DISSERTATION

EQUIANGULAR TIGHT FRAMES AND MUTUALLY UNBIASED BASES OVER FINITE FIELDS

Submitted by

Ian Jorquera

Department of Mathematics

In partial fulfillment of the requirements

For the Degree of Doctor of Philosophy

Colorado State University

Fort Collins, Colorado

Spring 2026

Doctoral Committee:

Advisor: Emily J. King

James Wilson
Clayton Shonkwiler
Ewan Davies

ABSTRACT

EQUIANGULAR TIGHT FRAMES AND MUTUALLY UNBIASED BASES OVER FINITE FIELDS

This paper concerns frames, equiangular lines, and mutually unbiased bases over finite fields. We find a necessary and sufficient condition for systems of equiangular lines over finite fields to be equiangular tight frames (ETFs). As is the case over subfields of $\mathbb{C}$, it is necessary for the Welch bound to be saturated, but there is an additional condition required involving sums of triple products. We also prove that similar to the case over $\mathbb{C}$, collections of vectors are similar to a regular simplex essentially when the triple products of their scalar products satisfy a certain property. Finally, we investigate switching equivalence classes of frames and systems of lines focusing on systems of equiangular lines in finite orthogonal geometries with maximal incoherent sets, drawing connections to combinatorial design theory. Concerning mutually unbiased bases (MUBs) over finite fields we show that, just as in the case over $\mathbb{C}$, their existence is equivalent to the existence of mutually unbiased Hadamard matrices. We give a necessary condition for the existence of $d \times d$ Hadamard matrices whose entries are from a finite field and are prime power roots of unity.

ACKNOWLEDGEMENTS

I would like to thank my friend Daniele for providing me a recipe for bread.

DEDICATION

I would like to dedicate this thesis to spoon and tigre who are cats.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

Chapter 1

Foundations

1.1 Introduction

Consider the following situation: you are planning a seating arrangement for an upcoming exam. You know that there will be n students taking the exam, and your goal is to devise a way to seat all of the students as spread out as possible. Throughout the semester you know you will hold your exams in one of three different exam rooms: the first room is fairly standard and is a square, the second room is new and would put students on the exterior of a sphere, and finally the third room puts students on the interior of the sphere. The interior of the sphere adds the addition difficult that students can see across the sphere and see student on the antipodal points of the sphere. This type of problem, of packing points in some space, so every point is as spread out as possible is a very common problem and shows up in many applications; The problem of packings points in a $(d-1)$-dimensional projective space or equivalently that of packing lines though the origin in a d-dimensional space that are maximally spread apart is an example that shows up in fields as diverse as compressed sensing [BFMW13], digital fingerprinting [MQKF13], quantum state tomography [RBSC04; FHS17], multiple description coding [SH03; MD14; Wel74a], and discrete geometry [Fej65]. A very related question is that of packing points on a Grassmannian, or k-dimensional subspaces in a d-dimensional space. Throughout this paper we wish to develop a variety of tools used in problems of this type, as well as expand on the multitude of applications and equivalent formulations of these problem.

Frame theory provides a fairly strong setting for studying the packing problems we will be primarily interested in: finding optimal packings of lines in a variety of spaces. The classical theory focuses on lines in $\mathbb{F}^d$ where $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$. In these cases a line ℓ can be represented by a vector φ which spans the line ℓ. The interior angle θ, between two lines ℓ_1 and ℓ_2 which are represented by the non-zero vectors φ_1 and φ_2, may be computed using the magnitude squared of the standard inner product $|\langle\varphi_1, \varphi_2\rangle|^2 = \|\varphi_1\|^2 \|\varphi_2\|^2 \cos^2(\theta)$. Hence, the study of line packings, by a choice of vector representatives, turns into a question about linear algebra: specifically related to inner products. This also allows us to quickly modify our motivating packing problem from being one of geometry, to one in terms of geometric algebra. By putting the vector representatives of each of the lines into the columns of a matrix Φ, studying the inner products can then be done by looking at the Gram matrix $\Phi^*\Phi$ which is Hermitian and positive semi-definite. The theory of packings of lines, under this perspective will be the primary focus of Section 2.1. The definition of a frame, provided in Definition 2.1.1, is much more general then just being a formalization for packing problems; frames were originally created to be generalizations of orthonormal bases, and what constitutes a nice frame, called a tight frame, in this regard is closely related to the spectrum of the Gram matrix, as shown in Proposition 2.1.4.

The simplest definition of a frame, in the finite setting, is a spanning set for a Hilbert space. Unlike that of an orthonormal basis, the vectors need not and often will not be linearly independent. We may then wish to maximize the size of the smallest set of vectors in the spanning set which are linearly dependent. This notion of optimality is algebraic in nature, and is often referred to in terms of algebraic spread. In Section 2.2, we will use the theory of matroids, developed in Section 1.4 to better understand the algebraic spread of frames, showing in Proposition 2.2.2 that frames with optimal algebraic spread have matroids which are uniform.

A more standard approach to understand what optimality might mean is through geometry and defining spread in geometric terms. Geometrically this might mean we want to find arrangements of lines in $\mathbb{F}^d$, whose pairwise interior angles are maximized. In this case we are considering a notion of distance that is equal to the interior angle between the lines. This distance is the geodesic distance between the lines, when viewing the collections of all lines through the origin as a Riemannian manifold: $d_g(\ell, \ell') = \theta$. It is fairly reasonable to then want to maximize the angles between lines, specifically we may wish to maximize the smallest pairwise angle in our arrangement of lines, because an arrangement would only be as good as its closest pair of lines. and a "nice" packings of lines would then be one with a high minimal angle between lines. In Section 2.3, we will look at the structure of frames which maximize this geometric spread, called Grassmannian frames, first by looking at the equivalently problem of minimizing the maximum magnitude of the inner products, and finding bounds on the maximum magnitudes, the Welch bound in Theorem 2.3.4 and the orthoplex bound in Theorem 2.3.9. In Theorem 2.3.4 we will also show that the frames which saturate the Welch bound are equiangular and tight, and called equiangular tight frames (ETFs). In Theorem 2.3.5, more commonly referred to as Gerzon's Bound, we will give an upper bound on the maximum number of lines in a space $V = \mathbb{F}^d$ which can be equiangular. Gerzon's bound will end being equal to the dimension of the space of self adjoint operators on V. It is an unknown problem whether there are infinitely many dimension's d in which there exists n equiangular lines in $\mathbb{F}^d$ which saturate Gerzon's bound. In complex spaces, $V = \mathbb{C}^d$, after looking at the highly symmetric nature of many such packings, Zauner conjectured in his PhD thesis in [Zau99; Zau11], that maximal collections of equiangular lines, which saturate Gerzon's bound, should exist in all dimensions. In the real setting the problem is vastly different and instead it is known that in many dimensions Gerzon's bound is not saturated. In fact [STDH07] shows that a necessarily condition for the existence of a maximal collection of real equiangular lines in $\mathbb{F}^d$, where $d > 3$ is that $\sqrt{d+2}$ is an odd integer. It is conjectured that the only dimensions over the reals in which Gerzon's bound is saturated are $d = 2, 3, 7$, and 23. This has been conjectured by many, in as early as [GR01]. More recently the conjecture was strengthened by Gillespie in [Gil18] who observed certain combinatorial structure in these dimensions and showed that any maximal collection of lines with the same combinatorial structure could only exist in these four dimensions.

The second bound is the orthoplex bound, which is a bound on the coherence for collections of lines which exceed Gerzon's bound and can no longer be equiangular. Known examples which saturate the orthoplex bound come from maximal sets of mutually unbiased bases (MUBs), collections of lines in $\mathbb{F}^d$ which form $d+1$ orthonormal bases, with the vectors of distinct bases maximal spread apart. The existence of the maximal collections of mutually unbiased bases is unknown in general, but in the complex setting they are known to exist, as eigenvectors of certain unitary maps, whenever the dimension d is a prime power, which we will see in Theorem 2.3.13.

These two bounds can be interpreted as ordaining greater importance to these two objects: equiangular tight frames and mutually unbiased bases, due to their optimality with respect to this notion of geometric spread. It is however not the case that frames with good geometric spread have good algebraic spread, nor vice versa. In Chapter 3, we extend the classical theory to a more general setting, loosening the underlying assumption that the spaces in which we are packing are inner product spaces and instead requiring that they only have non-degenerate scalar products. This allows us to consider the same frame theoretic objects in vector spaces over arbitrary fields. The theory of bilinear forms and scalar products for vector spaces over arbitrary fields is presented in Section 1.3 after a short recollection of Galois theory and linear maps presented in Section 1.2. In Chapter 3 we will give special attention to the theory of frames over finite fields and although frames over finite fields do not generalize in the sense of geometrically optimal packings, or Grassmannian frames, they generalize the structure in the classical settings which where known to be optimal packings. Therefore frames over finite fields can play a crucial role in understanding the existence of such objects whose importance was decreed by their optimality in the classical setting. The theory of frames over finite fields, or more generally over arbitrary fields was first presented in [GIJM22a; GIJM22b] who showed a connection between the existence of equiangular tight frames over $\mathbb{C}$ or $\mathbb{R}$ with the existence of equiangular tight frames over the real and complex finite field analogs. These results are shown in Section 3.2, in addition to Theorem 3.2.6 which shows a similar connection for mutually unbiased bases.

Sections 3.3 to 3.5 are very similar to [JK25], which is under review by the journal Finite Fields and their Applications. These sections build off previous work on frames over finite fields from [GIJM22a; GIJM22b; IKM21]. Other authors, such as [BLRTT09], have also investigated frames for binary vector spaces under the Hamming distance. Frames over finite fields have been shown to have many structural overlaps with frames over $\mathbb{R}$, and $\mathbb{C}$, in addition to vastly different behaviors, including the existence of infinite families of frames which saturate Gerzon's bound. Throughout, we present a number of explicit examples (Examples 1.3.17, 3.3.5, 3.3.17, 3.4.3, 3.4.8, 3.4.14, 3.5.8, 3.5.10 and 3.5.14) of collections of vectors over finite fields which behave in ways counter intuitive to researchers accustomed to working over characteristic zero.

In Section 3.1 we give an overview of frame theory over arbitrary fields using the weaker notion of a Hermitian scalar products instead of inner products used in frame theory over Hilbert spaces, paying special attention to commonly used results which do not hold over in this more general setting. The start of Section 3.3 looks at an equivalence of systems of equiangular lines, known as switching equivalence, which strongly corresponds to what is known in the complex setting, except with the addition of isotropic vectors, vectors that behave like zero with respect to the scalar product. The end of this section then presents some of the combinatorial connections to frames in orthogonal geometries, the finite field analog to real vector spaces.

Section 3.4 focuses on properties of tight frames and investigates the situations in which equiangular systems of lines are equiangular tight frames. In Theorem 3.4.16, we provide an additional necessary and sufficient condition such that saturating the Welch bound means that a set of equiangular lines forms an ETF, and in Theorem 3.4.19 we prove a corollary to Theorem 4.3 in [GIJM22b] where we show a connection between ETFs in orthogonal geometries to regular two-graphs.

In the last section we investigate the situations in which ETFs have subsets of their vectors whose triple products are all equal. In Theorem 3.5.7 we show that, just as in the real and complex settings, equal triple products can determine the existence of regular simplices. Likewise such sets can be considered to be incoherent sets of regular two-graphs which result in quasi-symmetric 2-designs, and in the case where Gerzon's bound is saturated, 4-designs, which is shown in Theorem 3.5.18.

Looking then at the second preordained object: mutually unbiased bases, we show that the existence of n MUBs in $\mathbb{C}^d$ implies the existence of n MUBs in $\mathbb{F}^d$, where $\mathbb{F}$ is a finite field, for fields of infinitely many characteristics. The goal of this section is determine cases for the non-existence of MUBs for vector spaces over finite fields, which can then help be understand when MUBs for complex vector spaces might exist. We build off the work in [MST21], which showed in Proposition 3.6.3 that the construction in prime power dimensions also holds over a set of characteristics of positive Dirichlet density. Just as in the complex setting, in Proposition 3.1.12 it is shown that the existence of mutually unbiased bases is equivalent to the existence of certain collections of Hadamard matrices whose entires are roots of unity. Necessary conditions for the existence of Hadamards can then be given based on the existence of vanishing sums of roots of unity, with some results following immediately from [LL96]. Lemma 3.6.7 gives one example of a necessary condition on the existence of a Hadamard matrix whose entires are mth roots of unity, where m is a prime power. Understanding better the cases where vanishing sums of roots of unity exist, and more importantly when they do not is an area of future work.

Another area of future work is in the design of algorithms to numerical find the objects which were bestowed with greater importance in Section 2.3 such as equiangular tight frames. In this section we present an algorithm, the alternating projections algorithm which in its simplest form takes in a random $d \times n$ matrix, and asks what is the closest $d \times n$ matrix which is a tight frame. And likewise given a random $d \times n$ matrix we can ask what is the closest $d \times n$ matrix whose columns are equiangular. The hope is that by repeatedly asking and alternating which of these questions we ask, we will eventually converge on a $d \times n$ matrix whose columns are an equiangular tight frame. This method can be extended to find nice packing in Grassmannian and as future work we want to extend this algorithm to find packing of lines over the quaternions, to help determine if such packings have similar symmetries as in the real and complex cases.

Finally Chapter 5 looks at an application of equiangular systems which saturate Gerzon's bound which give rise to nice measurement operators know as symmetric informationally complete positive operator-valued measures (SIC-POVMs).

1.2 Algebraic Foundations

Throughout we will use $\mathbb{F}$ to denote a field. If $\mathbb{F}$ is finite we will denote the field by the number of elements: $\mathbb{F}_q$ being the field with $q = p^\ell$ elements, with p a prime, unique up to isomorphism. The algebraic closure of $\mathbb{F}_p$ will be denoted by $\overline{\mathbb{F}_p}$. Often we will wish to consider additional structure, for example the field $\mathbb{C}$ is equipped with the involution of complex conjugation that encodes additional geometric structure coming from the fact that $\mathbb{C}$ is a degree 2 Galois extension of $\mathbb{R}$. For $\mathbb{F}_{q^2}$ where q is a prime power, there is a unique non-trivial involution $(-)^\sigma : \mathbb{F} \to \mathbb{F}$: the Frobenius involution defined by $a^\sigma = a^q$ coming from a degree two Galois extension over $\mathbb{F}_q$. In all other finite fields, the only involution is the trivial one.

We will call the **prime subfield** of a field $\mathbb{F}$ to be the smallest subfield containing 1. The **characteristic** of a field $\mathbb{F}$, denoted $\operatorname{char} \mathbb{F}$ is the smallest positive integer such that $nx = 0$ for all $x \in \mathbb{F}$, and if not such integer exists, then $\operatorname{char} \mathbb{F} = 0$. When the $\operatorname{char} \mathbb{F} = 0$ the prime subfield is $\mathbb{Q}$ and when $\operatorname{char} \mathbb{F} = p$ the prime subfield is $\mathbb{F}_p$.

In this section we will give an overview of the field theory used through out this paper, with a particular focus on finite fields, but we will point towards [LN96] for a more in-depth overview of finite fields and [DF04] for a more complete overview of arbitrary fields and Galois theory.

Fields

In this section we wish to review some of the ideas and topics in the study of fields, or more generally of rings. Much of the theory concerns itself with roots of polynomials and whether a field (or ring) contains all of the roots of a given polynomial. For example $x^2 + 1$ has no roots in $\mathbb{R}$, 2 roots in $\mathbb{C}$ and infinitely many roots in the quaternions $\mathbb{H}$ (where $\mathbb{H}$ is only a division ring and not a field). Over a field $\mathbb{F}$, a polynomial with coefficients in $\mathbb{F}$ of degree d has at most d roots up to multiplicity in $\mathbb{F}$. A root is called **simple** if its multiplicity is 1 and called a **repeated root** otherwise. If $f \in \mathbb{F}[x]$ with α a root, then α is a repeated root if and only if it is a root of both f and its **formal derivative** f', which is the resulting polynomial after applying the power rule to each term.

Let $f(x) \in \mathbb{F}[x]$. We say f **splits** over $\mathbb{F}$ if it can be written as a product of linear factors, and informally we will say $\mathbb{F}$ contains all its roots. The **splitting field** of $f(x)$ is the smallest field that contains $\mathbb{F}$ and all the roots of f (the smallest field in which f splits). For example we may consider the equation $x^2 + 1$ which is irreducible over $\mathbb{R}$, and whose roots would behave as $\pm\sqrt{-1}$.

The splitting field in this case would be $\mathbb{C}$. There is also additional algebraic structure here in the form of symmetries, as from the perspective of $\mathbb{R}$ the two added roots behave identically, in that they are both roots of $x^2 + 1$. We can formalize this by defining a field automorphism on $\mathbb{C}$ which maps $\sqrt{-1} \mapsto -\sqrt{-1}$ and keeps $\mathbb{R}$ fixed. This automorphism is that of complex conjugation.

More generally we can consider any polynomial over $\mathbb{F}$ which is irreducible: let $f(x)$ be irreducible and let α be a root of $f(x)$. Morally our goal is to add α to our field $\mathbb{F}$, where α may be considered to be a formal element that will satisfy the equation $f(\alpha) = 0$. If $\deg(f(x)) = d$ then the $f(x)$ gives a minimal linear dependence relation between $1, \alpha, \ldots, \alpha^d$, specifically $\sum_{k=0}^{d} \alpha^k = 0$, and so the elements of $1, \alpha, \ldots, \alpha^{d-1}$ would be linearly dependent over $\mathbb{F}$, defining an $\mathbb{F}$-vector space $\mathbb{K}$ spanned by the $1, \alpha, \ldots, \alpha^{d-1}$. Because $\mathbb{K}$ is defined by adding α, meaning $\mathbb{K}$ is the smallest field containing both $\mathbb{F}$ and α, we will write $\mathbb{K} = \mathbb{F}(\alpha)$. This vector space has the additional structure of multiplication, specifically that $f(\alpha) = 0$, allowing us to write α^d in terms of the lower degree terms. With this multiplicative structure $\mathbb{K}$ is in fact a field (whenever f is irreducible), and we would say $\mathbb{K}$ is a **field extension** of $\mathbb{F}$, denoted $\mathbb{K}/\mathbb{F}$. Furthermore we will define $[\mathbb{K} : \mathbb{F}] = \dim_{\mathbb{F}} \mathbb{K}$ to be the **degree** of the field extension. In general we say a field $\mathbb{K}$ is a field extension over the field $\mathbb{F}$ if $\mathbb{F} \subseteq \mathbb{K}$, and $\mathbb{F}$ is a **subfield** of $\mathbb{K}$. If $\mathbb{K}$ is an extension of $\mathbb{F}$, then it can always be viewed as a vector space over $\mathbb{F}$ by forgetting the multiplicative structure. Field extensions are in many ways transitive, as if $\mathbb{L}$ is a field extension of $\mathbb{K}$ and $\mathbb{K}$ a field extension of $\mathbb{F}$ then $\mathbb{L}$ is a field extension of $\mathbb{F}$ and $[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}]$.

If $\mathbb{K}$ is a field extension of $\mathbb{F}$ where $\alpha \in \mathbb{K}$ but $\alpha \notin \mathbb{F}$, either there is a linear dependence relation amongst the elements of $\left\{ \alpha^k \;\middle|\; k \in \mathbb{Z} \right\}$ or there is not. If it does not, we would call α **transcendental**, and say $\mathbb{K}$ is a transcendental extension over $\mathbb{F}$ if it contains any transcendental elements. As an example π is **transcendental** over $\mathbb{Q}$, meaning $\mathbb{Q}(\pi)/\mathbb{Q}$ is a transcendental extension. Alternatively, there may exist a linear dependence relation amongst the powers of α, in which case we would say that α is **algebraic** and the extension $\mathbb{F}(\alpha)/\mathbb{F}$ is an **algebraic extension** if it contains only algebraic elements. A extension being algebraic is equivalent to the extension being finite. In this case we will define the **minimal polynomial** $m_\alpha(x)$ to be the unique monic polynomial, of smallest degree, such that $m_\alpha(\alpha) = 0$. This tells us about the smallest linear dependence relation, as m_α would be irreducible: therefore $\mathbb{F}(\alpha) \cong \mathbb{F}[x]/(m_\alpha)$ and so $1, \alpha, \ldots, \alpha^{d-1}$ would form a basis for $\mathbb{F}(\alpha)$ over $\mathbb{F}$. The existence and uniqueness of the minimal polynomials follow from the polynomial ring $\mathbb{F}[x]$ being a principal ideal domain.

It is important to note that any algebraic extension $\mathbb{F}(\alpha)$ may not be the splitting field for $m_\alpha(x)$. If $\mathbb{F} = \mathbb{Q}$ then the field extension $\mathbb{Q}(\sqrt[3]{2})$ would be a degree 3 extension as $x^3 - 2$ is its minimal polynomial, however the minimal polynomial also has complex roots which are not contained in the field extension. We will say an algebraic field extension $\mathbb{K}/\mathbb{F}$ is **normal** if any irreducible polynomial f over $\mathbb{F}$ splits in $\mathbb{K}$ if it has at least one root in $\mathbb{K}$. A polynomial f is called **separable** if it has no repeated roots over its splitting field. An algebraic field extension $\mathbb{K}/\mathbb{F}$ is said to be **separable** if for every $\alpha \in \mathbb{K}$, the minimal polynomial over $\mathbb{F}$, $m_\alpha(x)$, is separable. A field $\mathbb{F}$ is called **perfect** if every irreducible polynomial f is separable. This is equivalent to every finite extension of $\mathbb{F}$ being a separable extension.

Proposition 1.2.1. *Let $\mathbb{F}$ be a field of characteristic 0, or a finite field, then $\mathbb{F}$ is perfect.*

This is a very powerful result as it tells us that the field extensions we will be concerned with in this paper will all be separable. An extension that is both normal and separable is called **Galois**. Galois extensions are particularly nice as they allow us to explicitly describe the structure of a field extension by looking at the symmetries of the elements in the extension. As in the case of $\mathbb{C}$ with the interchangeability of i and $-i$, for any field extension $\mathbb{K}/\mathbb{F}$ we will consider the automorphism of $\mathbb{K}$ which keep $\mathbb{F}$ fixed. The set of all such automorphisms form a group called the **Galois group**, denoted $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Before highlighting the fundamental result of Galois extensions we will highlight a failing of non-Galois extensions.

Example 1.2.2. As mention above the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension, and therefore not Galois. Consider any $\varphi \in \mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})$ and notice that $2 = \varphi(2) = \varphi(\sqrt[3]{2})^3$. And because $\sqrt[3]{2}$ is the only root of $x^3 - 2$ in the field extension this must mean $\varphi(\sqrt[3]{2}) = \sqrt[3]{2}$. So the Galois group is trivial. However notice that for the trivial extension $\mathbb{Q}/\mathbb{Q}$, the Galois group is also trivial. This means from the perspective of the Galois groups, these fields are indistinguishable.

Galois extensions avoid this, and Galois groups fully characterize the structure of a field extension. To formalize this a bit more: let $\mathbb{K}/\mathbb{F}$ be an algebraic field extension and $G = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ its Galois group. For any $H \leq G$ we will define the **fixed field** with respect to H as $\mathbb{K}^H$ which are all the elements fixed by the automorphism in H. It can be seen that $\mathbb{K}^H$ is an extension of $\mathbb{F}$ and $\mathbb{K}$ is an extension of $\mathbb{K}^H$. Galois extension then have a one-to-one correspondence between subgroup of their Galois groups and intermediate field extension of $\mathbb{F}$ which are contained in $\mathbb{K}$.

Theorem 1.2.3. *(Chapter 14.2 Theorem 14 [DF04]) Let $\mathbb{K}/\mathbb{F}$ be an algebraic field extension.*

- *If $H \leq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ then its fixed field $\mathbb{K}^H$ is an extension of $\mathbb{F}$ contained in $\mathbb{K}$.*
- *If $\mathbb{L}/\mathbb{F}$ is a intermediate field extension of $\mathbb{F}$ contained in $\mathbb{K}$, then $\mathrm{Gal}(\mathbb{K}/\mathbb{L}) \leq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.*
- *If $H \leq J \leq \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ then $\mathbb{K}^H \supseteq \mathbb{K}^J$. And for intermediate fields $\mathbb{F} \subseteq \mathbb{L} \subseteq E \subseteq \mathbb{K}$, then $\mathrm{Gal}(\mathbb{K}/\mathbb{L}) \geq \mathrm{Gal}(\mathbb{K}/E)$.*

This correspondence is a one-to-one correspondence if and only if $\mathbb{K}/\mathbb{F}$ is Galois.

Galois extensions are equivalently characterized in the following ways

Theorem 1.2.4. *(Chapter 14 [DF04]) Let $\mathbb{K}/\mathbb{F}$ be an algebraic field extension, then the following are equivalent:*

- *$\mathbb{K}/\mathbb{F}$ is Galois;*
- *$\mathbb{K}$ is the splitting field of some $f \in \mathbb{F}[x]$;*
- *$|\mathrm{Gal}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}]$;*
- *$|\mathrm{Gal}(\mathbb{K}/\mathbb{F})| \geq [\mathbb{K} : \mathbb{F}]$; and*
- *$\mathbb{F}$ is the fixed field of $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$.*

Some additional terminology we will use throughout includes a **number field**, which is any algebraic extension of $\mathbb{Q}$ and an **algebraic number**, which is any element $z \in \mathbb{C}$ which is also a contained in a number field. This is equivalent to its (monic) minimal polynomial having coefficients in $\mathbb{Q}$. Morally this is telling us that higher powers of z can be rewritten as rational linear combinations of the lower powers of z. An **algebraic integer** is an element $z \in \mathbb{C}$ whose minimal polynomial has integer coefficients, and therefore the higher powers of z can be rewritten as integer linear combinations of the lower powers of z. For E a number field, we will denote to collection of algebraic integers contained in E as O_E.

As we have seen in the characteristic 0 case, not all algebraic extensions are normal, and therefore not Galois. The story is different over finite fields in which all algebraic extensions are Galois. Consider a finite field $\mathbb{F}_q$ of $q = p^\ell$ elements, which can be viewed as an extension of its prime subfield $\mathbb{F}_p$. Notice that every element of $\mathbb{F}_q$ is a root of the polynomial $x^q - x \in \mathbb{F}_p[x]$. Because there are q elements of $\mathbb{F}_q$, this means $\mathbb{F}_q$ is the splitting field of $x^q - x$, and therefore is Galois over $\mathbb{F}_p$. Equivalently this can be seen by considering the Galois group of a degree k extension $\mathbb{F}_{q^k}/\mathbb{F}_q$ where q is any prime power. The **Frobenius automorphism**, σ where $x \mapsto x^q$ is a degree k automorphism that fixes $\mathbb{F}_q$. This means that the cyclic group, generated by the Frobenius automorphism, would be a k-element subgroup of the Galois group. This would then imply that the extension is Galois and that $\mathrm{Gal}(\mathbb{F}_{q^k}/\mathbb{F}_q) = \langle \sigma \rangle$.

As we saw previously the element of a finite field $\mathbb{F}_q$ are the roots of $x^q - x = x(x^{q-1} - 1)$ which means the non-zero elements are all $q - 1$ roots of 1. For this reason, for any prime power q there exists a finite field of q elements which is unique up to isomorphism. A element $\alpha \in \mathbb{F}_q$ is called **primitive** if it generates the multiplicative group $\mathbb{F}_q^\times$ in which case $\mathbb{F}_q \cong \mathbb{F}_p(\alpha) \cong \mathbb{F}_p[x]/(m_\alpha(x))$. Minimal polynomials of primitive elements are of particular interest in computational algebra, specifically those called Conway polynomials.

Because finite fields are Galois extensions over any one of their subfields, we can say a lot of the roots of irreducible polynomials. Let f be a degree n irreducible polynomial of $\mathbb{F}_q$, Its splitting field is $\mathbb{F}_{q^n}$ and if α is a root, then the n distinct roots of f are $\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{n-1}}$, and are called the **conjugates** of α. If the conjugates of α form a basis for the $\mathbb{F}_q$-vector space $\mathbb{F}_{q^n}$, we will call it a normal basis. More generally a **normal basis** is a basis for $\mathbb{K}/\mathbb{F}$ of the form

$\{\sigma(\alpha) : \sigma \in \text{Gal}(\mathbb{K}/\mathbb{F})\}$ for some fixed α. [Ian: *Normal basis exist if and only if $\mathbb{K}/\mathbb{F}$ is Galois. This is a non-trivial thing to prove though. I think i have this proof written up so i will copy it over when needed. I also might be missing a condition, but at the very least this is true for finite fields.*]

For a field extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ we will define the **trace** over $\mathbb{F}_q$ to be the linear $\mathbb{F}_q$-functional $\text{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ to be the map that takes an element $\alpha \in \mathbb{F}_{q^n}$ to the sum of its conjugates: $\alpha \mapsto \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$. The trace over the prime subfield, is then called the **absolute trace** and is denoted $\text{tr}_{\mathbb{F}_{q^n}}$. The trace $\text{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$ is surjective onto $\mathbb{F}_q$ and is invariant under conjugation. We will also define the **norm** over $\mathbb{F}_q$ to be the multiplicative map $N_{\mathbb{F}_{q^n}/\mathbb{F}_q} : \mathbb{F}_{q^n} \to \mathbb{F}_q$ to be the map that takes an element $\alpha \in \mathbb{F}_{q^n}$ to the product of its conjugates: $\alpha \mapsto \alpha \cdot \alpha^q \cdots \alpha^{q^{n-1}}$. The norm is a group homomorphism between the multiplicative groups, maps $\mathbb{F}_{q^n}$ onto $\mathbb{F}_q$, and is also invariant under conjugation. In more generality, we can define the trace and norm over any Galois extension, such that the trace of an element would be the sum of the Galois conjugates and the norm, the product. However it will generally not be the case that the trace and norm would be surjective, for example the norm for the extension $\mathbb{C}/\mathbb{R}$ which is the complex norm, is not surjective onto $\mathbb{R}$.

Through out this paper we will be primarily interested in degree 2 Galois field extensions, or field extensions which have a involution in their Galois group. This will allows to algebraically mimic the involution of complex conjugation. In the case of a finite field $\mathbb{F}_{q^2}/\mathbb{F}_q$ this involution is coming from the Frobenius automorphism: $x \mapsto x^q$.

A Spectral Theory

Let V and W be finite dimensional vector spaces over a common field $\mathbb{F}$, in which case $A : V \to W$ is said to be **linear** if $A(x + ry) = A(x) + rA(y)$ for all $r \in \mathbb{F}$ and $x, y \in V$. If $\dim_{\mathbb{F}}(V) = d$ then $V \cong \mathbb{F}^d$. This isomorphism is non-canonical and requires the choice a basis $\{v_1, \ldots, v_d\}$, where one isomorphism would then map v_j to the vector with 1 in the jth entry and 0 everywhere else. Fixing bases $(v_j)_{j=1}^d$ and $(w_j)_{j=1}^n$ for V and W respectively then allows us to write a linear map $A : V \to W$ as a matrix $A = [a_{ij}]_{i\in[n],j\in[d]}$, such that $A(v_j) = \sum_{k=1}^n a_{kj}w_k$.

Because the initial isomorphism $V \cong \mathbb{F}^d$ was non-canonical, we do not generally want the choice of matrix to cause any issues, but working with matrices is simply too convenient. So in regards to a matrix A we will say property P *is invariant under a change of basis* if P is true for MAM^{-1}, for all invertible matrices M. This allows us to work with a particular choice of basis to write down A and then to also consider any automorphism of $\mathbb{F}^d$, which would give rise to a new choice of basis. We will say matrices A and B are **similar** if there exists an invertible matrix M such that $A = MBM^{-1}$. As a slight abuse of notation we will use A to denote both a linear map and its corresponding matrix under a choice of basis. This should only cause minimal confusion. A common source for the study of linear maps over arbitrary fields is Chapters 12.2 and 12.3 in [DF04].

In understanding linear endomorphisms, maps $A : V \to V$ it will be helpful to understand the subspaces of V which are invariant under the map A. We say $\lambda \in \mathbb{F}$ is an **eigenvalue** if there exists a non-zero vector $v \in V$ such that $Av = \lambda v$, and in which case v is called an **eigenvector** and spans a 1-dimension subspace invariant under A. Rearranging the definition we can see that $(\lambda I - A)v = 0$ if and only if λ is a eigenvalue and v is its eigenvector. Furthermore, this means the linear map $(\lambda I - A)$ has zero determinant. In fact we will define the **characteristic polynomial** of A to be the degree d monic polynomial $c_A(x) = \det(xI - A)$ in which case the roots of $c_A(x)$ are exactly the eigenvalues of A. In general, it may be the case that the roots of $c_A(x)$ are not contained in the underlying field $\mathbb{F}$. Throughout we will assume that the underlying field contains all the roots of $c_A(x)$. *This seems to preclude one of the goals of this section, which is to dive into what sort of spectral theory holds for different kinds of fields.*

Also note that $c_A(A) = 0$, however $c_A(x)$ may not be the smallest degree polynomial that satisfies this property. Therefore we will define a second polynomial $m_A(x)$ called the **minimal polynomial** which is the unique monic polynomial of smallest degree such that that $m_A(A) = 0$. It is clear that $m_A(x)|c_A(x)$ but it is also the case that for λ a root of $c_A(x)$ that $m_A(\lambda) = 0$. This follows from the fact that that there exist a non zero v such that $Av = \lambda v$ and so $A^k v = \lambda^k v$. This means $p_A(A)v = p_A(\lambda)v$ so $p_A(\lambda) = 0$. This shows that if the degree of m_A and c_A disagree the polynomials only differ in the multiplicity of their roots and not the roots themselves. In general the characteristic polynomial does not divide the minimal polynomial, but because they share all their roots, the characteristic polynomial does divide some power of the minimal polynomial.

Understanding the multiplicities of the eigenvalues in the minimal polynomial and characteristic polynomials will play a critical role in understanding linear maps. Let λ be an eigenvalue of $A : V \to V$, then the **eigenspace** of A corresponding to λ, is $E_\lambda(A) := \{v \in V : Av = \lambda v\} = \ker(\lambda I - A)$. The dimension of $E_\lambda(A)$ is $\dim\ker(\lambda I - A)$. which is less then or equal to the multiplicity of the root λ in $c_A(x)$. We therefore say that the multiplicity of the root λ in $c_A(x)$ is the **algebraic multiplicity** and the multiplicity or dimension of $E_\lambda(A)$ is the **geometric multiplicity**. If the geometric and algebraic multiplicities agree for all eigenvalues then we say A is **diagonalizable**. If this is the case, there is a basis for V, the space on which A acts, in terms of the eigenvectors of A, and A is similar to a diagonal matrix: there would exist an invertible matrix P and diagonal matrix Λ such that $A = P\Lambda P^{-1}$. A matrix being diagonalizable can be equivalently written as a condition on the multiplicity of the roots of the minimal polynomial in the following way.

