\psi^2-2)c+\psi\right) = 0$ for $p > 19$.

Remark. The key in the proof of Proposition 3.9 is that equation (3.3.2) factors over $\mathbb{R}[\psi]$ as given in equation (3.3.3). Equation (3.3.2) is also stated in Roy's PhD dissertation [67, p. 89].

By using Theorem 3.3 it is easy to check that the vector $(\sqrt{2/3}, e^{i\pi/3}/\sqrt{6}, e^{-i\pi/3}/\sqrt{6})$ is an AL fiducial vector in $\mathbb{C}^3$. The construction of AL fiducial vectors in $\mathbb{C}^7$ and $\mathbb{C}^{19}$ is given by Appleby in [4]. However, a proof that the given vectors are in fact fiducial is not given in his work. One may interpret that the proofs are basic but require some extensive tedious algebra. We will give a short proof that Appleby's vectors [4] are fiducial.

Theorem 3.10. *AL fiducial vectors exist for $p = 7$ and $p = 19$.*

Proof. Let $f_{s,t}(\mathbf{z})$ be as defined in Theorem 3.3. Recall from Theorem 3.3 (and the remark following it) that an AL fiducial vector $\mathbf{z} \in \mathbb{C}^p$ with parameters a, b, and $c = \cos\theta$ exists if and only if the system of equations

$$\begin{gathered} f_{0,0}(\mathbf{z}) - 2/(p+1) = f_{0,r}(\mathbf{z}) - 1/(p+1) = f_{s,t}(\mathbf{z}) = 0, \\ \text{where } 0 < r \leq \lfloor p/2 \rfloor \text{ and } 0 < s \leq t \leq \lfloor p/2 \rfloor, \end{gathered} \tag{3.3.6}$$

has a solution. If $p = 7$, we may easily verify that

$$\begin{aligned} f_{0,0}(\mathbf{z}) &= 6a^4 + b^4, \\ f_{0,1}(\mathbf{z}) = f_{0,2}(\mathbf{z}) = f_{0,3}(\mathbf{z}) &= 5a^4 + 2a^2b^2, \\ f_{1,1}(\mathbf{z}) = f_{2,2}(\mathbf{z}) = f_{3,3}(\mathbf{z}) &= 4a^4c^2(4c^2 - 3) + a^2b^2 + 2a^3bc, \\ f_{1,2}(\mathbf{z}) = f_{1,3}(\mathbf{z}) = f_{2,3}(\mathbf{z}) &= 4a^4c^2 - a^4 + 4a^3bc(2c^2 - 1). \end{aligned}$$

It is therefore straightforward to check that the system (3.3.6) has a solution for $p = 7$ when

$$a = \sqrt{\tfrac{4-\sqrt{2}}{28}}, \quad b = \sqrt{\tfrac{2+3\sqrt{2}}{14}}, \quad c = \cos\theta = -\tfrac{\sqrt{\sqrt{2}+1}}{2}.$$

(the values of a, b, and θ are taken from Theorem 3.5 and Proposition 3.9.)

Analogously for $p = 19$, we have

$$\begin{aligned} f_{0,0}(\mathbf{z}) &= 18a^4 + b^4, \\ f_{0,r}(\mathbf{z}) &= 17a^4 + 2a^2b^2, \\ f_{r,r}(\mathbf{z}) &= 16a^4c^2(2c^2 - 1) + a^2b^2 + 2a^3bc(4c^2 - 3), \\ f_{r,2r}(\mathbf{z}) = f_{r,7r}(\mathbf{z}) = \overline{f_{r,8r}(\mathbf{z})} = \overline{f_{r,9r}(\mathbf{z})} &= a^4(16c^4 - 4c^2 + 3) + 4a^3bc(2c^2 - 1), \\ f_{r,3r}(\mathbf{z}) = f_{r,4r}(\mathbf{z}) = f_{r,5r}(\mathbf{z}) = \overline{f_{r,6r}(\mathbf{z})} &= 4a^4c^2 - a^4 + 4a^3bc(2c^2 - 1), \end{aligned}$$

for all $r \in \mathbb{Z}_{19}$ such that $1 \leq r \leq 9$. A direct evaluation at

$$a = \sqrt{\tfrac{10-\sqrt{5}}{190}}, \quad b = \sqrt{\tfrac{5+9\sqrt{5}}{95}}, \quad c = \cos\theta = \sqrt{\tfrac{\sqrt{5}-1}{8}}$$

shows that the system (3.3.6) has a solution for $p = 19$. □

Using Maple ™ and equation (3.3.2), Roy [67] confirms (numerically) that there are no other AL fiducial vectors for any odd $p < 400$. We conjecture that AL fiducial vectors only exist for $p \in \{3, 7, 19\}$ (see Conjecture 4.29). Except for a set of primes with density zero, we are able to confirm this conjecture, as follows.

Theorem 3.11. *For every prime p such that $p \equiv 3 \pmod 4$, there exists no AL fiducial vector in $\mathbb{C}^p$ unless $p \in \mathcal{P}$, where $\mathcal{P}$ is a set with zero density (in the set of all primes that are congruent to 3 modulo 4).*

In fact, in the proof of Theorem 3.11, we will see that $\mathcal{P}$ is the set of primes $p > 7$ such that $t(p) = -3$ and $p \equiv 11$ or $19 \pmod{24}$, where $t(p)$ denotes the trace of the Frobenius endomorphism of the elliptic curve $y^2 = x(x+1)(x+2)(x+3)$:

$$t(p) = -\sum_{x \in \mathbb{Z}_p} \left(\frac{x(x+1)(x+2)(x+3)}{p} \right).$$

The fact that the set $\mathcal{P}$ has density zero follows from Theorem 20 in [72].

Proof. Let $\mathbf{z} = (z_j)$ be an AL fiducial vector in $\mathbb{C}^p$ with parameters a, b, $c = \cos\theta$. We already know that such vector exists for $p = 3$ and $p = 7$. So assume $p > 7$. As in the proof of Proposition 3.9, by letting $\delta = \sqrt{p+1}$, and $\psi = \sqrt{\delta + 2}$ we get $a = 1/\sqrt{\delta(\delta+1)}$ and $b = \psi\, a$. Also, by Proposition 3.9 we have $c = 1/\psi$ if $p \equiv 3 \pmod 8$ and $c = -\psi/(\psi^2 - 2)$ if $p \equiv 7 \pmod 8$. Now, by letting $q = t(p)$ and using Lemma 3.19 and Lemma 3.20 we get the following: If $p \equiv 23 \pmod{24}$ then

$$f_{1,2}(\mathbf{z}) = (p + 2 - q)a^4c^4 + 2(q-3)a^4c^2 + 4a^3bc - qa^4$$

and if $p \not\equiv 23 \pmod{24}$ then

$$f_{1,2}(\mathbf{z}) = (p - 6 - q)a^4c^4 + 8a^3bc^3 + 2(q+1)a^4c^2 - 4a^3bc - qa^4.$$

By Theorem 3.3, we must have $f_{1,2}(\mathbf{z}) = 0$. Since a, b, c and p can be described in terms of ψ, we can describe $f_{1,2}(\mathbf{z})$ in terms of q and ψ. Solving for q, we get:

$$q = t(p) = \begin{cases} -3 & \text{for } p \equiv 11 \text{ or } 19 \pmod{24} \\ -\psi^2(3\psi^2 - 8)/(\psi^2 - 4)^2 & \text{for } p \equiv 23 \pmod{24} \\ \psi^2(5\psi^2 - 24)/(\psi^2 - 4)^2 & \text{for } p \equiv 7 \pmod{24} \end{cases}$$

For $p \equiv 23 \pmod{24}$ we can easily check that q is not an integer (in fact, if $p = 24\ell + 23$ and $\ell > 13$ then $-4 < q < -3$). This is impossible since $q = t(p)$ is an integer by definition. Similarly, the case $p \equiv 7 \pmod{24}$ when $p \neq 7$ is excluded. Thus the set

$$\mathcal{P} = \{p : p \text{ is prime}, \ p \equiv 11 \text{ or } 19 \pmod{24}, \ p > 7, \ t(p) = -3\}$$

has the desired properties. As mentioned before, the fact that the set $\mathcal{P}$ has density zero follows from Theorem 20 in [72]. □

Remark. By considering the identity $f_{1,4}(\mathbf{z}) = 0$ in the previous theorem, we may further restrict the forbidden set $\mathcal{P}$ to its proper subset $\{p \in \mathcal{P} | t'(p) = -3\}$, where $t'(p) = -\sum_{j\in\mathbb{Z}_p} \left(\frac{j(j+1)(j+4)(j+5)}{p}\right)$. Since this subset of $\mathcal{P}$ is still non-empty and has the same density as $\mathcal{P}$, namely zero, we have skipped the details.

3.4 Real Fiducial Vectors

We say a fiducial vector $\mathbf{z}$ of dimension d is *real* if $\mathbf{z} \in \mathbb{R}^d$.

Example 3.12. By Theorem 3.3, a vector $\mathbf{z} = (a, b, c) \in \mathbb{R}^3 \subset \mathbb{C}^3$ is fiducial if and only if $a^4 + b^4 + c^4 - 1/2 = a^2b^2 + b^2c^2 + c^2a^2 - 1/4 = abc(a + b + c) = 0$. It is easy to see that $(0, 1/\sqrt{2}, 1/\sqrt{2})$ is a solution to this system and is thus a real fiducial vector.

It seems that real fiducial vectors rarely exist as the assumption $\mathbf{z} \in \mathbb{R}^d$ is rather strong. On the other hand, searching for such fiducial vectors should be easier since one needs to deal with fewer variables (see the discussion before Corollary 2.72). In fact, the number of unknown real variables in a real fiducial vector in $\mathbb{C}^d$ is only d compared to the number of unknown real variables in a general fiducial vector in $\mathbb{C}^d$ which is $2d - 1$ (we may always assume $z_0 \in \mathbb{R}$). Despite this fact, we are able to find real fiducial vectors in dimension 7 and 19 where the coordinates only take 3 distinct values.

It would be quite interesting to know whether real fiducial vectors in dimensions other than $3, 7$, and 19 exist. In this section, we will discuss a special type of real fiducial vectors (called real Legendre) which have similar characteristics to the argument Legendre fiducial vectors. The consideration of real fiducial vectors is our idea.

3.4.1 Real Legendre Fiducial Vectors

Let p be a prime number. We call a fiducial vector $\mathbf{z} = (z_j) \in \mathbb{C}^p$ *real Legendre (RL)* if there exist $a, b, c \in \mathbb{R}$ such that

$$z_j = \begin{cases} a & \text{if } j = 0, \\ b & \text{if } \left(\frac{j}{p}\right) = 1, \\ c & \text{if } \left(\frac{j}{p}\right) = -1. \end{cases}$$

In the next two theorems, we will show that real Legendre fiducial vectors exist for $p \in \{7, 19\}$. Both of the results are new.

Theorem 3.13. *Let $\{\pm a\}$ be the set of real roots of $56\,x^4+8\,x^2-1$ and let $\{\pm b,\pm c\}$ be the set of real roots of $3136\,x^8-2240\,x^6+568\,x^4-56\,x^2+1$ with $a<0<b,c$. Then the RL vector $(a,b,b,c,b,c,c)\in\mathbb{R}^7$ is a fiducial vector in $\mathbb{C}^7$.*

Proof. By Theorem 3.3, a vector $\mathbf{z}=(\alpha,\beta,\beta,\gamma,\beta,\gamma,\gamma)\in\mathbb{R}^7$ is fiducial if and only if (α,β,γ) satisfies the following system:

$$\begin{aligned}
f_{0,0}(\mathbf{z}) &= \alpha^4+3(\beta^4+\gamma^4)=1/4,\\
f_{0,1}(\mathbf{z})=f_{0,2}(\mathbf{z})=f_{0,3}(\mathbf{z}) &= \alpha^2(\beta^2+\gamma^2)+\beta^4+\gamma^4+3\,\beta^2\gamma^2=1/8,\\
f_{1,1}(\mathbf{z})=f_{2,2}(\mathbf{z})=f_{3,3}(\mathbf{z}) &= (2\alpha(\beta+\gamma)+\beta^2+\gamma^2+\beta\gamma)\beta\gamma=0,\\
f_{1,2}(\mathbf{z})=f_{1,3}(\mathbf{z})=f_{2,3}(\mathbf{z}) &= \alpha^2\beta\gamma+\alpha(\beta^3+\gamma^3)+\beta\gamma(\beta+\gamma)^2=0.
\end{aligned}$$

Let $I=\langle f_{0,0}(\mathbf{z})-1/4, f_{0,1}(\mathbf{z})-1/8, f_{1,1}(\mathbf{z}), f_{1,2}(\mathbf{z})\rangle$. Using a computer algebra system, such as MAPLE ™, we may find the Gröbner basis G_γ of I with respect to the pure lexicographic monomial order induced by $\alpha>\beta>\gamma$. We observe that $G_\gamma=\{h(\gamma),\beta-f(\gamma),\alpha-g(\gamma)\}$, where

$$\begin{aligned}
h(x) &= 3136\,x^8-2240\,x^6+568\,x^4-56\,x^2+1,\\
f(x) &= -8/23\,x(784\,x^6-707\,x^4+184\,x^2-14),\\
g(x) &= -1/23\,x(9408x^6-3976\,x^4+276\,x^2+39).
\end{aligned}$$

Hence, if $(\alpha,\beta,\gamma)=(a,b,c)$ is a solution of the mentioned system of equations, we must have $h(c)=0$. Similarly, we get $h(b)=0$ and $56\,a^4+8\,a^2-1=0$. Now, since $h(0)=1>0$ and $h(1/4)<0$, we may assume $c\in(0,1/4)$. On the interval $(0,1/4)$, we have $f(x)>0$ and $g(x)<0$. Therefore $b=f(c)>0$ and $a=g(c)<0$. □

Remark. Since every fiducial vector has unit length, we have added the polynomial $\alpha^2+3\,\beta^2+3\,\gamma^2-1$ to the set of generators of I to reduce the degree of the polynomials in the Gröbner bases.