Proposition 1.2.5. *(E.g., Chapter 12.3 Corollary 25 [DF04]) Fix $A : V \to V$ and a basis $\{v_1, \ldots, v_d\}$. The following are equivalent*

- *The geometric and algebraic multiplicities of A agree for all eigenvalues;*
- *There exists an invertible matrix P and a diagonal matrix $\Lambda = (\lambda_j)_{j=1}^n$ such that $A = P\Lambda P^{-1}$ where $(\lambda_j)_{j=1}^n$ are the eigenvalues of A;*
- *The minimal polynomial $m_A(x)$ has no repeated roots.*

Diagonal matrices are particularly convenient, as they allow us to write a basis for our vector space V in terms of the eigenvectors of V. That is, the columns of P give an basis for V in terms of $\{v_1, \ldots, v_d\}$. If A is diagonalizable on V, then for any subset $U \subseteq V$ invariant under A, meaning for any $x \in U$ that $Ax \in U$, the restriction of A on U is also diagonalizable. To show this it is enough to show that every element $u \in U$ can be written as linear combination of eigenvectors which are all themselves contained in U: i.e., for any $u \in U$ which can be written as $u = v_1 + \cdots + v_r$ where each v_j is an eigenvector with distinct eigenvalues $\lambda_1, \ldots, \lambda_r$ respectively, then each $v_j \in U$. This can be shown by induction on r. If $r = 1$ then there is nothing to show. Otherwise, if $r > 1$ we can write any $u \in U$ as $u = v_1 + \cdots + v_r$. Notice that $Au - \lambda_1 u \in U$ and $Au - \lambda_1 u = (\lambda_2 - \lambda_1)v_2 + \cdots + (\lambda_r - \lambda_1)v_r \in U$ and so by induction each $v_j \in U$ for $2 \leq j \leq r$, and therefore $v_1 \in U$.

Often when studying multiple linear maps on the space V, it may be convenient, if possible, to choose a basis of common eigenvectors. This would require that every linear map shares the same eigenspaces. In this case we would call a collection of linear maps $\{A_j : V \to V\}$ **simultaneously diagonalizable** if there an invertible matrix P and diagonal matrices Λ_j such that $A_j = P\Lambda_j P^{-1}$. This is to say that the columns of P are the common eigenvectors of each A_j. Two diagonalizable linear maps A and B are simultaneously diagonalizable if and only if $AB = BA$.

Proposition 1.2.6. *For any field $\mathbb{F}$ two diagonalizable matrices A and B are simultaneously diagonalizable if and only if $AB = BA$*

Proof. ($\Rightarrow$) If $A = P\Lambda_A P^{-1}$ and $B = P\Lambda_B P^{-1}$, then

$$AB = P\Lambda_A P^{-1} P\Lambda_B P^{-1} = P\Lambda_A \Lambda_B P^{-1} = P\Lambda_B \Lambda_A P^{-1} = P\Lambda_B P^{-1} P\Lambda_A P^{-1} = BA.$$

($\Leftarrow$) Let v be an eigenvector of A with $Av = \lambda v$. The commutativity of A and B means that $A(Bv) = B(Av) = \lambda Bv$, meaning Bv is an eigenvector of A with the same eigenvalue. This means B maps eigenvectors of A with eigenvalue λ to eigenvectors of A with eigenvalue λ.

Because $AB = BA$ where A and B are both diagonalizable, we know that any basis of eigenvalues for A is also a basis of eigenvalues for B. If all the eigenvalues of A are distinct we are done, as this would imply that every eigenvector of A must also be an eigenvector of B. So fix an eigenvalue λ with an eigenspace E_λ. Because B is diagonalizable, we know it must also be diagonalizable on E_λ, as E_λ is invariant under the action of B. Repeating this for all eigenspaces of A gives us a basis in which both A and B are diagonal. □

For a field $\mathbb{F}$ with involution σ we will define the **conjugate transpose** is defined as $A^* = [a_{ji}^\sigma]_{ij} \in \mathbb{F}^{m\times n}$. In the case were the field involution is trivial we will use the terminology of **transpose** which will be denoted as $A^\intercal = [a_{ji}]_{ij} \in \mathbb{F}^{m\times n}$.

1.3 Geometric Algebra: Orthogonal and Unitary Spaces

In this section we wish to present the foundational spaces in which we will pack: quadratic and unitary spaces. In Chapter 2 we will primarily on the classical spaces, vector spaces defined over fields of characteristic 0, and in Chapter 3 we will consider fields of positive characteristic, but we will introduce the foundational topics in full generality, over more or less any field here.

Orthogonal Geometries

The archetypical orthogonal geometries, or quadratic spaces, are the finite dimensional vector spaces of $\mathbb{R}$, with the Euclidean geometry of angles that many mathematicians are accustomed. In general we will consider V to be a finite dimensional vector space over any field $\mathbb{F}$ of characteristic not equal to 2. In this case we will denote $\mathbb{F}^\times$ to be the invertible, i.e., non-zero, elements of $\mathbb{F}$. An element $a \in \mathbb{F}$ is a **square** if there exists some $x \in \mathbb{F}$ such that $x^2 = a$ and we will denote the set of non-zero squares as $\mathbb{F}^{\times 2}$.

We give a brief overview on bilinear forms of which inner products are a special case. We follow the terminology presented in [Gro02; Jac53; Wil09].

Let V be a finite dimensional vector space. A **symmetric bilinear form** is a function defined on pairs of vectors: $g(-,-) : V \times V \to \mathbb{F}$, that satisfies for any $u, v \in V$

$g(u,-) : V \to \mathbb{F}$ is linear; and

$g(u,v) = g(v,u)$.

Notice that these conditions imply linearity in the first term as well. Bilinear forms are more general then the definition above, allowing g to be bilinear map between two different $\mathbb{F}$-vector spaces to the underlying field, in which case they would not be symmetric, and linearity in the second term would be included in the definition. For our purposes we will assume symmetry.

The case presented above is an example of a **symmetric scalar product**, as it defines a product on V whose outputs are the underlying scalars. We will use the terminology of bilinear forms and scalar products interchangeably. Throughout we will be particularly interested in symmetric bilinear forms, or symmetric scalar products. We will also assume that the underlying field $\mathbb{F}$ has $\operatorname{char}\mathbb{F} \neq 2$ as the study of symmetric bilinear forms is fundamentally different in the characteristic 2 case and will not play a significant role in this paper.

Example 1.3.1. The archetypical example of a symmetric bilinear form is the standard dot product, for the vector space $\mathbb{F}^d$.

The study of bilinear forms is closely connected with the study of quadratic forms, as any bilinear form gives rise to the quadratic form $Q(v) = g(v, v)$. Likewise any quadratic form gives a bilinear form by $g(u, v) = \frac{1}{2}(Q(u+v) - Q(u) - Q(v))$ when 2 is invertible in $\mathbb{F}$. We will not give a formal definition of quadratic forms, but we will use the equivalence between bilinear forms and quadratic forms throughout this section. Notice that from this equivalence a bilinear form which is not identically zero for all $u, v \in V$ there must exist a vector $v \in V$ such that $Q(v) \neq 0$.

Unitary Geometries

Unitary geometries are vector spaces over fields with additional structure in the form of an involution, along with a scalar product that respects the involution. The archetypical unitary spaces, are the finite dimensional vector spaces over $\mathbb{C}$, along with complex conjugation which encapsulates the complex geometry many mathematicians are accustomed. In general we will consider V to be a finite dimensional vector space over any field $\mathbb{F}$, with an involution $(-)^\sigma : \mathbb{F} \to \mathbb{F}$.

Let $\mathbb{F}$ be a field with a field involution $(-)^\sigma : \mathbb{F} \to \mathbb{F}$. As in the previous subsection we will define some of the useful underlying objects but taking into account the additional structure of the involution. Define $\mathbb{F}^\times$ to denote the invertible, i.e., non-zero, elements of $\mathbb{F}$ and $\mathbb{F}_0 = \{\, a \in \mathbb{F} \mid a^\sigma = a \,\}$ to be the elements fixed by the involution, which play the analogous role that $\mathbb{R}$ plays to $\mathbb{C}$, as $\mathbb{C}_0 = \mathbb{R}$ with respect to complex conjugation. An element $a \in \mathbb{F}$ is a **σ-norm** if there exists some $x \in \mathbb{F}$ such that $x^\sigma x = a$ and we will denote the set of non-zero σ-norms as $\mathbb{F}^{\times(1+\sigma)}$, following the notation of [Gro02]. Notice that $\mathbb{F}^{\times(1+\sigma)}$ is a subgroup of the multiplicative elements fixed by the involution $\mathbb{F}_0^\times$ which is itself a subgroup of the multiplicative group $\mathbb{F}^\times$. Although we will allow σ to be trivial, making orthogonal geometries a special case of unitary ones, we will always require that there exists some $a \in \mathbb{F}$ such that $a + a^\sigma \neq 0$, for reasons we will see shortly.

We will now generalize the bilinear forms presented previously the allow for the additional structure of the involution, of which complex inner products are a special case. We follow the terminology presented in [Gro02; Jac53; Wil09]

Let V be a finite dimensional vector space. A **Hermitian scalar product**, is a function defined on pairs of vectors: $g(-,-) : V \times V \to \mathbb{F}$, that satisfies for any $u, v \in V$

$g(u,-) : V \to \mathbb{F}$ is linear; and

$g(u,v) = g(v,u)^\sigma$.

Notice that although these maps are not linear in the first term, they are quasi-linear, in that they respect addition and scalars pull out at the cost of the involution: $g(ku, v) = g(u,v)k^\sigma$. Under this definition symmetric bilinear forms can be considered a special case of the Hermitian scalar product with trivial involution. However the structural differences are significant enough to justify a separate treatment. Some authors will use the terminology of Hermitian form or sesquilinear form, instead of Hermitian scalar product.

As in the case of bilinear forms we can define Hermitian quadratic forms from Hermitian scalar products $Q(v) = g(v,v)$. It is generally not the case that Hermitian quadratic forms can be used to recover a Hermitian scalar product; however, it is still true that over a field $\mathbb{F}$ with non-trivial involution σ, any Hermitian scalar product g that is not identically zero will have some $v \in V$ such that $Q(v) \neq 0$. To see this first notice that because there must exist some $u, v \in V$ where $g(u,v) = k \neq 0$ we can rescale v where $v' = k^{-1}v$ such that $g(u,v') = 1$, in which case for any $a \in \mathbb{F}$ we have that $Q(u+av') = Q(u)+Q(av')+g(u,av')+g(u,av')^\sigma = Q(u)+Q(av')+a+a^\sigma$. It must be the case that for some $a \in \mathbb{F}$ that $a + a^\sigma \neq 0$, meaning one of $Q(u + av')$, $Q(u)$, or $Q(av')$ must be non-zero. For this reason, for unitary geometries, and also orthogonal geometries, we will always assume that there exists some $a \in \mathbb{F}$ such that $a + a^\sigma \neq 0$. This will be an ongoing assumption for the remainder of the paper.

It may be the case that some elements are indistinguishable from the zero vector, from the perspective of the symmetric form; these elements are called **isotropic** and are contained in the **radical**, which is defined for all subspaces $W \subseteq V$

$$\operatorname{rad} W = \{x \in W | g(x, y) = 0 \text{ for all } y \in W\} \subseteq W$$

which quantifies how degenerate a space is. In the case where the radical V is trivial, the space V is said to be **non-isotropic** (or **non-degenerate**) and the bilinear form is **non-degenerate**. If the space V contains non-zero isotropic elements, it is called an **isotropic** space (or a **degenerate** space).

Bilinear forms give a way of distinguishing elements through orthogonality. The condition of non-degeneracy requires that no non-zero elements behave like the zero vector in this regard. If for $u, v \in V$ we have that $g(u, v) = 0$ we say that u and v are **orthogonal**, and we define the **orthogonal compliment** of a subspace $W \subseteq V$ with respect to the space V as $W^\perp$ to be

$$W^\perp = \{v \in V | g(w, v) = 0 \text{ for all } w \in W\} \leq V.$$

If V is a non-isotropic space with a non-degenerate bilinear form, a subspace $W \subseteq V$ with the same scalar product restricted to W may not satisfy the condition of non-degeneracy, the radical of W maybe be non-trivial. In this case we can write the radical as $\operatorname{rad} W = W^\perp \cap W$ which gives us an equivalent condition for a subspace W being isotropic: if $\operatorname{rad} W = W^\perp \cap W \neq \{0\}$. A space W is called **totally isotropic** if $W \leq W^\perp$. If the scalar product for V is non-degenerate then the orthogonal compliment is an involution, that is $W^{\perp\perp} = W$, but in general it would be the case that $W \subseteq W^{\perp\perp}$. Notice that if a subspace $W \leq V$ is non-isotropic then $W \cap W^\perp = \{0\}$ and $W \cup W^\perp = V$, meaning $V = W \oplus W^\perp$. Alternatively we can consider the case where W is a totally isotropic subspace of a non-degenerate space V, meaning $W \subseteq W^\perp \subseteq V$. Let $k = \dim W$, and $n = \dim V$ and assume that $k \geq n/2$. Let $v_1, \ldots, v_n$ be a basis for V such that $v_1, \ldots, v_k$ is a basis for W. Because V is non-degenerate we know that the Gram matrix $G = [\langle v_j, v_k \rangle]$ is invertible, and we can decompose it as

$$G = \begin{bmatrix} 0_{k\times k} & * \\ * & * \end{bmatrix} = \begin{bmatrix} 0_{k\times k} & * \\ 0 & 0 \end{bmatrix} + \begin{bmatrix} 0_{k\times k} & 0 \\ * & * \end{bmatrix}$$

Looking at the ranks of the decomposition we know that $n = \operatorname{rank}(G) \leq \min(k, n-k) + (n-k) \leq 2(n-k)$, which give us that $\dim W \leq \frac{1}{2} \dim V$.

A vector space V along with a non-degenerate symmetric scalar product is called an **orthogonal geometry**, and the space V is called a **quadratic space**. In this case we will denote the scalar product as $\langle -, - \rangle$. We will further refer to **case O**, as the case where $\mathbb{F} = \mathbb{F}_q$ is a finite field of characteristic $p \neq 2$ and V is a finite-dimensional vector space over $\mathbb{F}_q$ along with the non-degenerate bilinear form $\langle -, - \rangle$. If $V = \mathbb{F}_q^d$ and $\langle u, v \rangle = u^\intercal v$, we say V is in the **real model**.

A vector space V along with a non-degenerate Hermitian scalar product is called an **Unitary geometry**, and the space V is called a **Unitary space**. Just as in the orthogonal geometry case we will denoted the scalar product as $\langle -, - \rangle$. We will further refer to **case U**, as the case where $\mathbb{F} = \mathbb{F}_{q^2}$ is a finite field, where q is a prime power and V is a finite-dimensional vector space over $\mathbb{F}_{q^2}$ along with the non-degenerate scalar product $\langle -, - \rangle$. If $V = \mathbb{F}_{q^2}^d$ and $\langle u, v \rangle = u^* v$, we say V is in the **complex model**.

Remark 1.3.2. In case U, where $\mathbb{F} = \mathbb{F}_{q^2}$ for a prime power q, it is the case that the non-zero elements fixed by the involution are exactly the non-zero squares with respect to the involution, $\mathbb{F}_0^\times = \mathbb{F}^{\times(1+\sigma)}$. To show this we will show that not only does the polynomial $x^{q+1} - b$ has a root in $\mathbb{F}_{q^2}$ when ever $b \in \mathbb{F}_0^\times$, but that it splits. Recall the norm $N_{\mathbb{F}_{q^2}/\mathbb{F}_q} : \mathbb{F}_{q^2}^\times \to \mathbb{F}_q^\times$ was surjective and mapped $x \mapsto x^{q+1}$. We also had that $|\ker N_{\mathbb{F}_{q^2}/\mathbb{F}_q}| = q + 1$ meaning every coset of elements that mapped to $b \in \mathbb{F}_q$ had size $q + 1$.

Because V is finite dimensional ($\dim(V) = d$), we can considering a basis $\{e_1, \ldots, e_d\}$ for V and interpret a scalar product $g(-, -)$ as a **Gram matrix**, with respect to the basis: $M =$

$[g(e_i, e_j)]_{ij} \in \mathbb{F}^{d \times d}$. In this case, $g(u, v) = u^*Mv$. The condition of linearity in the second term is implicit, the condition of symmetry is encoded by $M^* = M$, and the condition of non-degeneracy is encoded in if M is invertible. Any $d \times d$ matrix M such that $M^* = M$ gives rise to a Hermitian scalar form in this way.

Two scalar products f and g, and associated Gram matrices F and G are said to be equivalent, or congruent if there exists an invertible matrix $D \in GL(V)$ such that $D^*FD = G$.

This is defining equivalence up to a change of basis, and any equivalence classes will have Hermitian scalar product whose Gram matrices have a common rank. This is however not to say that any two bilinear forms of a common rank are equivalent. And although equivalence does not in general preserve the determinant of a Gram matrix, it preserves whether the determinant is a square (or σ-norm) or not. This motivates a useful invariant: the **discriminant** of V, which is defined for non-isotropic spaces, with non-degenerate hermitian scalar products.

$$\operatorname{discr}(V) = \det(M)\mathbb{F}^{\times(1+\sigma)} \in \mathbb{F}_0^{\times}/\mathbb{F}^{\times(1+\sigma)}$$

In the case where the involution is trivial we would write

$$\operatorname{discr}(V) = \det(M)\mathbb{F}^{\times 2} \in \mathbb{F}_0^{\times}/\mathbb{F}^{\times 2}.$$

The discriminant is invariant under the choice of basis for V. If $\operatorname{discr}(V) = \mathbb{F}^{\times(1+\sigma)}$, i.e., the determinant is a square, we say the discriminant is trivial. If V is isotropic, then we will define $\operatorname{discr}(V) = 0$.

Proposition 1.3.3. *Let $\mathbb{F}$ be a field with involution σ such that there exists some $a \in \mathbb{F}$ such that $a + a^\sigma \neq 0$ and $A \in \mathbb{F}^{d\times d}$ such that $A^* = A$, then A is congruent to a diagonal matrix*

$$\begin{bmatrix} b_1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & b_r & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

where each $b_i \in \mathbb{F}_0^\times$.

Proof. The proof of the first statement follows from the fact that a symmetric matrix $A^* = A$ defines a Hermitian scalar product $g(u, v) = u^*Av$ on $V = \mathbb{F}^d$. If A is the zero matrix, the result follows immediately. The proof will follow from induction on d. If $d = 1$, then A is a 1-by-1 matrix and the result follows immediately. Assume $d > 1$ and assume that A is non-zero in which case g would not be identically zero and therefore there would exist some $v_1 \in V$ such that $Q(v_1) = g(v_1, v_1) = b_1 \neq 0$. Let $V_1 = \operatorname{span}\{v_1\}$ be the 1-dimensional space spanned by v_1, and notice that V_1 is non-degenerate and so $V_1 \cap V_1^\perp = 0$, and therefore $V = V_1 \otimes V_1^\perp$. By induction we can find a basis $v_2, \dots v_d$ for $V_1^\perp$ such that $v_1, \dots, v_d$ are pairwise orthogonal and $Q(v_i) = b_i \neq 0$ for $1 \leq i \leq r$ for $r = \operatorname{rank}(A)$, while $Q(v_i) = 0$ for all $i > r$. Explicitly this give use the congruence

$$A = (P^{-1})^* \begin{bmatrix} b_1 & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & b_r & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} P^{-1}$$

where $P = \begin{bmatrix} v_1 & \cdots & v_d \end{bmatrix}$. □

Not that the result above does not imply that A is diagonalizable, unless $P^{-1} = P^*$ which in general should not be assumed the case. We can strengthen this result

Lemma 1.3.4. If $\langle -,-\rangle$ is a non-degenerate Hermitian scalar product for V over a field $\mathbb{F}$, then there exists a basis $v_1,\dots,v_d$ where $\langle v_j,v_j\rangle = b_j$, for $b_j \in \mathbb{F}_0^\times$ and all other products between basis elements are zero.

In case O, where $\mathbb{F} = \mathbb{F}_q$ is a finite field, with trivial involution, it can be made so that $b_j = 1$ for all $j < d$ and $b_d = \delta \in \mathbb{F}^\times$ is either a square or a non-square.

In the case where $\mathbb{F} = \mathbb{C}$ or in case U where $\mathbb{F} = \mathbb{F}_{q^2}$ is a finite field of q^2 element, it can be made so that $b_j = 1$ for all j

Proof. We have already shown the first part. Let $v_1,\dots,v_d$ be as in the proof above and notice because each $g(v_i,v_i) = b_i \in \mathbb{F}_0^\times = \mathbb{F}^{\times(1+\sigma)}$ there exists some α such that $\alpha^\sigma\alpha = b_i$ meaning $g(\alpha^{-1}v_i,\alpha^{-1}v_i) = 1$ which prove the statement for case U and when $\mathbb{F} = \mathbb{C}$. Notice that all this is requires is that the image $Q(V)$ is a subset of the squares. This is generally not the case for $\mathbb{F}_q$ and $\mathbb{R}$ as these are not algebraic closed.

Now we will consider case O where $\mathbb{F} = \mathbb{F}_q$, and V is a non-degenerate space with a non-degenerate bilinear form $\langle -,-\rangle$. The core of the proof will be that in the proof of Proposition 1.3.3 where we choice the v_i, we will show that in fact we could have chosen v_i such that $Q(v_i) = 1$ for all but $i = d$. Will start by showing that when $\dim V \geq 2$ and V is non-degenerate that $\langle -,-\rangle$ is **universal**, meaning for any $a \in \mathbb{F}$ there exists some $v \in V$ such that $Q(v) = a$.

Lemma 1.3.5. Let V be in case O where $\dim V = d \geq 2$ and $\langle -,-\rangle$ a non-degenerate bilinear form. The Q is universal.

Proof. There are two cases to consider, first the case where $\langle u,u\rangle = 0$ for some non-zero $u \in V$. In this case by the assumption that V is non-degenerate there must exists some $v \in V$ such that $\langle u,v\rangle = b \neq 0$. And therefore setting $v' = \frac{v}{2b}$ we have that $\langle u,v'\rangle = \frac{1}{2} \in \mathbb{F}^{\times(1+\sigma)}$. Notice that $Q(cu+v') = c^2Q(u) + c + Q(v') = c + Q(v')$. As $Q(v')$ is fixed and c is any field element, Q is universal.

The next case is when for all non-zero $v \in V$, that $Q(v) \neq 0$. Pick a basis $v_1,\dots,v_d$ as in Proposition 1.3.3. We will restrict our selves to the subspace W spanned by v_1 and v_2 in which case the corresponding Gram matrix is

$$\begin{bmatrix} b_1 & \\ 0 & b_2 \end{bmatrix}$$

Notice that for any vector $av_1+cv_2 \in W$ that $a^2b_1+c^2b_2 \neq 0$ which is equivalent to $a^2-c^2b \neq 0$ where $b = -\frac{b_2}{b_1}$. This must require that b is non-zero when ever either a or b is not zero. This therefore must imply that b is not a square. We want to show that $a^2 - c^2b$ can achieve any element in $\mathbb{F}_q$. Because b is a non-square, $x^2 - b$ is irreducible over $\mathbb{F}_q$. We can consider the degree two extension $\mathbb{F}_{q^2} = \mathbb{F}_q[x]/(x^2-b) = \mathbb{F}_q(\sqrt{b})$ and the norm $N : \mathbb{F}_{q^2} \to \mathbb{F}_q$ where $N(x) = x^\sigma x = x^{q+1}$. We can also define a automorphism by $\sqrt{b} \mapsto -\sqrt{b}$ which would be a non-trivial automorphism in the Galois group. However, because $|\operatorname{Gal}(\mathbb{F}_{q^2}/\mathbb{F})| = 2$, this must be the same as the Frobenius involution, meaning $\sqrt{b}^\sigma = -\sqrt{b}$. Because the norm is surjective any element $a + \sqrt{b}c \in \mathbb{F}_{q^2}$ which maps to $(a+\sqrt{b}c)(a-\sqrt{b}c) = a^2 - bc^2 \in \mathbb{F}_q$ must achieve all elements of $\mathbb{F}_q$. Therefore the quadratic form on W is universal and therefore the the quadratic form on all of V is universal. □

Now we will redo the proof of Proposition 1.3.3 using this fact. Because g is non-degenerate and universal there exist some $v_1 \in V$ such that $Q(v_1) = g(v_1, v_1) = 1$. Let $V_1 = \operatorname{span}\{v_1\}$ be the 1-dimensional space spanned by v_1, and notice that $V = V_1 \otimes V_1^\perp$. By induction we can find a basis $v_2, \dots v_d$ for $V_1^\perp$ such that $v_1, \dots, v_d$ are pairwise orthogonal and $Q(v_i) = 1 \neq 0$ for $1 \leq i < d$ and $Q(v_d) = \delta \neq 0$. □

This shows us that for case U or when $\mathbb{F} = \mathbb{C}$ all non-degenerate Hermitian scalar products are equivalent, and in case O there are only two different types of symmetric scalar products up to equivalence, based entirely on the the discriminant. We will discuss the case where $\mathbb{F} = \mathbb{R}$ in Section 1.3, as this case behave distinct from these two situations partially due to the fact that over $\mathbb{R}$ scalar products are not going to be universal in general.

Alternatively in case U, over the field $\mathbb{F}_{q^2}$ we can find a basis of isotropic vectors for V when ever $\dim V \geq 2$. This really follows from the fact that in case U there there will always be isotropic elements: pick a field element such that $a^\sigma a = -1$ of which there are $q+1$ solutions. Then the vector $v = \begin{bmatrix} 1 & a \end{bmatrix}^\intercal$ is isotropic.

Now assume U, V are both vector spaces with non-degenerate Hermitian scalar products. For any linear map $A : U \to V$ there is a unique **adjoint** which satisfies $\langle Au, v\rangle_V = \left\langle u, A^\dagger v\right\rangle_U$ for all $u \in U$ and $v \in V$. Because adjoints are uniquely defined, the adjoint of $A^\dagger$ is A, i.e., $(A^\dagger)^\dagger = A^{\dagger\dagger} = A$. For linear maps on spaces with degenerate Hermitian scalar products, adjoints are not unique and are usually defined as pairs of linear maps, and called adjoint pairs. By fixing bases we can explicitly write the adjoints for linear transformations: let U, V be vector spaces with non-degenerate Hermitian scalar products $\langle -, -\rangle_U$ and $\langle -, -\rangle_V$ respectively. Choose bases $u_1, \ldots, u_n$ and $v_1, \ldots, v_m$ for U and V, and let M and N be the corresponding invertible Gram matrices such that $\langle u, u'\rangle_U = u^* M u'$ and $\langle v, v'\rangle_V = v^* N v'$ Then for any map $A : U \to V$ the unique adjoint can be written as $A^\dagger = M^{-1} A^* N$.

Isometries

Of special importance are the linear maps between unitary spaces that preserve the geometry, the underlying scalar product. Such maps are called **isometries**: linear maps $A : V \to W$ such that for all $u, v \in V$ the map preserves the scalar products: $\langle Au, Av\rangle = \langle u, v\rangle$. Notice that $u, v \in V$ and $Au, Av \in W$. In the case where $W = V$ and the map A is a structure preserving automorphism we will call A **unitary** with respect to the scalar product. In the case where the field automorphism is the identity we call A **orthogonal**. The set of all unitary maps forms a subgroup of the general linear group $GL(V)$ called the **unitary group** of V, and is denoted $U(V)$. Notice that the condition of being unitary is equivalent to $A^\dagger A = I = AA^\dagger$, meaning $U(V) = \{U \in GL(V) : AA^\dagger = I\}$. When the field involution is trivial, we called the group of orthogonal linear automorphisms the **orthogonal group** denoted $O(V)$. We will also define the group $\Delta(V) = \{U : V \to V | UU^\dagger = cI, c \in \mathbb{F}^\times\} \leq GL(V)$, which are sometimes referred to as quasi-isometries. Let $W_1, W_2 \subseteq V$ be subsets. If there exists a isometry $U : W_1 \to W_2$ then we will say W_1 and W_2 are **isometrically equivalent** with respect to hermitian scalar product $\langle -, -\rangle$.

In case O and U, when we can exactly count the number of orthogonal or unitary maps.

Theorem 1.3.6. *(Theorem 9.11 [Gro02]) Let $V = \mathbb{F}_q^d$ be non-degenerate in case O and $d = 2k$.*

- *If* $\operatorname{discr} V = (-1)^k \mathbb{F}^{\times 2}$ *then* $|O(\mathbb{F}_q^d)| = 2q^{k(k-1)}(q^k - 1)\prod_{i=1}^{k=1}(q^{2i-1})$.
- *If* $\operatorname{discr} V \neq (-1)^k \mathbb{F}^{\times 2}$ *then* $|O(\mathbb{F}_q^d)| = 2q^{k(k-1)}(q^k + 1)\prod_{i=1}^{k=1}(q^{2i-1})$.

If $d = 2k+1$, *then* $|O(\mathbb{F}_q^d)| = 2q^{k^2}\prod_{i=1}^{k=1}(q^{2i-1})$

Theorem 1.3.7. *(Theorem 11.28 [Gro02]) Let $\mathbb{F}_{q^2}^d$ be in the complex model then*

$$|U(\mathbb{F}_{q^2}^d)| = q^{d(d-1)/2}\prod_{j=1}^{d}(q^j - (-1)^j)$$

[Ian: *proof of this in MUB notes. Copy over eventually. I just introduced terminology i havent presented*]

Let V be a vector space over a field $\mathbb{F}$ with field involution $(-)^\sigma$ with a non-degenerate Hermitian scalar product $\langle -, - \rangle : V \times V \to \mathbb{F}$. Excluding characteristic 2 for case O we have the following very powerful results.

Theorem 1.3.8. *(Witt) If W_1 and W_2 are non-isotropic and isometrically equivalent subspaces of V, then $W_1^\perp$ and $W_2^\perp$ are isometrically equivalent.*

Notice that if $W_1, W_2 \subseteq V$ are non-isotropic spaces we have the decomposition $V = W_1 \oplus W_1^\perp = W_2 \oplus W_2^\perp$. If W_1 and W_2 are isometrically equivalent, with isometry $A : W_1 \to W_2$, by Theorem 1.3.8 there is an isometry $B : W_1^\perp \to W_2^\perp$. Together this gives a unitary $U : V \to V$ by $v \in V \mapsto Ax + By$ where $v = x + y$ is the unique expression in $V = W_1 \oplus W_1^\perp$.

In fact we can generalize this even further, not requiring that W_1 nor W_2 be non-isotropic.

Theorem 1.3.9. *(Witt's Extension theorem) Any isometrically equivalence subspaces (even isotropic ones) of V can be extended to a unitary transformation on V.*

Proof of the previous two theorems, in full generality including that of characteristic 2 over division rings, can be found in [Jac53] or [Gro02].

The geometry of linear operators

Often when working with linear operators it will be helpful to impose a scalar product onto the space of linear operators. This will allows us to use non-degeneracy to show that an operator is the zero operator.

Definition 1.3.10. Let $M = \{A : V \to V\}$ be the $\mathbb{F}$-vector space of linear operators on a non-isotropic space V. Under a choice of basis, and assuming $\dim(V) = d$, we can consider M to be the space of $d \times d$ matrices. The **Frobenius scalar product** is then defined for $A, B \in M$ as

$$\langle A, B \rangle_F := \operatorname{tr}(A^\dagger B).$$

We note that in the case where $V = \mathbb{F}^n$ with the standard dot product or conjugate dot product (real or complex models), the adjoint operator on any map $A : \mathbb{F}^n \to \mathbb{F}^n$ is the conjugate transpose and the matrices $\{\, E_{ij} \mid i, j \in [n] \,\}$ form an orthonormal basis for M with respect to the Frobenius scalar product, as $\operatorname{tr}(E_{ij}E_{\ell k}) = 1$ when $j = \ell$ and $i = k$ and zero otherwise. Therefore, the Frobenius scalar product is a non-degenerate Hermitian scalar product on M, which is d^2 dimensional. This is true when ever V is non-degenerate.

We will also consider the subspace of self adjoint operators $L = \left\{\, A \in M \;\middle|\; A^\dagger = A \,\right\}$ which is an $\mathbb{F}_0$-vector space. Because $\mathbb{F}_0$ is either equal to $\mathbb{F}$ or $\mathbb{F}$ is a degree 2 extension of $\mathbb{F}_0$ we have that

$$\dim_{\mathbb{F}_0} L = d + \frac{k}{2}(d^2 - d)$$

where $k = \dim_{\mathbb{F}_0} \mathbb{F}$. This follows from picking a basis for V and treating A as a $d \times d$ matrix, in which case there are d entires for the diagonal, and the $d^2 - d$ off diagonal entires are determined by just the upper triangular entires which have either one or two $\mathbb{F}_0$ entries depending on $k = \dim_{\mathbb{F}_0} \mathbb{F}$.

This particular value will play an important role in the rest of this paper and so we will use the following notation

$$Z(d, \mathbb{F}) := d + \frac{\dim_{\mathbb{F}_0} \mathbb{F}}{2}(d^2 - d).$$

Let $V = \mathbb{F}_q^n$ be in the real model, in which case

$$\{ E_{\ell\ell} \mid \ell \in [n] \} \cup \{ E_{ij} + E_{ji} \mid i, j \in [n], i < j \}$$

forms an orthogonal basis for L. Notice that $\langle E_{\ell\ell}, (E_{ij} + E_{ji}) \rangle_F = 0$, and looking at the symmetrical terms we see that $\langle (E_{ij} + E_{ji}), (E_{\ell k} + E_{k\ell}) \rangle_F = 2$ when $i = \ell$ and $j = k$ and zero otherwise. This means that the Frobenius scalar product is a non-degenerate symmetric scalar product on L in the real model, but in general and particularly in case U, the Frobenius scalar product on the $\mathbb{F}_0$ vector space L_0 may be degenerate.

Inner Product Spaces

In the classical cases: orthogonal geometries over $\mathbb{R}$ and unitary geometries over $\mathbb{C}$, there is additional structure that can be exploited As we say in Lemma 1.3.4 in the case of unitary geometries over $\mathbb{C}$ all scalar products are equivalent, up to a change of basis to the standard dot product. Orthogonal geometries over $\mathbb{R}$ are different different story and are classified in the following way.

Proposition 1.3.11. *Let $\langle -, - \rangle$ be a non-degenerate symmetric scalar product for $V = \mathbb{F}^d$, then there exists a basis $v_1, \ldots, v_d$ where $\langle v_j, v_j \rangle = \pm 1$ and all other products between basis elements are zero. That is the corresponding Gram matrix is congruent to a unique diagonal matrix of the form*

$$\left[\begin{array}{c|c} I_p & 0 \\ \hline 0 & -I_{d-p} \end{array}\right]$$

This tells The number of 1s and -1s is invariant under any choice of basis. So we will define the **signature** to be the number of positive entries: $sig(V) = p$. Any non-degenerate symmetric scalar products for $\mathbb{R}^d$ are then equivalent if and only if they have the same signatures.

There are $d + 1$ different non-degenerate symmetric scalar products up to equivalence floating around for $\mathbb{R}^d$ and it may not be clear which if any is the ideal geometry to work with. However we can impose the additional property that for the quadratic space V for dimension at least 2 over $\mathbb{R}$

that any subspace $U \subseteq V$ should share a common discriminant, meaning $\mathrm{discr}(U) = \mathrm{discr}(V)$ for all $U \subseteq V$. The only equivalence class of symmetric scalar products that satisfy this assumption over $\mathbb{R}$ are the ones whose signature is d, i.e. with a Gram matrix congruent to the identity matrix. This case also has the very desirable property called **positivity** that for any $x \in \mathbb{R}^d$ that $\langle x, x \rangle > 0$ if and only if $x \neq 0$.

This special case of a real non-degenerate scalar product whose signature is d will be called an **inner product** and V an **inner product space**. A more standard definition in terms of positivity is as follows.

Definition 1.3.12. Let V be a finite dimensional vector space over a field $\mathbb{F} \subseteq \mathbb{C}$. An **inner product**, is a function $\langle -, - \rangle : V \times V \to \mathbb{F}$, that satisfies for any $u, v \in V$

$\langle u, - \rangle$ is linear;

$\langle u, v \rangle = \langle v, u \rangle^\sigma$;

$\langle u, u \rangle > 0$ if and only if $u \neq 0$

The property of positivity can also be used to describe the additional geometric notion of length, or distance with a norm. If $\langle -, - \rangle$ is an inner product then we will define the **norm** as a function $\|-\| : V \to \mathbb{F}$ such that $\|v\| = \sqrt{\langle v, v \rangle}$. Norms can be defined more generally, and do not always arise in this way, however we will only be concerned with the norms which arise from inner products.

Proposition 1.3.13. *(Cauchy-Schwarz inequality) Let V be a vector space over $\mathbb{R}$ or $\mathbb{C}$ and $\|-\| : V \to \mathbb{F}$ be a norm. The norm $\|-\|$ is induced by an inner product, meaning there exists an inner product $\langle -, - \rangle$ such that $\|x\| = \sqrt{\langle x, x \rangle}$ if and only if for all $x, y \in V$*

$$\|x + y\|^2 + \|x - y\|^2 = 2(\|x\|^2 + \|y^2\|)$$

Example 1.3.14. When $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$, then for $A, B \in \mathbb{F}^{d\times d}$, the Frobenius scalar product

$$\langle A, B\rangle_F = \operatorname{tr}(A^*B)$$

is an inner product. And so in this context we will refer to it as the **Frobenius inner product**, and its norm as the **Frobenius norm**

$$\|A\|_F = \sqrt{\operatorname{tr}(A^*A)}$$

Through out Chapter 2 we will be almost exclusively interested in vector spaces over $\mathbb{R}$ or $\mathbb{C}$ which are inner product spaces: in either case we will assume that the space $V = \mathbb{F}^d$ along with the standard dot product. Chapter 3 will focus on orthogonal and unitary geometries over finite fields.

Spectral Properties

Now that we have introduced the spaces, and operators we will work with, we will talk about some of the important and commonly used spectral properties. Specifically we wish to introduce the cases in which a diagonalization respects the equivalence of scalar products. That is we wish to understand the cases where a map A can be decomposed as $A = P^\dagger DP$ where $P^{-1} = P^\dagger$ and D is diagonal. Or in other words we want to know when there exists a orthonormal basis made up of the eigenvalues of A. If this is the case we will say A is **unitarily diagonalizable** over V. In the case of inner product spaces, this is known and maps which are unitarily diagonalizable are the maps which are normal. More generally for a non-degenerate space V a map A is said to be **normal** if $AA^\dagger = A^\dagger A$.

Theorem 1.3.15. *(Spectral Theorem. E.g Theorem 6.16 [FIS97]) Let V be a d-dimensional inner product space over $\mathbb{R}$ or $\mathbb{C}$, and A a linear map on V such that $c_A(x)$ splits. A is normal, if an only if A is unitarily diagonalizable, meaning there exists an orthonormal basis for V made up of* *eigenvectors of A. If $V = \mathbb{C}^d$ with the standard inner product, then as matrices*

$$A = Q\Lambda Q^*$$

Where Q is unitary and Λ is a diagonal matrix.

Note that self-adjoint matrices, where $A^* = A$, are normal. Likewise matrices of the form A^*A are self adjoint and therefore also normal. The proof we will give is a somewhat standard proof which appears in most text books, however we will not restrict our selves to the requirement that V be an inner product space until absolutely necessary. Most proofs utilize the norm induced by an inner product, but we will use non-degeneracy instead.

Before beginning the proof we will look at cases where the spectral theorem fails in case O and U. In general it is case that normal matrices are not unitarily diagonlizable, and often not even diagonalizable. One obvious reason is that the characteristic polynomial might not split in general. Additionally over $\mathbb{C}$ or $\mathbb{R}$ we can always scale vectors to be of unit norm, which is not possible in case O as seen in the following example.

Example 1.3.16. Consider the real model for $V = \mathbb{F}_5^2$ and consider the matrix

$$A = \begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix}$$

which is symmetric and therefore normal. A is also diagonlizable, where $A = P^{-1}DP$ Where

$$P = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \text{ and } D = \begin{bmatrix} 3 & 0 \\ 0 & 1 \end{bmatrix}.$$

Furthermore we can notice that the columns of P are orthogonal, but not unit norm meaning $P^\dagger P = 2I$, where two is not a square root in $\mathbb{F}$ and so no unitary diagonalization is possible. In the field extension $\mathbb{F}_{5^2}$ which contains the square root of 2, the matrix A is unitarily diagonalizable.

In case U this is not a problem as the norms of vectors $\langle x, x\rangle \in \mathbb{F}_0$ and therefore the norms of vectors are σ-norms with respect to the involution. However an even more insurmountable issue which could arise is when the eigenspaces are degenerate.

Example 1.3.17. Consider the real model for $V = \mathbb{F}_3^2$ and consider the matrix

$$A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix}$$

which is symmetric and therefore normal. A is however not diagonlizable, as $m_A(x) = x^2+x+1 = (x-1)^2$ has a repeated root. Notice that in this case the eigenspace of the only eigenvalue is

$$E_1(A) = \text{span}\left\{ \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix}, \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix} \right\}$$

which is degenerate.

We also note that the above example also applies to case U, as we can instead consider $V = \mathbb{F}_{3^2}$ to be in the complex model, in which case the single eigenspace would still be degenerate.

[Gur21] showed another issue that can arise, which is highlighted in the following Proposition.

Proposition 1.3.18. *(Lemma 2.1 [Gur21]) Let $V = \mathbb{F}_{q^2}^d$ be in the complex model and $A \in \mathbb{F}_{q^2}^{d\times d}$ a matrix. A is similar to a matrix $B \in \mathbb{F}_{q^2}^{d\times d}$ such that $B = B^*$ if and only if A is similar to a matrix $C \in \mathbb{F}_q^{d\times d}$ whose entires are in the fixed field.*

The proof of the spectral theorem utilizes the Schur decomposition, which can be defined for over $\mathbb{C}$ and sometimes in case O and U, as long as the examples above are avoided.

Theorem 1.3.19. *(Schur Decomposition. E.g Theorem 6.14 [FIS97]) Let V be either in case U or an inner product space and let A be a linear map in which $c_A(x)$ splits over $\mathbb{F}$. Assume also that* *every eigenspace of $A^\dagger$ is non-degenerate. Then there exists a orthonormal basis such that A is an upper triangular matrix. In other words, if $V = \mathbb{F}^d$ is in the complex model, there exists matrices Q, which is unitary, and U, which is upper triangular, such that*

$$A = QUQ^*.$$

We will note that in the case where V is an inner product space, every subspace is non-degenerate, and so every eigenspace is also non-degenerate.

Proof. Notice that is suffices to show that there exists an orthonormal basis $v_1, \dots, v_d$ such that $Av_j \in \operatorname{span}\{v_j, \dots, v_d\}$. We will show this with induction on d. When $d = 1$ then result follows immediately. When $d > 1$, we may consider a non-zero vector v_1 such that $\langle v_1, v_1 \rangle = 1$ and $A^\dagger v = \lambda v$, which is always possible by Lemma 1.3.4 as every eigenspace is assumed to be non-degenerate. Define the space $W = \operatorname{span}\{v\}$, which would be non-degenerate, and notice that for any $w \in W^\perp$ we have that $\langle Aw, v_1 \rangle = \left\langle w, A^\dagger v_1 \right\rangle = \langle w, \lambda v_1 \rangle = 0$. Because W is non-degenerate we also have that $V = W \oplus W^\perp$ meaning we can consider the map A restricted to $W^\perp$. In this case the characteristic polynomial would divide $c_A(x)$, and so still splits. Because the eigenspace in which v_1 was chosen from was non-degenerate we know that the compliment of W in the eigenspace is also non-degenerate, and therefore the eigenspaces of $A^\dagger$ restricted to $W^\perp$ are still non-degenerate. So by induction there exists a basis $v_2, \dots, v_d$ for $W^\perp$ such that $Av_j \in \operatorname{span}\{v_j, \dots, v_d\}$. Because v_1 is chosen to be unit norm and orthogonal to all the remaining vectors, the proof is complete. □

We now wish to give some properties of the eigenvalues and eigenspaces of linear maps and their adjoints, including the case where the linear map is normal.

Proposition 1.3.20. *Let V be in case U, or an inner product space, such that every eigenspace of A is non-degenerate. If λ is an eigenvalue of A, then λ^σ is an eigenvalue of $A^\dagger$. Furthermore if A is normal then $Av = \lambda v$ if and only if $A^\dagger v = \lambda^\sigma v$, and for λ and μ distinct eigenvalues of A the corresponding eigenspaces are orthogonal.*

Proof. Let $V = \mathbb{F}^d$ be in the complex model. First we will show how the eigenvalues between a map A and $A^\dagger$ are related. Let $Av = \lambda v$ and notice that for any $x \in \mathbb{F}^n$ that $0 = \langle (A - \lambda I)v, x\rangle = \left\langle v, (A - \lambda I)^\dagger v\right\rangle = \left\langle v, (A^\dagger - \lambda^\sigma I)x\right\rangle$, and because this is zero for all $x \in \mathbb{F}^n$, the map $(A^\dagger - \lambda^\sigma I)$ must not be invertible, by non-degeneracy, and so there must exists an eigenvector with eigenvalue λ^σ.

If A is normal, meaning $AA^\dagger = A^\dagger A$ then we can further note that when $Av = \lambda v$, and again considering the map $A - \lambda I$ and its adjoint $A^\dagger - \lambda^\sigma I$, we can notice that for any v, w which are eigenvectors for A with eigenvalue λ, living in a non-degenerate eigenspace that $0 = \langle (A - \lambda I)w, v\rangle = \left\langle w, (A - \lambda I)^\dagger v\right\rangle = 0$. Fixing any v and for all w we get that $(A - \lambda I)^\dagger v = 0$, meaning v is also an eigenvector of $A^\dagger$, but with eigenvalue λ^σ.

We will also note that if λ and μ are distinct eigenvalues with eigenvectors u, v we have $\langle u, Av\rangle = \mu \langle u, v\rangle = \lambda \langle u, v\rangle = \left\langle A^\dagger u, v\right\rangle$, meaning $\langle u, v\rangle = 0$. □

To prove Theorem 1.3.15, it would be enough to show that A is diagonalizable, in which case a combination of Proposition 1.3.20 and Lemma 1.3.4 would prove the result. To do this we utilizes the Schur decomposition, or a generalization of it.

Proof. (Theorem 1.3.15) Here we will use a modified version of the proof for the Schur decomposition. Notice that is suffices to show that there exists an orthonormal basis $v_1, \dots, v_d$ of eigenvectors, such that $Av_j \in \operatorname{span}\{v_j\}$. We will show this with induction on d. When $d = 1$ then result follows immediately. When $d > 1$, we may consider a non-zero vector v_1 such that $\langle v_1, v_1\rangle = 1$ and $Av = \lambda v$ (and also $A^\dagger v = \lambda^\sigma v$ by Proposition 1.3.20), which is always possible by Lemma 1.3.4 as every eigenspace is assumed to be non-degenerate. Define the space $W = \operatorname{span}\{v\}$, which would be non-degenerate, and notice that for any $w \in W^\perp$ we have that $\langle Aw, v_1\rangle = \left\langle w, A^\dagger v_1\right\rangle = \langle w, \lambda^\sigma v_1\rangle = 0$. Because W is non-degenerate we also have that $V = W \oplus W^\perp$ meaning we can consider the map A restricted to $W^\perp$. In this case the characteristic polynomial would divide $c_A(x)$, and so still splits. Because the eigenspace in which v_1 was chosen from was non-degenerate we know that the compliment of W in the eigenspace is also non-degenerate, and therefore the eigenspaces of A restricted to $W^\perp$ are still non-degenerate. Additionally for any element $x \in \mathbb{F}^d$ we can write $x = cv + w$ for c a constant and $w \in W^\perp$. Notice that A fixed W and $W^\perp$, and A being normal equivalently means that $AA^\dagger(cv+w) = A^\dagger A(cv+w)$. Expanding this gives us $AA^\dagger cv + AA^\dagger w = A^\dagger Acv + A^\dagger Aw$ and therefore $AA^\dagger w = +A^\dagger Aw$, meaning A is also normal when restricted to $W^\perp$. So by induction there exists a basis $v_2, \dots, v_d$ for $W^\perp$ such that $Av_j \in \operatorname{span}\{v_j\}$. Because v_1 is chosen to be unit norm and orthogonal to all the remaining vectors, the proof is complete. □

Notice that in the proof of Theorem 1.3.15 we actually proved the stronger statement

Theorem 1.3.21. *Let V be either in case U or an inner product space and let A be a linear map in which $c_A(x)$ splits over $\mathbb{F}$. Assume also that every eigenspace of A is non-degenerate. A is normal, if an only if A is unitarily diagonalizable, meaning there exists an orthonormal basis for V made up of eigenvectors of A. If $V = \mathbb{F}^d$ in the complex model, then as matrices*

$$A = Q\Lambda Q^*$$

where Q is unitary and Λ is a diagonal matrix.

Corollary 1.3.22. *Let A be a self adjoint matrix over $\mathbb{R}$ or $\mathbb{C}$, then*

$$A = U\Lambda U^*$$

where Λ is a real diagonal matrix and U is real orthogonal matrix if the entires of A are in $\mathbb{R}$.

Proof. From normality we knew that $Av = \lambda v$ if and only if $A^*v = \lambda^\sigma v$, which means $\lambda = \lambda^\sigma$ and is therefore real. Furthermore if the entries of A are real we can find eigenvectors with real entries. □

A similar statement can be made for maps on space in case U.

This proof of this lemma relies very heavily on Proposition 1.3.3 which could not be repeated in Case O. However, [PP72] finds necessary and sufficient conditions for matrices over algebraically closed fields (characteristic not equal to 2) to be unitarily diagonalizable.

To conclude this section we give a few more results related to the similarity of a matrix and its adjoint.

Theorem 1.3.23. *(Theorem I [TZ59]) For any field $\mathbb{F}$ with M an $n \times n$ matrix, there exists a invertible matrix S such that $S^\intercal = S$ and $SM = M^\intercal S$*

The proof of this result in fact proves a stronger statement, showing that for any invertible S such that $SM = M^\intercal S$, S is symmetric only if S is diagonalizable, and S can also be chosen to be in the intersection of the zero locus of $n - 1$ linear functionals. A statement of this stronger result can be found in Lemma 2.15 of [Kin25].

An exactly analogous result for the more general adjoint, as opposed to the transpose, is impossible: the eigenvalues of matrix A are almost never shared with the eigenvalues of A^*. This smallest example of this is with a 1×1 matrix: consider an element $a \in \mathbb{F}$ which is a field with involution σ, such that $a^\sigma \neq a$. In this case the linear map of multiplication by a, has a an eigenvalue of a and its adjoint, multiplication by a^σ has a different eigenvalue of a^σ as so are not similar. A generalization of similarity, consimilarity can be introduced in which can an matrix would be consimilar to its adjoint (see section 4.6 of [HJ13]).

Many authors have also looked at the special cases where A and A^* are similar, and showed that in this case there would exist an invertible matrix S such that $S = S^*$ where $SA = A^* S^{-1}$[Bar23]. In these cases some authors will use the terminology of pseudo-hermitian to refer to A.

1.4 Matroids

Now that we have given our vector spaces geometric structure, we wish to go back and look more into the algebraic structure and that of linear dependencies.

As we will see throughout this section, matroids act as important and useful tools in studying the dependence of a vectors. A more thorough overview of matroids can be found in [Oxl11] or [Cra86]. Throughout this section we will not impose any assumptions of the underlying fields, unless otherwise stated.

Definition 1.4.1. A **matroid** M is a pair $(E, \mathcal{I})$ where E is a finite set, called the **ground set** and $\mathcal{I} \subseteq \mathcal{P}(E)$ the **independent sets**, such that

(I1) $\varnothing \in \mathcal{I}$

(I2) (**Hereditary Property**) If $I \in \mathcal{I}$ and $J \subseteq I$ then $J \in \mathcal{I}$

(I3) (**Exchange**): If $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$ then there exists some $x \in I_2 - I_1$ with $I_1 \cup x \in \mathcal{I}$.

A matroid generalizes the notion of linear independence in vector spaces and independence in the form of acyclic subgraphs in graphs.First, we will note that every system of lines (more generally any collection of vectors) is a matroid with linear independence.

Example 1.4.2. Let $(\varphi_j)_{j=1}^n$ be a collection of vectors in $\mathbb{F}^d$ where $\mathbb{F}$ is any field. Then $M(\Phi) = ((\varphi_j)_{j=1}^n, \mathcal{I})$ with $\mathcal{I}$ the subsets of linearly dependent vectors is a matroid. We will often simplify this construction by writing $M(\Phi) = ([n], \mathcal{I})$ where $\mathcal{I}$ is instead just the indices of the vectors of each subset of linearly independent vectors. A matroid created in this fashion is called a **linear matroid**.

Matroids have many *cryptomorphic* definitions, which correspond to properties that determine the matroid.

Definition 1.4.3. Let $M = (E, \mathcal{I})$ be a matroid, a **circuit** is a subset $C \subseteq E$ such that every proper subset $I \subsetneq C$ is an independent set, that is $I \in \mathcal{I}$. A **basis** is an independence set $B \in \mathcal{I}$ of maximal size, meaning the addition of any other element $x \in E$ then $B \cup x \notin \mathcal{I}$.

Circuits can be thought of as minimally dependent sets, and for graphical matroid correspond to cycles in graphs. Every subset of E is either an independent set or is called a **dependent set** and so contains a circuit, a minimal dependent set. The size of the smallest circuit is called the **girth** of the matroid and for a representable matroid is equivalent to what we will later define as the **spark** of its vectors. As with bases of vector spaces and spanning trees of graphs, the bases of a matroid all have equal sizes.

Both the set of circuits and the set of bases as defined in definition 1.4.3 determine a matroid which we will see in theorems 1.4.6 and 1.4.7 and so motivate cryptomorphic definitions

Definition 1.4.4. A **matroid** M is a pair $(E, \mathcal{C})$ where E is a finite set, called the **ground set** and $\mathcal{C} \subseteq \mathcal{P}(E)$ the set of **circuits**, such that

(C1) $\varnothing \notin \mathcal{C}$

(C2) If $C_1, C_2 \in \mathcal{C}$ with $C_1 \subseteq C_2$ then $C_1 = C_2$

(C3) (Circuit Elimination) If $C_1, C_2 \in \mathcal{C}$ with $e \in C_1 \cap C_2$ there exists $C_3 \in C_1 \cap C_2 - e$ such that $C_3 \in \mathcal{C}$

Definition 1.4.5. A **matroid** M is a pair $(E, \mathcal{B})$ where E is a finite set, called the **ground set** and $\mathcal{B} \subseteq \mathcal{P}(E)$ the set of **bases**, such that

(B1) $\mathcal{B}$ is not empty

(B2) (exchange): if $B_1, B_2 \in \mathcal{B}$ with $B_1 \neq B_2$ then for any $x \in B_1 - B_2$ there exists some $y \in B_2 - B_1$ such that $B_1 - x + y \in \mathcal{B}$

The following theorems outline how to construct the independence sets given a matroid using the circuit definition and basis definition, showing that each definition is equivalent.

Theorem 1.4.6. *The Independence set definition and the circuit definitions are equivalent. That is if $M = (E, \mathcal{I})$ is a matroid, then $M = (E, \mathcal{C})$ is a matroid where $\mathcal{C} = \{C \subseteq E | C \notin \mathcal{I}$, and for all $I \subsetneq C, I \in \mathcal{I}\}$ is the set of circuits.*
Likewise if $M = (E, \mathcal{C})$ is a matroid, then $M = (E, \mathcal{I})$ is a matroid where $\mathcal{I} = \{I \in E |$ for all $C \in \mathcal{C}, C \nsubseteq I\}$.

Theorem 1.4.7. *The Independence set definition and the basis set definitions are equivalent. That is if $M = (E, \mathcal{I})$ is a matroid, then $M = (E, \mathcal{B})$ is a matroid where $\mathcal{B} = \{I \in \mathcal{I} | I$ is maximal$\}$ the set of bases.*
Likewise if $M = (E, \mathcal{B})$ is a matroid, then $M = (E, \mathcal{I})$ is a matroid where $\mathcal{I} = \{I \subseteq B | B \in \mathcal{B}\}$, is the downward closure of $\mathcal{B}$.

Example 1.4.8. A useful example of a matroid using the basis definition is the **uniform matroid** which is defined as $U_{d,n} = ([n], \binom{[n]}{d})$ where $\binom{[n]}{d}$ denotes all subsets of $[n]$ of size d.

The uniform matroid describes the structure of frames or more generally collections of vectors, with full spark.

To motivate some other powerful equivalent definitions of a matroids consider the linear matroid for the vectors $\Phi = \{\varphi_j\}_{j=1}^n$. Notice that for any subset $X \subseteq \Phi$ we can consider the span of the vectors in X, and the dimension of the span. The span of X may contain new vectors from Φ that were not in X originally, vectors that are linear combinations of the vectors in X. This defines a closure operation on linear matroids, $\text{cl}(X) = \text{span}(X) \cap \Phi$. The dimension of the $\text{span}(X)$, or the rank of X, is the size of the largest independence set contained in X. This means that the rank of a set X does not change after applying the closure operator. This also means that the closure of X is the maximal superset that does not change the rank.

Definition 1.4.9. Let $M = (E, \mathcal{I})$ be a matroid then the **rank function** $r : 2^E \to \mathbb{Z}_{\geq 0}$ will be defined for $X \subseteq E$ to be the size of the largest independent set contained in X. Likewise we can then define the **closure** $\text{cl} : 2^E \to 2^E$ as $\text{cl}(X) = \{x \in E | r(X \cup x) = r(X)\}$.

Both of which give cryptomorphic definitions for a matroid

Definition 1.4.10. Let E be a set. Then $r : 2^E \to \mathbb{Z}_{\geq 0}$ is the rank function for a matroid if and only if for all $X, Y \subseteq E$ the following are true

(R1) $0 \leq r(X) \leq |X|$

(R2) If $X \subseteq Y$ then $r(X) \leq r(Y)$

(R3) $r(X \cup Y) + r(X \cap Y) = r(X) + r(Y)$

With a rank function independence sets are the sets whose rank equal to the cardinality, the sets X where $r(X) = |X|$.

Definition 1.4.11. Let E be a set. Then $\text{cl} : 2^E \to 2^E$ is the closure operator for a matroid if and only if for all $X, Y \subseteq E$ the following are true

(Cl1) $X \subseteq \text{cl}(X)$

(Cl2) If $X \subseteq Y$ then $\text{cl}(X) \subseteq \text{cl}(Y)$

(CL3) $\text{cl}(\text{cl}(X)) = \text{cl}(X)$

(CL4) If $x \in E$ and $y \in \text{cl}(X \cup x) - \text{cl}(X)$ then $y \in \text{cl}(X \cup y)$

With the closure definition, we can describe independence, by elements not in a closure. That is y would be independent from some set X if $y \notin \text{cl}(X)$. This means that a set X is an independence set if any element is independent from all the rest, for $x \in X$, $x \notin \text{cl}(X - x)$. We leave a full proof of the equivalence of these cryptomorphic definitions to [Oxl11].

It is often useful to study structure up to equivalence classes. Two matroids $M = (E_1, \mathcal{I}_1)$ and $N = (E_2, \mathcal{I}_2)$ should be called equivalent if there exists a bijection on the ground sets E_1 and E_2 that preserves the independence sets. In the case of linear matroids, or equivalently representable matroids, we can express this situation in terms of multiplication by invertible matrices

Definition 1.4.12. Let $\Phi = \{\varphi_j\}_{j=1}, \Psi = \{\psi_j\}_{j=1} \subseteq V$ where $\dim V = d \geq 1$ Then the corresponding linear matroids $M(\Phi)$ and $M(\Psi)$ are **projectively equivalent** if there exists an invertible linear map $X : \operatorname{im}\Phi \to \operatorname{im}\Psi$ and invertible diagonal matrix $T \in \mathbb{F}^{n\times n}$ such that $\Psi = X\Phi T$. Furthermore $M(\Phi)$ and $M(\Psi)$ are **equivalent** if there exists a field automorphism $\alpha : \mathbb{F} \to \mathbb{F}$ such that Φ and $\alpha(\Psi)$ are projectively equivalent, where $\alpha(\Psi)$ is the result of applying the field automorphism element-wise thinking of Ψ as a matrix.

Proposition 1.4.13. *Let $M = (E, \mathcal{B})$ be a matroid. Then $M^* = (E, \mathcal{B}^*)$, called the* ***dual matroid****, where $\mathcal{B}^* = \{E - B | B \in \mathcal{B}\}$ is a matroid.*

Example 1.4.14. As an example we will look at the uniform matroid of $U_{d,n} = ([n], \binom{[n]}{d})$ where $\mathcal{B}^* = \{[n] - B | B \in \binom{[n]}{d}\} = \binom{[n]}{n-d}$ meaning $U^*_{d,n} = U_{n-d,n}$

In the construction of the dual matroid, we use basis elements of M to create the basis element of M^*, that is we may say that the complement of a basis (over E) is a basis of the dual matroid.

It is also useful to think about dual matroid under different definitions. We will first look at the complement of a circuit and a complement of an independent set.

Proposition 1.4.15. *Let M be a matroid with $\mathcal{I}$ its independent sets and $\mathcal{C}$ its circuits. Then for $I \in \mathcal{I}$, the set $E - I$ is a spanning set of M^* and for $C \in \mathcal{C}$, the set $E - C$ is a hyperplane of M^*, a maximally non-spanning independent set of M^*.*

We will also look at the rank and closure operators in the dual. For a matroid M on a ground set E we know that $r(E) = |B|$ for $B \in \mathcal{B}$ a base. This also means the dual rank of E should be $|E| - |B|$. This suggest that the dual rank, will be related to notation of the **nullity** of $A \subseteq E$, $n(A) = |A| - r(A)$

Proposition 1.4.16. *Let M be a matroid on the ground set E, with rank function $r : 2^E \to \mathbb{Z}_{\geq 0}$. The the dual matroid M^* has the dual rank function $r^* : 2^E \to \mathbb{Z}_{\geq 0}$ defined by*

$$r^*(A) = n(E) - n(E - A) = |A| + r(E - A) - r(E)$$

Furthermore M^* has the dual closure function $cl^* : 2^E \to 2^E$ defined by

$$cl^*(A) = \{a \in E | r^*(A \cup a) = r^*(A)\}$$

The closure operator gives a particularly useful method of determining if two matroids are dual.

Lemma 1.4.17. (Exercise 2.2.5 [Oxl11], Proposition 5.2.4 [Cra86]) Let M and N be two matroids over the same ground set E with closure operators cl_M and cl_N. Then $M = N^*$ if and only if for all partitions $(X, Y, \{z\})$ of E the element z is in exactly one of $\mathrm{cl}_M(X)$ or $\mathrm{cl}_N(Y)$

Proof. [Ian: *Do later.*] □

Chapter 2

On the Classical Theory of Frames

Frame theory provides a fairly strong setting for studying the packing problems such as finding optimal packings over real and complex lines through the origin. The classical theory focuses on lines in $\mathbb{F}^d$ where $\mathbb{F}$ is $\mathbb{R}$ or $\mathbb{C}$. In these cases a line ℓ can be represented by a vector φ which spans the line ℓ. The interior angle θ, between two lines ℓ_1 and ℓ_2 which are represented by the non-zero vectors φ_1 and φ_2, may be computed using the magnitude squared of the standard inner product $|\langle\varphi_1, \varphi_2\rangle|^2 = \|\varphi_1\|^2 \|\varphi_2\|^2 \cos^2(\theta)$. Hence, the study of line packings, by a choice of vector representatives, turns into a question about linear algebra: specifically related to inner products. This also allows us to quickly modify our motivating packing problem from being one of geometry, to one in terms of geometric algebra. Solution to these packing problems have important implications in fields as diverse as compressed sensing [BFMW13], digital fingerprinting [MQKF13], quantum state tomography [RBSC04; FHS17], multiple description coding [SH03; MD14; Wel74a], and discrete geometry [Fej65]. In certain cases, like when the lines are associated to an equiangular tight frame, the pairwise interior angle of such configurations is constant.

The simplest example of a "nice" line packing, which maximizes the pair wise interior angles is that of an orthonormal basis, or the lines spanned by its vectors, which is a maximal collection of lines whose pairwise angles are all $\pi/2$. More generally we will define frames which in some sense generalizes orthonormal bases, allowing for redundance, and only requiring a weakened version of Parseval's equality (Proposition 2.0.2 (iv)) which can be seen as a defining property of an orthonormal basis.

Properties of Orthogonality

To motivate the objects of interests we will review a few of the important properties of orthogonality in inner product spaces which frame theory generalizes. As a standard resource on linear algebraic over $\mathbb{R}$ or $\mathbb{C}$ we point towards [Axl24].

Lemma 2.0.1. (Pythagorean theorem) Let V be an inner product space with its induced norm, with a finite collection of orthogonal vectors $(x_j)_{j=1}^n$ then

$$\left\|\sum_{j=1}^n x_j\right\|^2 = \sum_{j=1}^n \|x_j\|^2$$

Proof. This follows from repeated application of the standard Pythagorean theorem. To see this we will use induction on n. Notice first that when $n = 1$ this follows trivially from $(x_j)_{j=1}^1$ having 1 vector. For $n = 2$, notice that for orthogonal vectors $x, y \in V$ we have that $\|v + w\|^2 = \langle x + y, x + y\rangle = \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle = \langle x, x\rangle + \langle y, y\rangle = \|x\|^2 + \|y\|^2$. Now fix $n > 2$ and notice that

$$\sum_{j=1}^{n+1} \|x_j\|^2 = \sum_{j=1}^{n} \|x_j\|^2 + \|x_{n+1}\|^2 = \left\|\sum_{j=1}^n x_j\right\|^2 + \|x_{n+1}\|^2 = \left\|\sum_{j=1}^n x_j + x_{n+1}\right\|^2 = \left\|\sum_{j=1}^{n+1} x_j\right\|^2$$

where the last step follows from the $n = 2$ case. □

Notice that any finite orthonormal collection of vectors $(e_j)_{j=1}^n$, is linearly independent. To see a proof sketch of this assume that $a_1e_1 + \cdots + a_ne_n = 0$, which means that $a_1e_1 + \cdots + a_{n-1}e_{n-1} = -a_ne_n$, Using orthogonality of $(e_j)_{j=1}^n$ we may show $\langle a_1e_1 + \cdots + a_{n-1}e_{n-1}, -a_ne_n\rangle = 0$, which must mean $a_n = 0$ and $a_1e_1 + \cdots + a_{n-1}e_{n-1} = 0$. This can be repeated to show $a_1 = \cdots = a_n = 0$. This shows that orthogonality implies linear independence. Other properties of orthonormal vectors, in particular orthonormal bases, are shown below without complete proof.

Proposition 2.0.2. *Let V be a finite inner product space with an orthonormal collection of vectors $(e_j)_{j=1}^n$. The following are equivalent*

(i) if $x \in V$ is such that $\langle x, e_j\rangle = 0$ for all $j \in [n]$ then $x = 0$

(ii) $(e_j)_{j=1}^n$ spans V.

(iii) $x = \sum_{j=1}^n \langle x, e_j\rangle e_j$ for all $x \in V$

(iv) $\|x\|^2 = \sum_{j=1}^n |\langle x, e_j\rangle|^2$ for all $x \in V$ (Parseval's equality)

In many applications of orthonormal bases (3) is of critical importance and highlights why orthonormal bases are often more desirable than general bases. (4) is relevant in defining a frame and acts as a generalization of the Pythagorean theorem so we will provide a proof that (4) is equivalent to the other 3 parts.

Proof. $(3) \Rightarrow (4)$: First for any $x \in V$ let $x = \sum_{j=1}^{n} \langle x, e_j \rangle e_j$ and notice that from the Pythagorean theorem $\|x\|^2 = \left\|\sum_{j=1}^{n} \langle x, e_j \rangle e_j\right\|^2 = \sum_{j=1}^{n} | \langle x, e_j \rangle |^2$.