Theorem 3.14. *Let $\{\pm a\}$ be the set of real roots of $76\,x^4+10\,x^2-5$ and let $\{\pm b,\pm c\}$ be the set of real roots of $144400\,x^8-34200\,x^6+3640\,x^4-160\,x^2+1$ with $b<0<a,c$. Then the RL vector in $\mathbb{C}^{19}$ with parameters (a,b,c) is a fiducial vector.*

Proof. The given RL vector $\mathbf{z}\in\mathbb{R}^{19}$ is fiducial if and only if $(\alpha,\beta,\gamma)=(a,b,c)$ is a solution to the following system:

$$\begin{aligned}
f_{0,0}(\mathbf{z}) &= \alpha^4 + 9(\beta^4 + \gamma^4) = 1/10,\\
f_{0,1}(\mathbf{z}) &= \alpha^2(\beta^2 + \gamma^2) + 4(\beta^4 + \gamma^4) + 9\,\beta^2\gamma^2 = 1/20,\\
f_{1,1}(\mathbf{z}) &= abc(\alpha + \beta + \gamma) + 2(\beta + \gamma)^2(\beta^2 + \gamma^2) = 0,\\
f_{1,2}(\mathbf{z}) &= 2\,\alpha\beta\gamma(\beta + \gamma) + \beta^4 + 3\,\beta^3\gamma + 7\,\beta^2\gamma^2 + 3\,\beta\gamma^3 + \gamma^4 = 0,\\
f_{1,3}(\mathbf{z}) &= \alpha(\beta + \gamma)(\beta^2 + \gamma^2) + 5\beta\gamma(\beta^2 + b\gamma + \gamma^2) = 0.
\end{aligned}$$

The rest of the proof is similar to the the proof of Theorem 3.13. □

Remark. As in dimension 7, adding the polynomial $\alpha^2 + 9\,\beta^2 + 9\,\gamma^2 - 1$ to the set of generators of I would reduce the degree of the polynomials in the Gröbner bases.

The following result is an analogous version of Theorem 3.11 for RL vectors.

Theorem 3.15. *For every prime p such that $p \equiv 3 \pmod 4$, there exists no RL fiducial vector in $\mathbb{C}^p$ unless $p \in \mathcal{P}$, where $\mathcal{P}$ is a set with zero density (in the set of all primes that are congruent to 3 modulo 4).*

Since the proof of the above theorem is similar to that of Theorem 3.11 and only involves some basic algebra, we have omitted the proof. However, in the proof of the Theorems 3.11 and 3.15, one can see that the exact same set $\mathcal{P}$ satisfies the conditions of these two theorems. This strongly suggests that one may find a one-to-one correspondence between the set of AL fiducial vectors and the set of RL fiducial vectors. If such a transformation is found then the proof of one of the mentioned theorems can be skipped. Now let us look at a crucial group for which a fiducial vector is invariant. We will discuss briefly why such a transformation (if any) cannot be in this group.

Let $\mathrm{C}(d)$ denote the *Clifford group*, the group of all unitary operations $\mathbf{U}$ which normalize the generalized Pauli group $\mathrm{GP}(d)$, i.e. $\mathbf{U}\,\mathrm{GP}(d)\,\mathbf{U}^* = \mathrm{GP}(d)$. Let $\mathbf{J}$ be the mapping that maps $(z_j) \in \mathbb{C}^d$ to $(\overline{z_j})$. The *extended Clifford group* is the group consisting of $\mathrm{C}(d)$ and all elements of the form $\mathbf{JU}$, where $\mathbf{U} \in \mathrm{C}(d)$. This group is denoted by $\mathrm{EC}(d)$. The relevance of the (extended) Clifford group to the equiangular set of lines arising from $\mathrm{GP}(d)$ has been discussed by several authors (for example see [4, 41]). Note that if $\mathbf{z}$ is a fiducial vector and $\mathbf{U} \in \mathrm{EC}(d)$ then $\mathbf{Uz}$ is also a fiducial vector. Therefore $\mathrm{EC}(d)$ lies in the automorphism group of the set of fiducial vectors in $\mathbb{C}^d$. Appleby [4] proves that for odd d the group $\mathrm{EC}(d)$ modulo its centre $\mathrm{I}(d)$ is isomorphic to the group $\mathrm{ESL}(2, \mathbb{Z}_d) \wr (\mathbb{Z}_d \times \mathbb{Z}_d)$, where $\mathrm{ESL}(2,\mathbb{Z}_d)$ denotes the group of all 2×2 matrices over $\mathbb{Z}_d$ with determinant equal to ± 1 and $\wr$ denotes the wreath product. On page 17 in [4], Appleby also describes a method to find the stability group of a given fiducial vector $\mathbf{z}\in\mathbb{C}^d$, the set of all $\mathbf{U}\in\mathrm{EC}(d)/\mathrm{I}(d)$ for which $\mathbf{z}$ is eigenvector. Applying the same method, it turns out that the stability group of the RL fiducial vector in dimension 7 (from Theorem 3.13) is isomorphic to the order 3 subgroup generated by

$$[\begin{pmatrix} -3 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} -3 \\ 0 \end{pmatrix}].$$

But the stability group of the AL fiducial vector in dimension 7 (from Theorem 3.10) is isomorphic to the order 6 subgroup (see [4]) generated by

$$[\begin{pmatrix} -2 & 0 \\ 0 & -3 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}],$$

and therefore the two AL and RL fiducial vectors in dimension 7 do not belong to the same orbit under the action of the extended Clifford group. Therefore, the transformation discussed in the previous paragraph cannot be found in $\mathrm{EC}(d)$. Similar argument shows that the two AL and RL fiducial vectors in dimension 19 do not belong to the same orbit under the action of the extended Clifford group. In fact, the stability group of the RL fiducial vector in dimension 19 (from Theorem 3.14) is isomorphic to the order 9 subgroup generated by

$$[\begin{pmatrix} 9 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} 11 \\ 0 \end{pmatrix}],$$

whereas the stability group of the AL fiducial vector in dimension 19 (from Theorem 3.10) is isomorphic to the order 18 subgroup (see [4]) generated by

$$[\begin{pmatrix} -9 & 0 \\ 0 & -2 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \end{pmatrix}].$$

3.5 Periodic Fiducial Vectors

We say that a sequence $(a_j)_{j\in\mathbb{Z}_d}$ is *periodic* if there exists $p\in\mathbb{Z}_d\setminus\{0\}$ such that $a_{j+p}=a_j$ for every $j\in\mathbb{Z}_d$. The smallest such p is called the *period* of the sequence. The following result is new.

Proposition 3.16. *There exists no fiducial vector in $\mathbb{C}^d$ such that the absolute values of its coordinates form a periodic sequence.*

Proof. Towards a contradiction assume that such a fiducial vector, namely $\mathbf{z} = (z_j)$, exists. Let p be the period of the sequence $(|z_j|^2)_{j\in\mathbb{Z}_d}$ and let $d = pk$ for some integer $k > 1$. For $j = 0 \ldots p-1$, let $R_j = |z_j|^2$. It follows from Corollary 3.4 that

$$k \cdot \sum_{j=0}^{p-1} R_j R_{j+s} = \frac{1+\delta_{s0}}{pk+1}.$$

We also know that $\sum_{j=0}^{p-1} R_j = 1/k$. By substituting the above values in the identity $\left(\sum_j R_j\right)^2 = \sum_j R_j^2 + \sum_{i\neq j} R_i R_j$, we get

$$\frac{1}{k^2} = \frac{2}{k(pk+1)} + (p-1)\cdot\frac{1}{k(pk+1)}.$$

Simplifying the above equation, we get $k = 1$, which is a contradiction. □

3.6 Number Theory Results

Here, we state some properties of the Legendre symbol that were used in the proof of theorems in this chapter.

For every $j \in \mathbb{Z}_p$ recall that $\left(\frac{j}{p}\right)$ denotes the the Legendre symbol. The basic properties of the Legendre symbol can be found in almost any introductory number theory textbook (for example see [3]). Also recall that $t(p)$ denotes the trace of the Frobenius endomorphism of the elliptic curve $y^2 = x(x+1)(x+2)(x+3)$:

$$t(p) = -\sum_{j\in\mathbb{Z}_p}\left(\frac{j(j+1)(j+2)(j+3)}{p}\right).$$

The following lemma is quite straightforward, but we include it for the sake of completeness:

Lemma 3.17. *For every odd prime p, we have*

(i) $\sum_{j\in\mathbb{Z}_p}\left(\frac{j}{p}\right) = 0$,

(ii) $\sum_{j\in\mathbb{Z}_p}\left(\frac{j(j+s)}{p}\right) = -1$ *for every fixed* $s \in \mathbb{Z}_p \setminus \{0\}$.

(iii) *If* $p \equiv 3 \pmod 4$ *then* $\sum_{j\in\mathbb{Z}_p}\left(\frac{(j-s)j(j+s)}{p}\right) = 0$ *for every fixed* $s \in \mathbb{Z}_p$.

Proof. Since $(-x)^2 = x^2$, there is at least one non-square $y \in \mathbb{Z}_p$. Since the Legendre symbol is multiplicative, we get $\left(\frac{yx}{p}\right) = -\left(\frac{x}{p}\right)$. This implies (i), because y is invertible. We have $\left(\frac{j^2}{p}\right) = 1$. Thus $\sum_{j\in\mathbb{Z}_p}\left(\frac{j(j+s)}{p}\right) = \sum_{j\in\mathbb{Z}_p\setminus\{0\}}\left(\frac{1+sj^{-1}}{p}\right) = -\left(\frac{1}{p}\right) = -1$ by (i). If $p \equiv 3 \pmod 4$ we have $\left(\frac{-x}{p}\right) = -\left(\frac{x}{p}\right)$. Since $(-j)^3 - (-j) = -(j^3 - j)$, we immediately get (iii). □

In the next three lemmas, we count the number of fixed points of certain maps on $\mathbb{Z}_p$ that involve the Legendre symbol $\left(\frac{j}{p}\right)$. The lemmas are very similar, but none of them quite implies another one and therefore we have included them all. However, since the proofs are similar, we have only presented one of the proofs. The key idea in all of them is to count the number of elements of the set $\{j \in \mathbb{Z}_p : (\left(\frac{j}{p}\right), \left(\frac{j+1}{p}\right), \ldots, \left(\frac{j+t-1}{p}\right)) = C\}$ for every given constant $C \in \{-1,1\}^t$. We will do this for $t = 2$, $t = 3$, and $t = 4$, respectively, in the next three lemmas.

Lemma 3.18. *For every odd prime p and $s \in \mathbb{Z}_p \setminus \{0\}$ and $j \in \mathbb{Z}_p$, let*

$$\kappa(j) = \left(\frac{j}{p}\right) - \left(\frac{j+s}{p}\right).$$

Also let $K(c) = |\{j : \kappa(j) = c\}|$. Then

$$K(0) = \tfrac{1}{2}(p-3), \quad K(2) = \tfrac{1}{4}\left(p - 1 - \left(\tfrac{-s}{p}\right) + \left(\tfrac{s}{p}\right)\right), \quad K(-2) = \tfrac{1}{4}\left(p - 1 + \left(\tfrac{-s}{p}\right) - \left(\tfrac{s}{p}\right)\right).$$

Proof. For every $\alpha = (\alpha_0, \alpha_1) \in \{-1,1\} \times \{-1,1\}$, let

$$k_p(\alpha) = \frac{1}{4}\sum_{j\in\mathbb{Z}_p\setminus\{0,-s\}}\left(\alpha_0\left(\frac{j}{p}\right)+1\right)\left(\alpha_1\left(\frac{j+s}{p}\right)+1\right).$$

By applying Lemma 3.17, we get

$$\begin{aligned} 4\,k_p(\alpha) &= (p - \alpha_0\alpha_1) - \left(\alpha_1\left(\frac{s}{p}\right)+1\right) - \left(\alpha_0\left(\frac{-s}{p}\right)+1\right) \\ &= p - 2 - \alpha_0\alpha_1 - \alpha_0\left(\frac{-s}{p}\right) - \alpha_1\left(\frac{s}{p}\right). \end{aligned} \tag{3.6.1}$$

On the other hand, for every $\delta \in \{-1,1\}$ and $x \neq 0$, the value of the expression

$$\frac{1}{2}\left(\delta\left(\frac{x}{p}\right)+1\right)$$

is equal to 1 if $\left(\frac{x}{p}\right) = \delta$ and 0 otherwise. Therefore $k_p(\alpha) = |\{j \in \mathbb{Z}_p : \left(\frac{j}{p}\right) = \alpha_0, \left(\frac{j+s}{p}\right) = \alpha_1\}|$. Hence $K(0) = k_p(1,1) + k_p(-1,-1)$, $K(2) = k_p(1,-1)$, and $K(-2) = k_p(-1,1)$. The result follows immediately using (3.6.1). □

Lemma 3.19. *For every prime p such that $p \equiv 3 \pmod 4$, and $j \in \mathbb{Z}_p$, let*

$$\mu(j) = 2\left(\frac{j}{p}\right) - \left(\frac{j-1}{p}\right) - \left(\frac{j+1}{p}\right).$$

Also let $M(c) = |\{j : \mu(j) = c, j \neq 0\}|$. Then

$$\begin{aligned} M(0) &= \begin{cases} \frac{1}{4}(p-3) & \textit{for } p \equiv 3 \pmod 8, \\ \\ \frac{1}{4}(p-7) & \textit{for } p \equiv 7 \pmod 8, \end{cases} \\ M(2) = M(-2) &= \frac{1}{4}(p-3), \\ M(4) = M(-4) &= \begin{cases} \frac{1}{8}(p-3) & \textit{for } p \equiv 3 \pmod 8, \\ \\ \frac{1}{8}(p+1) & \textit{for } p \equiv 7 \pmod 8. \end{cases} \end{aligned}$$

Remark. Note that the equality $k_p(\alpha_0, \alpha_1) = m_p(1, \alpha_0, \alpha_1) + m_p(-1, \alpha_0, \alpha_1)$ does not necessarily hold, where

$$m_p(\beta, \alpha_0, \alpha_1) = \frac{1}{8} \sum_{j \in \mathbb{Z}_p \setminus \{0, \pm 1\}} \left(\beta\left(\frac{j-1}{p}\right) + 1\right)\left(\alpha_0\left(\frac{j}{p}\right) + 1\right)\left(\alpha_1\left(\frac{j+1}{p}\right) + 1\right).$$

This is why Lemma 3.18 can not be implied from Lemma 3.19.