We will show $(4) \Rightarrow (1)$ by contrapositive: Assume there exists a vector $x \in V$ such that $\langle x, e_j \rangle = 0$ for all $j \in [n]$ but $\|x\| > 0$. However notice that $\sum_{j=1}^{n} | \langle x, e_j \rangle |^2 = \sum_{j=1}^{n} 0 = 0$, And so the (4) is not true. □

2.1 Frame Theory

[Ian: *use A^* not $A^\dagger$??*] Through out we will assume V is finite dimensional inner product space, real or complex, with inner product being the standard dot product. This means the adjoint of any linear map is just the conjugate transpose.

In continuing the traditional abuse of notation (citations?) we will identify sequences of vectors $\Phi = (\varphi_j)_{j=1}^{n} \subseteq V$ with their **synthesis operators** $\Phi : \mathbb{F}^n \to V$ defined as $\Phi(x) = \sum_{j=1}^{n} x_j \varphi_j$. The **analysis operator** $\Phi^* : V \to \mathbb{F}^n$ is the adjoint, or complex transpose, of the synthesis operator Φ, where $\Phi^* x = (\langle \varphi_j, x \rangle)_j$. Its **frame operator** is defined to be $\Phi\Phi^*$ where $x \mapsto \sum_{j=1}^{n} \langle \varphi_j, x \rangle \varphi_j$ and its **Gram matrix** is $\Phi^*\Phi = [\langle \varphi_j, \varphi_k \rangle]_{jk}$.

Definition 2.1.1. A finite collection of vectors $\Phi = (\varphi_j)_j$ from $\mathbb{F}^d$ is a frame for $\mathbb{F}^d$ if there exists optimal constants $0 < A \leq B < \infty$ such that

$$A \|x\|^2 \leq \sum_{j=1}^{n} | \langle x, \varphi_j \rangle |^2 \leq B \|x\|^2 \quad \forall x \in \mathbb{F}^d \tag{2.1}$$

where A is called the **lower frame bound** and B is called the **upper frame bound**.

- A frame is called **equal-norm** if there exists some $a \in \mathbb{F}$ such that $\|\varphi_j\|^2 = a$ for all j and **unit-norm** if $a = 1$.

- An equal-norm collection of vectors (φ_j) is called **equiangular** if there exists some $b \geq 0$ such that $| \langle \varphi_j, \varphi_k \rangle |^2 = b$ when $j \neq k$.

- A frame is called c-**tight** if $A = B$, in which case c is used to denote the single frame bound. $c = A = B = 1$ then the frame is called **Parseval**.

- If Φ is equal-norm, equiangular and tight, it is called an **equiangular tight frame**.

Here we have defined equal-norm and equiangular frames in terms of the squared modulus or square norm, which is equivalent to the more standard practice of defining equal norm as $\|\varphi_j\| = a$ and equiangular similarly. This definition is more easily generalized to the finite field case, where square roots may not exist.

We will denote a finite unit-norm tight frame as (a, c)-FUNTF and an equiangular tight frame as (a, b, c)-ETF. Notice that orthonormal bases are exactly unit-norm Parseval frames, or $(1, 1)$-FUNTFs or $(1, 0, 1)$-ETFs. As we will see in next few results, we can always assume that either $a = 1$ or $c = 1$, in which case the other parameters are determined, and so we will often refer to (a, b, c)-ETFs as just ETFs. This suggests that a "nice" frame, which is not an orthonormal basis would be a tight frame.

A powerful tool in study of frames, particularly in the classical setting, is the use of the spectral theorem (Theorem 1.3.15), or more generally in analyzing the eigenvalues and diagonalizations of the Gram matrix, which is often done through the help of singular values, and singular value decompositions. First recall the spectral theorem

Theorem 2.1.2. *(Spectral Theorem) Let A be a $d \times d$ matrix over $\mathbb{F}$ either $\mathbb{R}$ or $\mathbb{C}$. A is **normal**, meaning $A^*A = AA^*$, if an only if A is orthogonally diagonalizable, meaning*

$$A = U\Lambda U^*$$

Where U is such that $U^*U = I$ and Λ is a diagonal matrix.

Notice that because this is a diagonalization, the entires of Λ are the eigenvalues of A. It just has the added feature that the eigenvectors are orthogonal. Furthermore $A^* = U^*\Lambda^*U$

Let Φ be a $d \times n$ matrix, and because both $\Phi^*\Phi$ and $\Phi\Phi^*$ are normal, this is a very helpful theorem, it it further happens that the eigenvalue of $\Phi\Phi^*$ (and $\Phi^*\Phi$) are real and non-negative, regardless of if $\mathbb{F}$ was $\mathbb{R}$ or $\mathbb{C}$. This tells us that $\Phi\Phi^* = U\Lambda U^*$ where U is a $d \times d$ unitary, and Λ a $d \times d$ diagonal matrix. By taking the square roots of the eigenvalues we can write $\Phi\Phi^* = U\Sigma\Sigma^*U^*$ where Σ is the $d \times n$ diagonal matrix whose diagonal entires are the square roots of the diagonal entries of Λ. Let V be an $n \times n$ unitary matrix in which case we can further write $\Phi\Phi^* = U\Sigma V^*V\Sigma^*U^*$. We can then pick V such that $\Phi = U\Sigma V^*$. This also means that $\Phi^*\Phi = V\Sigma^*U^*U\Sigma V^* = V\Sigma^*\Sigma V^*$. Meaning the non-zero eigenvalue of $\Phi^*\Phi$ and $\Phi\Phi^*$ are the same.

Definition 2.1.3. Let A be a $m \times n$ matrix with elements in $\mathbb{F}$. The **singular value decomposition**, often referred to as the SVD, is a factorization

$$B = U\Sigma V^*$$

Where U is an $m \times m$ unitary matrix, V is an $n \times n$ unitary matrix, and Σ is a $m \times n$ diagonal matrix with non-increasing non-negative real diagonal entries. The first $\min(m, n)$ diagonal values of Σ are denoted $(\sigma_j)_{j=1}^{\min(m,n)}$ and are called the **singular values** of B, and the number of non-zero singular values is equal to the rank of B.

The singular values can be equivalently defined as the square roots of the first $\min(m, n)$ eigenvalues of $\Phi^*\Phi$. Every matrix has a singular value decomposition but in general, this decomposition is not unique. However with a fixed ordering on the singular values, the matrix Σ is uniquely determined by the matrix B, and we can gain a lot of information from the singular values and the SVD of Φ. Through out we will always assume the singular values are ordered to be decreasing.

[Ian: *I guess this is called The Rayleigh-Ritz theorem? sort of?*]

Proposition 2.1.4. *Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of vectors in $\mathbb{F}^d$, with SVD $\Phi = U\Sigma V^*$. Then Φ is a frame with optimal bounds A and B if and only if $n \geq d$, $\sigma_d^2 = A$ and $\sigma_1^2 = B$. Furthermore, Φ is a c-tight frame if and only if the rows of Φ are orthogonal with norm $\sqrt{c}$.*

Proof. Using the SVD of Φ we can write

$$\Phi\Phi^* = U\Sigma V^*(U\Sigma V^*)^* = U\Sigma V^* V\Sigma^* U^* = U\Sigma\Sigma^* U^* \tag{2.2}$$

And to compute the frame bounds we notice that for any $x \in F^d$ the frame operator allows us to express $\langle \Phi\Phi^* x, x\rangle = \left\langle \sum_{j=1}^n \langle x, \varphi_j\rangle \varphi_j, x \right\rangle = \sum_{j=1}^n \langle x, \varphi_j\rangle \langle \varphi_j, x\rangle = \sum_{j=1}^n | \langle x, \varphi_j\rangle |^2$ meaning

$$\sum_{j=1}^n | \langle x, \varphi_j\rangle |^2 = \langle \Phi\Phi^* x, x\rangle = \langle U\Sigma\Sigma^* U^* x, x\rangle = \langle \Sigma^* U^* x, \Sigma^* U^* x\rangle = \|\Sigma^* U^* x\|^2$$

And so our frame bounds are determined by the maximum and minimum of $\|\Sigma^* U^* x\|^2$. Consider a unit norm vector for x we would have $\|U^* x\| = 1$. To maximize $\|\Sigma^* U^* x\|$ we would need $U^* x = \mathbf{e}_1$, which happens when x is equal to the first column of U. This maximizes $\|\Sigma^* U^* x\|^2 = \|\sigma_1 \mathbf{e}_1\| = \sigma_1^2$, which follows from the imposed order of the singular values on Σ and the Pythagorean theorem. Likewise for the same reason if x is the last column of U then $\|\Sigma^* U^* x\|^2$ is minimized. If $n \geq d$ we would have $\|\Sigma^* U^* x\|^2 = \|\Sigma^* \mathbf{e}_d\| = \|\sigma_d \mathbf{e}_d\| = \sigma_d^2$. Case 2: If $n < d$ then $\|\Sigma^* U^* x\|^2 = \|\Sigma^* \mathbf{e}_d\|^2 = 0$ this follows from Σ^* being a diagonal matrix with $n < d$ diagonal elements so the dth column of Σ^* is zero, and so $\Sigma^* \mathbf{e}_d = 0$. This means for Φ to be a frame we must have $n \geq d$ which means there will be a dth non-zero singular value in the SVD in which case we would have

$$\sigma_d^2 \|x\|^2 \leq \sum_{j=1}^n | \langle x, \varphi_j\rangle |^2 \leq \sigma_1^2 \|x\|^2$$

with optimal bounds $A = \sigma_d^2$ and $B = \sigma_1^2$. This concludes the first part of the proof.

For the second part, assume Φ is c-tight and notice that the frame operator $\Phi\Phi^* = (\Phi^*)^*\Phi^*$, meaning $\Phi\Phi^*$ is the Gram matrix of the analysis operator Φ^*, meaning it represents inner products between conjugates of the rows. That is $\Phi\Phi^* = (\langle {\Phi_k}^*, {\Phi_j}^* \rangle)_{jk}$[1], where Φ_k represents the kth row of Φ and so from equation 2.2 we have that

$$(\langle \Phi_k^*, {\Phi_j}^* \rangle)_{jk} = U\Sigma\Sigma^* U^* = UcI_d U^* = cI_d$$

Where the last three steps follow from the fact that the frame being tight means the singular values must all be $\sqrt{c}$ for some positive c. Furthermore, under conjugate symmetry, we know that $(\langle \Phi_j, \Phi_k \rangle)_{jk} = (\langle \Phi_k^*, {\Phi_j}^* \rangle)_{jk}$ This is equivalent to the rows of Φ being linearly independent and $\|\Phi_j\| = \sqrt{\langle \Phi_j, \Phi_j \rangle} = \sqrt{c}$ for all j. The other direction follows identically. □

Notice that the second part of the proof of this proposition shows that a frame is tight if and only if the frame operator is a positive multiple of the identity, more specifically when $\Phi\Phi^* = cI$ where c is the frame bound. Later in Lemmas 3.1.5 and 3.4.1 we will explore more equivalent notions of tightness. We have also shown that frames must have at least as many vectors as the dimension, but we can strengthen this by observing that the first d singular values must be non-zero meaning the rank of Φ must be d.

Corollary 2.1.5. *Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of vectors in $\mathbb{F}^d$. Then Φ is a frame if and only if the vectors of Φ spans $\mathbb{F}^d$.*

As another corollary we can combine frames to get a new frame, oftentimes retaining the same properties.

Corollary 2.1.6. *Let $\Phi = (\varphi_j)_{j=1}^n$ and $\Psi = (\psi_j)_{j=1}^m$ be tight frames for $\mathbb{F}^d$ with frame bounds c and c' respectively. Their concatenation $(\varphi_1, \ldots, \varphi_n, \psi_1, \ldots \psi_m)$ is a tight frame with frame bound $c + c'$.*

Proof. From proposition 2.1.4, we know that the frame operators for both frames are multiples of the identity matrix: $\Phi\Phi^* = cI_d$ and $\Psi\Psi^* = c'I_d$. Notice that the union of both frames has as its

[1] Ian: *idicies flipped?*

synthesis matrix the augmented matrix $\begin{pmatrix} \Phi & \Psi \end{pmatrix}$. And so the frame operator

$$\begin{pmatrix} \Phi & \Psi \end{pmatrix} \begin{pmatrix} \Phi & \Psi \end{pmatrix}^* = \begin{pmatrix} \Phi & \Psi \end{pmatrix} \begin{pmatrix} \Phi^* \\ \Psi^* \end{pmatrix} = \Phi\Phi^* + \Psi\Psi^* = cI_d + c'I_d = (A+B)I_d$$

Therefore the union of both tight frames is a tight frame with frame bound $c + c'$. □

Proposition 2.1.7. *Let $\Phi = (\varphi_j)_{j=1}^n$ be a frame for $\mathbb{F}^d$. If $(\lambda_k)_{k=1}^d$ are the eigenvalues of the frame operator $\Phi\Phi^*$ then*

$$\sum_{k=1}^{d} \lambda_k = \sum_{j=1}^{n} \|\varphi_j\|^2$$

And if Φ is a FUNTF then the frame bound is $c = n/d$. More generally for an (a, c)-equal norm tight frame $na = cd$.

Proof. Recall that the sum of the eigenvalues of a matrix is equal to the trace of the matrix and that the trace of a product of matrices is invariant under cyclic permutations of the matrices, meaning

$$\sum_{k=1}^{d} \lambda_k = \operatorname{tr}(\Phi\Phi^*) = \operatorname{tr}(\Phi^*\Phi) = \sum_{j=1}^{n} \|\varphi_j\|^2$$

Furthermore notice that if Φ is an FUNTF with frame bound c we know from proposition 2.1.4 that $\Phi\Phi^* = cI$ and so $\operatorname{tr}(\Phi\Phi^*) = \operatorname{tr}(cI) = dc$. And like wise we know that $\operatorname{tr}(\Phi^*\Phi) = \sum_{j=1}^{n} \|\varphi_j\|^2 = n$, so $n = dc$ meaning $c = n/d$. □

To conclude this section we will highlight that Parseval frames (and up to rescaling tight frames) can be viewed as projections of orthonormal bases.

Definition 2.1.8. A linear operator $P : V \to V$ is called a **projection** if $P^2 = P$. Furthermore, a projection P is called an **orthogonal projection** if P is Hermitian, that is $P = P^*$.

The next result is a special case of what was originally proven in [Neu43]. A more contemporary treatment of the result can be found in [CFMPS13], and an operator theoretic approach can be found in [HL00].

Theorem 2.1.9. *(Naimark's Theorem) The collection of vectors $\Phi = (\varphi_j)_{j=1}^n$ is a Parseval frame for $\mathbb{F}^d$ if and only if there exists an inner product space $W \supseteq V$ with orthonormal basis $(e_j)_{j=1}^n$ and orthogonal projection $P : W \to W$ onto V such that $\varphi_j = Pe_j$ for all j.*

Proof. We will first show the $\Leftarrow$ direction: Assume $V \subseteq W$, meaning W is a super set of dimension n with basis $(e_j)_{j=1}^n$ and $P : W \to W$ an orthogonal projection onto V, which means P fixes V. Notice that for any $x \in V \subseteq W$ we have that

$$\sum_{j=1}^n |\langle x, Pe_j\rangle|^2 = \sum_{j=1}^n |\langle P^*x, e_j\rangle|^2 = \sum_{j=1}^n |\langle Px, e_j\rangle|^2 = \sum_{j=1}^n |\langle x, e_j\rangle|^2 = \|x\|^2$$

which follows from proposition Proposition 2.0.2 (iv), Parseval's equality, as $(e_j)_{j=1}^n$ is an orthonormal basis. This means the collection of vectors $(Pe_j)_{j=1}^n$ is a Parseval frame for $V = \mathbb{F}^d$.

Now for the $\Rightarrow$ direction: assume that $\Phi = (\varphi_j)_{j=1}^n$ is a Parseval frame for $\mathbb{F}^d$ and by proposition 2.1.4 we know that $\Phi\Phi^* = I_d$, meaning the d rows of Φ are n-dimensional orthonormal vectors. Case 1: if $d = n$ then $\Phi\Phi^* = I_d = \Phi^*\Phi$ and the result follows immediately. Case 2: Assume that $n > d$ then it is the case that the d n-dimensional orthonormal row vectors can be extended to an orthonormal basis over $\mathbb{F}^n$. That is there exists $n-d$, n-dimensional vectors $(v_\ell)_{\ell=1}^{n-d}$ such that the rows of Φ and $(v_\ell)_{\ell=1}^{n-d}$ form an orthonormal basis. Let Ψ be the matrix whose rows are $(v_\ell)_{\ell=1}^{n-d}$ and we will denote the columns as $(\psi_j)_{j=1}^n$. Notice the matrix

$$X = \begin{pmatrix} \Phi \\ \Psi \end{pmatrix}$$

is invertible as $XX^* = I$ and $X^*X = I$ so the columns of X form an orthonormal basis for $\mathbb{F}^n$.

Finally, consider the projection of $\mathbb{F}^n$ onto the first d coordinates which would map this orthonormal basis onto $(\varphi_j)_{j=1}^n$ as desired. □

This theorem can be extended to tight frames with frame bound c by first rescaling to get a Parseval frame. This theorem provides a very powerful duality of tight frames which share many of the properties of the original frame.

Definition 2.1.10. Let $\Phi = (\varphi_j)_{j=1}^n$ be a c-tight frame for $\mathbb{F}^d$ and consider a collection of vectors $\Psi = (\psi_j)_{j=1}^n$ in $\mathbb{F}^{n-d}$. If $\Phi^*\Phi + \Psi^*\Psi = cI$ then we call Ψ a **Naimark complement** of Φ.

From this definition Naimark compliments are a symmetric relationship. Naimark compliments always exists, and have been studied extensively by various authors [CFMPS13; KM25]

Proposition 2.1.11. *Let $\Phi = (\varphi_j)_{j=1}^n$ be a c-tight frame for $\mathbb{F}^d$ and $\Psi = (\psi_j)_{j=1}^n$ a Naimark complement. Then Ψ is a c-tight frame for $\mathbb{F}^{n-d}$. Furthermore, if Φ is equiangular or equal-norm then so is Ψ.*

Proof. If Ψ is a tight frame we know that $\Phi\Phi^* = cI_d$, meaning there are d eigenvalues of $\Phi\Phi^*$ which are c. And because the non-zero eigenvalues of $\Phi\Phi^*$ and $\Phi^*\Phi$ agree, $\Phi^*\Phi$ has d non-zero eigenvalues which are each c and $n-d$ eigenvalues which are 0. Since Ψ is the Naimark complement of Φ we know that $\Phi^*\Phi + \Psi^*\Psi = cI$ and so $\Psi^*\Psi = cI - \Phi^*\Phi$ has $n-d$ non-zero eigenvalues that are c and d eigenvalues that are 0. To see this notice that $\operatorname{tr}(\Psi^*\Psi) = \operatorname{tr}(cI) - \operatorname{tr}(\Phi^*\Phi) = (n-d)c$. Notice also that the only eigenvalues of $\Psi^*\Psi$ are 0 and c: that is for x an eigenvalue for some vector v, $cIv - \Phi^*\Phi v = xIv$ which means $(c-x)Iv = \Phi^*\Phi v$ and so $c-x$ is an eigenvalue of $\Phi^*\Phi$ meaning $c-x$ is either c or 0 so x is either 0 or c. This therefore means Ψ is a frame for $\mathbb{F}^{n-d}$ with singular values $\sigma_1 = \sigma_{n-d} = \sqrt{c}$ and so Ψ is a c-tight frame.

From the definition of Naimark complement, we know that

$$\left\langle \begin{pmatrix} \varphi_j \\ \psi_j \end{pmatrix}, \begin{pmatrix} \varphi_k \\ \psi_k \end{pmatrix} \right\rangle = \langle \varphi_j, \varphi_k \rangle + \langle \psi_j, \psi_k \rangle = c\delta_{j,k}$$

Now assume that Φ is equiangular. This means when $j \neq k$ we have that $\langle \psi_j, \psi_k \rangle = -\langle \varphi_j, \varphi_k \rangle$ and so $|\psi_j, \psi_k|^2 = |\langle \varphi_j, \varphi_k \rangle|^2$ meaning Ψ is equiangular. Likewise if Φ is equal norm, we have for any j that $\langle \psi_j, \psi_j \rangle = c - \langle \varphi_j, \varphi_j \rangle$ and so Ψ is equal norm. □

Naimark complements are not necessarily unique.

2.2 Algebraic Spread and Linear Dependence

A key advantage to interpreting data with a frame, as opposed to an orthonormal basis, is to make the data more robust to noise and loss of information. Frames achieve this robustness through redundancies. However, a frame is defined as collection of vectors that spans a non-isotropic space. And it is often important to distinguish good frames from bad frames with notions of geometric and algebraic spread. In the next section we will explore the notions of geometric spread, coming from the inner product, and here we will focus on a notion of algebraic spread and the frames with good algebraic spread. Algebraic spread encapsulates how mutually linearly dependent a collection of data is, and is formalized with the definition of spark.

Definition 2.2.1. Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of vectors in $\mathbb{F}^d$, then the **spark** of Φ is defined as

$$\operatorname{spark}\Phi = \min\{m \mid (\varphi_{j_k})_{k=1}^m \subseteq (\varphi_j)_{j=1}^n \text{ linearly dependent, } j_1 < j_2 < \cdots < j_m\}$$

If $\operatorname{spark}(\Phi) = \dim(\operatorname{im}\Phi) + 1$ then we say Φ is full spark.

This means the spark is the size of the smallest subset of linearly dependent vectors. A system of lines being full spark means any subset of d vectors forms a basis for the span of all the lines. In general $1 \leq \operatorname{spark}(\Phi) \leq \operatorname{rank}(\Phi) + 1$, which suggests that while the rank encapsulates the maximal (linear) independence of a collection of vectors the spark in a sense encapsulates the worst-case, or minimal dependence, of a collection of vectors. The spark captures a sense of how mutually redundant the vectors are.

Matroids act as important and useful tools in studying the dependence of a lines and their algebraic spread. As we had seen in Section 1.4, circuits can be thought of as minimally dependent sets, and we called the size of the smallest circuit the **girth** of the matroid and for a representable matroid is exactly the **spark** of its vectors. This allows us to interpret frames as matroids. Here will will highlight so important results related to the matroids of frames, or more generally for linear matroids.

Proposition 2.2.2. *A collection of vectors $\Phi = (\varphi_j)_{j=1}^n$ in $\mathbb{F}^d$ (over ant field $\mathbb{F}$) has full spark if and only if $M(\Phi)$ is the uniform matroid, $U_{d,n} = ([n], \binom{[n]}{d})$ by the basis definition 1.4.5.*

Proof. Assume $M(\Phi)$ is the uniform matroid meaning any collection of less than or equal to d vectors is linearly independent as all subsets of size d are linearly dependent and so not circuits. This also means any subset of $d+1$ vectors is a circuit, and so the girth of the matroid is $d+1$. Now assume that the collection of vectors $(\varphi_j)_{j=1}^n$ has spark $d+1$. This means the girth of the matroid $M(\Phi) = ([n], \mathcal{I})$ is $d+1$ and so every subset of $d+1$ vectors is dependent and so must contain a circuit, and because circuits are of size at least $d+1$, then every such subset is a circuit, meaning every subset of size d is in $\mathcal{I}$, which form the basis. □

Proposition 2.2.3. *Φ is full rank if and only if $M(\Phi) = M(\Phi^\dagger \Phi)$*

We will prove this result in more generality later.

In the previous section we introduced the Naimark complement, which was a complementary construction for a tight frame. And as seen previously, Naimark complements shared many nice properties such as having equiangular vectors if and only if the original frame did. We will continue this duality of properties and relate their corresponding matroids and spark.

Theorem 2.2.4. *Let $\Phi = (\varphi_j)_{j=1}^n$ be a c-tight frame for $\mathbb{F}^n$, with $\Psi = (\psi_j)_{j=1}^n$ a Naimark compliment in $\mathbb{F}^n$. Then $M(\Psi) = M(\Phi)^*$*

We will postpone the proof of this theorem until Chapter 3 where will will prove this theorem allowing for the underlying fields to be of positive characteristic.

Corollary 2.2.5. *A c-tight frame $\Phi = (\varphi_j)_{j=1}^n$, is full spark if and only if its Naimark complements $\Psi = (\psi_j)_{j=1}^n$ is full spark.*

Proof. Recall that if Ψ is the Naimark complement of Φ then Φ is the Naimark complement of Ψ and so it suffices to only show one direction.

Assume Φ is full spark which means that $M(\Phi) = U_{d,n}$. And so $M(\Psi) = M(\Phi)^* = U_{d,n}^* = U_{n-d,n}$ and so from proposition 2.2.2 Ψ has full spark. □

2.3 Geometric Spread and Packing Problems

In this section we will present a different notion of spread, coming from the underlying geometry of a collection of vectors. This perspective is frequently used in the context of studying optimal packings of lines.

Frame theory provides a very natural setting for studying packings of lines through the origin. Because a system of lines $(\ell_j)_{j=1}^n$ in $\mathbb{F}^d$, is a collection of points in the projective space $\mathbb{FP}^{d-1}$, which is a Riemannian manifold when $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$: we can say the distance between lines is exactly the geodesic distance between points. The geodesic distance is exactly the non-obtuse angle between the lines which can be easily computed with the choice of unit norm representatives $(\varphi_j)_{j=1}^n$ for the lines. Therefore the distance between any two lines, can be computed by looking at the standard dot product where $|\langle \varphi_j, \varphi_k \rangle|^2 = \cos^2\theta$. Through out this entire section we will assume that $\mathbb{F} = \mathbb{R}$ or $\mathbb{C}$ along with the standard inner product. This is by no means the only distance which can be used the understand geometric spread. In Chapter 4, we will look at a few different notions of distance, such at the chordal distance which are in some sense more interesting when studying subspace packings, or packings of points on a Grassmannian.

Maximizing the minimum distance between any two lines is therefore equivalent to minimizing the maximum modulus squared of the inner product of the vector representatives. We will use this as our notion of "geometric spread".

Definition 2.3.1. For a collection of vectors $\Phi = (\varphi_j)_{j=1}^n$ in $\mathbb{F}^d$ the **coherence squared** is defined to be

$$\mu^2(\Phi) = \max_{j \neq k} \frac{|\langle \varphi_j, \varphi_k \rangle|^2}{\|\varphi_j\|^2 \|\varphi_k\|^2}$$

In the case where Φ is a collection of unit vectors this simplifies to be

$$\mu^2(\Phi) = \max_{j \neq k} |\langle \varphi_j, \varphi_k \rangle|^2.$$

Most authors define and work with the **coherence** μ, which is the square root of what we have defined, $\mu(\Phi) = \sqrt{\mu^2(\Phi)}$. However this definition will be the correct generalization for Chapter 3.

For the remainder of this section we will assume any collection of vectors is a collection of unit vectors.

Definition 2.3.2. A collection of unit vectors $\Phi = (\varphi_j)_{j=1}^n$ in $\mathbb{F}^d$ is called a **Grassmannian Frame** if it is a minimizer for the coherence squared. That is Φ is a Grassmannian frame if

$$\Phi \in \arg\min_{\Psi} \mu^2(\Psi)$$

First we will justify the naming of Grassmannian frame when $n \geq d$

Proposition 2.3.3. *(Lemma 2 [FJM18], Proposition 4 [JKM19]) If $\Phi = (\varphi_j)_{j=1}^n$ is a Grassmannian frame, then Φ is a frame.*

Finding Grassmannian frames is a big open problem in general. For a current leaderboard and a more in-depth overview of many of the well-known constructions of complex Grassmannian frames we point to [JKM19].

In some special cases, Grassmannian frames correspond to objects in frame theory. In this section we will highlight some of the wellknown constructions of Grassmannian frames, by first finding lower bounds on the coherence and then determine objects from frame theory which saturate those bounds. This chapter will focus on two such bounds: often referred to as the Welch bound and the Simplex bound. In general the existence of these objects is unknown.

The Welch Bound and Equiangular Tight Frames

[Ian: *find original sources??*]The following interpretation, using the variance of eigenvalues, was shown to the authors by Dustin Mixon's in a talk they had given at the the Rocky Mountain Algebra and Combinatorics at the Colorado State University in Fort collins. A more standard analysis looks at $\left\|\Phi\Phi^* - \frac{n}{d} I_d\right\|_F$ which is equal to $E[\lambda^2] - E[\lambda]^2$.

Consider a collection of vectors $\Phi = (\varphi_j)_{j=1}^n$ such that $n > d$. Because the coherence is defined as a maximum of the modulus squared of the inner products, a simple lower bound would be to consider the average modulus squared of the inner products, which can be written in terms of the Frobenius norm.

$$\begin{aligned}
\mu^2(\Phi) = \max_{j\neq k} |\langle \varphi_j, \varphi_k\rangle|^2 &\geq avg_{j\neq k}|\,\langle \varphi_j, \varphi_k\rangle\,|^2 \\
&= \frac{1}{n(n-1)} \sum_{j\neq k} |\,\langle \varphi_j, \varphi_k\rangle\,|^2 \\
&= \frac{1}{n(n-1)} \left(\sum_{j=1}^{n} \sum_{k=1}^{n} |\,\langle \varphi_j, \varphi_k\rangle\,|^2 - \sum_{j=1}^{n} |\,\langle \varphi_j, \varphi_j\rangle\,|^2 \right) \\
&= \frac{1}{n(n-1)} \left(\|\Phi^*\Phi\|_F^2 - n \right) \qquad (2.3)
\end{aligned}$$

Next using properties of the Frobenius norm, in that it is defined with the trace, we will write the Frobenius norm in terms of common eigenvalues of $\Phi^*\Phi$ and $\Phi\Phi^*$

$$\|\Phi^*\Phi\|_F^2 = \sum_{i=1}^{n} \lambda_i^2 = \sum_{i=1}^{d} \lambda_i^2 = \|\Phi\Phi^*\|_F^2$$

where $(\lambda_i)_{i=1}^{d}$ are the common eigenvalues as $n > d$. This equation highlights that the Frobenius norm squared can be viewed as d times the second moment of the eigenvalues, that is $\mathbb{E}[\lambda^2] = \frac{1}{d}\|\Phi^*\Phi\|_F^2$. The first moment or the expected value of the eigenvalues can be computed as

$$\mathbb{E}[\lambda] = \frac{1}{d}\operatorname{tr}(\Phi\Phi^*) = \frac{1}{d}\operatorname{tr}(\Phi^*\Phi) = \frac{n}{d}.$$

Together we can use these to write a formula for the variance of the eigenvalues which must be positive

$$0 \leq E[\lambda^2] - E[\lambda]^2 = \frac{1}{d}\|\Phi^*\Phi\|_F^2 - \frac{n^2}{d^2}.$$

Multiplying by d and substituting Equation (2.3) gives

$$0 \leq n(n-1)\max_{j\neq k} |\langle \varphi_j, \varphi_k\rangle|^2 + n - \frac{n^2}{d}$$
$$\frac{(n-d)}{d(n-1)} \leq \max_{j\neq k} |\langle \varphi_j, \varphi_k\rangle|^2$$

This results is often referred to as the Welch bound, or the Welch-Rankin bound, and was independently proven by L. R. Welch in [Wel74b] and as a corollary of a sphere packing bound by Robert Rankin in [Ran55], which we will show in the following subsection.

Theorem 2.3.4. *(Welch bound) Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of unit norm vectors in $\mathbb{F}$ such that $n > d$*

$$\mu^2(\Phi) \geq \frac{n-d}{d(n-1)}$$

with equality if and only if Φ is an ETF

Proof. All that is left to show is the case of equality. To understand this case we will investigate the two times we used an existing bound. The first was bounding the maximum modulus squared by the average. In the case of equality, where the maximum equals the average is the case were every inner product has the same modulus squared. This is exactly the case where Φ is equiangular.

The next bound we used was in bounding the variance by 0. Equality in this case, when the variance of the eigenvalues is 0 is exactly the case where all the eigenvalues of equal and non-zero. This would mean that every eigenvalue would be $\frac{n}{d}$, and Φ would therefore be a tight frame for $\mathbb{F}^d$. □

It is important to note that for any particular choice of d and n, such that $n > d$, an ETF may not exist, and so the coherence squared would be greater then that of the above bound and would be maximized by a collection of vectors what didn't form an ETF. To this end, it is relevant to understand that cases in which ETFs exist. In trying to understand when ETF exist for particular choices of n and d we will first look at the cases where equiangular lines exist.

Theorem 2.3.5. *(Gerzon's Bound. Theorem 3.5 [LS73]) Let $\mathbb{F}$ be either $\mathbb{R}$ or $\mathbb{C}$ and let $k = \dim_{\mathbb{R}} \mathbb{F}$ be 1 or 2 respectively. An equiangular system of n vectors Φ for $\mathbb{F}^d$ exists only if $n \leq d + \frac{k}{2}(d^2 - d)$. In the case of equality Φ is a tight frame.*

We will delay the proof of this result until Theorem 3.4.13 where we will prove this result for nearly all quadratic spaces and unitary spaces. Recall that we had introduced the notation $Z(d, \mathbb{F}) := d + \frac{\dim_{\mathbb{F}_0} \mathbb{F}}{2}(d^2 - d)$, which counted the dimension of the space of self adjoint matrices over $\mathbb{F}$.

This result does give one important implication to the Welch Bound: in the case where n is greater then that of Gerzon's bound, $Z(d, \mathbb{F})$, Grassmannian frames will not be equiangular. In general it is an unknown whether systems of equiangular vectors which saturate Gerzon's bounds exists for all d. In the case where $\mathbb{F} = \mathbb{R}$ this is know to be false. See [FM16] for tables on the existence of ETFs and [STDH07] for criterions for existence of ETFs, including for maximal ETFs that either $d < 3$ or $\sqrt{d+2}$ is an odd integer. In fact for $d < 89^2$, the only dimensions which maximal systems of equiangular lines are known to exists are $d = 2, 3, 7$, and 23. It has been conjectured independently by multiple authors including [Gil18; GR01] that these are the only dimensions in which Gerzon's bound is saturated over $\mathbb{R}$.

Conjecture 2.3.6. There exists an equiangular tight frame of $\binom{d+1}{2}$ vectors in $\mathbb{R}^d$ if and only if $d = 2, 3, 7$ or 23.

This conjecture is often referred to as the Gillespie conjecture after Neil Gillespie, who in 2018 considered the additional structure of incoherence sets, defining an incoherence bound, and showing that equiangular systems which saturate Gerzon's bound and the incoherence bound can only exists when $d = 2, 3, 7$ or 23 [Gil18]. This conjecture and evidence for it predate Gillespie, including in [GR01; STDH07]. We will expand on the study of incoherence sets, for frame over fields of positive characteristic in Section 3.5. The implication of the insaturability of Gerzon's for many real vector spaces, is that when $d \notin \{2, 3, 7, 23\}$ maximal systems of equiangular lines,

[2] Ian: *find source, i found this in the first finite field paper but they didnt have a source*

are not ETFs, and likewise Grassmannian frames of $n > Z(d, \mathbb{F})$ vectors are not ETFs, nor even equiangular.