Lemma 3.20. *For every prime p such that $p \equiv 3 \pmod 4$, and $j \in \mathbb{Z}_p$, let*

$$\nu(j) = \left(\frac{j+3}{p}\right) - \left(\frac{j+2}{p}\right) - \left(\frac{j+1}{p}\right) + \left(\frac{j}{p}\right).$$

Also let $N(c) = |\{j : \nu(j) = c\}|$. Then

$$\begin{aligned} N(0) &= \frac{1}{8}\left(3p - 10 - 3t(p) - 2\left(\left(\frac{2}{p}\right) + 1\right)\left(\left(\frac{3}{p}\right) + 1\right)\right), \\ N(2) = N(-2) &= \frac{1}{4}\left(p - 4 + t(p)\right), \\ N(4) = N(-4) &= \frac{1}{16}\left(p - 6 - t(p) + 2\left(\left(\frac{2}{p}\right) + 1\right)\left(\left(\frac{3}{p}\right) + 1\right)\right), \end{aligned}$$

where

$$t(p) = -\sum_{j \in \mathbb{Z}_p} \left(\frac{j(j+1)(j+2)(j+3)}{p}\right).$$

Chapter 4

Constructions of Equiangular Sets of Lines

In this chapter, we discuss some known constructions of equiangular set of lines in complex spaces. We also give some new methods for constructing specific equiangular set of lines in complex and quaternionic spaces.

4.1 The Regular d-Simplex

The most intuitive construction of a tight equiangular set of lines is obtained by considering an orthonormal basis. This gives d lines in a d-dimensional space for every d. To take this one step further, one may consider a regular simplex to get a tight equiangular set of $d+1$ lines in a d-dimensional space for every d. We study this object in detail, especially because we will need it in Section 4.4. Notice that by letting $k = 2$ in Corollary 2.20, it follows that there exists no tight equiangular set of $d+2$ lines in $\mathbb{A}^d$ for all $d > \dim_{\mathbb{R}} \mathbb{A}$.

Consider the standard basis $\mathcal{B} = \{\mathbf{e}_j : j \in \mathbb{Z}_{d+1}\}$ of $\mathbb{C}^{d+1}$ and let

$$\mathbf{m} = \frac{1}{d+1}\left(\sum_{j\in\mathbb{Z}_{d+1}} \mathbf{e}_j\right) = \frac{1}{d+1}\mathbf{1}_{d+1},$$

where $\mathbf{1}_{d+1}$ is the all-ones vector of dimension $d+1$. If you consider each $\mathbf{e}_j$ as a point in the $(d+1)$-dimensional complex space, then $\mathcal{B}$ is called the *regular d-simplex* and $\mathbf{m}$ may be considered as its center of mass. Consider the following set of lines:

$$\mathcal{R} = \left\{ \left[\frac{\mathbf{e}_j - \mathbf{m}}{|\mathbf{e}_j - \mathbf{m}|} \right] : j \in \mathbb{Z}_{d+1} \right\}. \tag{4.1.1}$$

Since all of the vectors $\mathbf{e}_j - \mathbf{m}$ are orthogonal to the all-ones vector $\mathbf{1}_{d+1}$, they all lie in the d-dimensional subspace ${\mathbf{1}_{d+1}}^{\perp}$ of $\mathbb{C}^{d+1}$. This means that $\mathcal{R}$ is in fact a set of $d+1$ lines in $\mathbb{C}^d$. We also have

$$\langle \mathbf{e}_i - \mathbf{m}, \mathbf{e}_j - \mathbf{m} \rangle = \delta_{ij} - \frac{2}{d+1} + \frac{d+1}{(d+1)^2} = \delta_{ij} - \frac{1}{d+1}.$$

Therefore for every distinct $\mathbf{v}, \mathbf{w} \in \mathcal{R}$, we have

$$\langle \mathbf{v}, \mathbf{w} \rangle = \frac{-1/(d+1)}{1 - 1/(d+1)} = -\frac{1}{d},$$

which is exactly the relative bound in Theorem 2.13 with $n = d+1$. Hence $\mathcal{R}$ is a tight equiangular set of $d+1$ lines in $\mathbb{C}^d$, which is often referred to as the *regular d-simplex.*

Definition 4.1. *The set of lines $\mathcal{R}$ given in equation (4.1.1) is called the* regular d-simplex*.*

Let $\mathbf{V}_{\mathcal{R}}$ denote the $(d+1) \times (d+1)$ matrix with the column vectors $(\mathbf{e}_j - \mathbf{m})/|\mathbf{e}_j - \mathbf{m}|$, where $j \in \mathbb{Z}_{d+1}$, as its columns. Then

$$\mathbf{V}_{\mathcal{R}} = a\mathbf{I}_{d+1} + b\mathbf{J}_{d+1},$$

where

$$a = \sqrt{\frac{d}{d+1}}, \quad b = -\frac{1}{\sqrt{d(d+1)}}, \tag{4.1.2}$$

gives a different but equivalent presentation of the regular d-simplex.

Example 4.2. Here, we give an explicit construction of the regular 5-simplex in $\mathbb{R}^5$. Consider the set C of columns of the 6×6 matrix

$$\mathbf{V}_{\mathcal{R}} = \sqrt{\tfrac{5}{6}}\mathbf{I}_6 - \tfrac{1}{\sqrt{30}}\mathbf{J}_6 = \tfrac{1}{\sqrt{30}}(5\mathbf{I}_6 - \mathbf{J}_6).$$

For every distinct $\mathbf{v}, \mathbf{w} \in C$ we have $\langle \mathbf{v}, \mathbf{w} \rangle = -1/5$ and $\langle \mathbf{v}, \mathbf{v} \rangle = 1$. Since every vector in C is orthogonal to the all-ones vector $\mathbf{1}_6$, we may embed C in $\mathbb{R}^5$. To give such an embedding, note that the rows of the following matrix are mutually orthogonal:

$$\begin{pmatrix} 1 & -1 & 0 & 0 & 0 & 0 \\ 1 & 1 & -2 & 0 & 0 & 0 \\ 1 & 1 & 1 & -3 & 0 & 0 \\ 1 & 1 & 1 & 1 & -4 & 0 \\ 1 & 1 & 1 & 1 & 1 & -5 \\ 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Hence, by normalizing each row of the above matrix we get a 6×6 unitary matrix $\mathbf{U}$. Since $\mathbf{U}$ preserves the inner product and $(\mathbf{U}\mathbf{v})_6 = 0$ for every $\mathbf{v} \in C$, the mapping $\phi : \mathbb{R}^6 \to \mathbb{R}^5$ defined by $\phi(\mathbf{v}) = ((\mathbf{U}\mathbf{v})_1, (\mathbf{U}\mathbf{v})_2, (\mathbf{U}\mathbf{v})_3, (\mathbf{U}\mathbf{v})_4, (\mathbf{U}\mathbf{v})_5)^T$ gives the desired embedding. That is, the set $\mathcal{L} = \{[\phi(\mathbf{v})] : \mathbf{v} \in C\} \subset \mathbb{R}^5$ is a regular 5-simplex. The unit vectors representing the set $\mathcal{L}$ are given as the columns of the following matrix (we are stating these values explicitly as we will need them to give a construction of a tight equiangular set of 6 lines in $\mathbb{H}^2$; see Example 4.24):

$$\begin{pmatrix} 3/\sqrt{15} & -3/\sqrt{15} & 0 & 0 & 0 & 0 \\ 1/\sqrt{5} & 1/\sqrt{5} & -2/\sqrt{5} & 0 & 0 & 0 \\ 1/\sqrt{10} & 1/\sqrt{10} & 1/\sqrt{10} & -3/\sqrt{10} & 0 & 0 \\ \sqrt{6}/10 & \sqrt{6}/10 & \sqrt{6}/10 & \sqrt{6}/10 & \sqrt{6}/10 & 0 \\ 1/5 & 1/5 & 1/5 & 1/5 & 1/5 & -1 \end{pmatrix}$$

For every set of lines $\mathcal{L}$, let $\mathbf{V}_{\mathcal{L}}$ denote the matrix whose columns span the lines in $\mathcal{L}$. The following observation shows that among all tight equiangular sets of $n > d$ lines in $\mathbb{C}^d$, the regular d-simplex is the only set $\mathcal{L}$ for which the matrix $\mathbf{V}_{\mathcal{L}}$ is of the form $a\mathbf{I}_n + b\mathbf{J}_n$ for some $a, b \in \mathbb{C}$. One direction of this implication is clear and we will prove the other one.

Theorem 4.3. *Let $\mathcal{L} = \{[\mathbf{v}_1], \ldots, [\mathbf{v}_n]\}$ be a tight equiangular set of n lines in $\mathbb{C}^d$, with $n > d$. By embedding $\mathbb{C}^d$ in $\mathbb{C}^n$, we may assume that each $\mathbf{v}_i$ is in $\mathbb{C}^n$. Let $\mathbf{V}_{\mathcal{L}}$ be the $n \times n$ matrix with the column vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n$ as its columns. Then $\mathbf{V}_{\mathcal{L}} = a\mathbf{I}_n + b\mathbf{J}_n$ for some $a, b \in \mathbb{C}$ if and only if $\mathcal{L}$ and $\mathcal{R}$ are equivalent, i.e. $n = d+1$ and $\mathcal{L}$ is the regular d-simplex.*

Proof. We know $\mathbf{V}_{\mathcal{R}}$ is of the form $a\mathbf{I}_n + b\mathbf{J}_n$. To prove the other direction, assume $\mathbf{V}_{\mathcal{L}} = a\mathbf{I}_n + b\mathbf{J}_n$. The eigenvalues of $\mathbf{V}_{\mathcal{L}}$ are a (with multiplicity $n-1$) and $a+nb$ (with multiplicity

1). Since the columns of $\mathbf{V}_{\mathcal{L}}$ cannot be the same, it follows that $a \neq 0$. Therefore, $n-1 \leq \operatorname{rank}_{\mathbb{C}}(\mathbf{V}_{\mathcal{L}}) \leq d < n$. Hence $n = d+1$. It also follows that $\operatorname{rank}_{\mathbb{C}}(\mathbf{V}_{\mathcal{L}}) = d = n-1$ and therefore $a+nb = 0$. Since each column of $\mathbf{V}_{\mathcal{L}}$ is a unit vector, we have $|a+b|^2+(n-1)|b|^2 = 1$. Substituting $a = -nb$, we get $n(n-1)|b|^2 = 1$. Therefore

$$\begin{aligned}
\mathbf{V}_{\mathcal{L}}{}^*\mathbf{V}_{\mathcal{L}} &= (\overline{a}\mathbf{I}_n + \overline{b}\mathbf{J}_n)(a\mathbf{I}_n + b\mathbf{J}_n) \\
&= |a|^2\mathbf{I}_n + (2\Re(a\overline{b}) + n|b|^2)\mathbf{J}_n \\
&= n^2|b|^2\mathbf{I}_n - n|b|^2\mathbf{J}_n \\
&= \frac{n}{n-1}\mathbf{I}_n - \frac{1}{n-1}\mathbf{J}_n \\
&= (1+\frac{1}{d})\mathbf{I}_{d+1} - \frac{1}{d}\mathbf{J}_{d+1} \\
&= \mathbf{V}_{\mathcal{R}}{}^*\mathbf{V}_{\mathcal{R}}.
\end{aligned}$$

Thus $\mathcal{L}$ and $\mathcal{R}$ have the same Gram matrix and therefore are equivalent by Definition 1.30.

□

The following fact is a rather obvious observation, however we are stating it as a proposition since we will need it later on.

Proposition 4.4. *For every $2 \leq n \leq d+1$, there exists a set $\mathcal{L}$ of n lines in $\mathbb{R}^d$ such that for every distinct $[\mathbf{v}], [\mathbf{w}] \in \mathcal{L}$, we have $\langle \mathbf{v}, \mathbf{w} \rangle = -1/(n-1)$.*

Proof. For every $2 \leq n \leq d+1$, the regular $(n-1)$-simplex of n lines in $\mathbb{R}^{n-1} \subseteq \mathbb{R}^d$ has the desired property. □

Example 4.5. Here are 4 lines in $\mathbb{R}^5$ satisfying Proposition 4.4:

$$[\frac{1}{\sqrt{12}}(-3,1,1,1,0)], \quad [\frac{1}{\sqrt{12}}(1,-3,1,1,0)], \quad [\frac{1}{\sqrt{12}}(1,1,-3,1,0)], \quad [\frac{1}{\sqrt{12}}(1,1,1,-3,0)].$$

4.2 Difference Set Construction

Here we present a known method for constructing tight equiangular set of lines using difference sets. We also give a generalization of a known upper bound on the number of a flat equiangular set of lines.