In the complex case where $\mathbb{F} = \mathbb{C}$ the situation is different, and the corresponding conjecture is as follows

Conjecture 2.3.7. (Zauner's weak Conjecture) For all $d \geq 2$ there exists an equiangular tight frame of d^2 vectors in $\mathbb{C}^d$.

The conjecture stated above is a weaker version of the conjecture that appeared originally in Zauner's 1999 PhD thesis[3]. Currently no infinite family of d^2 equiangular lines is known, but d^2 $\leftarrow\boxed{\text{I}}$ equiangular lines in C^d have been explicitly constructed in all dimensions $d \leq 53$ with sporadic further dimensions up to $5,799$ (as of March 2025 [3]).

The Orthoplex Bound and Maximal Sets of Mutually Unbiased Basis

An alternative way to view a collection of lines, or a collection of unit vector representatives is to consider the projection maps onto the lines. Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of unit vectors in $\mathbb{F}^d$, and consider the projection maps $P_j = \varphi_j \varphi_j^*$ which projects $\mathbb{F}^d$ onto the line spanned by φ_j. These projections, by construction have a common trace, where $\operatorname{tr} P_j = \operatorname{tr}(\varphi_j \varphi_j^*) = \operatorname{tr}(\varphi_j^* \varphi_j) = 1$. Trace being linear, allows us associate these matrices which have trace 1 with the matrices in the kernel of the trace function, by shifting each projection. Therefore we will consider the de-traced projections $Q_j = P_j - \frac{1}{d} I_d$ which live in a subspace. The collection of Q_j matrices live in the space of trace zero self adjoint matrices. We will denote this space to be

$$L_0 = \{A \in L : A^\dagger = A, \operatorname{tr}(A) = 0\}$$

Because the image of the trace, is one dimensional $\dim_{\mathbb{F}_0} L_0 = \dim_{\mathbb{F}_0} L - 1 = Z(d, \mathbb{F}) - 1$ is 1 less then the space of all self adjoint matrices.

[3] Ian: *I dont actually know what appear in Zauner's thesis lol*

Looking at the Frobenius inner product of these traceless operators gives us the following

$$\begin{aligned}\langle Q_j, Q_k\rangle_F &= \left\langle P_j - \frac{1}{d}I_d, P_k - \frac{1}{d}I_d\right\rangle \\ &= \operatorname{tr}(P_jP_k) - \frac{1}{d}\operatorname{tr}(P_j) - \frac{1}{d}\operatorname{tr}(P_k) + \frac{1}{d^2}\operatorname{tr}(I_d) \\ &= |\langle\varphi_j, \varphi_k\rangle|^2 - \frac{1}{d}\end{aligned}$$

and likewise that $\|P_j\|_F^2 = \frac{d-1}{d}$, meaning the de-traced normalized projections $\left(\sqrt{\frac{d}{d-1}}Q_j\right)_{j=1}^n$ live on the unit sphere contained in the space of trace 0 self adjoint matrices.

Under this interpretation we have translated our packing problem, about packings of lines, into a more well known problem about packings of a sphere and so we can apply the well known Rankin bounds for packings on real spheres. Originally proven in [Ran55], more recent treatments can be found in [EZ01].

Theorem 2.3.8. *(Rankin Sphere Packing Bounds)Consider a collection $(x_j)_{j=1}^d$ of points on the unit sphere S^{d-1} in $\mathbb{R}^d$. Then*

$$\max_{j\neq k}\langle x_j, x_k\rangle \geq \frac{-1}{n-1}$$

and equality occurs only if $n \leq d+1$. If $n > d+1$ then

$$\max_{j\neq k}\langle x_j, x_k\rangle \geq 0$$

and equality occurs only if $n \leq 2d$.

The first rankin bound, applied to the de-traced normalized projections $(\sqrt{\frac{d}{d-1}}Q_j)_{j=1}^n$ gives us

$$\max_{j\neq k}\frac{d}{d-1}\langle Q_j, Q_k\rangle = \max_{j\neq k}\frac{d}{d-1}(|\langle\varphi_j, \varphi_k\rangle|^2 - \frac{1}{d}) \geq \frac{-1}{n-1}$$

and so

$$\mu^2(\Phi) = \max_{j\neq k}|\langle\varphi_j, \varphi_k\rangle|^2 \geq \frac{n-d}{d(n-1)}$$

which recovers the Welch Bound. Using the second rankin bound we get a new bound for the case in which the welch bound does not apply, referred to as the orthoplex bound.

Theorem 2.3.9. *(Orthoplex Bound) Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of unit norm vectors in $\mathbb{F}$ such that $n > Z(d, \mathbb{F})$*

$$\mu^2(\Phi) \geq \frac{1}{d}$$

with equality only if $n \leq 2(Z(d, \mathbb{F}) - 1)$.

Proof. In the case where $n > (\mathcal{Z}(d, \mathbb{F}) - 1) + 1$. We can conclude from the second Rankin bound that

$$\max_{j \neq k} \langle Q_j, Q_k \rangle = \max_{j \neq k} (|\langle \varphi_j, \varphi_k \rangle|^2 - \frac{1}{d}) \geq 0$$

giving us

$$\mu^2(\Phi) = \max_{j \neq k} |\langle \varphi_j, \varphi_k \rangle|^2 \geq \frac{1}{d}$$

□

Just as in the case of the welch bound we wish to understand structures which saturate this bound. Its also important to note that this bound depends only on the dimension of the space in which the lines are packed, and not the number of lines. Meaning the existence of an example which saturates the bound for $n > Z(d, \mathbb{F})$ lines, gives rise to systems of m lines for all $Z(d, \mathbb{F}) < m \leq n$. The examples, that we will introduction, of Grassmannian frames which saturate the orthoplex bound come from collections of maximal sets of mutually unbiased bases.

Definition 2.3.10. Two orthonormal bases $\mathcal{B} = \{v_1, \ldots, v_d\}$ and $\mathcal{B}' = \{v'_1, \ldots, v'_d\}$ for $\mathbb{F}^d$ are said to be **mutually unbiased (MU)** if

$$|\langle v_j, v'_k \rangle|^2 = \frac{1}{d}$$

for all $v_j \in \mathcal{B}$, and $v'_k \in \mathcal{B}'$. More generally two vectors $u, v \in \mathbb{F}^d$ are said to be mutually unbiased if $|\langle u, v \rangle|^2 = \frac{1}{d}$.

A collection of n orthonormal bases $\{B_0, \ldots, B_{n-1}\}$ for $\mathbb{F}^d$ which are pairwise mutually unbiased would be called a collection of n **Mutually Unbiased Bases (MUBs)** for $\mathbb{F}^d$. Using Corollary 2.1.6 we can see that a collection of n MUBs, and specifically the nd vectors in each of the n bases, would be an n-tight frame for $\mathbb{F}^d$. We will denote a collection of MUBs as a matrix $B = \left[B_0|\cdots|B_{n-1}\right]$.

Notice that a collection of n MUBs would saturate the orthoplex bound when $nd > Z(d, \mathbb{F})$. In the case where $\mathbb{F} = \mathbb{R}$, this would require that $n > \frac{1}{2}(d+1)$, and when $\mathbb{F} = \mathbb{C}$, this would require that $n > d$. Furthermore if we had a collection of n MUBs where $nd > Z(d, \mathbb{F})$, we could remove vectors and still saturate the orthoplex bound.

Example 2.3.11. In $\mathbb{C}^4$ the following 20 vectors is a collection of 5 MUBs, which would be a Grassmannian Frame.

$$\frac{1}{2}\left[\begin{array}{cccc|cccc|cccc|cccc|cccc}
2 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 2 & 0 & 0 & 1 & 1 & -1 & -1 & -1 & -1 & 1 & 1 & -i & -i & i & i & -i & -i & i & i \\
0 & 0 & 2 & 0 & 1 & -1 & -1 & 1 & -i & i & i & -i & -i & i & i & -i & -1 & 1 & -1 & 1 \\
0 & 0 & 0 & 2 & 1 & -1 & 1 & -1 & -i & i & -i & i & -1 & 1 & -1 & 1 & -i & i & i & -i
\end{array}\right]$$

Notice that by removing the last 3 columns, we are still left with 17 vectors which saturate the orthoplex bound, and so would also be a Grassmannian frame, even through not a collection of MUBs.

[Ian: *talk about the physical meaning of these things. completeness*] [Ian: *"later Wootters and Fields [16] showed that measurements in MUB provide the minimal as well as optimal way of complete specification of the density matrix". i guess look into the wootters and fields paper?*] Now we wish to understand the cases in which collections of MUBs exists and how many MUBs can exist for any particular d. In particular we wish to understand the largest number of MUBs over $\mathbb{F}^d$ for any d and field $\mathbb{F}$.

Definition 2.3.12. $\mathcal{M}_d\mathbb{F}$ will denote the maximum number of MUBs in $\mathbb{F}^d$.

The existence of MUBs, is of particular interest in quantum computing as the existence of complex MUBs provide particularly nice measurement operators called POVMs, which we will discuss in Chapter 5. Therefore we will focus primarily on the case of complex MUBs.

Theorem 2.3.13. *(Theorem 6.1 [MW24]) Let $d = p_1^{k_1} \cdots p_r^{k_r}$ then*

$$\min(p_1^{k_1} + 1, \dots, p_r^{k_r} + 1) \leq \mathcal{M}_d\mathbb{C} \leq d + 1$$

We will prove this in two parts, first we will prove the upper bound for any d, and then second we will provide a construction for $d + 1$ MUBs for when $d = p^k$ is a prime power.

Proof. (upper bound) We will prove the upper bound in Proposition 3.6.2. This result was originally proven in [Ivo81]. □

Proof. ($d = p^k$ construction: Section 4.3 [BBRV02]) The construction provided in [BBRV02] is constructive but relies on the existence of symmetric matrices over finite fields which satisfy determinant conditions. Explicit construct is given when d is prime, or a prime squared. We will give the explicit construction for the case for d being prime and an outline for a proof that it is a maximal collection of MUBs. A construction for the case were d is prime was first shown in [Ivo81].

Fix d a prime and let $e_1, \dots, e_d$ to be the standard basis for $\mathbb{C}^d$. Here we can define X_d to be the translation operator (Pauli X operator) such that $X_d e_j = e_{j+1}$ and $X_d e_d = e_1$, and the modulation operator (Pauli Z) operator Z_d where $Z_d e_j = \omega^j e_j$ where $\omega = e^{2\pi i/d}$ is a primitive dth root of unity. X_d being Hermitian, and Z_d diagonal implies that the operators $Z_d, X_d Z_d^k$ for all $0 \leq k \leq d - 1$ are unitarily diagonlizable: therefore each basis of eigenvectors is an orthonormal basis. It can be shown that because each basis of eigenvectors is different up to a cyclic shift and a phases that they would form a collection of $d + 1$ MUBs. □

The construction in the case where d is prime power, in combination with tensors products gives the lower bound in Theorem 2.3.13.

This construction implies that when $d = p^k$ is a prime power then $\mathcal{M}_d\mathbb{C} = d + 1$. It may be reasonable to ask if this is true in general for all d. And for all composite dimensions, d is a product of distinct prime powers, $d > 6$ this question is entirely unknown. And those reading closely will also know that the smallest composite number is 6. The study of MUBs in $\mathbb{C}^d$ where d is a composite number has been an area of much interest in the quantum computing community; a literature review can be found in [MW24].

It is generally believed that in composite dimensions, that the upper bound of $d + 1$ is not saturated. In fact in the case $d = 6$ it has been conjectured that $\mathcal{M}_6\mathbb{C} = 3$. To shed new insights into this problem in composite dimensions we will look at MUBs over finite fields, a perspective presented by [MST21] which we will expand on in Chapter 3. Before we do we will give many of the well known results in the MUBs literature.

Theorem 2.3.14. *(Theorem 6.2 [MW24]) If $\{B_0, \ldots, B_{d-1}\}$ is a collection of d MUBs in $\mathbb{C}^d$, then there exists a orthonormal basis B_d such that $\{B_1, \ldots, B_d\}$ is a collection of $(d + 1)$ MUBs.*

Proof. If easy ill prove it. But this wont play a significant rule for me, just a useful thing to know. □

There are many equivalent statements of the MUBs problem. In this paper we will focus on one equivalence: finding n MUBs in $\mathbb{C}^d$ is equivalent of finding $n-1$, rank-d MU Hadamard matrices.

Consider a collection of n MUBs in $\mathbb{F}^d$, $B = \begin{bmatrix} B_0 | \cdots | B_{n-1} \end{bmatrix}$. Denote $\hat{B}_j = B_0^{-1}B_j$ and notice that after multiplying by B_0^{-1} we have the matrix $\hat{B} = \begin{bmatrix} \hat{B}_0 | \cdots | \hat{B}_{n-1} \end{bmatrix}$ which is a collection of n MUBs such that $\hat{B}_0 = I_d$. Furthermore considering the inner products between the vectors of $\hat{B}_j$ and $\hat{B}_0$ we can further determine that any entry b of $\hat{B}_j$ for $j > 0$ must satisfy the condition $|b|^2 = d^{-1}$. This gives us the following equivalent condition to the existence of n MUBs, in terms of the existence of Hadamard matrices.

Definition 2.3.15. A $d \times d$ matrix $H = [h_{ij}]$ is called a rank-d **(complex) Hadamard matrix** if $H^*H = dI$ and every entry satisfies $|h_{ij}|^2 = 1$. This means that the entires of H live on the unit circle. A rank-d Hadamard Matrix whose entries are mth roots of unity is called a **Butson-Type Hadamard**, $BH(m,d)$.

Proposition 2.3.16. *A collection of n MUBs $B = \begin{bmatrix} B_0 | \cdots | B_{n-1} \end{bmatrix}$ in $\mathbb{F}^d$ exists if and only if a collection of $n-1$ rank-d Hadamard matrices $\{H_1,\dots,H_{n-1}\}$ exist such that the product $\frac{1}{\sqrt{d}}H_j^\dagger H_k$ is a Hadamard matrix for all $j \neq k$.*

We will delay the proof of this statement until Proposition 3.1.12 once we introduce MUBs in more generality.

Two $d \times d$ Hadamard matrices H and K will therefore be called **Mutually unbiased (MU)** if they satisfy the condition that $\frac{1}{\sqrt{d}}H^\dagger K$ is also a Hadamard matrix. Therefore the existence of n MUBs is equivalent the existence of $n-1$ MU Hadamard matrices. Throughout this paper we will be particularly interested in Butson-Type Hadamards, as their existence, or more specifically their non-existence, often comes down to whether or not there exists a vanishing sum of mth roots of unity as each row is a vanishing sum of d entries.

Theorem 2.3.17. *(Main Theorem in [LL00]) There exists a vanishing sum of n, mth roots of unity if and only if $n \in \mathbb{N}p_1 + \cdots + \mathbb{N}p_r$ where $p_1,\dots,p_r$ are the prime divisors of m.*

This result give immediate consequences on the non-existence of some $BH(m,d)$ Hadamards. In the case where $m = p^k$ is a prime power then a rank-d Hadamard exists only if $p|d$. Furthermore in the case where $m = 2$, the $BH(2,d)$ Hadamard matrices have entires which are ± 1, and are usually referred to as **real Hadamard matrices** or depending on the context just **Hadamard matrices**. The previous result then implies that real Hadamard matrices exist only if $2|d$. However a stronger statement can be made: a real Hadamard matrix exists only if $d = 2$ or $4|d$.

Chapter 3

Frames over Finite Fields

3.1 Foundations Remixed

Although frames over finite fields do not generalize in the sense of optimal packings, or grassmannian frames, they generalize the structure in the classical settings which where known to be optimal packings. Therefore frames over finite fields can play a crucial role in understanding the existence of such objects and their structures. [GIJM22a; GIJM22b] showed a connection between the existence of ETFs in $\mathbb{C}$ or $\mathbb{R}$ with the existence of ETFs in orthogonal and unitary geometries.

Through out this chapter we will be almost exclusively interested in cases O and U as outlined in Section 1.3 which we will recall.

Definition 3.1.1. Case O: $\mathbb{F} = \mathbb{F}_q$ is a finite field of characteristic $p \neq 2$ and V is a d-dimensional vector space over $\mathbb{F}_q$ along with a non-degenerate bilinear form $\langle -, - \rangle$. If $V = F_q^d$ and $\langle u, v \rangle = u^\intercal v$, we say V is in the **real model**.

Case U: $\mathbb{F} = \mathbb{F}_{q^2}$ is a finite field of characteristic $p \neq 2$, along with the field involution $x^\sigma = x^q$, and V is a d-dimensional vector space over $\mathbb{F}_{q^2}$ along with a non-degenerate Hermitian scalar product $\langle -, - \rangle$.

Lemma 1.3.4 gave us an important result on the classification of such geometries.

Lemma 3.1.2. (renumber to be: Lemma 1.3.4, or just have no number) If $\langle -, - \rangle$ is a non-degenerate Hermitian scalar product for V, then there exists a basis $v_1, \ldots, v_d$ where $\langle v_j, v_j \rangle = b_j$, for $b_j \in \mathbb{F}_0^\times$ and all other products between basis elements are zero. Furthermore, in Case U, it can be made so that $b_j = 1$ for all j. And in case O, it can be made so that $b_j = 1$ for all $j < d$ and $b_d = \delta \in \mathbb{F}_0^\times$ is either a square or a non-square.

This told us that in case O, the discriminant which could be either a square or non-square, fully classified the types of geometries we could see. In the real case, this was not the case and the types of geometries were classified by the signature. In Case U there is only one type of geometry up to equivalence, which aligns with what we had seen in the complex case.

Example 3.1.3. [Ian: *move to chapter 1?*] Consider the following two matrices which can be interpreted as the Gram matrices of symmetric scalar products for $\mathbb{F}_3^2$, both of which have trivial discriminant and define equivalent scalar products

$$M = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad N = \begin{bmatrix} 2 & 0 \\ 0 & 2 \end{bmatrix}$$

where $2 \equiv -1 \pmod 3$ is not a square. [Ian: *give the matrix that shows this to be true*]

It is also important to recall that the discriminant was not preserved in subspaces, even when the radical was trivial. These fact will result in surprising differences between the results known in classical frame theory and for frame over finite fields.

Example 3.1.4. Let $V = \mathbb{F}_3^3$, with e_1, e_2, e_3 the standard basis and consider the non-degenerate scalar product defined by the matrix

$$N = \begin{bmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

which has trivial discriminant. Notice that the subspaces spanned by e_1, e_3 is also non-degenerate but the scalar product has non-square discriminant. Finally consider the subspace spanned by $e_1 + e_3, e2$ which is degenerate and so has a non-trivial radical.

Here we continue with the traditional abuse of notation (e.g., in Section 2.1 and in [GIJM22a; GIJM22b; IKM21]): identifying sequences of vectors $\Phi = (\varphi_j)_{j=1}^n \subseteq V$ with their **synthesis operators** $\Phi : \mathbb{F}^n \to V$ defined as $\Phi(x) = \sum_{j=1}^n x_j \varphi_j$. We will always assume any sequence of vectors lives in a finite dimensional vector space V with a non-degenerate Hermitian scalar product, but it may be the case that the scalar product restricted to $\operatorname{im} \Phi \subseteq V$ is degenerate.

The **analysis operator** $\Phi^\dagger : V \to \mathbb{F}^n$ is the adjoint of the synthesis operator Φ, where $\Phi^\dagger x = (\langle \varphi_j, x\rangle)_j$. Its **frame operator** is defined to be $\Phi\Phi^\dagger$ where $x \mapsto \sum_{j=1}^n \langle \varphi_j, x\rangle \varphi_j$ and its **Gram matrix** is $\Phi^\dagger\Phi = [\langle \varphi_j, \varphi_k\rangle]_{jk}$.

We are interested in sequences of vectors which have additional structure. We call a sequence of vectors Φ a **frame** for V if its vectors span V. We then call a frame Φ **non-degenerate** if its frame operator is invertible. If a frame $\Phi : \mathbb{F}^n \to V$ satisfies $\Phi\Phi^\dagger = cI$ for some $c \in \mathbb{F}$, we say Φ is a c**-tight frame**. In the special case when $c = 0$ we call Φ a **totally isotropic tight frame**. These definition are generalization of the results from [Ian: *ref them here*]. Note that all frames in real or complex vector spaces are non-degenerate and none are totally isotropic. [Ian: *Move to earlier on: Geometrically, tightness is a generalization of the Pythagorean theorem, in the sense that when $\Phi\Phi^\dagger = cI$ for any $x \in V$, right multiplication by the frame operator gives $cx = \sum_{j=1}^n \langle \varphi_j, x\rangle \varphi_j$ and so $c\langle x, x\rangle = \sum_{j=1}^n \langle \varphi_j, x\rangle \langle x, \varphi_j\rangle$. This is exactly the Pythagorean theorem when the vectors of Φ are unit norm and an orthogonal basis, in which case $c = 1$.*] The condition for a frame to be tight can be expressed in many different ways, a few of which we highlight below.

Lemma 3.1.5. (Proposition 3.5 [GIJM22a]) Let $\Phi : \mathbb{F}^n \to V$ be a frame, then the following are equivalent:

(i) Φ is a c-tight frame meaning $\Phi\Phi^\dagger = cI$;

(ii) $\Phi\Phi^\dagger\Phi = c\Phi$; and

(iii) $(\Phi^\dagger\Phi)^2 = c\Phi^\dagger\Phi$.

Often in this paper we will consider collections of vectors $\Phi = (\varphi_j)_{j=1}^n \subseteq V$ that do not span the non-isotropic space V in which they live. In these cases we can still consider them to be **frames for their spans**, if $\operatorname{im}\Phi \subseteq V$ is a non-isotropic subspace, meaning the Hermitian form for V is non-degenerate when restricted to $\operatorname{im}\Phi$. The following lemmas can help characterize this situation.

Lemma 3.1.6. (Proposition 3.11 [GIJM22a]) If Φ is a frame then $\ker \Phi^\dagger\Phi = \ker\Phi$ and $\operatorname{im}\Phi^\dagger\Phi = \operatorname{im}\Phi^\dagger$

Lemma 3.1.7. Let $\Phi : \mathbb{F}^n \to V$ be the synthesis operator for a collection of vectors. Then $\operatorname{rank}(\Phi^\dagger\Phi) = \operatorname{rank}(\Phi)$ if and only if $\operatorname{im}\Phi$ is non-isotropic, i.e., $\Phi : \mathbb{F}^n \to \operatorname{im}\Phi$ is a frame.

Proof. The backwards direction follows from Lemma 3.1.6.

For the other direction, assume that $\operatorname{rank}(\Phi^\dagger\Phi) = \operatorname{rank}(\Phi) = \dim(\operatorname{im}\Phi)$. This then means $\ker(\Phi^\dagger\Phi) = \ker(\Phi)$. We will show that $\operatorname{rad}\operatorname{im}(\Phi) = \{u \in \operatorname{im}(\Phi) | \langle u, v\rangle = 0 \text{ for all } v \in \operatorname{im}(\Phi)\} = \{0\}$

Let $u \in \operatorname{rad}\operatorname{im}(\Phi) \subseteq \operatorname{im}(\Phi)$. We can then write $u = \Phi x$ in which case $\Phi^\dagger\Phi x = 0$, and then since $\ker(\Phi^\dagger\Phi) = \ker(\Phi)$, $x \in \ker\Phi$, i.e., $u = 0$. □

Lemma 3.1.8. (Corollary 3.9 of [GIJM22a]) Φ is a totally isotropic tight frame if and only if $\operatorname{im}\Phi^\dagger$ is a totally isotropic subspace of $\mathbb{F}^n$. Furthermore if V is a d-dimensional non-isotropic space then V admits a 0-tight frame with n vectors only if $n \geq 2d$.

As described through out Chapter 2, frames provided and algebraic setting for studying the geometry of systems of lines, that is packings in projective space. In the real and complex setting it was often advantageous to represent a line through the origin by a vector, specifically by a unit vector. But this is often not possible in finite fields, due to the lack of square roots, making it difficult to scale vectors. Instead we will often work with the generalization of equal-norm vectors (allowing zero for the "norm") where we refer to the **magnitude** or **norm** of a vector φ as $\langle\varphi, \varphi\rangle$. But even this is not always possible for any given system of lines.

In general for a system of lines $\Phi = (\varphi_j)_{j=1}^n \in V$, if $\frac{\langle\varphi_1,\varphi_1\rangle}{\langle\varphi_j,\varphi_j\rangle}$ is a square for every vector $\varphi_j \in \Phi$ (i.e. there exists some non-zero α_j such that $\frac{\langle\varphi_1,\varphi_1\rangle}{\langle\varphi_j,\varphi_j\rangle} = \alpha_j\alpha_j^\sigma$) then we could rescale each vector to get a equal norm system of vectors $\{\alpha_j\varphi_j\}_{j=1}^n$ who all share the common magnitude equal to the magnitude of φ_1. Furthermore to rescale an equal norm system of vectors $\Phi = (\varphi_j) \in V$ with vectors of magnitude $a \neq 0$ to vectors of unit norm, it would need to be the case that $a = \alpha\alpha^\sigma$ for some non-zero α, in which case $\left\{\frac{1}{\alpha}\varphi_j\right\}_{j=1}^n$ would be a unit norm system of vectors. We note, however, that a may often be 0, and so scaling a is frequently not possible.

To study systems of lines, specifically the "distances" between lines induced by the scalar products, we can limit ourselves to looking at equal norm systems of lines which satisfy a condition analogous to that of the modulus squared of the inner product of two unit vectors.

Definition 3.1.9. Given $a, b \in \mathbb{F}_0$ we say $\Phi = (\varphi_j)_{j=1}^n \subseteq V$ is an (a, b)**-equiangular system** in V if the following two conditions hold.

(i) $\langle \varphi_j, \varphi_j \rangle = a$ for all j

(ii) $\langle \varphi_j, \varphi_k \rangle \langle \varphi_k, \varphi_j \rangle = b$ for all $j \neq k$

Instead of scaling by a it is often the case that $b \neq 0$; so, we may want to scale a system of lines such that $b = 1$. Let $\Phi = (\varphi_j)_{j=1}^n$ be an (a, b)-equiangular system of lines. If there exists a non-zero $\alpha \in \mathbb{F}$ such that $b = \frac{1}{(\alpha\alpha^\sigma)^2}$ then $\{\alpha\varphi_j\}_{j=1}^n$ would be an $(\alpha\alpha^\sigma a, 1)$-equiangular system of lines.

Definition 3.1.10. Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of vectors in a d-dimensional non-isotropic space V. We call Φ an (a, b, c)**-equiangular tight frame**, or an (a, b, c)**-ETF** for V if (i) Φ is a (a, b)-equiangular system of vectors and (ii) Φ is an c-tight frame for V.

We can also define MUBs over finite fields: assuming $\operatorname{char} \mathbb{F} \nmid d$ we will say two vectors u, v are **mutually unbiased (MU)** if

$$\mu^2(u, v) = \frac{\langle u, v \rangle \langle v, u \rangle}{\langle u, u \rangle \langle v, v \rangle} = d^{-1}.$$

This requires that the vectors themselves have non-zero norm in which case we will scale u and v to be unit norm, meaning $\langle u, u \rangle = 1 = \langle v, v \rangle$. Furthermore if B and B' are orthonormal bases, meaning $\langle u, u \rangle = 1$ for all $u \in B$ and $\langle u, v \rangle = 0$ for all $u \neq v$ in B (and likewise for B'), then B and B' are called **mutually unbiased (MU)** if $\langle u, v \rangle \langle v, u \rangle = d^{-1}$ for all $u \in B$ and $v \in B'$. A collection of n orthonormal basis which are pairwise MU are then called a collection of n **Mutually Unbiased Bases (MUBs)** for $\mathbb{F}^d$. Just as in the case for inner product spaces, we will write a collection of n MUBs in $\mathbb{F}_q^d$, as a matrix $B = \begin{bmatrix} B_0 | \cdots | B_{n-1} \end{bmatrix}$ where the columns of each

B_j form an orthonormal basis. Just as before $\mathcal{M}_d\mathbb{F}$ will denote the maximum number of MUBs in $\mathbb{F}^d$.

Definition 3.1.11. Fix a field $\mathbb{F}$ with involution σ and consider $V = \mathbb{F}^d$ to be a unitary space. A $d \times d$ matrix $H = [h_{ij}]$ is a rank-d **Hadamard matrix** if $H^\dagger H = dI$ and every entry satisfies $h_{ij}^\sigma h_{ij} = 1$. A rank-d Hadamard Matrix whose entries are mth roots of unity is called a **Butson-Type Hadamard**, $BH(m, d)$.

Over the finite field $\mathbb{F}_{q^2}$ the condition $x^\sigma x = x^{q+1} = 1$, meaning every rank-d Hadamard is Butson-Type $BH(q + 1, d)$ Hadamard.

Proposition 3.1.12. *Let $\mathbb{F} = F_{q^2}$ and let $V = \mathbb{F}^d$ be in the complex model. Fix α such that $\alpha^\sigma\alpha = d$. A collection of n MUBs $B = \left[B_0|\cdots|B_{n-1}\right]$ in $\mathbb{F}_{q^2}^d$ exists if and only if a collection of $n-1$ rank-d Hadamard matrices $\{H_1, \ldots, H_{n-1}\}$ exist such that the product $\alpha^{-1}H_j^\dagger H_k$ is a Hadamard matrix for all $j \neq k$.*

Proof. Let $B = \left[B_0|\cdots|B_{n-1}\right]$ be a collection of n MUBs in $\mathbb{F}_{q^2}^d$. Because B_0 is a unitary, we can multiply by its inverse $B_0^{-1} = B_0^\dagger$ to get that $\hat{B} = B_0^\dagger B = \left[I_d|B_0^\dagger B_1|\cdots|B_0^\dagger B_{n-1}\right]$, which is also a collection of n MUBs. Let α be a root of $x^{q+1} - d$, and notice that $H_j := \alpha B_0^\dagger B_j$ is a hadamard matrix, because $H_j^\dagger H_j = \alpha^\sigma B_j^\dagger B_0 \alpha B_0^\dagger B_j = dI$ and looking at the scalar product between the columns of $H_0 = \alpha I$ and H_j give that the entires of each H_j has magnitude 1 for all $j > 0$. Likewise for $j \neq k$ we have that $B_j^\dagger B_k$ must have entires which have magnitude d^{-1}. Likewise $(B_j^\dagger B_k)^\dagger(B_j^\dagger B_k) = I$. This also means that $\alpha^{-1}H_j^\dagger H_k = \alpha^{-1}\alpha^\sigma B_j^\dagger B_0 \alpha B_0^\dagger B_k = \alpha^\sigma B_j^\dagger B_k$, and so $(\alpha^{-1}H_j^\dagger H_k)^\dagger(\alpha^{-1}H_j^\dagger H_k) = \alpha B_k^\dagger B_j \alpha^\sigma B_j^\dagger B_k = dI$

For the other direction, consider a collection of hadamard matrices $\{H_1, \ldots, H_{n-1}\}$, which satisfy the given property. Notice that $B = \left[I|\alpha^{-1}H_1 \cdots |\alpha^{-1}H_{n-1}\right]$ is a collection of n MUBs. □

Just as in the classical setting, a collection of n MUBs for $\mathbb{F}^d$ is a $(1, n)$-equal norm tight frame.

3.2 Back to Reality

Before we continue the study of frames over finite fields we wish to draw connections between the existence of frames over $\mathbb{C}$ and $\mathbb{R}$ to frames over finite fields. The main results here are the result from Section 7 of [GIJM22a] that show that ETFs are defined by polynomial equation and therefore define semi-algebraic sets. Two number theoretic results are then used to show the existence of ETFs over $\mathbb{C}$ with algebraic entires, which are then used to construct ETFs in finite fields. Before we present these result, we will give a brief overview of the number theory necessary, which will also use through out this chapter.

As a slight, but insignificant, abuse of notation we will consider integers as elements of any field $\mathbb{F}$: we consider an action $\cdot : \mathbb{Z} \times \mathbb{F} \to \mathbb{F}$ where $n \cdot r = r + \cdots + r$ added n-times, which defines a ring homomorphism $\mathbb{Z} \to \mathbb{F}$ by $n \mapsto (n \cdot 1)$. More generally we can consider a ring of algebraic integers $R \subseteq \overline{\mathbb{Q}}$ to be contained in our field, by considering a nontrivial ring homomorphism $\pi : R \to \mathbb{F}$ as defining an action on $\mathbb{F}$. For example, let $\mathbb{F}_{25} = \mathbb{F}_5[x]/(x^2 - 3) = \mathbb{F}_5(\alpha)$, where $\alpha^2 = 3$. We can consider the ring of algebraic integers $R = \mathbb{Z}[\sqrt{3}]$ and the map $\pi : R \to \mathbb{F}_{25}$ by $\sqrt{3} \mapsto \alpha$. We will often conflate algebraic integers, as elements of $\mathbb{C}$, with their images in $\mathbb{F}$. We will use $\equiv$ to represent equality in the image of π if it not clear from context, or $\equiv_p$ if $\mathbb{F} = \mathbb{F}_{p^\ell}$ is a finite field. Often the notion of equality will be clear from context, and will will use $=$. If M is a matrix with entries in R, a ring of algebraic integers, we will consider $\overline{M}$ to be the point-wise image of M under π. For $m \in R$ where $\pi(m) \neq 0$ we can also consider the action of elements from the field of fractions of R as $\frac{n}{m} \mapsto \pi(n)\pi(m)^{-1}$.

Case U

First we will consider the specific implication related to case U. Throughout we will consider a d-dimensional non-degenerate space V over a finite field $\mathbb{F}_{q^2}$. There exists a basis of V such that the Gram matrix associated with the Hermitian scalar product is the identity matrix. Therefore we can always assume, by choosing such a basis $e_1, \ldots, e_d$ that $\langle u, v \rangle = u^* v$ and we my identify $V \cong \mathbb{F}_{q^2}^d$ under this choice of basis: V will always be in the complex model.

Recall from Remark 1.3.2 that $\mathbb{F}_{q^2}$ contains all of the roots of $x^\sigma x - a = x^{q+1} - a$ where $a \in F_0^\times$.

Definition 3.2.1. A (real) **integral semialgebraic set** is a subset of $\mathbb{R}^n$ generated by sets of the form $\{x \in \mathbb{R}^n : f(x) \geq 0\}$ where $f(x) \in \mathbb{Z}[x_1, \dots, x_n]$.