Recall that an (n, d, λ)-*cyclic difference set* is a set $D = \{\alpha_1, \ldots, \alpha_d\} \subseteq \mathbb{Z}_n$ such that each element in $\mathbb{Z}_n \setminus \{0\}$ can be represented as a difference $\alpha_i - \alpha_j$ in exactly λ different ways. Hence $\lambda(n-1) = d(d-1)$. The existence of a cyclic difference set is known for many parameters (n, d, λ). We refer the reader to [13, 10] to find a list of such parameters. The following theorem is a known result that illustrates a connection between difference sets and equiangular set of lines.

Theorem 4.6. [84] *Let $D = \{\alpha_1, \ldots, \alpha_d\} \subseteq \mathbb{Z}_n$ be a cyclic (n, d, λ)-difference set and ω be a primitive n-th root of unity and $d \geq 2$. For every $r \in \mathbb{Z}_n$, define*

$$\mathbf{z}^{(r)} = \frac{1}{\sqrt{d}} \left(\omega^{r\alpha_j}\right)_{j \in \mathbb{Z}_d}.$$

Then $\left\{\left[\mathbf{z}^{(r)}\right] : r \in \mathbb{Z}_n\right\}$ is an equiangular set of n lines in $\mathbb{C}^d$ with common angle $\cos^{-1}\left(\frac{\sqrt{d-1}}{d}\right)$.

Proof. Recall that δ_{sr} denotes the Kronecker delta. We have

$$d^2|\langle \mathbf{z}^{(r)}, \mathbf{z}^{(s)} \rangle|^2 = |\sum_{j=1}^{d} \omega^{\alpha_j(s-r)}|^2 = \sum_{j=1}^{d}\sum_{j'=1}^{d} \omega^{(\alpha_j - \alpha_{j'})(s-r)}.$$

Since $D = \{\alpha_1, \ldots, \alpha_d\}$ is a cyclic (n, d, λ)-difference set, we get

$$d^2|\langle \mathbf{z}^{(r)}, \mathbf{z}^{(s)} \rangle|^2 = d + \sum_{x \in \mathbb{Z}_n \setminus \{0\}} \lambda \omega^{x(s-r)} = d + \delta_{sr}\lambda(n-1) + (1-\delta_{sr})(-1).$$

Since $\lambda(n-1) = d(d-1)$, we have

$$d^2|\langle \mathbf{z}^{(r)}, \mathbf{z}^{(s)} \rangle|^2 = d + \delta_{sr} d(d-1) - (1-\delta_{sr}) = d - 1 + \delta_{sr}(d^2 - d + 1).$$

Thus $|\langle \mathbf{z}^{(r)}, \mathbf{z}^{(s)} \rangle| = \sqrt{d-1}/d + \delta_{rs}(1 - \sqrt{d-1}/d)$. Therefore $\left\{\left[\mathbf{z}^{(r)}\right] : r \in \mathbb{Z}_n\right\}$ is an equiangular set of n lines in $\mathbb{C}^d$ with common angle θ, where $\cos\theta = \frac{\sqrt{d-1}}{d}$. □

We would like to emphasize that the construction given in Theorem 4.6 yields a tight equiangular set of n lines in $\mathbb{C}^d$ if and only if $n = d^2 - d + 1$. This is because if θ is the common angle then

$$\cos\theta = \frac{\sqrt{d-1}}{d} \geq \sqrt{\frac{n-d}{d(n-1)}}$$

and equality occurs if and only if $n = d^2 - d + 1$.

An equiangular set of lines is called *flat* if the absolute values of all the coordinates of the vectors representing the lines are the same. Note that in the above construction $|\mathbf{z}^{(r)}| = 1/\sqrt{d}$ for all r and therefore $\left\{\left[\mathbf{z}^{(r)}\right] : r \in \mathbb{Z}_n\right\}$ is a flat equiangular set of lines. The following construction is due to König [58] for prime q and is due to Xia, et al. [84] for prime power q.

Lemma 4.7. [84] *For every prime power q, there exists a flat tight equiangular set of $d^2 - d + 1$ lines in $\mathbb{C}^d$, where $d = q + 1$.*

Proof. Let $n = d^2 - d + 1 = q^2 + q + 1$ and α be a generator of the multiplicative group $\mathbb{F}_{q^3} \setminus \{0\}$. Let $\mathrm{Tr} : \mathbb{F}_{q^3} \to \mathbb{F}_q$ defined by $\mathrm{Tr}\,(x) = x + x^q + x^{q^2}$ be the trace mapping. Then $D = \{t \in \mathbb{Z}_n : \mathrm{Tr}\left(\alpha^t\right) = 0\}$ is a cyclic $(n, q+1, 1)$ difference set (this is known as the Singer difference set and may equivalently be constructed using lines in PG(2,q); see [13] for more details). The result follows from Theorem 4.6. □

The following theorem shows that in fact a flat equiangular set of $d^2 - d + 1$ lines in $\mathbb{C}^d$ is the best possible. This result was given by Roy [67] for $\mathbb{C}^d$. Since the result follows from Theorem 2.3, we present it for $\mathbb{A}^d$, where $\mathbb{A}$ is an associative composition algebra.

Theorem 4.8. *There are at most $\binom{d}{2} \dim_{\mathbb{R}} \mathbb{A} + 1$ flat equiangular lines in $\mathbb{A}^d$.*

Proof. Let $\mathcal{L}$ be a flat equiangular set of n lines in $\mathbb{A}^d$ and let $\mathcal{L}' = \{[\mathbf{e}_i] : i \in \mathbb{Z}_d\}$ be the standard basis for $\mathbb{A}^d$. Then $\mathcal{L} \cup \mathcal{L}'$ is an $(\{n; d\}, 2, d)$-multipartite equiangular set of lines. Hence using Theorem 2.6, we have $n + d \leq d + \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A} + 2 - 1$. Thus $n \leq \binom{d}{2} \dim_{\mathbb{R}} \mathbb{A} + 1$. □

Note that $\binom{d}{2} \dim_{\mathbb{R}} \mathbb{C} + 1 = d^2 - d + 1$.

4.3 Conference and Hadamard Matrices

Here, we present a general framework for constructing tight equiangular set of lines in $\mathbb{C}^d$ by assuming an extra condition on its corresponding Gram matrix. A construction of a tight equiangular set of $2d$ lines in $\mathbb{R}^d$ by Zauner [85] and a recent construction of a tight equiangular set of $2d \pm 1$ lines in $\mathbb{C}^d$ by Renes [65] fall under this framework. We use the well-known conference and Hadamard matrices to replicate Zauner's and Renes' constructions.

A Gram matrix of any set of n lines in $\mathbb{C}^d$ can be written in the form

$$\mathbf{G} = \mathbf{I}_n + \mathbf{S} + i\mathbf{A},$$

where $\mathbf{S}$ is a real symmetric matrix with zero diagonal and $\mathbf{A}$ is a real skew symmetric matrix with zero diagonal. Recall that an $\mathbb{R}$-algebra is a vector space over $\mathbb{R}$ equipped with multiplication. We only work with the $\mathbb{R}$-algebra of square matrices of a fixed order. Notice that the $\mathbb{R}$-algebra spanned by $\{\mathbf{I}_n, \mathbf{S}, \mathbf{A}\}$ has dimension at least 3 (unless $\mathbf{S} = \mathbf{0}$ or $\mathbf{A} = \mathbf{0}$). Using Corollary 2.28, we have the following lemma.

Lemma 4.9. *Let* $\mathbf{S}$ *(and* $\mathbf{A}$*) be real symmetric (and skew symmetric) matrices with zero diagonal such that the* $\mathbb{R}$*-algebra spanned by* $\{\mathbf{I}_n, \mathbf{S}, \mathbf{A}\}$ *has dimension* 3 *(or less when* $\mathbf{S} = \mathbf{0}$ *or* $\mathbf{A} = \mathbf{0}$*). Then* $\mathbf{G} = \mathbf{I}_n + \mathbf{S} + i\mathbf{A}$ *is a Gram matrix of a tight equiangular set of* n *lines in* $\mathbb{C}^d$ *if and only if the off-diagonal entries of* $\mathbf{G}$ *have squared absolute value* $(n-d)/d(n-1)$ *and*

$$r - \lambda + 1 = t - \mu + 2 = \gamma + 2 = \frac{n}{d},$$

where

$$\mathbf{S}^2 = r\mathbf{I}_n + t\mathbf{S}, \qquad \mathbf{A}^2 = \lambda\mathbf{I}_n + \mu\mathbf{S}, \qquad \mathbf{SA} + \mathbf{AS} = \gamma\mathbf{A}.$$

Remark. The assumption that the $\mathbb{R}$-algebra spanned by $\{\mathbf{I}_n, \mathbf{S}, \mathbf{A}\}$ has dimension 3, implies that the matrices $\mathbf{S}^2, \mathbf{A}^2$, and $\mathbf{SA} + \mathbf{AS}$ must be an $\mathbb{R}$-linear combination of $\mathbf{I}, \mathbf{S}$, and $\mathbf{A}$. Since $\mathbf{S}$ is symmetric and $\mathbf{A}$ is skew symmetric, it follows that $\mathbf{S}^2$ and $\mathbf{A}^2$ are symmetric matrices and $\mathbf{SA} + \mathbf{AS}$ is a skew symmetric matrix. Therefore, the above matrices are written in the specific form given in Lemma 4.9.

Theorem 4.10. *Let* $s, a \in \mathbb{R}$*. Let* $\mathbf{S} = s(\mathbf{J}_n - \mathbf{I}_n)$ *and let* $\mathbf{A}$ *be a real skew symmetric* $(0, \pm a)$*-matrix with zero diagonal such that the* $\mathbb{R}$*-algebra spanned by* $\{\mathbf{I}_n, \mathbf{S}, \mathbf{A}\}$ *has dimension* 3*. If* $\mathbf{G} = \mathbf{I}_n + \mathbf{S} + i\mathbf{A}$ *is a Gram matrix of a tight equiangular set of* n *lines in* $\mathbb{C}^d$ *then* $|2d - n| \leq 1$ *and*

$$s = \frac{2d-n}{2d}, \qquad a^2 = \frac{n-d}{d(n-1)} - s^2.$$

Proof. Suppose a, s and $\mathbf{A}$ are such that $\mathbf{G}$ is a Gram matrix of a tight equiangular set of n lines in $\mathbb{C}^d$. We have $s^2 + a^2 = (n-d)/d(n-1)$. Write $\mathbf{SA} + \mathbf{AS} = \gamma\mathbf{A}$ or equivalently $s(\mathbf{J}_n\mathbf{A} + \mathbf{A}\mathbf{J}_n) = (\gamma + 2s)\mathbf{A}$. If $s = 0$ then $\gamma = 0$ and Lemma 4.9 implies that $n = 2d$ and we are done. So, we may assume $s \neq 0$. Since $\mathbf{S} = s(\mathbf{J}_n - \mathbf{I}_n)$, it follows that the span of $\{\mathbf{I}_n, \mathbf{J}_n, \mathbf{A}\}$ has also dimension 3. If $n = 2$ then there are only two possibilities for the 2×2 skew symmetric matrix $\mathbf{A}$ and in either case $\mathbf{A}\mathbf{J}_2 + \mathbf{J}_2\mathbf{A} = \mathbf{0}$. If $n > 2$, since $\mathbf{A}\mathbf{J}_n$ has constant rows and is an $\mathbb{R}$-linear combination of $\mathbf{I}_n, \mathbf{J}_n$ and $\mathbf{A}$, we must have $\mathbf{A}\mathbf{J}_n = k\mathbf{J}_n$ for some k. This is because in at least one row of the skew symmetric matrix $\mathbf{A}$ the values a and $-a$ each appear at least once. Therefore $\mathbf{J}_n\mathbf{A} = -(\mathbf{A}\mathbf{J}_n)^T = -k\mathbf{J}_n$. Hence, we get $\mathbf{J}_n\mathbf{A} + \mathbf{A}\mathbf{J}_n = \mathbf{0}$ for all $n \geq 2$, which implies $\gamma = -2s$. Since $\gamma + 2 = n/d$, we get the desired value of s. By substituting $\mathbf{S} = s(\mathbf{J}_n - \mathbf{I}_n)$ in $\mathbf{S}^2 = r\mathbf{I}_n + t\mathbf{S}$, we get

$$s^2(n-2)\mathbf{J}_n + s^2\mathbf{I}_n = ts\mathbf{J}_n + (r - ts)\mathbf{I}_n.$$

By comparing both sides, we get $t = (n-2)s$ and $r = (n-1)s^2$. It follows from Lemma 4.9 that $\lambda = (n-1)s^2 + 1 - n/d$ and $\mu = (n-2)s + 2 - n/d$, where $\mathbf{A}^2 = \lambda\mathbf{I}_n + \mu\mathbf{S}$. Therefore, one of the eigenvalues of $\mathbf{A}$ is $\sqrt{\lambda + \mu s(n-1)} = (n/2d)\sqrt{(2d-n)^2 - 1}$. Since $\mathbf{A}$ is a skew symmetric matrix, its eigenvalues are zero or purely imaginary and therefore we must have $|2d - n| \leq 1$. □

Given n and d such that $n = 2d$, if a conference matrix (defined below) of order $2d$ exists then we may construct matrices $\mathbf{S}$ and $\mathbf{A}$ that satisfy the conditions given in Theorem 4.10. This is also possible for $n = 2d \pm 1$ if skew-type Hadamard matrices (defined below) of order $2d + 1 \pm 1$ exist. Before we state these results formally (Theorems 4.13 and 4.14), let us give a brief background on conference and skew-type Hadamard matrices.

A *conference matrix* of order n is an $n \times n$ $(0, \pm 1)$-matrix $\mathbf{C}$ with zero diagonal satisfying $\mathbf{C}\mathbf{C}^T = (n-1)\mathbf{I}_n$. Note that n is necessarily even. Multiplying a row or a column of a conference matrix by -1 yields another conference matrix. A conference matrix is called *normalized* if all entries in its first row and first column (except the $(1,1)$ entry) are 1. The *core* of a normalized conference matrix $\mathbf{C}$ consists of all the rows and columns of $\mathbf{C}$ except the first row and column. It is well known that the core of every normalized conference matrix of order $n \equiv 0 \pmod 4$ is skew symmetric and the core of every normalized conference matrix of order $n \equiv 2 \pmod 4$ is symmetric [49]. It is conjectured [49] that conference matrices of order n exist for all $n \equiv 2 \pmod 4$ as long as $n - 1$ is a sum of two squares. It is known that a conference matrix of order n exists when $n - 1$ is an odd prime power, $n = 5(9^{2t+1}) + 1$ for some integer $t \geq 0$ and $n < 66$ is even and $n \neq 22, 34, 58$. For more details and more examples of conference matrices, see [49].

A *tournament* of order n is a complete digraph on n vertices. It is regular if each vertex dominates and is dominated by exactly $(n-1)/2$ vertices. A special class of tournaments has been studied in literature under the name of *extreme tournaments*, *doubly regular tournaments*, and *strongly regular tournaments* in analogy to the notion of strongly regular graphs. A tournament is called strongly regular if it is regular and for each vertex v the set of vertices dominating v also form a regular tournament. It is necessary that $n \equiv 3 \pmod 4$. Therefore we have the following.

Proposition 4.11. *The $(0, \pm 1)$-adjacency matrix of a strongly regular tournament is a skew symmetric matrix $\mathbf{T}$ that satisfies $\mathbf{T}^2 = -n\mathbf{I}_n + \mathbf{J}_n$ and $\mathbf{T}\mathbf{J}_n = \mathbf{0}$.*

It follows that the matrix

$$\mathbf{C} = \begin{pmatrix} 0 & \mathbf{1}_n{}^T \\ -\mathbf{1}_n & \mathbf{T} \end{pmatrix}$$

is a skew symmetric conference matrix of order $n+1$. Conversely, the core of any conference matrix of order $n+1$ with $n \equiv 3 \pmod 4$ is the adjacency matrix of a strongly regular tournament. Also note that $\mathbf{C}$ is skew symmetric conference matrix of order $n+1$ if and only if $\mathbf{H} = \mathbf{C} + \mathbf{I}_{n+1}$ is a *skew-type Hadamard matrix* of order $n+1$, that is a matrix $\mathbf{H}$ of order $n+1$ such that $\mathbf{H}\mathbf{H}^T = (n+1)\mathbf{I}_{n+1}$ and $\mathbf{H}+\mathbf{H}^T = 2\mathbf{I}_{n+1}$. The equivalence of strongly regular tournaments and skew-type Hadamard matrices was first discovered by Reid and Brown [64].

Conjecture 4.12 (Seberry)**.** *A skew-type Hadamard matrix of order N exists if and only if $N = 1, 2$ or $4|N$.*

This conjecture is confirmed for $N < 188$. It also true when $N-1$ is a prime power that is 3 modulo 4. Also, the existence of a skew-type Hadamard matrix of order N implies the existence of a skew-type Hadamard matrix of order 2^tN for all integers $t \geq 0$. For a complete list of known skew-type Hadamard matrices, see [24].

Now, we are ready to give necessary conditions on d such that the converse of Theorem 4.10 is true, in the sense that if $|2d - n| \leq 1$ then there is a tight equiangular set of n lines in $\mathbb{C}^d$ that has a Gram matrix $\mathbf{G} = \mathbf{I}_n + \mathbf{S} + i\mathbf{A}$ such that $\{\mathbf{I}_n, \mathbf{S}, \mathbf{A}\}$ forms a three dimensional algebra. The first theorem is due to Zauner [85] and the second one is due to Renes [65] in a weaker form.

Theorem 4.13. [85] *If a conference matrix of order $2d$ exists, then there exists a tight equiangular set of $2d$ lines in $\mathbb{C}^d$.*

Proof. Assume $\mathbf{C}$ is a conference matrix of order $2d$. Choose $\mathbf{S} = \mathbf{0}$ and $\mathbf{A} = (n-1)^{-1/2}\mathbf{C}$ with $n = 2d$. It is easy to see that the $\mathbb{R}$-algebra spanned by $\{\mathbf{I}_n, \mathbf{S}, \mathbf{A}\}$ has dimension 3 and $\mathbf{S}$ and $\mathbf{A}$ satisfy the hypotheses of Lemma 4.9 with $r = t = \mu = 0$ and $\lambda = -1$. Therefore $\mathbf{G} = \mathbf{I}_n + \mathbf{S} + i\mathbf{A}$ is a Gram matrix of a tight equiangular set of $2d$ lines in $\mathbb{C}^d$. □

Theorem 4.14. [65] *For odd d, if there exists a skew type Hadamard matrix of order $2d+2$ then there exists a tight equiangular set of $2d+1$ lines in $\mathbb{C}^d$. For even d, if there exists* *a skew type Hadamard matrix of order* $2d$ *then there exists a tight equiangular set of* $2d-1$ *lines in* $\mathbb{C}^d$.

Proof. Write $d = 2m - \epsilon$ and $n = 2d + 2\epsilon - 1$ where $\epsilon \in \{0, 1\}$. Assume $\mathbf{H}$ is a skew-type Hadamard matrix of order $4m$. Normalize the conference matrix $\mathbf{H} + \mathbf{I}_{4m}$ and let $\mathbf{T}$ be its core. Choose $\mathbf{S} = s(\mathbf{J}_n - \mathbf{I}_n)$ and $\mathbf{A} = a\mathbf{T}$ where s and a are as in Theorem 4.10. Using Proposition 4.11, we may check that the $\mathbb{R}$-algebra spanned by $\{\mathbf{I}_n, \mathbf{S}, \mathbf{A}\}$ has dimension 3 and $\mathbf{S}$ and $\mathbf{A}$ satisfy the hypotheses of Lemma 4.9 with $r = (n-1)s^2$, $t = (n-2)s$, $\lambda = (n-1)s^2 + 1 - n/d$, $\mu = (n-2)s + 2 - n/d$ and $\gamma = -2s$. It follows that $\mathbf{G} = \mathbf{I}_n + \mathbf{S} + i\mathbf{A}$ is a Gram matrix of a tight equiangular set of n lines in $\mathbb{C}^d$. □

4.4 Equiangular Sets of Lines in Small Dimensions

In this section, we give a summary of known as well as new constructions of equiangular sets of lines in small dimensions. We discuss various analytic and numerical constructions and different methods for constructing such lines. Some of the results are new.

4.4.1 Tight Equiangular Sets of Lines in $\mathbb{C}^2$

In this part, we discuss several methods for constructing tight equiangular sets of n lines in $\mathbb{C}^2$ with $n \leq 4$. The first construction is new and is inspired by the fact that $\mathbb{CP}^1$, the 1-dimensional complex projective space, written as

$$\mathbb{CP}^1 = \{[(z_1, z_2)] \subset \mathbb{C}^2 : |z_1|^2 + |z_2|^2 = 1\},$$

can be identified with S^2, the 3-dimensional real unit sphere, written as

$$S^2 = \{(a, b, c) \in \mathbb{R}^3 \, : \, a^2 + b^2 + c^2 = 1\}.$$

We will thoroughly describe this identification. The identification between S^2 and $\mathbb{CP}^1$, especially when it is defined from $\mathbb{CP}^1$ to S^2, is known as the Hopf mapping and is of great importance in homotopy theory. See the remark following Theorem 4.17 for some more details. In the next section, we will generalize this idea to construct equiangular sets of lines in $\mathbb{H}^2$. Recall that by Corollary 2.12 an equiangular set of lines in $\mathbb{C}^2$ has size at most 4.

Definition 4.15. *Define* $\psi : S^2 \to \mathbb{CP}^1$ *by*

$$\psi(a, b, c) = \left[\left(\frac{1}{\sqrt{2(1-c)}}(a+bi), \sqrt{\frac{1-c}{2}}\right)\right],$$

when $c \neq 1$ *and* $\psi(0, 0, 1) = [(1, 0)]$.

The mapping ψ is well-defined, i.e. $\psi(a, b, c) \in \mathbb{CP}^1$. This is because for every $(a, b, c) \in S^2$, we have

$$\begin{aligned} |\psi(a,b,c)|^2 &= \frac{|a+bi|^2}{2(1-c)} + \frac{1-c}{2} \\ &= \frac{a^2+b^2}{2(1-c)} + \frac{1-c}{2} \\ &= \frac{1-c^2}{2(1-c)} + \frac{1-c}{2} = 1. \end{aligned}$$

The spaces S^2 and $\mathbb{CP}^1$ are equivalent, both topologically and metrically. In the following lemma, we give an explicit formula that relates the inner product of any two elements in S^2 with the inner product of their images in $\mathbb{CP}^1$. It may seem vague at this point, but the absence of the absolute value on the right hand side of the formula given in Lemma 4.16, is particularly useful and crucial for the construction of equiangular sets of lines in $\mathbb{C}^2$.

Lemma 4.16. *For every* $\mathbf{v}, \mathbf{w} \in S^2$*, we have*

$$|\langle \psi(\mathbf{v}), \psi(\mathbf{w}) \rangle|^2 = \frac{1 + \langle \mathbf{v}, \mathbf{w} \rangle}{2}.$$

Proof. Write $\mathbf{v} = (a, b, c)$ and $\mathbf{w} = (a', b', c')$ with $a^2 + b^2 + c^2 = 1$ and $a'^2 + b'^2 + c'^2 = 1$. If one of the $\mathbf{v}$ or $\mathbf{w}$, say $\mathbf{w}$, is $(0, 0, 1)$ then

$$|\langle \psi(\mathbf{v}), \psi(\mathbf{w}) \rangle|^2 = |\langle \psi(\mathbf{v}), (1,0) \rangle|^2 = \frac{a^2+b^2}{2(1-c)} = \frac{1-c^2}{2(1-c)} = \frac{1+c}{2} = \frac{1+\langle \mathbf{v}, \mathbf{w} \rangle}{2}.$$

Thus, we may assume $c \neq 1$ and $c' \neq 1$. We have

$$\begin{aligned} 2\sqrt{(1-c)(1-c')}\,\langle \psi(\mathbf{v}), \psi(\mathbf{w}) \rangle &= (a-bi)(a'+b'i) + (1-c)(1-c') \\ &= \alpha + (1-c)(1-c') + \beta\, i, \end{aligned}$$

where

$$\begin{aligned} \alpha &= aa' + bb', \\ \beta &= ab' - a'b. \end{aligned}$$

Since $\alpha^2+\beta^2 = (a^2+b^2)(a'^2+b'^2) = (1-c^2)(1-c'^2)$ and $cc'+\alpha = \langle \mathbf{v}, \mathbf{w}\rangle$, we have

$$\begin{aligned}
4(1-c)(1-c')|\langle\psi(\mathbf{v}),\psi(\mathbf{w})\rangle|^2 &= (\alpha+(1-c)(1-c'))^2+\beta^2 \\
&= (1-c^2)(1-c'^2)+2\alpha(1-c)(1-c')+(1-c)^2(1-c')^2 \\
&= (1-c)(1-c')\big((1+c)(1+c')+2\alpha+(1-c)(1-c')\big) \\
&= (1-c)(1-c')\big(2+2cc'+2\alpha\big) \\
&= 2(1-c)(1-c')\left(1+\langle\mathbf{v},\mathbf{w}\rangle\right).
\end{aligned}$$

□

Theorem 4.17. *For every $n = 2, 3, 4$, there exists a tight equiangular set of n lines in $\mathbb{C}^2$.*

Proof. Using Proposition 4.4 with $d = 3$, consider the set $\mathcal{L}$ of n lines in $\mathbb{R}^3$ such that for every distinct $[\mathbf{v}], [\mathbf{w}] \in \mathcal{L}$, we have $\langle \mathbf{v}, \mathbf{w}\rangle = -1/(n-1)$. Since the lines of $\mathbb{R}^3$ may be identified with the points on S^2 and the lines of $\mathbb{C}^2$ may be identified with the elements of $\mathbb{CP}^1$, the mapping $\psi : S^4 \to \mathbb{CP}^1$ given in Definition 4.15 maps $\mathcal{L}$ to a set of lines $\psi(\mathcal{L})$ of $\mathbb{C}^2$. For every $[\mathbf{v}], [\mathbf{w}] \in \mathcal{L}$, by Lemma 4.22, we have

$$|\langle\psi(\mathbf{v}),\psi(\mathbf{w})\rangle|^2 = \frac{1+\langle\mathbf{v},\mathbf{w}\rangle}{2} = \frac{1-1/(n-1)}{2} = \frac{n-2}{2(n-1)},$$

which is exactly the relative bound given in Theorem 2.13 for $d = 2$. □

Remark. The mapping ψ defined in Definition 4.15 is, in a sense, the inverse of the mapping $\phi : \mathbb{C}^2 \to \mathbb{C}\times\mathbb{R}$ given by

$$\phi(z_1, z_2) = \left(\frac{2z_1\overline{z_2}}{|z_1|^2+|z_2|^2}, \frac{|z_1|^2-|z_2|^2}{|z_1|^2+|z_2|^2}\right),$$

which is known as the *Hopf mapping*. Notice that for any $c \in \mathbb{C}$, $\phi(cz_1, cz_2) = \phi(z_1, z_2)$. That is, every point on a line in $\mathbb{C}^2$ is mapped to the same point in $\mathbb{C}\times\mathbb{R}$. Hence ϕ induces a mapping $\phi_0 : \mathbb{CP}^1 \to S^2$ given by

$$\phi_0(x_1+y_1 i, x_2+y_2 i) = \left(2(x_1x_2+y_1y_2), 2(x_2y_1-x_1y_2), x_1^2+y_1^2-x_2^2-y_2^2\right).$$

This is because $|\phi_0(z_1, z_2)| = 1$, $\mathbb{C}\times\mathbb{R}$ may be identified with $\mathbb{R}^3$, and every line in $\mathbb{C}^2$, i.e. a point in $\mathbb{CP}^1$, may be represented by (z_1, z_2) with $|z_1|^2+|z_2|^2 = 1$. Therefore, to be precise, the mapping ψ is the inverse of ϕ_0.