Many frame theoretic objects form closed integral semialgebraic sets.

Lemma 3.2.2. The set of all ETF of n vectors in $\mathbb{C}^d$ forms a (real) integral semialgebraic set. Likewise the set of all collections of n MUBs in $\mathbb{C}^d$ forms a (real) integral semialgebraic set

Proof. I will hold off on this. □

Lemma 3.2.3. If S is a nonempty closed integral semialgebraic set, S contains a element whose entries are real algebraic numbers.

Proof. prove this? or no □

This tells us that the existence of n MUBs in $\mathbb{C}^d$ further implies that there are n MUBs in $\mathbb{C}^d$ with algebraic numbers, and likewise that there exists an ETF of n vectors in $\mathbb{C}^d$ with algebraic entries when ever an ETF exists with complex entries. To prove the penultimate theorems, we need to following lemma.

Lemma 3.2.4. (finite field paper) Let E be a Galois number field. Given $z_1, \dots, z_n \in \mathcal{O}_E$ there exists infinity many ideals $\mathfrak{p} \subset \mathcal{O}_E$ which satisfy the following conditions

(i) $\mathcal{O}_E/\mathfrak{p}$ is a finite field

(ii) $\mathfrak{p}$ is closed under complex conjugation

(iii) $\mathfrak{p}$ does not contain $z_1, \dots, z_n$.

Furthermore

$$|\{\mathcal{O}_E/\mathfrak{p} : \mathfrak{p} \subset \mathcal{O}_E \text{ is an ideal satisfying (i)-(iii)}\}|$$

is infinite.

Proof. prove this too? □

Next we will prove the main result in the case of complex MUBs, and nearly identical proof can be used for ETFs, a proof of which can be found in Theorem 7.5 of [GIJM22a]

Theorem 3.2.5. *If $B \in \mathbb{C}^{nd\times d}$ is a collection of n MUBs in $\mathbb{C}^d$ with entires in E, a Galois number field, then for infinity many pairwise coprime q, when $d \nmid q$ there exists some non-zero $a \in \mathcal{O}_E$ and a $*$-homomorphism $f : \mathcal{O}_E \to \mathbb{F}_{q^2}$ such that $a^{-1}f(aB)$ forms n MUBs in $\mathbb{F}_{q^2}^d$ in the complex model.*

Proof. Let $a \in \mathcal{O}_E$ such that aB is a matrix whose entires are algebraic integers.

Select an ideal $\mathfrak{p}$, of which there are infinity many, such that $a, d \notin \mathfrak{p}$. From a lemma above, we know that $\mathcal{O}_E/\mathfrak{p}$ is a finite field, and becasue $\mathfrak{p}$ does not contain a nor d, by a slight abuse of notation both a and d are invertible in $\mathcal{O}_E/\mathfrak{p}$ for every choice of $\mathfrak{p}$.

Consider the finite field $K = \mathcal{O}_E/\mathfrak{p}$ and let $\pi_K : \mathcal{O}_E \to K$ be its corresponding projection map. Since $\mathfrak{p}$ is closed under conjugation there is a well defined involution $(-)^\sigma : K \to K$ such that $\pi_K(x)^\sigma = \pi_K(\overline{x})$. We will write $a^{-1}\pi_K(aB) = \left[a^{-1}\pi_K(aB_1)|\cdots|a^{-1}\pi_K(aB_n)\right]$, and we can verify that

$$(a^{-1}\pi_K(aB_j))^* a^{-1}\pi_K(aB_j) = I \neq 0$$

and likewise

$$((a^{-1}\pi_K(aB_\ell))^* a^{-1}\pi_K(aB_k))_{ij}((a^{-1}\pi_K(aB_k))^* a^{-1}\pi_K(aB_\ell))_{ji} = d^{-1}.$$

Therefore $a^{-1}\pi_K(aB)$ is a collection of n MUBs over K^d. □

Finally this given us our main result for the section.

Theorem 3.2.6. *If $B \in \mathbb{C}^{nd\times d}$ is a collection of n MUBs in $\mathbb{C}^d$ then there exists n MUBs in $\mathbb{F}_{q^2}^d$ in the complex model for infinity many pairwise coprime q.*

Proof. Consider $B \in \mathbb{C}^{nd\times d}$ a collection of n MUBs in $\mathbb{C}^d$, this implies we may assume B has algebraic entires, meaning the result follows from the penultimate theorem. □

Theorem 3.2.7. *(Theorem 7.1 [GIJM22a]) If $\Phi \in \mathbb{C}^{n\times d}$ is a ETF of n vectors in $\mathbb{C}^d$ then there exists an ETF of n vectors in $\mathbb{F}_{q^2}^d$ in the complex model for infinity many pairwise coprime q.*

This results above provides a new framework for tackling open problems related to ETFs and MUBs. For example Zauner's MUB conjecture in $\mathbb{C}^6$.

Conjecture 3.2.8. In $\mathbb{C}^6$ there does exists more then 3 MUBs.

We can now state an equivalent conjecture using the contrapositive of this sections main theorem.

Conjecture 3.2.9. There are at most finitly many coprime q where $\mathbb{F}_{q^2}^6$ has more then 3 MUBs.

Case O

Although the results above can be directly used to give the same results in the case O setting, stronger results exist for real ETFS. In [GIJM22b] the authors showed that the existence of real ETFs imply the existence of ETFs in orthogonal geometries and showed the converse is also true when the characteristic is sufficiently large. To show this we will need the following result

Proposition 3.2.10. *(Proposition 3.1 [GIJM22b]) Let M be an $n \times n$ matrix with entires in a ring of algebraic integers R which also contains all the eigenvalues of M. Then*

(a) $\operatorname{rank}(\bar{M}) \leq \operatorname{rank}(M)$ with equality when M is diagonalizable and for every non-zero eigenvalue λ of M, that $\bar{\lambda} \neq 0$.

(b) Furthermore if M is nonzero with integer entries, symmetric, singular, and each row sums to λ_0, such that the corresponding eigenspace is 1-dimensional. Consider the minimal polynomial $m_M(x) = (x - \lambda_0)h(x)$ and set $\epsilon = 1$ if $h(\bar{M}) = 0$ and $\epsilon = 0$ otherwise. If every non-zero eigenvalue $\lambda \neq \lambda_0$, $\bar{\lambda} \neq 0$ then $\operatorname{rank}(\bar{M}) = \operatorname{rank}(M) - \epsilon$.

Proof. [Ian: *idk probably should prove this*] □

Theorem 3.2.11. *(Proposition 3.2 [GIJM22b]) Suppose $G = S + aI$ is the Gram matrix of some real $d \times n$ ETF Φ, where $S \in \mathbb{Z}^{n\times n}$ is the signature matrix. Fix a finite field $\mathbb{F}_q$, where $q = p^\ell$ is an odd prime power, with $\delta^2 = n - 1$ if $n = 2d$. Then with*

$$a \equiv \begin{cases} \sqrt{\frac{d(n-1)}{n-d}} & n \neq 2d \\ \delta & n = 2d \end{cases} \quad \textit{and} \quad c \equiv \begin{cases} \sqrt{\frac{n^2(n-1)}{d(n-d)}} & n \neq 2d \\ 2\delta & n = 2d \end{cases}$$

the matrix $\bar{G} = \bar{S} + aI$ is the Gram matrix of an $(a, 1, c)$-ETF Ψ in an orthogonal geometry on $\mathbb{F}_q^{d'}$ where $d' \leq d$, with equality when $c \neq 0$.

[Ian: Keep or move to simplex section or just comment? Furthermore, if $a \neq 0$, $c \neq 0$, and there is a collection $\kappa \subseteq [n]$ of where $\Phi|_\kappa$ forms a regular s-simplex of then $\Psi|_\kappa$ is a regular s-simplex*]*

Proof. [Ian: *need to proof read this again as it has been a while since i worked through this*] Assume $n \neq 2d$ and in which case let $G = S + \hat{a}I$ be the Gram of a $d \times n$ real ETF Φ with frame constant $\hat{c}$. In which case g is a square matrix with ± 1 off the diagonal and $\hat{a} = \sqrt{\frac{d(n-1)}{n-d}}$ on the diagonal. The spectrum of G is d copies of $\hat{c} = \frac{n}{d}\sqrt{\frac{d(n-1)}{n-d}}$ and $n-d$ copies of 0. This is because the non-zero eigen values of $G = \Phi^\dagger\Phi$ and $\Phi\Phi^\dagger$ are equal. The Seidel adjacency matrix, or signature matrix, $S = G - \hat{a}I$ has 0 on diag and ± 1 on the off diag. This means that the characteristic polynomial, must be monic.S has as its spectrum d copies of $\sqrt{\frac{(n-d)(n-1)}{d}} = \hat{c} - \hat{a}$ and $n-d$ copies of $-\sqrt{\frac{d(n-1)}{(n-d)}} = -\hat{a}$. Because these are the roots of a monic characteristic polynomial they must be algebraic integers, meaning they are wither integers or irrational. Recall that irrational roots of a polynomials come in $\pm$ pairs. This means if the $n - d$ copies of $-\sqrt{\frac{d(n-1)}{(n-d)}}$ were irrational then there would need to exist $n - d$ copies of the positive root, meaning $n - d = d$, but by assumption this is not the case. This therefore means that $\hat{a} = \sqrt{\frac{d(n-1)}{(n-d)}}$ and $\hat{c} - a = \sqrt{\frac{(n-d)(n-1)}{d}}$ are integer and likewise $\hat{c} = \frac{n}{d}\hat{a}$ is an integer as well. This means that G has integer entries.

Not looking at the Gram matrix over $\mathbb{F}_q$ we can see that $\bar{G}$ not only satisfies $\bar{G}^2 = c\bar{G}$ but has entries in $\mathbb{F}_p$, the base field. If $\hat{c} \not\equiv 0$ then $\operatorname{rank}(G) = d$, which follows from Proposition 3.2.10(b).

By Proposition 3.4.5 we have that G is the Gram matrix of a $(a, 1, c)$-ETF Ψ of n vectors in $\mathbb{F}_p^d$ with $a \equiv \hat{a}$ and $c \equiv \hat{c}$.

[Ian: *Need to proove $n = 2d$ case*]

For the last claim, we know that that for if Φ contains a regular s-simplex, with index set κ, that $a = s$, $|\kappa| = \sqrt{\frac{d(n-1)}{n-d}} + 1$ and $\Delta(\varphi_j, \varphi_k, \varphi_\ell) = -1$ for all distinct $j, k, \ell \in \kappa$. Furthermore we also know that

$$\sum_{j \in \kappa} \Delta(\varphi_\ell, \varphi_k, \varphi_j) = s + 1$$

for a fixed $\ell \in \kappa$ and all $k \notin \kappa$. Notice that all of these are preserved when mapped to $\mathbb{F}_q$. That is $\Delta(\psi_j, \psi_k, \psi_\ell) \equiv_p \Delta(\varphi_j, \varphi_k, \varphi_\ell) = -1 = -\left(\frac{a}{s}\right)^3$ for all distinct $j, k, \ell \in \kappa$ because $a \equiv_p s$. And likewise

$$\sum_{j \in \kappa} \Delta(\psi_\ell, \psi_k, \psi_j) \equiv_p \sum_{j \in \kappa} \Delta(\varphi_\ell, \varphi_k, \varphi_j) = s + 1 = \frac{s+1}{s} ab$$

for the same fixed $\ell \in \kappa$ and all $k \notin \kappa$. Finally because $a^2 = s^2 b$ and $\frac{a}{s} = 1$ we know that Φ_κ is a regular simplex. [Ian: *I need to verfiy the discriminant of the simplex too. But i suspect it will work out. im not sure how to show it atm.*] □

Theorem 3.2.12. *(Proposition 3.3 [GIJM22b]) If there exists an ETF of n vectors in a d-dimensional orthogonal geometry over $\mathbb{F}_q$ where $q = p^\ell$ is odd and $p > 2n - 5$ then there exists a real ETF of n vectors for $\mathbb{R}^d$ with the same n and d.*

The requirement that $p > 2n - 5$ is not known to be tight. [Ian: *There are some interesting examples in connections-to-reality.tex which i should add at some point, and better develope.*]

The authors are unaware of any similar results for real MUBs. [Ian: *future research Q: MUBS in case O, can this then be used to spit out results about the existance of real MUBS?*]

3.3 Structural Similarities

Switching Equivalence

In studying frames it is helpful to create a notion of equivalence. More generally we will introduce a notion of equivalence for systems of lines, inspired by the switching equivalence of graphs [VS66].

Definition 3.3.1. Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ where V is a non-isotropic d-dimensional space. We say that Φ and Ψ are **unitarily equivalent** if there exists a unitary $U : V \to V$ such that $\Psi = U\Phi$.

More generally, we say that Φ and Ψ are **switching equivalent** if there exists a unitary $U : V \to V$ and diagonal matrix $T = \operatorname{diag}(t_1, \dots, t_n) \in \mathbb{F}^{n\times n}$ with entries satisfying $t_i t_i^\sigma = 1$ such that $\Psi = U\Phi T$.

The notion of switching equivalence may also be referred to as projective unitary equivalence [CW16]. Both unitary equivalence and switching equivalence are equivalence relations which—as we will see in this section—preserve much of the underlying information of systems of lines.

The following result is related to Proposition 3.12 of [GIJM22a], which concerned a sort of scaled unitary equivalence of frames; here, we consider unitary equivalence of any collections of vectors, including frames for their spans.

Lemma 3.3.2. Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ where V is a d-dimensional non-isotropic space. Φ and Ψ are unitarily equivalent if and only if $\Psi^\dagger\Psi = \Phi^\dagger\Phi$ and $\ker(\Phi) = \ker(\Psi)$.

Proof. For the forward direction assume that Φ and Ψ are unitarily equivalent. In which case there exists an isometry U such that $\Psi = U\Phi$ and so $\Psi^\dagger\Psi = \Phi^\dagger U^\dagger U\Phi = \Phi^\dagger\Phi$. And because U is an isometry $\ker(\Phi) = \ker(\Psi)$.

For the other direction assume that $\Psi^\dagger\Psi = \Phi^\dagger\Phi$ and $\ker(\Phi) = \ker(\Psi)$. We will construct an invertible linear map $A : \operatorname{im}\Phi \to \operatorname{im}\Psi$ such that $\Psi x = A(\Phi x)$ for any $x \in \mathbb{F}^n$. First we will show that this map is well defined on $\operatorname{im}\Phi$. Let $\Phi x = \Phi y$, meaning $x - y \in \ker(\Phi)$, and notice that because $\ker\Phi = \ker\Psi$ we have that $x - y \in \ker(\Psi)$ and so $A\Phi x = A\Phi y$. So A is a well-defined linear map on the images. $A^{-1} : \operatorname{im}\Psi \to \operatorname{im}\Phi$ can be constructed in a similar fashion $A^{-1}(\Psi x) = \Phi x$. Notice also that because $\Psi^\dagger\Psi = \Phi^\dagger\Phi$, the isomorphism A satisfies $\langle A\Phi x, A\Phi y\rangle = \langle \Psi x, \Psi y\rangle = \langle \Phi x, \Phi y\rangle$ and so $\operatorname{im}\Phi$ and $\operatorname{im}\Psi$ are isometrically equivalent. By Witt's Extension theorem (see, e.g., [Jac53]), we know that A extends to an unitary transformation $U : V \to V$ such that $\Psi = U\Phi$. □

In the case where Φ and Ψ are frames then $\Psi^\dagger\Psi = \Phi^\dagger\Phi$ implies $\ker(\Phi) = \ker(\Psi)$ in which case $U : V \to V$ is uniquely determined on all of V.

Finally, we note that from Lemma 3.1.7 the condition of $\operatorname{rank}(\Phi) = \operatorname{rank}(\Psi) = \operatorname{rank}(\Phi^\dagger\Phi)$ and $\Psi^\dagger\Psi = \Phi^\dagger\Phi$ implies unitary equivalence.

All of the above results for unitary equivalence may be reformulated for switching equivalence.

Lemma 3.3.3. Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ where V is a d-dimensional non-isotropic space. Φ and Ψ are switching equivalent if and only if $\Psi^\dagger\Psi = T^\dagger\Phi^\dagger\Phi T$ where $T = \operatorname{diag}(t_1, \dots, t_n)$ is a diagonal matrix with $t_i t_i^\sigma = 1$ and $\ker(\Phi T) = \ker(\Psi)$.

Proof. For the forward direction assume that Φ and Ψ are switching equivalent. In that case there exists an isometry U and a diagonal matrix $T = \operatorname{diag}(t_1, \dots, t_n)$ with entries satisfying $t_i t_i^\sigma = 1$ such that $\Psi = U\Phi T$ meaning Ψ and ΦT are unitarily equivalent so $\Psi^\dagger\Psi = T^\dagger\Phi^\dagger U^\dagger U\Phi T = T^\dagger\Phi^\dagger\Phi T$ and $\ker(\Phi T) = \ker(\Psi)$. For the backwards direction assume $\Psi^\dagger\Psi = T^\dagger\Phi^\dagger\Phi T$ and $\ker(\Phi T) = \ker(\Psi)$. Then $\Psi^\dagger\Psi = (\Phi T)^\dagger\Phi T$, so by Lemma 3.3.2, there exists a isometry such that $\Psi = U\Phi T$. □

Corollary 3.3.4. *Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ where V is a d-dimensional non-isotropic space. Φ and Ψ are unitarily equivalent if $\Psi^\dagger\Psi = \Phi^\dagger\Phi$ and $\operatorname{rank}(\Phi) = \operatorname{rank}(\Psi) = \operatorname{rank}(\Phi^\dagger\Phi)$.*

Likewise Φ and Ψ are switching equivalent if $\Psi^\dagger\Psi = T^\dagger\Phi^\dagger\Phi T$ where $T = \operatorname{diag}(t_1, \dots, t_n)$ with $t_i t_i^\sigma = 1$ and $\operatorname{rank}(\Phi) = \operatorname{rank}(\Psi) = \operatorname{rank}(\Phi^\dagger\Phi)$

Proof. The second statement implies the first when $T = I$; so, we will only show the second. Assume that $\Psi^\dagger\Psi = T^\dagger\Phi^\dagger\Phi T$ and $\operatorname{rank}(\Phi) = \operatorname{rank}(\Psi) = \operatorname{rank}(\Phi^\dagger\Phi)$. Multiplication by T does not change the rank so this implies that $\ker(\Phi T) = \ker(T^\dagger \Phi^\dagger \Phi T) = \ker(\Psi)$ because of the original assumptions and that $\ker(\Phi T) \subseteq \ker(T^\dagger \Phi^\dagger \Phi T)$ and $\ker(\Psi) \subseteq \ker(\Psi^\dagger \Psi)$. And so the corollary follows from Lemma 3.3.2. □

Example 3.3.5 shows the necessity of equal ranks for Φ and Ψ in Corollary 3.3.4.

Example 3.3.5. Consider the following matrices which represent collections of vectors in $\mathbb{F}_3^4$ with the standard dot product

$$\Phi = \begin{bmatrix} 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{bmatrix} \text{ and } \Psi = \begin{bmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 1 & 0 \end{bmatrix}$$

Notice that Φ and Ψ have differing ranks and so are not unitarily equivalent. However both have the same Gram matrix

$$G = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

Furthermore Φ is unitarily equivalent to itself but $\operatorname{rank}(\Phi) \neq \operatorname{rank}(\Phi^\dagger \Phi)$.

In the complex case switching equivalence can be determined by the m-products of a system of lines, and in special cases by the triple products. We would like to generalize those results here.

Definition 3.3.6. Let $\Phi = (\varphi_j)_{j=1}^n \subseteq V$ where V is a d-dimensional non-isotropic space. An m**-product** or m**-vertex Bargmann invariant** is defined as

$$\Delta(\varphi_{j_1}, \ldots, \varphi_{j_m}) = \langle \varphi_{j_1}, \varphi_{j_2} \rangle \langle \varphi_{j_2}, \varphi_{j_3} \rangle \ldots \langle \varphi_{j_m}, \varphi_{j_1} \rangle .$$

When $m = 2$, these are called **double products**, and when $m = 3$, these are called **triple products**.

Many authors such as [GP77; BE98; AFF11; CW16; FJKM18; Wal20] have independently studied the structural importance of m-products for characterizing line packings in $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{H}$. In this section we wish to generalize some of these results to finite fields.

Lemma 3.3.7. Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ where V is a d-dimensional non-isotropic space. If Φ and Ψ are switching equivalent, then their m-products are all equal.

Proof. Since Φ and Ψ are switching equivalent, there exists a unitary $U : V \to V$ and $T = \operatorname{diag}(t_1, \ldots, t_n)$ with $t_i t_i^\sigma = 1$ such that $\psi_j = t_j U \varphi_j$ for all $j \in [n]$ Thus for any $\{j_1, \ldots, j_m\} \subseteq [n]$

$$\begin{aligned}
\Delta(\psi_{j_1}, \ldots, \psi_{j_m}) &= \langle \psi_{j_1}, \psi_{j_2} \rangle \langle \psi_{j_2}, \psi_{j_3} \rangle \ldots \langle \psi_{j_m}, \psi_{j_1} \rangle \\
&= \langle t_1 U\varphi_{j_1}, t_2 U\varphi_{j_2} \rangle \langle t_2 U\varphi_{j_2}, t_3 U\varphi_{j_3} \rangle \ldots \langle t_m U\varphi_{j_m}, t_1 U\varphi_{j_1} \rangle \\
&= t_1^\sigma t_2 t_2^\sigma t_3 \ldots t_m^\sigma t_1 \langle U\varphi_{j_1}, U\varphi_{j_2} \rangle \langle U\varphi_{j_2}, U\varphi_{j_3} \rangle \ldots \langle U\varphi_{j_m}, U\varphi_{j_1} \rangle \\
&= \langle U\varphi_{j_1}, U\varphi_{j_2} \rangle \langle U\varphi_{j_2}, U\varphi_{j_3} \rangle \ldots \langle U\varphi_{j_m}, U\varphi_{j_1} \rangle \\
&= \langle \varphi_{j_1}, \varphi_{j_2} \rangle \langle \varphi_{j_2}, \varphi_{j_3} \rangle \ldots \langle \varphi_{j_m}, \varphi_{j_1} \rangle \\
&= \Delta(\varphi_{j_1}, \ldots, \varphi_{j_m}).
\end{aligned}$$

□

For the remainder of this section we will assume any field $\mathbb{F} = \mathbb{F}_q$ is a finite field of case U or O where q is odd. For case U, we have $\mathbb{F} = \mathbb{F}_{q^2}$ with the field involution $a^\sigma = a^q$, and in Case O, $\mathbb{F} = \mathbb{F}_q$ with field involution $a^\sigma = a$. Because q is odd, in both cases for any element $aa^\sigma \in \mathbb{F}^\times$, we have that there exists some γ such that $\gamma^2 = aa^\sigma$. This follows immediately when σ is trivial, and for case U, notice that we may choose $\gamma = a^{(q+1)/2}$. With this observation we can define a non-unique square root function $\sqrt{-} : \mathbb{F}_q^{\times 2} \to \mathbb{F}_q$ such that $\left(\sqrt{a}\right)^2 = a$, and we will assume the choice of such a function is fixed throughout, making the following definition well-defined in Case O or U, with odd characteristic.

Definition 3.3.8. Let $\Phi = (\varphi_j)_{j=1}^n \subseteq V$ where V is a d-dimensional non-isotropic space. If $\Delta(\varphi_j, \varphi_k) \neq 0$, define the **exponential gauge** of φ_j and φ_k, denoted $\eta_{j,k}$, as

$$\eta_{j,k} = \frac{\langle \varphi_j, \varphi_k \rangle}{\sqrt{\Delta(\varphi_j, \varphi_k)}}.$$

Otherwise, set $\eta_{j,k} = 0$.

Note that over $\mathbb{C}$, $\sqrt{\Delta(\varphi_j, \varphi_k)}$ would be the modulus of the inner product of the vectors and thus $\eta_{j,k}$ would be the signum of the inner product, which is the complex exponent of the gauge, except when the inner product is zero [AFF11]. In case O we note that $\eta_{j,k} = 1$ for all j, k, and in general $\eta_{j,k}\eta_{k,j} = 1$

The following generalizes Lemma 2.1 of [CW16].

Proposition 3.3.9. *Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ be frames for V, a d-dimensional non-isotropic space. For each $j \neq k$, let $\eta_{j,k,\varphi}$ be the exponential gauges of Φ and $\eta_{j,k,\psi}$ the exponential gauges of Ψ. Then Φ and Ψ are switching equivalent if and only if the following two conditions hold:*

(i) For all $j, k \in [n]$, $\Delta(\varphi_j, \varphi_k) = \Delta(\psi_j, \psi_k)$.

(ii) For all $j, k \in [n]$, there exist $\beta_j, \beta_k \in \mathbb{F}$ where $\beta_j\beta_j^\sigma = 1$ and $\beta_k\beta_k^\sigma = 1$ such that

$$\eta_{j,k,\psi} = \eta_{j,k,\varphi}\beta_j^\sigma\beta_k. \tag{3.1}$$

Proof. Given $j, k \in [n]$, let $\gamma_{j,k,\varphi} := \sqrt{\Delta(\varphi_j, \varphi_k)}$ and $\gamma_{j,k,\psi} := \sqrt{\Delta(\psi_j, \psi_k)}$.

We first assume that Φ and Ψ are switching equivalent, i.e., there exists a unitary $U : V \to V$ and elements $t_1, \ldots, t_n$ where $t_i t_i^\sigma = 1$ such that $\psi_j = t_j U\varphi_j$ for all $j \in [n]$. Let $j, k \in [n]$ with $j \neq k$. Thus, Lemma 3.3.7 implies that $\Delta(\varphi_j, \varphi_k) = \Delta(\psi_j, \psi_k)$ and further that $\gamma_{j,k,\varphi} = \gamma_{j,k,\psi}$. Also,

$$\begin{aligned}\eta_{j,k,\psi}\gamma_{j,k,\psi} = \langle\psi_j, \psi_k\rangle = \langle t_j U\varphi_j, t_k U\varphi_k\rangle &= t_j^\sigma t_k \langle U\varphi_j, U\varphi_k\rangle \\ = t_j^\sigma t_k \langle\varphi_j, \varphi_k\rangle &= t_j^\sigma t_k \eta_{j,k,\varphi}\gamma_{j,k,\varphi}.\end{aligned}$$

If $\gamma_{j,k,\varphi} = \gamma_{j,k,\psi} = 0$, then $\eta_{j,k,\varphi} = \eta_{j,k,\psi} = 0$; otherwise, one can divide both sides by $\gamma_{j,k,\varphi}$. In either case, after setting $\beta_j = t_j$ for all $j \in [n]$, condition (ii) holds.

For the other implication, assume that (i) and (ii) hold. (i) implies that for any $j \neq k$, $\gamma_{j,k,\varphi} = \gamma_{j,k,\psi}$. Let $\tilde{\varphi}_j = \beta_j \varphi_j$ for all $j \in [n]$. Further, we use (ii) to calculate

$$\begin{aligned} \langle \tilde{\varphi}_j, \tilde{\varphi}_k \rangle = \langle \beta_j \varphi_j, \beta_k \varphi_k \rangle &= \beta_j^\sigma \beta_k \langle \varphi_j, \varphi_k \rangle \\ &= \beta_j^\sigma \beta_k \eta_{j,k,\varphi} \gamma_{j,k,\varphi} \\ &= \eta_{j,k,\psi} \gamma_{j,k,\psi} = \langle \psi_j, \psi_k \rangle . \end{aligned}$$

This shows that $\Psi^\dagger \Psi = T^\dagger \Phi^\dagger \Phi T$ where $T = \mathrm{diag}(\beta_1, \ldots, \beta_n)$

Thus from Φ and Ψ being frames and Corollary 3.3.4, $(\tilde{\varphi}_j)_{j=1}^n$ is unitarily equivalent to Ψ, implying that Φ and Ψ are switching equivalent. □

The following generalizes Theorem 2.2 of [CW16].

Theorem 3.3.10. *Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ be frames for V, where V is a d-dimensional non-isotropic space. If $\langle \varphi_j, \varphi_k \rangle \neq 0$ and $\langle \psi_j, \psi_k \rangle \neq 0$ for any $j, k \in [n]$ with $j \neq k$, then Φ and Ψ are switching equivalent if and only if the following two conditions hold:*

(i) For all $j, k \in [n]$, $\Delta(\varphi_j, \varphi_k) = \Delta(\psi_j, \psi_k)$.

(ii) For all $j, k, \ell \in [n]$, $\Delta(\varphi_j, \varphi_k, \varphi_\ell) = \Delta(\psi_j, \psi_k, \psi_\ell)$.

Proof. One implication follows immediately from Lemma 3.3.7. For the other implication, suppose that the double and triple products of Φ and Ψ are equal. For each $j \neq k$, let $\eta_{j,k,\varphi}$ be the exponential gauges of Φ and $\eta_{j,k,\psi}$ the exponential gauges of Ψ. Since the double products are equal, for any $j \neq k$, there exists $\beta_{j,k} \in \mathbb{F}_q$ such that $\Delta(\varphi_j, \varphi_k) = \Delta(\psi_j, \psi_k) = \beta_{j,k} \neq 0$. Let $\gamma_{j,k} = \sqrt{\beta_{j,k}} \neq 0$. Consider $j \neq k \neq \ell \neq j$. Then

$$\eta_{j,k,\varphi} \eta_{k,\ell,\varphi} \eta_{\ell,j,\varphi} \gamma_{j,k} \gamma_{k,\ell} \gamma_{\ell,j} = \Delta(\varphi_j, \varphi_k, \varphi_\ell) = \Delta(\psi_j, \psi_k, \psi_\ell) = \eta_{j,k,\psi} \eta_{k,\ell,\psi} \eta_{\ell,j,\psi} \gamma_{j,k} \gamma_{k,\ell} \gamma_{\ell,j},$$

implying that

$$\eta_{j,k,\varphi} \eta_{k,\ell,\varphi} \eta_{\ell,j,\varphi} = \eta_{j,k,\psi} \eta_{k,\ell,\psi} \eta_{\ell,j,\psi}.$$

Fix ℓ and note that $\eta_{j,k}^{-1} = \eta_{j,k}^{\sigma} = \eta_{k,j}$ to obtain

$$\eta_{j,k,\psi} = \eta_{j,k,\varphi}\left(\eta_{k,\ell,\varphi}\eta_{\ell,k,\psi}\right)\left(\eta_{j,\ell,\varphi}\eta_{\ell,j,\psi}\right)^{\sigma}.$$

For any $j \in [n]$, set $\beta_j = \eta_{j,\ell,\varphi}\eta_{\ell,j,\psi}$. Then (ii) in Proposition 3.3.9 is satisfied, and Φ and Ψ are switching equivalent. □

Corollary 3.3.11. *Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ be (a,b)-equiangular systems that are frames for V, where V is a d-dimensional non-isotropic space. Then Φ and Ψ are switching equivalent if and only if for all $j < k < \ell$, $\Delta(\varphi_j, \varphi_k, \varphi_\ell) = \Delta(\psi_j, \psi_k, \psi_\ell)$.*

Proof. If $b = 0$, then the Gram matrices of both Φ and Ψ are aI_n, and Corollary 3.3.4 yields that Φ and Ψ are unitarily equivalent and thus switching equivalent (with necessarily the same triple products, Lemma 3.3.7). We now assume $b \neq 0$ and are able to apply Theorem 3.3.10. Note that

$$\Delta(\varphi_j, \varphi_k) = \Delta(\psi_j, \psi_k) = \begin{cases} a^2 & j = k \\ b & j \neq k \end{cases}$$

Further note that

$$\begin{aligned}
&\Delta(\varphi_j, \varphi_j, \varphi_j) = a^3 \\
&\Delta(\varphi_j, \varphi_k, \varphi_k) = \langle \varphi_j, \varphi_k\rangle \langle \varphi_k, \varphi_k\rangle \langle \varphi_k, \varphi_j\rangle = ab, \quad j \neq k \\
&\Delta(\varphi_j, \varphi_k, \varphi_\ell) = \langle \varphi_j, \varphi_k\rangle \langle \varphi_k, \varphi_\ell\rangle \langle \varphi_\ell, \varphi_j\rangle = \langle \varphi_\ell, \varphi_j\rangle \langle \varphi_j, \varphi_k\rangle \langle \varphi_k, \varphi_\ell\rangle = \Delta(\varphi_\ell, \varphi_j, \varphi_k) \\
&\Delta(\varphi_j, \varphi_k, \varphi_\ell) = \langle \varphi_j, \varphi_k\rangle \langle \varphi_k, \varphi_\ell\rangle \langle \varphi_\ell, \varphi_j\rangle = \left(\langle \varphi_j, \varphi_\ell\rangle \langle \varphi_\ell, \varphi_k\rangle \langle \varphi_k, \varphi_j\rangle\right)^{\sigma} = \left(\Delta(\varphi_j, \varphi_\ell, \varphi_k)\right)^{\sigma}.
\end{aligned}$$

Thus, it suffices to check the triple products for $j < k < \ell$. □

Now we will show that in general, without the requirement of non-zero scalar products or (a,b)-equiangularity, switching equivalence cannot be characterized for frames by the triple products alone and may require the n-products where n is the number of vectors. That is, we will show that there are two frames that have the same double and triple products but are not switching equivalent. The following generalizes Example 2.5 from [CW16].

Example 3.3.12. Let $(e_j)_{j=1}^n$ be the standard basis for $\mathbb{F}_q^n$, along with the standard dot product, where q is an odd prime and $n > 3$, which is a non-isotropic space. For $z \in \{\pm 1\}$ consider the collection of $n+1$ vectors

$$v_j = \begin{cases} e_j + e_{j+1} & 1 \leq j < n \\ e_n + ze_1 & j = n \\ e_n & j = n+1 \end{cases}$$

where for either choice of z, $(v_j)_{j=1}^{n+1}$ forms a frame for $\mathbb{F}_q^n$ with the following scalar products

- $\langle v_j, v_{j+1} \rangle = 1$ for $j \leq n$
- $\langle v_1, v_n \rangle = z$, $\langle v_{n-1}, v_{n+1} \rangle = 1$
- $\langle v_i, v_j \rangle = 0$ in all other cases where $i \neq j$

This means that the only non zero m-products of distinct vectors are

- $\Delta(v_j) = 2$ for $j \leq n$ and $\Delta(v_{n+1}) = 1$
- $\Delta(v_j, v_{j+1}) = 1$ for $j \leq n$, $\Delta(v_{n-1}, v_{n+1}) = 1$, and $\Delta(v_1, v_n) = 1$
- $\Delta(v_{n-1}, v_n, v_{n+1}) = 1$
- $\Delta(v_1, v_2, \ldots, v_n) = z$

This is not an equiangular system as the non-consecutive vectors have scalar products that are zero. For either choice of z the m-products are equivalent for all $m < n$ and differ only for the n-products. Since the n-products are not equal, Lemma 3.3.7 implies the two sequences are not switching equivalent.