The Hopf mapping ϕ is well-known, especially to algebraic topologist, and is of particular importance in homotopy theory. We refer the interested reader to Vick [80] and Martin [60].

Example 4.18. In this example, we give an explicit construction of a tight equiangular set of 4 lines in $\mathbb{C}^2$, using the method described in the proof of Theorem 4.17. First, consider the regular 3-simplex $\mathcal{L}$ in $\mathbb{R}^3$. Similar to the construction given in Example 4.2, $\mathcal{L}$ may be given as the columns of the following matrix:

$$\begin{pmatrix} \sqrt{6}/3 & -\sqrt{6}/3 & 0 & 0 \\ \sqrt{2}/3 & \sqrt{2}/3 & -2\sqrt{2}/3 & 0 \\ 1/3 & 1/3 & 1/3 & -1 \end{pmatrix}$$

For every distinct $[\mathbf{v}], [\mathbf{w}] \in \mathcal{L}$ we have $\langle \mathbf{v}, \mathbf{w} \rangle = -1/3$. By applying the mapping ψ, given in Definition 4.15, to the columns of the above matrix, we get the following equiangular set of 4 lines in $\mathbb{C}^2$:

$$\mathcal{L} = \left\{ [\begin{pmatrix} r+si \\ u \end{pmatrix}], [\begin{pmatrix} -r+si \\ u \end{pmatrix}], [\begin{pmatrix} -2si \\ u \end{pmatrix}], [\begin{pmatrix} 0 \\ 1 \end{pmatrix}] \right\},$$

where $r = \sqrt{6}/3$, $s = \sqrt{2}/3$, and $u = \sqrt{1/3}$.

Now, we describe a second approach to construct an equiangular set of 4 lines in $\mathbb{C}^2$. Recall that a unit vector $\mathbf{z} \in \mathbb{C}^2$ is fiducial if $\{[\mathbf{X}^i\mathbf{Y}^j\mathbf{z}] : i, j \in \mathbb{Z}_2\}$ is an equiangular set of 4 lines in $\mathbb{C}^2$, where $\mathbf{X}$ and $\mathbf{Y}$ are the Pauli matrices for $\mathbb{Z}_2$. We say that two fiducial vectors $\mathbf{z}$ and $\mathbf{z}'$ are *equivalent* if $[\mathbf{z}'] = [\mathbf{X}^i\mathbf{Y}^j\mathbf{z}]$ for some $i, j \in \mathbb{Z}_2$, that is $\mathbf{z}'$ and $\mathbf{X}^i\mathbf{Y}^j\mathbf{z}$ represent the same line. The following theorem is given in [66] with no proof.

Theorem 4.19. [66] *A vector* $\mathbf{z} \in \mathbb{C}^2$ *is fiducial if and only if, up to equivalence,*

$$\mathbf{z} = \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{3+\sqrt{3}} \\ e^{k\pi/4}\sqrt{3-\sqrt{3}} \end{pmatrix},$$

where $k \in \{1, 3\}$.

Proof. Using Theorem 3.3, $\mathbf{z} = \begin{pmatrix} z_0 \\ z_1 \end{pmatrix} \in \mathbb{C}^2$ is fiducial if and only if

$$\begin{array}{rclclcl} f_{0,0}(\mathbf{z}) & = & |z_0|^4 + |z_1|^4 & = & r_0^4 + r_1^4 & = & \frac{2}{3}, \\ f_{0,1}(\mathbf{z}) & = & 2|z_0|^2|z_1|^2 & = & 2r_0^2r_1^2 & = & \frac{1}{3}, \\ f_{1,1}(\mathbf{z}) & = & 2\Re(z_0^2\overline{z_1}^2) & = & 2r_0^2r_1^2\cos(2\theta_0 - 2\theta_1) & = & 0, \end{array}$$

where $z_j = r_je^{i\theta_j}$ $(j = 0, 1)$. Since $\mathbf{z}$ and $e^{-i\theta_0}\mathbf{z}$ are equivalent, we may assume $\theta_0 = 0$. Thus, the third equality is equivalent to $\theta_1 = k\pi/4$ with $k \in \{1, 3\}$. Also, since $\mathbf{z} = \left(r_0, r_1e^{i\theta_1}\right)^T$ and $e^{-i\theta_1}\mathbf{X}\mathbf{z} = \left(r_1, r_0e^{-i\theta_1}\right)^T$ are equivalent, we may assume $r_0 > r_1$. Now, solving the first two equalities for r_0 and r_1, we get the desired values. □

4.4.2 The Uniqueness of the Equiangular Set of 4 Lines in $\mathbb{C}^2$

Suppose $\mathbf{G}$ is a Gram matrix of an equiangular set of 4 lines in $\mathbb{C}^2$. Write $\mathbf{G} = \mathbf{I}_4 + \frac{1}{\sqrt{3}}\mathbf{W}$. We may assume that $\mathbf{W}$ has the following form:

$$\begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & a & b \\ 1 & \overline{a} & 0 & c \\ 1 & \overline{b} & \overline{c} & 0 \end{pmatrix}$$

where $|a| = |b| = |c| = 1$. We must have $\mathbf{G}^2 = 2\mathbf{G}$ or equivalently $\mathbf{W}^2 = 3\mathbf{I}_4$. This is equivalent to

$$\begin{cases} a+b & = & \overline{a}+c & = & b+c & = & 0, \\ 1+b\overline{c} & = & 1+ac & = & 1+a\overline{b} & = & 0. \end{cases}$$

Solving for a, b, and c, we get $(a,b,c) \in \{(i,-i,i),(-i,i,-i)\}$.

The set of lines induced by these two solutions are, however, equivalent. This is because one of the Gram matrices is obtained from the other one by interchanging row 3 and row 4 as well as column 3 and column 4. Thus, we have the following result.

Theorem 4.20. *The Gram matrix of any equiangular set of* 4 *lines in* $\mathbb{C}^2$*, up to equivalence, is equal to* $\mathbf{I}_4 + \frac{1}{\sqrt{3}}\mathbf{W}$ *where*

$$\mathbf{W} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & i & -i \\ 1 & i & 0 & i \\ 1 & -i & i & 0 \end{pmatrix}.$$

4.4.3 Tight Equiangular Sets of Lines in $\mathbb{H}^2$

In this section we give explicit constructions of tight equiangular sets of n lines in $\mathbb{H}^2$ with $n \leq 6$. The method is almost identical to the first method described in Section 4.4.1 for constructing tight equiangular sets of lines in $\mathbb{C}^2$. These constructions are new and are based on the fact that $\mathbb{HP}^1$, the 1-dimensional quaternionic projective space, written by

$$\mathbb{HP}^1 = \{(q_1, q_2) \in \mathbb{H}^2 : |q_1|^2 + |q_2|^2 = 1\},$$

can be identified with S^4, the unit sphere in $\mathbb{R}^5$, written by

$$S^4 = \{(a,b,c,d,e) \in \mathbb{R}^5 : a^2+b^2+c^2+d^2+e^2 = 1\}.$$

We will thoroughly describe this identification. The identification between S^4 and $\mathbb{HP}^1$ is once again known as the Hopf mapping. This mapping inspired us to relate the regular simplices in real spaces with tight equiangular set of lines in quaternionic spaces. Notice that, by Corollary 2.12, an equiangular set of lines in $\mathbb{H}^2$ has size at most 6.

Definition 4.21. *Define $\psi : S^4 \to \mathbb{HP}^1$ by*

$$\psi(a,b,c,d,e) = \left[\left(\frac{1}{\sqrt{2(1-e)}}(a+bi+cj+dij), \sqrt{\frac{1-e}{2}}\right)\right],$$

when $e \neq 1$ and $\psi(0,0,0,0,1) = (1,0)$.

The mapping ψ is well-defined, i.e. $\psi(a,b,c,d,e) \in \mathbb{HP}^1$. This is because for every $(a,b,c,d,e) \in S^4$ we have

$$\begin{aligned} |\psi(a,b,c,d,e)|^2 &= \frac{|a+bi+cj+dij|^2}{2(1-e)} + \frac{1-e}{2} \\ &= \frac{a^2+b^2+c^2+d^2}{2(1-e)} + \frac{1-e}{2} \\ &= \frac{1-e^2}{2(1-e)} + \frac{1-e}{2} = 1. \end{aligned}$$

It is understood that S^4 and $\mathbb{HP}^1$ are equivalent, both topologically and metrically. Similar to Lemma 4.16, we give an explicit formula that relates the inner product of any two elements in S^4 with the inner product of their images in $\mathbb{HP}^1$. This lemma is crucial for our constructions.

Lemma 4.22. *For every $\mathbf{v}, \mathbf{w} \in S^4$, we have*

$$|\langle \psi(\mathbf{v}), \psi(\mathbf{w}) \rangle|^2 = \frac{1+\langle \mathbf{v}, \mathbf{w} \rangle}{2}.$$

Proof. Write $\mathbf{v} = (a,b,c,d,e)$ and $\mathbf{w} = (a',b',c',d',e')$ with $a^2+b^2+c^2+d^2+e^2 = 1$ and $a'^2+b'^2+c'^2+d'^2+e'^2 = 1$. If one of the $\mathbf{v}$ or $\mathbf{w}$, say $\mathbf{w}$, is $(0,0,0,0,1)$ then

$$|\langle \psi(\mathbf{v}), \psi(\mathbf{w}) \rangle|^2 = |\langle \psi(\mathbf{v}), (1,0) \rangle|^2 = \frac{a^2+b^2+c^2+d^2}{2(1-e)} = \frac{1-e^2}{2(1-e)} = \frac{1+e}{2} = \frac{1+\langle \mathbf{v}, \mathbf{w} \rangle}{2}.$$

Thus, we may assume $e \neq 1$ and $e' \neq 1$. We have

$$\begin{aligned} 2\sqrt{(1-e)(1-e')}\,\langle \psi(\mathbf{v}), \psi(\mathbf{w}) \rangle &= (a-bi-cj-dij)(a'+b'i+c'j+d'ij) + (1-e)(1-e') \\ &= \alpha + (1-e)(1-e') + \beta\, i + \gamma\, j + \delta\, ij \end{aligned}$$

where

$$\begin{aligned}\alpha &= aa' + bb' + cc' + dd',\\ \beta &= ab' - ba' - cd' + dc',\\ \gamma &= ac' + bd' - ca' - db',\\ \delta &= ad' - bc' + cb' - da'.\end{aligned}$$

Since $\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = (a^2 + b^2 + c^2 + d^2)(a'^2 + b'^2 + c'^2 + d'^2) = (1 - e^2)(1 - e'^2)$ and $ee' + \alpha = \langle \mathbf{v}, \mathbf{w} \rangle$, we have

$$\begin{aligned}4(1-e)(1-e')|\langle \psi(\mathbf{v}), \psi(\mathbf{w})\rangle|^2 &= (\alpha + (1-e)(1-e'))^2 + \beta^2 + \gamma^2 + \delta^2\\ &= (1-e^2)(1-e'^2) + 2\alpha(1-e)(1-e') + (1-e)^2(1-e')^2\\ &= (1-e)(1-e')\big((1+e)(1+e') + 2\alpha + (1-e)(1-e')\big)\\ &= (1-e)(1-e')\big(2 + 2ee' + 2\alpha\big)\\ &= 2(1-e)(1-e')\left(1 + \langle \mathbf{v}, \mathbf{w}\rangle\right).\end{aligned}$$

□

Theorem 4.23. *For every $2 \leq n \leq 6$, there exists a tight equiangular set of n lines in $\mathbb{H}^2$.*

Proof. Using Proposition 4.4 with $d = 5$, consider the set $\mathcal{L}$ of n lines in $\mathbb{R}^5$ such that for every distinct $\mathbf{v}, \mathbf{w} \in \mathcal{L}$, we have $\langle \mathbf{v}, \mathbf{w} \rangle = -1/(n-1)$. Since the lines of $\mathbb{R}^5$ may be identified with the points on S^4 and the lines of $\mathbb{H}^2$ may be identified with the elements of $\mathbb{HP}^1$, the mapping $\psi : S^4 \to \mathbb{HP}^1$ given in Definition 4.21 maps $\mathcal{L}$ to a set of lines $\psi(\mathcal{L})$ of $\mathbb{H}^2$. For every $\mathbf{v}, \mathbf{w} \in \mathcal{L}$, by Lemma 4.22, we have

$$|\langle \psi(\mathbf{v}), \psi(\mathbf{w})\rangle|^2 = \frac{1 + \langle \mathbf{v}, \mathbf{w}\rangle}{2} = \frac{1 - 1/(n-1)}{2} = \frac{n-2}{2(n-1)},$$

which is exactly the relative bound given in Theorem 2.13 for $d = 2$. □

Define $\phi : \mathbb{H}^2 \to \mathbb{H} \times \mathbb{R}$ by

$$\phi(q_1, q_2) = \left(\frac{2q_1\overline{q_2}}{|q_1|^2 + |q_2|^2}, \frac{|q_1|^2 - |q_2|^2}{|q_1|^2 + |q_2|^2}\right).$$

Notice that for any $c \in \mathbb{H}$, $\phi(cq_1, cq_2) = \phi(q_1, q_2)$. That is, every point on a line in $\mathbb{H}^2$ is mapped to the same point in $\mathbb{H} \times \mathbb{R}$. Since every line in $\mathbb{H}^2$, i.e. a point in $\mathbb{HP}^1$ may be represented by (q_1, q_2) with $|q_1|^2 + |q_2|^2 = 1$, ϕ induces a mapping from $\phi_0 : \mathbb{HP}^1$ to $\mathbb{H} \times \mathbb{R}$ by

$$\phi_0(q_1, q_2) = \left(2q_1\overline{q_2},\, |q_1|^2 - |q_2|^2\right).$$

Since $|\phi_0(q_1, q_2)| = 1$, by identifying the vectors in $\mathbb{H} \times \mathbb{R}$ of norm 1 with S^4, the mapping ϕ_0 can be considered as the inverse of ψ.

Example 4.24. In this example, we give the explicit construction of a tight equiangular set of 6 lines in $\mathbb{H}^2$, using the method described in the proof of Theorem 4.23. First, consider the regular 5-simplex $\mathcal{L}$ in $\mathbb{R}^5$. As described in Example 4.2, $\mathcal{L}$ may be given as the columns of the following matrix:

$$\begin{pmatrix} 3/\sqrt{15} & -3/\sqrt{15} & 0 & 0 & 0 & 0 \\ 1/\sqrt{5} & 1/\sqrt{5} & -2/\sqrt{5} & 0 & 0 & 0 \\ 1/\sqrt{10} & 1/\sqrt{10} & 1/\sqrt{10} & -3/\sqrt{10} & 0 & 0 \\ \sqrt{6}/10 & \sqrt{6}/10 & \sqrt{6}/10 & \sqrt{6}/10 & \sqrt{6}/10 & 0 \\ 1/5 & 1/5 & 1/5 & 1/5 & 1/5 & -1 \end{pmatrix}$$

For every distinct $[\mathbf{v}], [\mathbf{w}] \in \mathcal{L}$ we have $\langle \mathbf{v}, \mathbf{w} \rangle = -1/5$. By applying the mapping ψ, given in Definition 4.21, to the columns of the above matrix, we get the following equiangular set of 6 lines in $\mathbb{H}^2$:

$$\begin{aligned} \mathcal{L} \;=\; \{ & [\begin{pmatrix} r + si + \frac{1}{4}j + tij \\ u \end{pmatrix}], [\begin{pmatrix} -r + si + \frac{1}{4}j + tij \\ u \end{pmatrix}], [\begin{pmatrix} -2si + \frac{1}{4}j + tij \\ u \end{pmatrix}], \\ & [\begin{pmatrix} \frac{-3}{4}j + tij \\ u \end{pmatrix}], [\begin{pmatrix} -tij \\ u \end{pmatrix}], [\begin{pmatrix} 0 \\ 1 \end{pmatrix}]\}, \end{aligned}$$

where $r = \sqrt{6}/4$, $s = \sqrt{2}/4$, $t = \sqrt{15}/20$, and $u = \sqrt{2/5}$.

Example 4.25. By Theorem 2.34, there exist at most 5 MUBs in $\mathbb{H}^2$. Here we construct 5 MUBs in $\mathbb{H}^2$. Consider ψ, given in Definition 4.21, as mapping from S^4 to $\mathbb{H}^2$. Also, consider the standard basis $\{\mathbf{e}_j : 0 \leq j \leq 4\}$ of $\mathbb{R}^5$ as a set of points of S^4. Then

$$\mathcal{B} = \{\{\psi(\mathbf{e}_j), \psi(-\mathbf{e}_j)\} : 0 \leq j \leq 4\}$$

is a set of 5 MUBs in $\mathbb{H}^2$. This is because, by Lemma 4.22, we have

$$|\langle \psi(\pm\mathbf{e}_j), \psi(\pm\mathbf{e}_k) \rangle|^2 = \frac{1 + \langle \pm\mathbf{e}_j, \pm\mathbf{e}_k \rangle}{2} = \frac{1}{2},$$

and

$$|\langle\psi(\mathbf{e}_j),\psi(-\mathbf{e}_j)\rangle|^2 = \frac{1+\langle\mathbf{e}_j,-\mathbf{e}_j\rangle}{2} = 0,$$

for every distinct $0 \le j,k \le 4$.

4.4.4 Tables of Known Constructions

As before, $\mathbb{A}$ stands for any of the associative composition algebras $\mathbb{R},\mathbb{C},\mathbb{H}$. Recall from Theorem 2.8 that an equiangular set of lines in $\mathbb{A}^d$ has size at most $d+\binom{d}{2}\dim_{\mathbb{R}}\mathbb{A}$. Also, recall from Corollary 2.19 that if $n > d+1 > 2$ and there exists a tight equiangular set of n lines in $\mathbb{A}^d$, then

$$n \ge d + \frac{1+\sqrt{\frac{8d}{\dim_{\mathbb{R}}\mathbb{A}}+1}}{2}.$$

To be specific, we have the following lower and upper bounds for each of the associative composition algebras.

Corollary 4.26. *If there exists a tight equiangular set of $n > d+1 > 2$ lines in $\mathbb{A}^d$ then*

$$\begin{array}{rcccll} d+\dfrac{1+\sqrt{8d+1}}{2} & \le & n & \le & \frac{1}{2}d^2+\frac{1}{2}d, & \textit{when } \mathbb{A}=\mathbb{R},\\ d+\dfrac{1+\sqrt{4d+1}}{2} & \le & n & \le & d^2, & \textit{when } \mathbb{A}=\mathbb{C},\\ d+\dfrac{1+\sqrt{2d+1}}{2} & \le & n & \le & 2d^2-d, & \textit{when } \mathbb{A}=\mathbb{H}. \end{array}$$

In the following tables, we give a summary of the existence or non-existence of a tight equiangular set of n lines in $\mathbb{A}^d$, where $\mathbb{A} \in \{\mathbb{R},\mathbb{C},\mathbb{H}\}$. In each cell, corresponding to the value n and the space $\mathbb{A}^d$, the notation

✓ means that a tight equiangular set of n lines in $\mathbb{A}^d$ exists,

× means that no tight equiangular set of n lines in $\mathbb{A}^d$ exists,

[✓] means that an approximate tight equiangular set of lines n in $\mathbb{A}^d$ exists,

?× means that it is conjectured that no tight equiangular set of lines n in $\mathbb{A}^d$ exists.

In the "comments" column, we give a pointer to why a tight equiangular set of n lines in $\mathbb{A}^d$ exists. To avoid repetitions in the tables, we would like to state that for a given n and d, the non-existence of a tight equiangular set of n lines in $\mathbb{A}^d$ is due to Corollary 4.26, unless explained in the "comments" column. Also, all of the notations ?× and [✓] are based on the extensive numerical evidence that we have gathered.

$d = 2$				
n	$\mathbb{R}^d$	$\mathbb{C}^d$	$\mathbb{H}^d$	comments
2	✓			standard basis
3	✓			regular simplex
4	×	✓		W-H orbit (Theorem 4.19), Theorem 4.17
5	×	×	✓	Theorem 4.23
6	×	×	✓	Theorem 4.23

Table 4.1: The existence of tight equiangular set of n lines in $\mathbb{A}^2$, $\mathbb{A} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$

$d = 3$				
n	$\mathbb{R}^d$	$\mathbb{C}^d$	$\mathbb{H}^d$	comments
3	✓			standard basis
4	✓			regular simplex
5	×	×	[✓]	
6	✓			icosahedron
7	×	✓		Theorem 4.14
8	×	?×	[✓]	
9	×	✓		W-H orbit [85, 66], Example 2.29
10 – 13	×	×	[✓]	
14	×	×	?×	
15	×	×	[✓]	

Table 4.2: The existence of tight equiangular set of n lines in $\mathbb{A}^3$, $\mathbb{A} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$

$d = 4$				
n	$\mathbb{R}^d$	$\mathbb{C}^d$	$\mathbb{H}^d$	comments
4	✓			standard basis
5	✓			regular simplex
6	×	×	[✓]	
7	×	✓		Theorem 4.14
8	×	✓		[43], Theorem 4.13
$9-10$	×	?×	[✓]	[43]
$11-12$	×	?×	[✓]	
13	×	✓		Lemma 4.7
$14-15$	×	?×	[✓]	
16	×	✓		W-H orbit [85, 66]
$17-21$	×	×	[✓]	
$22-28$	×	×	?×	

Table 4.3: The existence of tight equiangular set of n lines in $\mathbb{A}^4$, $\mathbb{A} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$

$d = 5$				
n	$\mathbb{R}^d$	$\mathbb{C}^d$	$\mathbb{H}^d$	comments
5	✓			standard basis
6	✓			regular simplex
7	×	×	×	
8	×	?×	[✓]	
9	?×	?×	[✓]	
10	✓			[78]
11	×	✓		[78], Theorem 4.14
$12-15$	×	?×	[✓]	[78]
$16-20$	×	?×	[✓]	
21	×	✓		Lemma 4.7
$22-24$	×	?×	[✓]	
25	×	✓		W-H orbit [85]
$26-28$	×	×	[✓]	
$29-45$	×	×	?×	

Table 4.4: The existence of tight equiangular set of n lines in $\mathbb{A}^5$, $\mathbb{A} \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$

4.5 A List of Open Problems

In this final section, we list a number of intriguing questions and open problems that are raised for further studies.

Conjecture 4.27 (Zauner 1999)**.** *For every d there exists a fiducial vector in $\mathbb{C}^d$. See [85].*

Conjecture 4.28 (Appleby 2005)**.** *Every fiducial vector is an eigenvector of an order* 3 *unitary matrix of a very special form. See [4].*

Conjecture 4.29. *[Khatirinejad 2007] AL fiducial vectors only exist for $p \in \{3, 7, 19\}$. See [53] and Theorem 3.11.*

Question 4.30. Given $d \geq 2$, are all equiangular sets of d^2 lines in $\mathbb{C}^d$ a Weyl-Heisenberg orbit? If not, find such constructions of equiangular set lines.

Question 4.31. Suppose $\mathcal{L}$ is a flat (or almost flat) and tight equiangular set of lines. What can be said about $\mathcal{L}$?

Problem 4.32. Can we generalize the AL fiducial vectors to all prime power dimensions?

Problem 4.33. Could we use any numerical fiducial vector and give an exact proof that it is in fact a fiducial vector? (Possible method (?): bounding the degree and the coefficients of the minimal polynomials of the coordinates of the fiducial vector.)

Problem 4.34. Prove the existence of a fiducial vector $\mathbf{z} \in \mathbb{C}^{13}$ s.t. $\mathbf{z}_{3j} = \mathbf{z}_j \, (\forall j)$. See Example 2.74.

Problem 4.35. Would an assumption like $\mathbf{z}_{f(j)} = \mathbf{z}_j \, (\forall j)$ for a specific function f make the search for a fiducial vector $\mathbf{z}$ easier?

Problem 4.36. Find Gram matrices where each off-diagonal entry is of the form $\frac{1}{\sqrt{d+1}}\omega^k$ for some fixed root of unity ω. See Example 2.29.

Problem 4.37. For given d, k, and $n_1, \ldots, n_k$ find an $(\{n_1; \ldots; n_k\}, k, d)$-MEL. See Definition 2.1.

Question 4.38. Would MELs (other than MUBs) yield a new 2-design?

Question 4.39. What unitary matrices $\mathbf{U}$ have the property that map the set of fiducial vectors to itself? All of the elements of the well-known extended Clifford group do. Anything else?

Bibliography

[1] R. Julian R. Abel, Charles J. Colbourn, and Jeffrey H. Dinitz. Mutually orthogonal latin squares (MOLS). In Charles J. Colbourn and Jeffrey H. Dinitz, editors, *Handbook of combinatorial designs*. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[2] W. O. Alltop. Complex sequences with low periodic correlations. *IEEE Trans. Inform. Theory*, 26(3):350–354, 1980.

[3] George E. Andrews. *Number theory*. Dover Publications Inc., New York, 1994. Corrected reprint of the 1971 original [Dover, New York; MR0309838 (46 #8943)].

[4] D. M. Appleby. Symmetric informationally complete-positive operator valued measures and the extended Clifford group. *J. Math. Phys.*, 46(5):052107, 29, 2005.

[5] D. M. Appleby, Hoan Bui Dang, and Christopher A. Fuchs. Physical significance of symmetric informationally-complete sets of quantum states. *arXiv:0707.2071v1 [quant-ph] 13 Jul 2007*, 2007.

[6] Michael Aschbacher, Andrew M. Childs, and Paweł Wocjan. The limitations of nice mutually unbiased bases. *J. Algebraic Combin.*, 25(2):111–123, 2007.

[7] Brandon Ballinger, Grigoriy Blekherman, Henry Cohn, Noah Giansiracusa, Elizabeth Kelly, and Achill Schuermann. Experimental study of energy-minimizing point configurations on spheres. *arXiv:math/0611451v2*, 2007.

[8] Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. A new proof for the existence of mutually unbiased bases. *Algorithmica*, 34(4):512–528, 2002. Quantum computation and quantum cryptography.

[9] E. Bannai, A. Munemasa, and B. Venkov. The nonexistence of certain tight spherical designs. *Algebra i Analiz*, 16(4):1–23, 2004.