In general, switching equivalence of collections of vectors (regardless of if they form frames) is completely determined by the m-products for all $m \leq n$. This result over $\mathbb{C}$ is due to [CW16], but their proof holds for any non-isotropic spaces with almost no modifications, which we emulate here. We note that this result was discovered in an equivalent form years earlier in [GP77].

Proposition 3.3.13. *Let $\Phi = (\varphi_j)_{j=1}^n, \Psi = (\psi_j)_{j=1}^n \subseteq V$ be collections of vectors in V, a d-dimensional non-isotropic space with $\ker(\Phi) = \ker(\Psi)$. Then Φ and Ψ are switching equivalent if and only if $\Delta(\varphi_{j_1}, \varphi_{j_2}, \ldots, \varphi_{j_m}) = \Delta(\psi_{j_1}, \psi_{j_2}, \ldots, \psi_{j_m})$ for all $m \leq n$ where $1 \leq j_\ell \leq n$ for all ℓ, that is all m-products for Φ and Ψ are equal.*

Proof. We have already shown the forward direction in Lemma 3.3.7. For the other direction we follow the same approach used in [CW16] which utilizes the correlation network of a frame, which was introduced in [Str07].

Assume that the m-products of Φ and Ψ are equal. Let $\Gamma(\Phi)$ be the correlation network of Φ: a graph whose vertices are the indices $1, 2, \ldots, n$ where vertex j corresponds to the vector φ_j, and an edge, denoted (j, k), exists between j and k when $\langle \varphi_j, \varphi_k \rangle \neq 0$. Notice that $\Delta(\varphi_j, \varphi_k) = 0$ if and only if $\langle \varphi_j, \varphi_k \rangle = 0$ meaning $\Gamma(\Phi) = \Gamma(\Psi)$. Call their common correlation network Γ. We may assume that Γ is connected, as if it were not we could restrict ourselves to looking at each component individually. Because Γ is connected there exists a spanning tree T for Γ. Fix a root vertex r and let $c_r = 1$. Let v be a child vertex of r and because $\Delta(\varphi_r, \varphi_v) = \Delta(\psi_r, \psi_v)$ we know that there exists some unimodular constant c_v (i.e. $c_v^\sigma c_v = 1$) where $\langle \varphi_r, \varphi_v \rangle = c_v^\sigma \langle \psi_r, \psi_v \rangle = \langle c_r \psi_r, c_v \psi_v \rangle$. Repeating this process inductively we have that for every non-root vertex k whose parent vertex is j in the tree, that

$$c_k = \left(\frac{\langle \varphi_j, \varphi_k \rangle}{\langle c_j \psi_j, \psi_k \rangle} \right)^\sigma$$

which satisfies $\Delta(\varphi_j, \varphi_k) = \Delta(\psi_j, \psi_k) = \Delta(c_j \psi_j, c_k \psi_k)$ and $\langle \varphi_j, \varphi_k \rangle = c_k^\sigma \langle c_j \psi_j, \psi_k \rangle = \langle c_j \psi_j, c_k \psi_k \rangle$. This process gives us a collection of unimodular constants $c_1, \ldots, c_n$ for each vertex of Γ such that by construction $\langle \varphi_j, \varphi_k \rangle = \langle c_j \psi_j, c_k \psi_k \rangle$ whenever (j, k) is an edge in the spanning tree T.

Now, we must show that our chosen constants respect the other non-zero scalar products. Let $e = (\ell, k)$ be an edge of the graph Γ such that e is not an edge of T. The addition of e into T creates a unique cycle in $e \cup T$ with vertices $(j_1, j_2, \ldots, j_{m-2}, \ell, k)$ of $m \leq n$ vertices. By the initial assumption and the fact that each c_j is unimodular we know that

$$\Delta(\varphi_{j_1},\dots,\varphi_{j_{m-2}},\varphi_\ell,\varphi_k)=\Delta(\psi_{j_1},\dots,\psi_{j_{m-2}},\psi_\ell,\psi_k)=\Delta(c_{j_1}\psi_{j_1},\dots,c_{j_{m-2}}\psi_{j_{m-2}},c_\ell\psi_\ell,c_k\psi_k)$$

This means that

$$\begin{aligned}&\langle\varphi_{j_1},\varphi_{j_2}\rangle\cdots\langle\varphi_{j_{m-2}},\varphi_\ell\rangle\langle\varphi_\ell,\varphi_k\rangle\langle\varphi_k,\varphi_{j_1}\rangle\\ &\qquad=\langle c_{j_1}\psi_{j_1},c_{j_2}\psi_{j_2}\rangle\cdots\langle c_{j_{m-2}}\psi_{j_{m-2}},c_\ell\psi_\ell\rangle\langle c_\ell\psi_\ell,c_k\psi_k\rangle\langle c_k\psi_k,c_{j_1}\psi_{j_1}\rangle\end{aligned}$$

From the construction of the unimodular constants we know that $\langle\varphi_i,\varphi_j\rangle=\langle c_i\psi_i,c_j\psi_j\rangle$ when $(i,j)\in T$ so it must be the case that $\langle\varphi_\ell,\varphi_k\rangle=\langle c_\ell\psi_\ell,c_k\psi_\ell\rangle$ for the added edge e. □

Combinatorial Designs: Two-Graphs and Quasi-Symmetric Designs

In this section, we will present a short overview on t-designs, two-graphs, and quasi-symmetric designs which are used frequently in this paper along with some examples connecting them to systems of lines in orthogonal geometries. For a more complete overview see [CL91; Tay77]. In the most basic sense, combinatorial design theory concerns collections of subsets of a given set which have certain additional properties. To that end, the following notation will be useful. If Ω is a finite set with n elements, then for $k\le n$, $\Omega^{\{k\}}$ is the collection of all k-element subsets of Ω. A **t-(n,k,λ) design** is a pair $(\Omega,\mathcal{B})$ where Ω is a set of n points and $\mathcal{B}\subseteq\Omega^{\{k\}}$, where the elements of $\mathcal{B}$ are called **blocks**, are such that any t points are contained in exactly λ blocks. If r is the number of blocks in a t-design, with $t\ge 2$, that contain any given point, then $|\mathcal{B}|k=nr$ and $r(k-1)=(n-1)\lambda$.

Lemma 3.3.14 (Fisher's inequality)**.** In a 2-design if $k<n$ then $|\mathcal{B}|\ge n$. And in the case where $|\mathcal{B}|=n$ then $r=k$

A t-design is called a **quasi-symmetric t-$(n,k,\lambda;s_1,s_2)$ design** if the intersection of any two distinct blocks has s_1 or s_2 points, such that $s_1\le s_2$. It can be shown that s_2-s_1 divides $k-s_1$

and $r - \lambda$. As an example, one could consider the lines in a plane over a finite field $\mathbb{F}_q^2$. Any pair of points defines a unique line, meaning that the lines define a 2-$(q^2, q, 1)$ design. Furthermore, each pair of lines either intersects in a unique point or are parallel. Thus, the lines form a quasi-symmetric 2-$(q^2, q, 1; 0, 1)$ design.

Another type of design, which is intimately related to equiangular lines in $\mathbb{R}^d$, and which we will show is also related to equiangular lines in orthogonal geometries, is a two-graph.

Definition 3.3.15. Let Ω be a set of size n, called the **point set** and $\mathcal{B} \subseteq \Omega^{\{3\}}$, called the **coherent triples**. A pair $(\Omega, \mathcal{B})$ is a **two-graph** if every 4-element subset of Ω contains an even number of elements of $\mathcal{B}$ as subsets.

A two-graph $(\Omega, \mathcal{B})$ is called **regular** if every 2 element subset of Ω is contained in an equal number of the coherent triples in $\mathcal{B}$. In this case $(\Omega, \mathcal{B})$ is a 2-$(n, 3, \ell)$ design for some integer ℓ.

Let $(\Omega, \mathcal{B})$ be a two-graph. Then a subset $\Gamma \subseteq \Omega$ is **coherent** if $|\Gamma| \geq 3$ and every 3-element subset of Γ is a coherent triple, that is $\Gamma^{\{3\}} \subseteq \mathcal{B}$. Likewise $\Gamma \subseteq \Omega$ is **incoherent** if $|\Gamma| \leq 2$ or no 3-element subset of Γ is a coherent triple, that is $\Gamma^{\{3\}} \cap \mathcal{B} = 0$. If $(\Omega, \mathcal{B})$ is a regular two-graph, and therefore a 2-$(n, 3, \ell)$ design, then every coherent triple is contained in m coherent quadruples where $|\Omega| = 3\ell - 2m$ and in which case we will refer to $(\Omega, \mathcal{B})$ as a **regular two-graph with parameters** (n, ℓ, m).

Given an undirected graph $G = (V, E)$ where $n = |V|$ we can construct a two-graph $(V, \mathcal{B}_G)$ where $\mathcal{B}_G$ is the set of all triples of vertices where the number of edges in the induced subgraph is odd. Two graphs G_1 and G_2, with the same vertex set V are called **switching equivalent** if there is a set of vertices $X \subseteq V$ where switching all edges and non-edges of G_1 between X and the compliment $G_1 - X$ result in G_2. Graphs that are switching equivalent give rise to equal two-graphs. In fact any two-graph $(\Omega, \mathcal{B})$, represents a class of switching equivalent graphs since in any induced subgraph on 3 vertices, switching changes and even number of edges.

We will make use of the **Seidel adjacency matrix** $S \in \mathbb{Z}^{n \times n}$ to connect two-graphs to equiangular lines. Label the vertices in V as $[n]$, and then define S as follows

$$S_{ij} := \begin{cases} -1 & \text{If } i \text{ and } j \text{ are adjacent} \\ 0 & \text{If } i = j \\ 1 & \text{If } i \text{ and } j \text{ are not adjacent} \end{cases}$$

The spectrum of a Seidel adjacency matrix is invariant under switching equivalence, and it is the spectrum which is critical in the connection to equiangular lines. So, we can sensibly define a non-unique Seidel adjacency matrix for any two-graph to be the Seidel adjacency matrix of any graph that induces the two-graph. An equivalent condition for a regular two-graph is that the spectrum of any of its Seidel adjacency matrices has exactly two eigenvalues. Furthermore let G_x be the unique graph which is switching equivalent to G and where x is isolated, and removed. Then a non-trivial, non-complete two-graph is regular if and only if there exists some $x \in V$ where G_x is strongly regular with parameters $k = 2\mu$. In this case the parameters of the regular two-graph and the strongly regular graph align, in that $k = \ell$ and $\lambda = m$.

Definition 3.3.16. A graph $G = (V, E)$ is a **strongly regular graph (SRG)** with parameters (v, k, λ, μ) if it is not complete nor empty and has $n = |V|$, k the degree or valency of each vertex, λ the number of shared neighbors for any pair of adjacency vertices, and μ the number of shared neighbors for any pair of non-adjacency vertices.

A graph $G = (V, E)$ is a **p-modular strongly regular graph (SRG$_p$)** with parameters (v, k, λ, μ) if it is not complete nor empty and has $n = |V|$, k is equivalent to the degree of each vertex modulo p, λ is equivalent to the number of shared neighbors for any pair of adjacency vertices modulo p, and μ is equivalent to the number of shared neighbors for any pair of non-adjacency vertices modulo p.

We use SRGs and SRG$_p$s only in the proof of Theorem 3.4.19, and so we will not give an in-depth overview. For an overview of SRGs and their connections two-graphs we point to [CL91] and for an overview of SRG$_p$s we point to [GIJM22b].

Let Φ be an (a, b)-equiangular system of n lines in an orthogonal geometry W of characteristic not equal to 2, where $b \neq 0$. In this case the angle between any two vectors is either β or $-\beta$ where $\beta^2 = b$. This suggests we can consider $\frac{1}{\beta}(\Phi^\dagger\Phi - aI)$ to be the image of a Seidel adjacency matrix for a graph $G = (V, E)$ under the map $\pi : \mathbb{Z} \to \mathbb{F}$, where the vertex set $V = \Phi$ are the vectors, and there is a edge between φ_i and φ_j if $\langle \varphi_i, \varphi_j \rangle = -\beta$. This means that Φ gives rise to a well-defined two-graph $(\Phi, \mathcal{C})$ where $\mathcal{C}$ is the set of all triples of vectors $\{\varphi_j, \varphi_k, \varphi_\ell\}$ where $\Delta(\varphi_j, \varphi_k, \varphi_\ell) = \langle \varphi_j, \varphi_k \rangle \langle \varphi_k, \varphi_\ell \rangle \langle \varphi_\ell, \varphi_j \rangle = -\beta^3$. This conditions exactly corresponds to the triple $\{\varphi_j, \varphi_k, \varphi_\ell\}$ having an odd number of edges in the graph corresponding to Φ. The "correct" choice of β is not immediately obvious as finite fields are not ordered, and we will explore the question of choosing a particular β in Section 3.5. Just as for graphs, systems of equiangular lines which are switching equivalent, give rise to equal two-graphs: Corollary 3.3.11 tells us that the parity of negative inner products in any triple product uniquely determines switching equivalence for ETFs in $\mathbb{R}^d$.

Likewise in some cases a two-graph can be used to construct a system of equiangular lines over an orthogonal geometry of dimension equal to the multiplicity of any non-zero eigenvalue. It is however not always the case that the two-graphs constructed from systems of equiangular lines over orthogonal geometries themselves give rise to switching equivalent systems of lines or even lines in the same dimensional space, and so we caution the reader: for the preservation of sensible structure, restrictions on β and the characteristics must be made.

Example 3.3.17. Consider $\mathbb{F}_{11}^2$ in the real model, with the standard dot product.

$$\Phi = \begin{bmatrix} 0 & 3 & 8 \\ 1 & 5 & 5 \end{bmatrix} \qquad \Phi^\dagger\Phi = \begin{bmatrix} 1 & 5 & 5 \\ 5 & 1 & 5 \\ 5 & 5 & 1 \end{bmatrix}$$

Φ is a $(1, 3, 7)$-ETF. By picking $\beta = 5$ we can see that the resulting two-graph is the trivial two-graph $(\{1, 2, 3\}, \{\})$, a graph that induces this two-graph is the trivial graph on 3 vertices, which has Seidel adjacency matrix $J - I \in \mathbb{Z}^{3\times 3}$ with eigenvalues 2 with multiplicity 1 and -1 with multiplicity 2. This means we can construct $-I - J + I = -J$ which has -1 on the diagonal, and -1 off the diagonal. The matrix $-J$ is rank 1 meaning this gives rise to a $(-1, 1)$-equiangular frame for a 1 dimensional orthogonal geometry. If instead we used the eigenvalue of 2 we would get $2I - J + I = 3I - J$ which would be a rank 2 matrix and therefore the Gram matrix of a $(2, 1)$-equiangular frame for a 2 dimensional orthogonal geometry, and therefore an ETF. Picking $\beta = -5 \equiv 6$ would result in a similar behavior.

3.4 Conditions for Tightness

In this section we will explore sufficient conditions for collections of lines to be tight.

In Section 3.1 we defined tightness to be a property of frames. However, as we will see in this section, many equivalent notions of tightness are enough to guarantee that a collection of vectors has a non-isotropic image, and hence would be a tight frame for their span.

Lemma 3.1.5 Revisited

Lemma 3.4.1. Let $c \neq 0$ and $\Phi = (\varphi_j)_{j=1}^n$ be a collection of vectors in a non-isotropic space V, then the following are equivalent and imply that $\Phi : \mathbb{F}^n \to \operatorname{im}\Phi$ is a c-tight frame for $\operatorname{im}\Phi$.

(i) $\Phi\Phi^\dagger = cI$ on $\operatorname{im}\Phi$

(ii) $\Phi\Phi^\dagger\Phi = c\Phi$

Proof. First we will show (i) implies (ii) which in turn implies $\Phi : \mathbb{F}^n \to \operatorname{im}\Phi$ is a c-tight frame. Notice that (i) immediately implies (ii) and by counting ranks we can conclude from $\Phi\Phi^\dagger\Phi = c\Phi$ where $c \neq 0$ that

$$\operatorname{rank}(c\Phi) = \operatorname{rank}(\Phi\Phi^\dagger\Phi) \leq \min(\operatorname{rank}(\Phi), \operatorname{rank}(\Phi^\dagger\Phi)) = \operatorname{rank}(\Phi^\dagger\Phi),$$

where the last equality follows from $\operatorname{rank}(\Phi) \geq \operatorname{rank}(\Phi^\dagger\Phi)$. So $\operatorname{rank}(\Phi) = \operatorname{rank}(\Phi^\dagger\Phi)$. By Lemma 3.1.7 we know that $\operatorname{im}\Phi$ is non-isotropic. This shows $\Phi : \mathbb{F}^n \to \operatorname{im}\Phi$ is a frame. This also implies (i) from (ii) by Lemma 3.1.5. □

We note that this result does not guarantee that the $\operatorname{discr}(\operatorname{im}\Phi)$ agrees with $\operatorname{discr}(V)$, and in general it will not. An explicit example is shown in Example 3.4.3.

Definition 3.4.2. Let $M = [M_{ij}]_{i,j\in[n]}$ be a square matrix, and denote the columns by $m_1, \ldots, m_n$. Select a subset of the columns $(m_j)_{i\in K}$ that forms a basis for $\operatorname{im} M$. Define a **basic submatrix** of M to be $M_b = [M_{ij}]_{i,j\in K}$

In case O, [GIJM22a], showed that the $\operatorname{discr}(\operatorname{im}\Phi) = (\det((\Phi^\dagger\Phi)_b))\mathbb{F}_q^{\times 2}$ for any basic submatrix $(\Phi^\dagger\Phi)_b$ of the Gram matrix.

Example 3.4.3. let $V = \mathbb{F}_5^3$ be an orthogonal geometry in the real model where $\operatorname{discr}(\mathbb{F}_5^3)$ is trivial and consider the system of lines

$$\Phi = \begin{bmatrix} 0 & 2 & 3 \\ 4 & 2 & 2 \\ 4 & 2 & 2 \end{bmatrix} \qquad \Phi^\dagger\Phi = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 4 \\ 1 & 4 & 2 \end{bmatrix},$$

which is a $(2,1)$-equiangular system of lines. We can also see that $\dim(\operatorname{im}\Phi) = 2$. From Lemma 3.4.1 and because $3\Phi = \Phi\Phi^\dagger\Phi$ we know that Φ is an $(2,1,3)$-ETF for $\operatorname{im}\Phi$. Looking at a basic submatrix formed from the first two columns of $\Phi^\dagger\Phi$, whose determinant is 3, we can see that the discriminant of Φ is not a square. Now consider the orthogonal geometry $\mathbb{F}_5^2$ with a scalar product having Gram matrix $\operatorname{diag}(1,3)$ and consider the frame for $\mathbb{F}_5^2$,

$$\Psi = \begin{bmatrix} 0 & 2 & 3 \\ 2 & 1 & 1 \end{bmatrix}$$

which is also a $(2,1,3)$-ETF where $\Phi^\dagger\Phi = \Psi^\dagger\Psi$.

We note that case (iii) from Lemma 3.1.5 does not imply that $\operatorname{im}\Phi$ is non-isotropic in general, as $\operatorname{rank}(\Phi)$ and $\operatorname{rank}(\Phi^\dagger\Phi)$ may not agree. However we provide a few situations where (iii) does imply $\operatorname{im}\Phi$ is non-isotropic. First we give conditions on square matrices which make them the Gram matrices for some frame.

Proposition 3.4.4. *(Theorem 3.13 [GIJM22a]) Let G be an $n \times n$ matrix with entires in $\mathbb{F}_{q^2}$. Then G is the Gram matrix of some frame for a unitary geometry $\mathbb{F}_{q^2}^d$ if and only if*

(i) $G = G^*$

(ii) $\operatorname{rank}(G) = d$

Additionally G is the Gram matrix for a c-tight frame with $c \in \mathbb{F}_{q^2}$ if and only if

(iii) $G^2 = cG$

Furthermore G is the Gram matrix of some (a, b, c)-ETF for $a, b \in \mathbb{F}_{q^2}$ if and only if

(iv) $G_{ii} = a$ *for all* $i \in [n]$

(v) $G_{ij}G_{ji} = b$ *for all* $i \neq j$ *in* $[n]$

Proposition 3.4.5. *(Theorem 3.15 [GIJM22a], Proposition 2.12 [GIJM22b]) Let G be an $n \times n$ matrix with entires in $\mathbb{F}_q$ for some odd prime power q. Then G is the Gram matrix of some frame for an orthogonal geometry $\mathbb{F}_q^d$ if and only if*

(i) $G = G^\intercal$

(ii) $\operatorname{rank}(G) = d$

(iii) $(\det(G_b)) = \operatorname{discr}(\mathbb{F}_q^d)$

Additionally G is the Gram matrix for a c-tight frame with $c \in \mathbb{F}_q$ if and only if

(iv) $G^2 = cG$

Furthermore G is the Gram matrix of some (a, b, c)-ETF for $a, b \in \mathbb{F}_q$ if and only if *(v)* $G_{ii} = a$ *for all* $i \in [n]$

(vi) $G_{ij}^2 = b$ *for all* $i \neq j$ *in* $[n]$

We also give a more direct instance where (iii) from Lemma 3.1.5 implies that $\operatorname{im}\Phi$ is non-isotropic. The proof uses CR-decompositions which in some cases can fill the gap from the lack of spectral theory, and positive definiteness, in the positive characteristic setting.

Proposition 3.4.6. *Let* $M \in \mathbb{F}^{n\times m}$ *be any matrix over any field, with* $\operatorname{rank}(M) = r$*. Then there exist matrices* $C \in \mathbb{F}^{n\times r}$ *and* $R \in \mathbb{F}^{r\times m}$ *such that* $M = CR$ *and* $\operatorname{rank}(C) = \operatorname{rank}(R) = \operatorname{rank}(M) = r$*.*

Proof. Let C be a matrix with r linearly independent columns of M. This means $C \in \mathbb{F}^{n\times r}$ and has rank r. Then because every column of M is a linear combination of the columns of C we can construct the matrix $R \in \mathbb{F}^{r\times m}$ where the ith column of R is the coefficients in the linear combination of the columns of C to make the ith column of M. This gives us $M = CR$. Finally notice that $\operatorname{rank}(R) = r$, because if it were less than the product CR would not have rank r. □

This decomposition gives us some very nice properties. It is important to note that this decomposition is not unique. Because $C : \mathbb{F}^r \to \mathbb{F}^n$ is full rank it is injective and so has a left inverse C^- where $C^-C = I_r$ and because $R : \mathbb{F}^n \to \mathbb{F}^r$ is full rank it is surjective, and so has a right inverse R^- where $RR^- = I_r$.

Theorem 3.4.7. *Let* $\Phi = (\varphi_j)_{j=1}^n$ *be an equal norm collection of vectors in a non-isotropic space* V*, with* $\langle \varphi_j, \varphi_j \rangle = a$ *for all* j*, such that* $\frac{na}{d} \neq 0$ *where* $d := \dim(\operatorname{im}\Phi)$*. If* $\operatorname{char}\mathbb{F} > d$ *and* $(\Phi^\dagger\Phi)^2 = \frac{na}{d}\Phi^\dagger\Phi$ *Then* Φ *is an* $\frac{na}{d}$*-tight frame for* $\operatorname{im}\Phi$*.*

Proof. Let $\Phi = (\varphi_j)_{j=1}^n$ be a collection of equal norm vectors with $\langle \varphi_j, \varphi_j \rangle = a \neq 0$ in a non-isotropic space V such that $d := \dim(\operatorname{im}\Phi)$, over a field $\mathbb{F}$ with $\operatorname{char}\mathbb{F} > d$ and $(\Phi^\dagger\Phi)^2 = \frac{na}{d}\Phi^\dagger\Phi$.

Consider a CR-decomposition for the Gram matrix $\Phi^\dagger\Phi = CR$ where $C \in \mathbb{F}^{n\times r}$ and $R \in \mathbb{F}^{r\times n}$, such that $r = \operatorname{rank}(\Phi^\dagger\Phi) = \operatorname{rank}(C) = \operatorname{rank}(R)$. This gives us the following

$$\begin{aligned} CRCR &= \frac{na}{d} CR \\ \Rightarrow \quad C^- CRCRR^- &= \frac{na}{d} C^- CRR^- \\ \Rightarrow \quad RC &= \frac{na}{d} I_r \end{aligned}$$

Now looking at the trace we can determine

$$na = \operatorname{tr}(\Phi^\dagger\Phi) = \operatorname{tr}(CR) = \operatorname{tr}(RC) = \operatorname{tr}\left(\frac{na}{d} I_r\right) = \frac{na}{d}\operatorname{rank}(\Phi^\dagger\Phi),$$

where the equalities are in $\mathbb{F}$. Since $na/d \neq 0$ and $\operatorname{char}\mathbb{F} > d$, we conclude that as integers $\operatorname{rank}(\Phi^\dagger\Phi) = d$. Thus, Lemma 3.1.7 implies that $\Phi : \mathbb{F}^n \to \operatorname{im}\Phi$ is a frame and further by Lemma 3.1.5 an $\frac{na}{d}$-tight frame. □

Naimark Complements

In Hilbert spaces, every tight frame has a (non-unique) Naimark complement, which preserves some of the key properties of the frame [DL98; Neu43]. Over finite dimensions, the Naimark complement of a tight frame (respectively, ETF) of n vectors for a d-dimensional space always is a tight frame (respectively, ETF) of n vectors for an $(n-d)$-dimensional space. This decreases the parameter space which one needs to explore when analyzing such frames. For more on the properties of the Naimark complement over the reals and complexes and issues when trying to extend the complement to non-tight frames, see [CFMPS13; KM25]. In this section, we expand the theory of Naimark complements in the case of frames over fields of non-zero characteristic building off of the work in [GIJM22a]. In the real and complex setting a Naimark complement need only satisfy $cI_n = \Phi^\dagger\Phi + \Psi^\dagger\Psi$ for c the tight frame bound. From this it can be shown that $\Phi\Psi^\dagger = 0$ and $\Psi\Phi^\dagger = 0$, through the positive definiteness of inner products, which in essence means the stacked matrix $\begin{bmatrix} \Phi \\ \Psi \end{bmatrix}$ would be a scaled unitary. This single condition is not quite sufficient in the more general setting.

Example 3.4.8. Consider the following matrices

$$\Phi = \begin{bmatrix} 1 & 1 \end{bmatrix} \quad \text{and} \quad \Psi = \begin{bmatrix} 1 & 2 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix},$$

where Φ is a 2-tight frame in the real model for $\mathbb{F}_3^1$ and Ψ is a system of lines in the real model for $\mathbb{F}_3^4$. Notice that

$$2I = \Phi^\dagger\Phi + \Psi^\dagger\Psi = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix} + \begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix};$$

however, Ψ is not even a frame for its image since $\operatorname{rank}(\Psi^\dagger\Psi) = 1 < 2 = \operatorname{rank}(\Psi)$ (Lemma 3.1.7). We can also see that

$$\Psi\Phi^\dagger = \begin{bmatrix} 0 & 1 & 1 & 1 \end{bmatrix}^\intercal.$$

Definition 3.4.9. Let $\Phi : \mathbb{F}^n \to V$ be a c-tight frame ($c \neq 0$) for a d-dimensional non-isotropic space V. Then the synthesis operator $\Psi : \mathbb{F}^n \to W$ for a collection of vectors is a **Naimark complement** if $cI_n = \Phi^\dagger\Phi + \Psi^\dagger\Psi$ and $\Psi\Phi^\dagger = 0$

We also note that the geometries of $\operatorname{im}\Phi$ and $\operatorname{im}\Psi$ need not be the same, in the sense that they need not share a discriminant.

Lemma 3.4.10. Let $\Phi : \mathbb{F}^n \to V$ be a c-tight frame ($c \neq 0$) for a d-dimensional non-isotropic space V and $\Psi : \mathbb{F}^n \to W$ a Naimark complement then $\operatorname{im}\Psi$ is non-isotropic and $\Psi : \mathbb{F}^n \to \operatorname{im}\Psi$ is a c-tight frame with $\dim(\operatorname{im}\Psi) = n - d$. Additionally $\operatorname{im}\Psi^\dagger = (\operatorname{im}\Phi^\dagger)^\perp$, and $\operatorname{discr}(\operatorname{im}\Psi) = c^n \operatorname{discr}(V)$. Furthermore, if Φ is a (a, b, c)-ETF, then $\Psi : \mathbb{F}^n \to \operatorname{im}\Psi$ is an $(c - a, b, c)$-ETF.

Proof. Using the fact that $\Psi\Phi^\dagger = 0$ and because $\mathbb{F}^n$, V, and W are all non-isotropic, we have that $(\Psi\Phi^\dagger)^\dagger = \Phi\Psi^\dagger = 0$. We can also determine that

$$\begin{aligned} cI_n &= \Phi^\dagger\Phi + \Psi^\dagger\Psi \\ \Rightarrow \quad c\Psi &= \Psi\Phi^\dagger\Phi + \Psi\Psi^\dagger\Psi \\ \Rightarrow \quad c\Psi &= \Psi\Psi^\dagger\Psi \end{aligned}$$

By Lemma 3.4.1 we know that since $\operatorname{im}\Psi$ is non-isotropic, $\Psi : \mathbb{F}^n \to \operatorname{im}\Psi$ is a c-tight frame.

Finally, we will look at the dimension of $\operatorname{im}\Psi$. Notice that because $cI_n = \Phi^\dagger\Phi + \Psi^\dagger\Psi$ and the non-isotropy, we have that

$$n = \operatorname{rank}(cI_n) = \operatorname{rank}(\Phi^\dagger\Phi + \Psi^\dagger\Psi) \leq \operatorname{rank}(\Phi^\dagger\Phi) + \operatorname{rank}(\Psi^\dagger\Psi) = d + \operatorname{rank}(\Psi);$$

so, $\operatorname{rank}(\Psi) \geq n - d$. Because $\Phi\Psi^\dagger = 0$ we know that $\operatorname{im}\Psi^\dagger \subseteq \ker\Phi$ meaning $\dim(\operatorname{im}\Psi^\dagger) \leq n - d$, i.e., $\operatorname{rank}(\Psi) = n - d$.

Notice that $\operatorname{im}(\Psi^\dagger\Psi) = \operatorname{im}(cI - \Phi^\dagger\Phi) = \operatorname{im}(\Phi^\dagger\Phi)^\perp$, and so by Lemma 3.1.6, we have that $\operatorname{im}(\Psi^\dagger) = \operatorname{im}(\Phi^\dagger)^\perp$.

This also means that $\mathbb{F}^n = \operatorname{im}(\Psi^\dagger) \oplus \operatorname{im}(\Phi^\dagger)$. Thus, $\operatorname{discr}(\operatorname{im}(\Psi^\dagger))\operatorname{discr}(\operatorname{im}(\Phi^\dagger)) = \operatorname{discr}(\mathbb{F}^n) = \mathbb{F}^{\times 2}$, giving us that $\operatorname{discr}(\operatorname{im}(\Psi^\dagger)) = \operatorname{discr}(\operatorname{im}(\Phi^\dagger))$. It follows from Lemma 3.18 of [GIJM22a] that $\operatorname{discr}(\operatorname{im}(\Phi^\dagger)) = \det(\Phi^\dagger\Phi)\operatorname{discr}(V)$ and $\operatorname{discr}(\operatorname{im}(\Psi^\dagger)) = \det(\Psi^\dagger\Psi)\operatorname{discr}(\operatorname{im}\Psi)$. Putting this together, we get that $\operatorname{discr}(\operatorname{im}\Psi) = c^d \operatorname{discr}(V)/c^{n-d} = c^{-n}\operatorname{discr}(V) = c^n \operatorname{discr}(V)$.

Finally, assume that Φ was an (a, b, c)-ETF. By $cI_n = \Phi^\dagger\Phi + \Psi^\dagger\Psi$ we know $\langle \psi_j, \psi_j \rangle = c - \langle \varphi_j, \varphi_j \rangle$ and for $j \neq k$ that $\langle \psi_j, \psi_k \rangle = -\langle \varphi_j, \varphi_k \rangle$, and so $\langle \psi_j, \psi_k \rangle \langle \psi_k, \psi_j \rangle = (-1)^2 \langle \varphi_j, \varphi_k \rangle \langle \varphi_k, \varphi_j \rangle = b$ □

We note that if Ψ were known to be a frame for W then the condition $\Psi\Phi^\dagger = 0$ follows from $\Phi^\dagger\Phi + \Psi^\dagger\Psi = cI$. Naimark complements always exists for non-degenerate tight frames over finite fields but the discriminant will depend on the field and c.

Theorem 3.4.11. *(Proposition 3.22 [GIJM22a]) Let $\Phi : \mathbb{F}_{q^2}^n \to V$ be a c-tight frame ($c \neq 0$) for a d-dimensional unitary geometry V. Then there exists a Naimark complement $\Psi : \mathbb{F}_{q^2}^n \to W$ for an $(n-d)$-dimensional unitary geometry W.*

Theorem 3.4.12. *(Proposition 3.23 [GIJM22a]) Let $\Phi : \mathbb{F}_q^n \to V$ be a c-tight frame ($c \neq 0$) for a d-dimensional orthogonal geometry V. Then there exists a Naimark complement $\Psi : \mathbb{F}_q^n \to W$ for an $(n-d)$-dimensional orthogonal geometry W with $\operatorname{discr}(W) = c^n \operatorname{discr}(V)$.*

In fact Proposition 3.23 of [GIJM22a] gives a stronger statement allowing $\Psi^\dagger\Psi$ to be any scalar multiple of $cI - \Phi^\dagger\Phi$, which in turn allows for the discriminants to be equal.

Tightening Equiangularity

Now we wish to characterize the situations when (a, b)-equiangular systems of lines are ETFs. The following result is originally due to Gerzon, but was generalized in the finite field setting by [GIJM22a].