[10] Leonard D. Baumert and Daniel M. Gordon. On the existence of cyclic difference sets with small parameters. In *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, volume 41 of *Fields Inst. Commun.*, pages 61–68. Amer. Math. Soc., Providence, RI, 2004.

[11] John J. Benedetto and Matthew Fickus. Finite normalized tight frames. *Adv. Comput. Math.*, 18(2-4):357–385, 2003.

[12] Ingemar Bengtsson, Wojciech Bruzda, Åsa Ericsson, Jan-Åke Larsson, Wojciech Tadej, and Karol Życzkowski. Mutually unbiased bases and Hadamard matrices of order six. *J. Math. Phys.*, 48(5):052106, 21, 2007.

[13] Thomas Beth, Dieter Jungnickel, and Hanfried Lenz. *Design theory. Vol. I*, volume 69 of *Encyclopedia of Mathematics and its Applications*. Cambridge University Press, Cambridge, second edition, 1999.

[14] Bernhard G. Bodmann and Vern I. Paulsen. Frames, graphs and erasures. *Linear Algebra Appl.*, 404:118–146, 2005.

[15] P. Oscar Boykin, Meera Sitharam, Mohamad Tarifi, and Pawel Wocjan. Real mutually unbiased bases. *www.arxiv.org/quant-ph/0502024*, 2005.

[16] P. Oscar Boykin, Meera Sitharam, Pham Huu Tiep, and Pawel Wocjan. Mutually unbiased bases and orthogonal decompositions of Lie algebras. *Quantum Inf. Comput.*, 7(4):371–382, 2007.

[17] A. R. Calderbank, P. J. Cameron, W. M. Kantor, and J. J. Seidel. Z_4-Kerdock codes, orthogonal spreads, and extremal Euclidean line-sets. *Proc. London Math. Soc. (3)*, 75(2):436–480, 1997.

[18] Peter G. Casazza. The art of frame theory. *Taiwanese J. Math.*, 4(2):129–201, 2000.

[19] Carlton M. Caves, C. A. Fuchs, and R. Schack. Unknown quantum states: the quantum de finetti representation. *J. Math. Phys.*, 43:4537–4559, 2002.

[20] Henry Cohn and Abhinav Kumar. Universally optimal distribution of points on spheres. *J. Amer. Math. Soc.*, 20(1):99–148 (electronic), 2007.

[21] John H. Conway, Ronald H. Hardin, and Neil J. A. Sloane. Packing lines, planes, etc.: packings in Grassmannian spaces. *Experiment. Math.*, 5(2):139–159, 1996.

[22] John H. Conway and Derek A. Smith. *On quaternions and octonions: their geometry, arithmetic, and symmetry.* A K Peters Ltd., Natick, MA, 2003.

[23] H. S. M. Coxeter. *Regular complex polytopes.* Cambridge University Press, Cambridge, second edition, 1991.

[24] Robert Craigen and Hadi Kharaghani. Hadamard matrices and Hadamard designs. In Charles J. Colbourn and Jeffrey H. Dinitz, editors, *Handbook of combinatorial designs.* Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[25] Ingrid Daubechies, A. Grossmann, and Y. Meyer. Painless nonorthogonal expansions. *J. Math. Phys.*, 27(5):1271–1283, 1986.

[26] D. de Caen. Large equiangular sets of lines in Euclidean space. *Electron. J. Combin.*, 7:Research Paper 55, 3 pp. (electronic), 2000.

[27] P. Delsarte, J. M. Goethals, and J. J. Seidel. Bounds for systems of lines and Jacobi polynomials. *Philips Research Reports*, 30(3):91–105, 1975.

[28] P. Delsarte, J. M. Goethals, and J. J. Seidel. Spherical codes and designs. *Geometriae Dedicata*, 6(3):363–388, 1977.

[29] R. J. Duffin and A. C. Schaeffer. A class of nonharmonic Fourier series. *Trans. Amer. Math. Soc.*, 72:341–366, 1952.

[30] H.-D. Ebbinghaus, H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, and R. Remmert. *Numbers*, volume 123 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991. With an introduction by K. Lamotke, Translated from the second 1988 German edition by H. L. S. Orde, Translation edited and with a preface by J. H. Ewing, Readings in Mathematics.

[31] Douglas R. Farenick. *Algebras of linear transformations*. Universitext. Springer-Verlag, New York, 2001.

[32] Douglas R. Farenick and Barbara A. F. Pidkowich. The spectral theorem in quaternions. *Linear Algebra Appl.*, 371:75–102, 2003.

[33] Steven T. Flammia. On SIC-POVMs in prime dimensions. *J. Phys. A*, 39(43):13483–13493, 2006.

[34] Christopher A. Fuchs and Masahide Sasaki. Squeezing quantum information through a classical channel: measuring the "quantumness" of a set of quantum states. *Quantum Inf. Comput.*, 3(5):377–404, 2003.

[35] Chris Godsil. *Algebraic combinatorics*. Chapman and Hall Mathematics Series. Chapman & Hall, New York, 1993.

[36] Chris Godsil and Aidan Roy. Equiangular lines, mutually unbiased bases, and spin models. *arXiv:quant-ph/0511004 v2*, 2006.

[37] Chris Godsil and Gordon Royle. *Algebraic graph theory*, volume 207 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2001.

[38] J.-M. Goethals and J. J. Seidel. The regular two-graph on 276 vertices. *Discrete Math.*, 12:143–158, 1975.

[39] J.-M. Goethals and J. J. Seidel. The football. *Nieuw Arch. Wisk. (3)*, 29(1):50–58, 1981.

[40] Solomon W. Golomb and Guang Gong. *Signal design for good correlation*. Cambridge University Press, Cambridge, 2005. For wireless communication, cryptography, and radar.

[41] Markus Grassl. On SIC-POVMs and MUBs in dimension 6. *http://arXiv.org/abs/quant-ph/0406175*, 2004.

[42] Markus Grassl. Tomography of quantum states in small dimensions. *Electronic Notes in Discrete Mathematics*, 20:151–164, 2005.

[43] J. Haantjes. Equilateral point-sets in elliptic two- and three-dimensional spaces. *Nieuw Arch. Wiskunde (2)*, 22:355–362, 1948.

[44] Kenneth Hoffman and Ray Kunze. *Linear algebra*. Second edition. Prentice-Hall Inc., Englewood Cliffs, N.J., 1971.

[45] S. G. Hoggar. Two quaternionic 4-polytopes. In *The geometric vein*, pages 219–230. Springer, New York, 1981.

[46] Stuart G. Hoggar. 64 lines from a quaternionic polytope. *Geom. Dedicata*, 69(3):287–289, 1998.

[47] Thomas W. Hungerford. *Algebra*, volume 73 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1980. Reprint of the 1974 original.

[48] A. Hurwitz. Über die composition der quadratischen formen von beliebig vielen variabeln. *Gtt. Nachrichten*, pages 309–316, 1898.

[49] Yury J. Ionin and Hadi Kharaghani. Balanced generalized weighing matrices and conference matrices. In Charles J. Colbourn and Jeffrey H. Dinitz, editors, *Handbook of combinatorial designs*. Chapman & Hall/CRC, Boca Raton, FL, second edition, 2007.

[50] I. D. Ivanović. Geometrical description of quantal state determination. *J. Phys. A*, 14(12):3241–3245, 1981.

[51] Deepti Kalra. Complex equiangular cyclic frames and erasures. *Linear Algebra Appl.*, 419(2-3):373–399, 2006.

[52] Phillip Kaye, Raymond Laflamme, and Michele Mosca. *An introduction to quantum computing*. Oxford University Press, Oxford, 2007.

[53] Mahdad Khatirinejad. On the Weyl-Heisenberg orbits of equiangular lines. *Journal of Algebraic Combinatorics*, doi:10.1007/s10801-007-0104-1, 2007.

[54] Andreas Klappenecker and Martin Rötteler. Constructions of mutually unbiased bases. In *Finite fields and applications*, volume 2948 of *Lecture Notes in Comput. Sci.*, pages 137–144. Springer, Berlin, 2004.

[55] Andreas Klappenecker and Martin Rötteler. Mutually unbiased bases are complex projective 2-designs. *arXiv:quant-ph/0502031v2*, 2005.

[56] Andreas Klappenecker, Martin Rötteler, Igor E. Shparlinski, and Arne Winterhof. On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states. *J. Math. Phys.*, 46(8):082104, 17, 2005.

[57] Andrei B. Klimov, José L. Romero, Gunnar Björk, and Luis L. Sánchez-Soto. Geometrical approach to mutually unbiased bases. *J. Phys. A*, 40(14):3987–3998, 2007.

[58] Hermann König. Cubature formulas on spheres. In *Advances in multivariate approximation (Witten-Bommerholz, 1998)*, volume 107 of *Math. Res.*, pages 201–211. Wiley-VCH, Berlin, 1999.

[59] P. W. H. Lemmens and J. J. Seidel. Equiangular lines. *J. Algebra*, 24:494–512, 1973.

[60] Daniel Martin. *Manifold theory.* Horwood Publishing Series in Mathematics & Applications. Horwood Publishing Limited, Chichester, 2002. Introduction for mathematical physicists, Revised reprint of the 1991 edition.

[61] Howard H. Mitchell. Determination of all primitive collineation groups in more than four variables which contain homologies. *Amer. J. Math.*, 36(1):1–12, 1914.

[62] Bishwarup Mondal, Roopsha Samanta, and Robert W. Heath, Jr. Congruent Voronoi tessellations from equiangular lines. *Appl. Comput. Harmon. Anal.*, 23(2):254–258, 2007.

[63] Michael A. Nielsen and Isaac L. Chuang. *Quantum computation and quantum information.* Cambridge University Press, Cambridge, 2000.

[64] K. B. Reid and Ezra Brown. Doubly regular tournaments are equivalent to skew Hadamard matrices. *J. Combinatorial Theory Ser. A*, 12:332–338, 1972.

[65] Joseph M. Renes. Equiangular tight frames from Paley tournaments. *Linear Algebra Appl.*, 426(2-3):497–501, 2007.

[66] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *J. Math. Phys.*, 45(6):2171–2180, 2004.

[67] Aidan Roy. *Complex lines with restricted angles.* PhD thesis, University of Waterloo, 2005.

[68] Walter Rudin. *Function theory in the unit ball of* $\mathbf{C}^n$, volume 241 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science].* Springer-Verlag, New York, 1980.

[69] Dilip V. Sarwate. Meeting the Welch bound with equality. In *Sequences and their applications (Singapore, 1998)*, Springer Ser. Discrete Math. Theor. Comput. Sci., pages 79–102. Springer, London, 1999.

[70] A. J. Scott, Jonathan Walgate, and Barry C. Sanders. Optimal fingerprinting strategies with one-sided error. *Quantum Inf. Comput.*, 7(3):243–264, 2007.

[71] J. J. Seidel. *Geometry and combinatorics*. Academic Press Inc., Boston, MA, 1991. Selected works of J. J. Seidel, Edited and with a preface by D. G. Corneil and R. Mathon.

[72] Jean-Pierre Serre. Quelques applications du theoreme de densite de Chebotarev. *Publications mathematiques de l'I.H.E.S.*, 54:123–201, 1981.

[73] P. D. Seymour and Thomas Zaslavsky. Averaging sets: a generalization of mean values and spherical designs. *Adv. in Math.*, 52(3):213–240, 1984.

[74] Igor E. Shparlinski and Arne Winterhof. Constructions of approximately mutually unbiased bases. In *LATIN 2006: Theoretical informatics*, volume 3887 of *Lecture Notes in Comput. Sci.*, pages 793–799. Springer, Berlin, 2006.

[75] Thomas Strohmer and Robert W. Heath, Jr. Grassmannian frames with applications to coding and communication. *Appl. Comput. Harmon. Anal.*, 14(3):257–275, 2003.

[76] Mátyás A. Sustik, Joel A. Tropp, Inderjit S. Dhillon, and Robert W. Heath, Jr. On the existence of equiangular tight frames. *Linear Algebra Appl.*, 426(2-3):619–635, 2007.

[77] J. A. Tropp. Complex equiangular tight frames. In *Proc. SPIE Wavelets XI*, pages 590412.01–11, San Diego, August 2005.

[78] J. H. van Lint and J. J. Seidel. Equilateral point sets in elliptic geometry. *Nederl. Akad. Wetensch. Proc. Ser. A 69=Indag. Math.*, 28:335–348, 1966.

[79] J. H. van Lint and R. M. Wilson. *A course in combinatorics*. Cambridge University Press, Cambridge, second edition, 2001.

[80] James W. Vick. *Homology theory*, volume 145 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1994. An introduction to algebraic topology.

[81] L. R. Welch. Lower bounds on the maximum cross-correlation of signals. *IEEE Trans. Inform. Theory*, 20:397–399, 1974.

[82] Pawel Wocjan and Thomas Beth. New construction of mutually unbiased bases in square dimensions. *Quantum Inf. Comput.*, 5(2):93–101, 2005.

[83] William K. Wootters and Brian D. Fields. Optimal state-determination by mutually unbiased measurements. *Ann. Physics*, 191(2):363–381, 1989.

[84] Pengfei Xia, Shengli Zhou, and Georgios B. Giannakis. Achieving the Welch bound with difference sets. *IEEE Trans. Inform. Theory*, 51(5):1900–1907, 2005.

[85] Gerhard Zauner. *Quantum designs–Foundations of a non-commutative theory of designs (in German).* PhD thesis, University of Vienna, 1999.

[86] Fuzhen Zhang. Quaternions and matrices of quaternions. *Linear Algebra Appl.*, 251:21–57, 1997.

Index