Theorem 3.4.13. *(Gerzon's Bound. Theorem 4.2 [GIJM22a]) Let V be a non-isotropic space, with $d = \dim V$, $k = \dim_{\mathbb{F}_0} \mathbb{F} \in \{1, 2\}$, and $a^2 \neq b$, then there exists an (a, b)-equiangular system of n lines in V only if $n \leq d + \frac{k}{2}(d^2 - d)$. In the case of equality there exists some $c \in \mathbb{F}_0$ such that $\Phi\Phi^\dagger = cI$. If $c \neq 0$ or if Φ is in case U or O then Φ is an (a, b, c)-ETF for V.*

Proof. Let $\varphi_1, \varphi_2, \ldots, \varphi_n$ be an (a, b)-equiangular system of vectors in V where $n > d := \dim V$, such that $a^2 \neq b$, and so $b \neq 0$. As in the proof of Theorem 2.3.9, we will the corresponding projection $P_j = \varphi_j\varphi_j^\dagger$ which maps V onto the span of φ_j. These projections live in the $\mathbb{F}_0$ vector space L of self adjoint operators on V which has dimension $\dim_{\mathbb{F}_0} L = Z(d, \mathbb{F}) = d + \frac{k}{2}(d^2 - d)$ where $k = \dim_{\mathbb{F}_0} \mathbb{F}$. This space of self adjoint matrices has a possibly degenerate hermitian scalar product $\langle A, B\rangle = \operatorname{tr}(AB)_F$.

Notice that $\langle P_j P_k\rangle_F = \operatorname{tr}(\varphi_j\varphi_j^\dagger\varphi_k\varphi_k^\dagger) = \langle\varphi_j, \varphi_k\rangle\langle\varphi_j, \varphi_k\rangle = b$ when $j \neq k$ and $\left\langle\varphi_j\varphi_j^\dagger\varphi_j\varphi_j^\dagger\right\rangle_F = a^2$. Therefore the Gram matrix of these projections is $G = [\langle P_j P_k\rangle_F] = bJ_n + (a^2 - b)I_n$, where J_n is the $n \times n$ all 1s matrix. From this we can determine that G has eigenvalues $a^2 + (n-1)b$ and

a^2-b, where $a^2-b\neq 0$ from the initial assumption, however $a^2+(n-1)b$ may still be zero. Here we want to show that the eigenvalues are all non-zero, as this will show that the columns of G are linearly independent. If the projections $(P_j)_{j=1}^n$ were linearly dependent, this would then show its self in the form of a non-zero element in the kernel of G. But if G has all non-zero eigenvalues its kernel would be trivial and therefore the projections would be linearly independent in the vector space L.

Consider a vector $v\in\ker G$ which is the case if and only if $bJ_nv=-(a^2-b)I_nv$. Because $a^2-b\neq 0$ this means v must at be a scalar multiple of the all ones vector. So $\ker G=\text{span}(1^n)$ when $a^2+(n-1)b=0$ and otherwise $\ker G=0$. If $\ker G=0$ we would have that $n\leq Z(d,\mathbb{F})$ as desired. If $\ker G=\text{span}(1^n)$, when $a^2+(n-1)b=0$, it may still be the case that that this kernel element did not come from a linear dependence on the projection matrices. If it did it would have come from $\sum_{k=1}^n P_k=\sum_k \varphi_k\varphi_k^\dagger=0$. Looking at the trace we will see that $0=\text{tr}(\sum_k\varphi_k\varphi_k^\dagger)=\text{tr}(\Phi\Phi^\dagger)=\text{tr}(\Phi\Phi^\dagger)=na$. Therefore $n\equiv 0$, or $\operatorname{char}\mathbb{F}|n$. However if this was the case $0=a^2+(n-1)b=a^2-b\neq 0$. So the projection matrices would be linearly independent meaning $m\leq Z(d,\mathbb{F})$ as desired.

Now consider the case where $a=0$. This would mean that $\langle P_j,P_j\rangle_F=\text{tr}(P_j)=0$ for all j, and so the projections are not only contained in the space of self adjoint matrices, they are in fact contained in the space L_0 of self adjoint trace zero matrices which has dimension $\dim_{\mathbb{F}_0}L=Z(d,\mathbb{F})-1=d+\frac{k}{2}(d^2-d)-1$. Therefore even if the sum of the projection is zero, this would be a minimal dependence relation, and any $n-1$ of the projection would still be linearly independent in the space L_0, and so $n-1\leq Z(d,\mathbb{F})-1$ giving us the same result that $n\leq Z(d,\mathbb{F})$.

Finally we want to look at the case of equality when $n=Z(d,\mathbb{F})$. This will require us to show that there exists some $c\in\mathbb{F}$ such that $\Phi\Phi^\dagger=cI$. As we have already seen if $\ker G=0$ this means that there exists not all zero constants $a_1,a_2,\ldots,a_n,c\in\mathbb{F}_0$, with $c\neq 0$ and with out loss of generality $a_1=1$ such that $\sum_k a_k\varphi_k\varphi_k^\dagger=cI$. We want to show that $a_k=1$ for all k. Notice that $\text{tr}(\varphi_k\varphi_kI)=a\neq 0$ meaning letting $P_{n+1}=I$ and looking at the Gram matrix

$H = [\langle P_j P_k \rangle_F]_{j\in[n+1],k\in[n+1]}$ we have that

$$H = \begin{bmatrix} G & 1^n \\ (1^n)^\intercal & d \end{bmatrix}$$

where we know that the vector $x = \begin{bmatrix} a_1 & \cdots & a_n & -c \end{bmatrix}^\intercal \in \ker H$. Notice that this gives us $n+1$ linear equation coming from $Hx = 0$. For $1 < j \leq n$ we have that $a^2 a_j + b(\sum_{i\neq j} a_i) - c = 0 = a^2 a_1 + b(\sum_{i\neq 1} a_i) - c$, meaning $a^2 a_j - ba_j = 0 = a^2 a_1 - ba_1$. Because $a^2 - b \neq 0$ this gives us that $a_j = a_1 = 1$ for all $1 \leq j \leq n$. This means that $\Phi\Phi^\dagger = \sum_k \varphi_k \varphi_k^\dagger = cI$.

Now we will consider the case where $\ker G = \text{span}(1^n)$, which means $a = 0$. This also means that $\Phi\Phi^\dagger = 0$.

If $c \neq 0$, Lemma 3.4.1 gives us that Φ is a tight frame for V.

In case O or U this is also the case regardless of c. In either case due to Proposition 3.4.5 or Proposition 3.4.4 we know that $\Phi^\dagger\Phi$ is the Gram matrix for a frame $\Psi = (\psi_j)_{j=1}^n$ for some space V of dimension $\dim V = \text{rank}(\Phi^\dagger\Phi) \leq d$. However from Gerzon's bound, $\dim V = \text{rank}(\Phi^\dagger\Phi) = d$ and so $\text{rank}(\Phi) = \text{rank}(\Phi^\dagger\Phi) = d$ and therefore Φ would be an ETF for V. □

[Ian: *notes: We must require $a^2 \neq b$ (In the real/complex case this excluded the case where all the lines are the same).*]

Theorem 3.4.13 gives the **absolute bound** on the number of equiangular lines depending on the space. Although no bound is known relative to the parameter b we can still characterize the situations in which an (a, b)-equiangular systems of lines Φ is an ETF depending only on the parameters a, b and the Gram matrix $\Phi^\dagger\Phi$.

Let $\Phi : \mathbb{F}^n \to V$ be an (a, b, c)-ETF where $d = \dim(V)$. Looking at the traces of $\Phi^\dagger\Phi$ and $\Phi\Phi^\dagger$ we have the following relation:

$$\text{tr}(\Phi^\dagger\Phi) = na = dc = \text{tr}(\Phi\Phi^\dagger). \tag{3.2}$$

Looking at $(\Phi^\dagger\Phi - aI)^2$, [GIJM22a] showed that

$$a(c-a) = (n-1)b. \tag{3.3}$$

When $\operatorname{char}\mathbb{F}$ does not divide $d(n-1)$, putting (3.2) and (3.3) together yields

$$b = \frac{(n-d)}{d(n-1)}a^2. \tag{3.4}$$

We note that $a^2(n-d) = d(n-1)b$ is always true regardless of the characteristic. Unlike in the real or complex setting, satisfying this equality, known as the **Welch bound**, does not guarantee that an equiangular system of lines is an ETF.

Example 3.4.14. Consider the following $(2,1)$-system of equiangular lines which is a frame for $\mathbb{F}_5^7$ in the real model

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 1 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 & 4 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 & 4 & 0 & 2 \\ 0 & 1 & 1 & 2 & 1 & 2 & 2 & 3 \\ 1 & 0 & 1 & 2 & 3 & 2 & 2 & 3 \\ 1 & 1 & 0 & 2 & 3 & 4 & 4 & 1 \end{bmatrix}$$

which also satisfies $(n-1)b \equiv 2 \equiv \frac{n-d}{d}a^2$. However, Φ is not a tight frame since $\Phi\Phi^\dagger$ is not diagonal.

Under additional constraints, i.e., concerning sums of triple products of the vectors in Φ, we can come up with a sufficient condition for being an ETF. Sums of triple products have been leveraged previously to understand the algebraic structure of ETFs over characteristic zero [Kin19; Zhu15]. If $\Phi = (\varphi_j)_{j=1}^n$ is an (a,b,c)-ETF for V, where $\dim V = d$ we have that

$$\sum_{\ell=1}^{n} \Delta(\varphi_j, \varphi_k, \varphi_\ell) = \langle \varphi_j, \varphi_k \rangle \left\langle \varphi_k, \sum_{\ell=1}^{n} \langle \varphi_\ell, \varphi_j \rangle \varphi_\ell \right\rangle = \langle \varphi_j, \varphi_k \rangle \langle \varphi_k, c\varphi_j \rangle = cb. \tag{3.5}$$

Here we will create a non-degenerate scalar product on linear operators and use non-degeneracy to show that an operator is the zero operator because the scalar product with every other operator is 0.

Definition 3.4.15. Let $L = \{A : V \to V\}$ be the $\mathbb{F}$-vector space of linear operators on a non-isotropic space V. Under a choice of basis we can consider L to be the space of $d \times d$ matrices where $\dim(V) = d$. The **Frobenius scalar product** is then defined for $A, B \in L$ as

$$\langle A, B \rangle_F := \operatorname{tr}(A^\dagger B).$$

We note that in the case where $V = \mathbb{F}^n$ with the standard dot product or conjugate dot product, the adjoint operator on any map $A : \mathbb{F}^n \to \mathbb{F}^n$ is the conjugate transpose and the matrices $\{\, E_{ij} \mid i, j \in [n] \,\}$ form an orthonormal basis for L with respect to the Frobenius scalar product, as $\operatorname{tr}(E_{ij} E_{\ell k}) = 1$ when $j = \ell$ and $i = k$ and zero otherwise. Therefore, the Frobenius scalar product is a non-degenerate Hermitian scalar product on L.

We may also consider the subspace of self adjoint operators $L_0 = \left\{\, A \in L \;\middle|\; A^\dagger = A \,\right\}$ which is an $\mathbb{F}_0$-vector space. Let $V = \mathbb{F}_q^n$ be in the real model for case O, in which case

$$\{\, E_{\ell\ell} \mid \ell \in [n] \,\} \cup \{\, E_{ij} + E_{ji} \mid i, j \in [n], i < j \,\}$$

forms an orthogonal basis for L_0, Notice that $\langle E_{\ell\ell}, (E_{ij} + E_{ji}) \rangle_F = 0$. Looking at the symmetrical terms we see that $\langle (E_{ij} + E_{ji}), (E_{\ell k} + E_{k\ell}) \rangle_F = 2$ when $i = \ell$ and $j = k$ and zero otherwise. This means that the Frobenius scalar product is a non-degenerate symmetrical scalar product on L_0 in the real model, but in general and particularly in case U, the Frobenius scalar product may be degenerate.

Theorem 3.4.16. *Let $\Phi = (\varphi_j)_{j=1}^n$ be an (a, b)-equiangular system in a non-isotropic space V where $\dim(\operatorname{im} \Phi) = d$, such that $\operatorname{char} \mathbb{F} > d$ and $\frac{na}{d} \neq 0$. Then $\Phi : \mathbb{F}^n \to \operatorname{im} \Phi$ is an $(a, b, \frac{n}{d}a)$-ETF if and only if $(n-1)b = \frac{n-d}{d}a^2$ and $\sum_{\ell=1}^n \Delta(\varphi_j, \varphi_k, \varphi_\ell) = \frac{nab}{d}$ for all $j \neq k$ in $[n]$.*

Proof. The forward implication immediately follows from (3.4) and (3.5). For the other implication, it suffices to show that $(\Phi^\dagger\Phi)^2 = \frac{na}{d}(\Phi^\dagger\Phi)$, because when $\operatorname{char}\mathbb{F} > d$, Theorem 3.4.7 gives us that $\operatorname{im}\Phi$ is non-isotropic and so $\Phi : \mathbb{F}^n \to \operatorname{im}\Phi$ would be a $\frac{na}{d}$-tight frame.

Because $\mathbb{F}^n$ is non-isotropic with a non-degenerate scalar product, we know that the Frobenius scalar product on $\mathbb{F}^{n\times n}$ is a non-degenerate Hermitian scalar product. This means we can show that $(\Phi^\dagger\Phi)^2 - \frac{na}{d}(\Phi^\dagger\Phi) = 0$ by showing that $\left\langle(\Phi^\dagger\Phi)^2 - \frac{na}{d}(\Phi^\dagger\Phi), A\right\rangle_F = 0$ for all $A \in \mathbb{F}^{n\times n}$, or likewise showing that $\left\langle(\Phi^\dagger\Phi)^2 - \frac{na}{d}(\Phi^\dagger\Phi), E_{ij}\right\rangle_F = 0$ for all i, j. We will look at two cases, first when $i = j$ and then when $i \neq j$.

$$\begin{aligned}
\left\langle(\Phi^\dagger\Phi)^2 - \frac{na}{d}\Phi^\dagger\Phi, E_{jj}\right\rangle_F &= \left\langle(\Phi^\dagger\Phi)^2, E_{jj}\right\rangle_F - \frac{na}{d}\left\langle\Phi^\dagger\Phi, E_{jj}\right\rangle_F \\
&= \operatorname{tr}((\Phi^\dagger\Phi)^2E_{jj}) - \frac{na}{d}\operatorname{tr}(\Phi^\dagger\Phi E_{jj}) \\
&= \sum_{k=1}^{n}\langle\varphi_j,\varphi_k\rangle\langle\varphi_k,\varphi_j\rangle - \frac{na}{d}\langle\varphi_j,\varphi_j\rangle \\
&= a^2 + (n-1)b - \frac{na^2}{d} \\
&= (n-1)b - \frac{(n-d)a^2}{d} = 0,
\end{aligned}$$

where the last equality follows from the assumption $(n-1)b = \frac{n-d}{d}a^2$. We also need to consider the elements E_{ij} where $i \neq j$, and assume that $b \neq 0$

$$\begin{aligned}
\left\langle(\Phi^\dagger\Phi)^2 - \frac{na}{d}\Phi^\dagger\Phi, E_{ij}\right\rangle_F &= \left\langle(\Phi^\dagger\Phi)^2, E_{ij}\right\rangle_F - \frac{na}{d}\left\langle\Phi^\dagger\Phi, E_{ij}\right\rangle_F \\
&= \operatorname{tr}((\Phi^\dagger\Phi)^2E_{ij}) - \frac{na}{d}\operatorname{tr}(\Phi^\dagger\Phi E_{ij}) \\
&= \sum_{k=1}^{n}\langle\varphi_j,\varphi_k\rangle\langle\varphi_k,\varphi_i\rangle - \frac{na}{d}\langle\varphi_j,\varphi_i\rangle \qquad (3.6) \\
&= \frac{1}{\langle\varphi_i,\varphi_j\rangle}\left(\sum_{k=1}^{n}\Delta(\varphi_j,\varphi_k,\varphi_i) - \frac{na}{d}b\right) \\
&= 0,
\end{aligned}$$

where the last equality follows from $\sum_{k=1}^{n} \Delta(\varphi_j, \varphi_k, \varphi_i) = \frac{nab}{d}$. Notice also that if $b = 0$, (3.6) would be 0, and so we would get the same result. This gives us $(\Phi^\dagger\Phi)^2 = \frac{na}{d}(\Phi^\dagger\Phi)$ as desired. And so by Theorem 3.4.7 we have that $\Phi : \mathbb{F}^n \to \operatorname{im}\Phi$ is an $(a, b, \frac{na}{d})$-ETF. □

Theorem 3.4.17. *Let $\Phi = (\varphi_j)_{j=1}^n$ be an (a, b)-equiangular system which is also a frame for a non-isotropic d-dimensional space V, such that* $\operatorname{char}\mathbb{F} \nmid d$ *and $\frac{na}{d} \neq 0$. Then $\Phi : \mathbb{F}^n \to V$ is an $(a, b, \frac{n}{d}a)$-ETF if and only if $(n-1)b = \frac{n-d}{d}a^2$ and $\sum_{\ell=1}^{n} \Delta(\varphi_j, \varphi_k, \varphi_\ell) = \frac{nab}{d}$ for all $j \neq k$ in $[n]$.*

Proof. In this case because Φ is a frame for V, $(\Phi^\dagger\Phi)^2 = \frac{na}{d}(\Phi^\dagger\Phi)$ would imply that Φ is also a $\frac{na}{d}$-tight frame. The proof is then nearly identical to Theorem 3.4.16 and so we have that $\Phi : \mathbb{F}^n \to V$ is an $(a, b, \frac{na}{d})$-ETF. □

Now we want to look at one consequence of Lemma 3.1.8 and (3.4) which was originally noted in Remark 2.15 in [GIJM22b].

Remark 3.4.18. Consider an (a, b, c)-ETF $\Phi = (\varphi_j)_{j=1}^n$ for a d dimensional space where $n > d$. If $b = 0$, then with the relation $a(c - a) = (n-1)b$ this must imply that either a or $c - a$ are zero. If a is zero, then the corresponding Gram matrix $G = 0$, which is not possible by Lemma 3.1.7, so a can not equal 0, when $b = 0$. Now we will consider the case where $c - a = 0$, or in other words $c = a \neq 0$. We also know that $na = dc$ which suggests that $n = d$. So when $n > d$ we can conclude that $b \neq 0$.

Two-graphs and ETFs in Orthogonal Geometries

Looking specifically at orthogonal geometries, we can determine many analogous combinatorial equivalent notions to tightness. The following is a corollary of Theorem 4.3 from [GIJM22b] which generalizes some of the results from [Sei76; Wal09].

Theorem 3.4.19. *Fix a prime $p > n$. Let Φ be an $(a, 1)$ equiangular system of n vectors which is also a frame for a d-dimensional orthogonal space V over the field $\mathbb{F}_{p^\ell}$ whose induced two-graph is non-trivial and $n > d$. Φ is an $(a, 1, c)$-ETF for V if and only if the induced two-graph is regular.*

Proof. Fix a prime $p > n$. Let $\Phi = (\varphi_j)_{j=1}^n$ be an $(a, 1)$-equiangular frame for $V = \mathbb{F}_{p^\ell}^d$.

($\Rightarrow$) Let Φ be an $(a, 1, c)$-ETF, then Φ is switching equivalent to some ETF Ψ such that

$$\Psi^\dagger \Psi = \begin{bmatrix} a & (1^{n-1})^\intercal \\ 1^{n-1} & aI_{n-1} + \overline{\Sigma} \end{bmatrix}$$

where 1^{n-1} is the all ones vector with $n - 1$ entries, and Σ is the adjacency matrix for G_{φ_1} with $v = n - 1$ vertices. From Theorem 4.3 of [GIJM22b] we know that Σ is the adjacency matrix of G_{φ_1} which is a $(n - 1, k, \lambda, \mu)$-SRG$_p$, with parameter chosen minimally, satisfying $k \equiv_p 2\mu$, $v \equiv_p 3k - 2\lambda - 1$ and that there exists some $\delta \in \mathbb{F}_{p^{\ell'}}$ such that $\delta^2 \equiv (\lambda - \mu)^2 + 4(k - \lambda)$.
Notice that if $\operatorname{char} \mathbb{F} = p > n$ we would have that G_{φ_1} is an $(n - 1, k, \lambda, \mu)$-SRG, and because $k - 2\mu \leq n - 2\mu \leq n < p$ we have that $k = 2\mu$. And so Φ induces a regular two-graph.

($\Leftarrow$) Assume that Φ is an $(a, 1)$-equiangular system of lines which induces a regular two-graph with parameters (n, ℓ, m) which satisfy $n = 3m - 2\ell$. Because the induced two-graph is regular there exists a vector φ_1, such that G_{φ_1} is strongly regular, meaning there is a switching equivalent system of equiangular lines Ψ where

$$\Psi^\dagger \Psi = \begin{bmatrix} a & (1^{n-1})^\intercal \\ 1^{n-1} & aI_{n-1} + \overline{\Sigma} \end{bmatrix}$$

such that Σ, as an integer matrix, is the adjacency matrix of G_{φ_1} which is a $(v := n - 1, k := m, \lambda := \ell, \mu := \frac{m}{2})$-SRG with $k = 2\mu$, $v = 3k - 2\lambda - 1$ and $(\lambda - \mu)^2 + 4(k - \lambda) = (\ell - \frac{m}{2})^2 + 4(m - \ell)$ being the square of an integer. This means that Theorem 4.3 from [GIJM22b] implies that Φ is a $(a, 1, c)$-ETF where c is a square root of $(\ell - \frac{m}{2})^2 + 4(m - \ell)$. □

We note that a similar result holds for $b \neq 1$, but requires passing to field extensions and rescaling.

Corollary 3.4.20. *Let Φ be a (a, b) equiangular system of n lines in a d-dimensional orthogonal space V over the field $\mathbb{F}_{p^\ell}$ where $p > n$, then Φ is an (a, b, c)-ETF for V only if n is even*

Proof. This follows from the fact that regular two-graphs have an even number of points [CL91].

□

3.5 Equiangular Cliques and Cocliques

Simplices: Equiangular Cliques

In this section and in Section 3.5 we generalize concepts like the binder [FJKM18], pillars [LS73], and incoherent sets [Gil18] by looking at collections of vectors whose triple products are equal. These correspond to the cliques and cocliques of two-graphs induced by equiangular systems of lines.

In this section we wish to study the minimal dependent subsets of frames and when they are themselves tight frames for their spans, and more specifically when they are ETFs. This has been studied for real and complex frames in [FJKM18].

Definition 3.5.1. A collection of $s+1$ vectors $\Phi = (\varphi_j)_{j=1}^{s+1}$ for s a positive integer is called a **regular s-simplex** if $\Phi : \mathbb{F}^{s+1} \to V$ is an (a, b, c')-ETF for an s-dimensional non-isotropic space V.

We use the notation c' with the prime as we will mainly explore when regular s-simplices are subsets of an (a, b, c)-ETF.

In this section we will assume any field $\mathbb{F} = \mathbb{F}_q$ is a finite field of case U or O where q is odd, as this will allow us to use Theorems 3.4.11 and 3.4.12 which will be necessary for the following analysis. We will also assume that $s > 1$, in which case $b \neq 0$ by Remark 3.4.18. Existence of simplices in certain dimensions depends only on the characteristic of the field.

Let $\Phi = (\varphi_j)_{j=1}^{s+1}$ be a regular s-simplex, an (a, b, c')-ETF for V, with $s > 1$; then, we know that $c' \neq 0$ from Lemma 3.1.8 as $s+1 < 2s$. This means there exists a Naimark complement $C : \mathbb{F}^{s+1} \to W$ where $W = \mathbb{F}$ is a 1-dimensional space and C is a $(c'-a, (c'-a)^2, c')$-ETF by Lemma 3.4.10 with $\operatorname{discr}(W) = (c')^{s+1} \operatorname{discr}(V)$.

The discriminant then determines the geometry and therefore the scalar product on $W = \mathbb{F}$. We will denote the scalar product on W as $x \cdot_m y := \langle x, y\rangle_{\mathbb{F}} = x^\sigma m y$ where we can choose $m = 1$ if and only if $\operatorname{discr}(W)$ is trivial. If the discriminant is non-trivial then m must be some non-square element of $\mathbb{F}_0$. This makes $\cdot_m$ an example of an isotopy. In case U, we may always assume that $m = 1$ up to isomorphism, and in case O we may assume that $x \cdot_m y = xym$ where $m \in \mathbb{F}_0$ is possible a non-square. Because $C = \{c_j\}_{j=1}^{s+1}$ is a collection of non-zero constants we have that $c_j \cdot_m c_j = c_j^\sigma m c_j = c' - a$, which is a square if and only if the discriminant of W is trivial. This means that $\operatorname{discr}(V) = (c' - a)(c')^{s+1}\mathbb{F}^{\times 2}$ which follows from Theorem 3.4.12. Likewise

$$b = (c_j \cdot_m c_k)(c_k \cdot_m c_j) = c_j^\sigma m c_k c_k^\sigma m c_j = c_j^\sigma m c_j c_k^\sigma m c_k = (c' - a)^2.$$

In this case we have that $(s + 1)(c' - a) = c'$ which rearranges to give $a = s(c' - a)$, meaning that $a = 0$ if and only if $\operatorname{char}\mathbb{F}$ divides s. We can also directly compute $c' = \sum_{j=1}^{s+1} c_j^\sigma m c_j = (s+1)(c'-a)$ meaning such a Naimark complement could only exist when $\operatorname{char}\mathbb{F}$ does not divide $s + 1$ as $c' \neq 0$. This proves the *only if* direction of the following lemma.

Lemma 3.5.2. (Example 2.16 in [GIJM22b]) Fix a finite field $\mathbb{F}$ (in Case O or U). A regular s-simplex $\Phi : \mathbb{F}^{s+1} \to V$ for some s-dimensional space V exists if and only if $\operatorname{char}\mathbb{F}$ does not divide $s + 1$.

Proof. All that remains is to prove the *if* direction. Assume that $\operatorname{char}\mathbb{F}$ does not divide $s + 1$ for some fixed integer s. In this case we can construct a collection of constants $C = (c_j)_{j=1}^{s+1}$ such that $a := c_j^\sigma c_j \neq 0$ and is equal for all j. This means C is an $(a, a^2, (s + 1)a)$-ETF. By construction $(s+1)a \neq 0$; so, there exists a Naimark complement which is an $((s+1)a - a, a^2, (s+1)a)$-ETF $\Phi : \mathbb{F}^{s+1} \to V$ where $\dim(V) = s$. Thus, there exists a regular s-simplex. □

Lemma 3.5.3. Let $\Phi = (\varphi_j)_{j=1}^{s+1}$ be a regular s-simplex for V an s dimensional space. Then the vectors are minimally dependent; i.e., they are dependent but any proper subset is independent.

We could prove the lemma using matroid theory, but we use the results from this paper.

Proof. By the work above, any simplex Φ has a Naimark complement Ψ which is a sequence of scalars with the same modulus. Applying $\operatorname{im}\Psi^\dagger = (\operatorname{im}\Phi^\dagger)^\perp$ from Lemma 3.4.10, we see that any linear combination of the columns of Φ that is equal to 0 has coefficients a scaling of the elements of Ψ. Thus, there is no way to make a linear combination with a non-empty strict subset of the $s+1$ vectors in Φ be equal to zero. □

Let $\Phi : \mathbb{F}^n \to W$ be an (a,b,c)-ETF for some d-dimensional space. We say a collection of $s+1$ vectors $\Phi|_\kappa := (\varphi_j)_{j\in\kappa}$ where $\kappa \subseteq [n]$ ($|\kappa| = s+1$) is a **sub-ETF** if it forms an (a,b,c')-ETF for $\operatorname{im}\Phi|_\kappa$. The existence of sub-ETFs in SICs are analyzed in [ABDF17; DBBA13] to make progress on solving Zauner's conjecture. Furthermore, if $\operatorname{im}\Phi|_\kappa$ is s-dimensional then we say Φ contains the regular s-simplex $\Phi|_\kappa := (\varphi_j)_\kappa$ in which case $b = (c'-a)^2$. Notice that because a and b are equal in the entire frame Φ and in any regular s-simplex, we have that $(s+1)a = sc'$ where $c' \neq 0$, and multiplying by n we get $(s+1)dc = nsc'$. Because a simplex is an ETF we also have that $a(c'-a) = sb$ and so by multiplying by s we get that $a^2 = s^2 b$.

Example 3.5.4. Consider the unitary geometry $V = \mathbb{F}_{5^2}^3$ where $\mathbb{F}_{5^2} = \mathbb{F}_5[\alpha]/(\alpha^2+\alpha+1)$ with the standard Hermitian scalar product. Consider the following frame for V:

$$\Phi = \begin{bmatrix} 1 & 1 & 1 & 4 & 4 & 4 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \alpha & \alpha^2 & 4 & 4\alpha & 4\alpha^2 \\ 4 & 4\alpha^2 & 4\alpha & 0 & 0 & 0 & 1 & \alpha^2 & \alpha \end{bmatrix},$$

where Φ is a $(2,1,1)$-ETF. Then Φ contains 12 regular 2-simplices which correspond to the Hesse configuration, which encodes the affine geometry of $\mathbb{F}_3^2$. There are no other simplices of any other size. Φ is a finite field analog of the Hesse SIC for $\mathbb{C}^3$ [Hug07].

Proposition 3.5.5. *Fix $s > 1$ Let $\Phi = (\varphi_j)_{j=1}^n$ be an (a,b,c)-ETF for V, a d-dimensional non-isotropic space. Φ contains a regular s-simplex $\Phi|_\kappa := (\varphi_j)_{j\in\kappa}$, an (a,b,c')-ETF for $\operatorname{im}\Phi|_\kappa$ only if $a^2 = s^2 b$. This equation is equivalent to $\frac{a^2}{b} = s^2$ and implies $(n-d)s^2 \equiv d(n-1)$.*

If $\operatorname{char}\mathbb{F}$ does not divide $sd(n-1)$ then $\frac{n-d}{d(n-1)} \equiv \frac{1}{s^2}$

Proof. We have already shown that if a regular s-simplex exists it would satisfy $\frac{a^2}{b} = s^2$. Notice that this in combination with the parameters of the original frame which satisfy $(n-d)a^2 = d(n-1)b$ would give us $(n-d)s^2 \equiv d(n-1)$. If $\operatorname{char}\mathbb{F}$ does not divide $sd(n-1)$ we can rearrange this to get $\frac{n-d}{d(n-1)} = \frac{1}{s^2}$. □

This also suggests that in the case where $a = 0$, which could only happen when $\operatorname{char}\mathbb{F}$ divides s, we would also have that $\operatorname{char}\mathbb{F}$ divides d or $n-1$.

ETFs with Respectable Characteristics

Throughout this section we will assume that $\operatorname{char}\mathbb{F} \nmid s$ and therefore any regular simplex would have $a \neq 0$. Let $\Phi = (\varphi_j)_{j=1}^n$ be an (a, b, c)-ETF for a d-dimensional non-isotropic space V, and assume that Φ contains a regular s-simplex $(\varphi_j)_{j\in\kappa}$. In this case we have $\frac{s+1}{s}a = c'$ and thus $c' - a = \frac{a}{s}$. From before we have $\operatorname{discr}(V) = (c'-a)(c')^{s+1}\mathbb{F}^{\times 2}$, which means if s is odd then $(c')^{s+1}$ is a square meaning $\operatorname{discr}(\operatorname{im}\Phi|_\kappa) = \frac{a}{s}\mathbb{F}^{\times 2}$. If s is even then $(c')^{s+1}$ is a square if and only if c' is. Meaning $\operatorname{discr}(\operatorname{im}\Phi|_\kappa) = (s+1)\mathbb{F}^{\times 2}$. More generally,

$$\operatorname{discr}(\operatorname{im}\Phi|_\kappa) = \left(\frac{a}{s}\right)^s (s+1)^{s+1}\mathbb{F}^{\times 2}.$$

Over characteristic zero, saturating the Welch bound is sufficient to be an ETF. We showed in Theorem 3.4.16 that the critical additional information needed over positive characteristic involves sums of triple products. We have a similar result for when an ETF contains a regular s-simplex, which may be seen as a corollary to Theorem 3.4.16.

Corollary 3.5.6. *Consider a field $\mathbb{F}$ such that $\operatorname{char}\mathbb{F} > s+1$. Let $\Phi = (\varphi_j)_{j=1}^n$ be an (a, b, c)-ETF for a d-dimensional non-isotropic space V. Φ contains a regular s-simplex $\Phi|_\kappa := (\varphi_j)_{j\in\kappa}$ if and only if $|\kappa| = s+1$, $a^2 = s^2 b$, $\dim(\operatorname{im}\Phi|_\kappa) = s$ and*

$$\sum_{\ell\in\kappa} \Delta(\varphi_j, \varphi_k, \varphi_\ell) = \frac{(s+1)ab}{s} = \frac{(s+1)a^3}{s^3} \tag{3.7}$$

for all $j \neq k$ in κ

Proof. ($\Rightarrow$) First, we assume that Φ contains a regular s-simplex $\Phi|_\kappa := (\varphi_j)_{j\in\kappa}$. From the work above we know that $|\kappa| = s+1$ where $a^2 = s^2 b$, and $\dim(\operatorname{im}\Phi|_\kappa) = s$. Likewise because $(\varphi_j)_{j\in\kappa}$ is an $(a, b, \frac{s+1}{s}a)$-ETF we know that

$$\sum_{\ell\in\kappa} \Delta(\varphi_j, \varphi_k, \varphi_\ell) = \frac{(s+1)ab}{s}$$

for all $j \neq k$ in κ.

($\Leftarrow$) Now consider a sub-collection of vectors $\Phi|_\kappa = (\varphi_j)_{j\in\kappa}$ where $|\kappa| = s+1$, $a^2 = s^2 b$, $\dim(\operatorname{im}\Phi|_\kappa) = s$, and (3.7) is satisfied. Then by Theorem 3.4.16 we have that $(\varphi_j)_{j\in\kappa}$ is an ETF and therefore a regular s-simplex □

We note that a similar corollary follows from Theorem 3.4.17. Let $\Phi = (\varphi_j)_{j=1}^{s+1}$ be a regular s-simplex, an (a, b, c')-ETF, with $s > 1$. As before we have a Naimark complement $C : \mathbb{F}^{s+1} \to \mathbb{F}$, a $(c'-a, (c'-a)^2, c')$-ETF. Because C is a collection of constants we have that that the triple products of C satisfy

$$(c_j \cdot_m c_k)(c_k \cdot_m c_\ell)(c_\ell \cdot_m c_j) = c_j^\sigma m c_k c_k^\sigma m c_\ell c_\ell^\sigma m c_j = c_j^\sigma m c_j c_k^\sigma m c_k c_\ell^\sigma m c_\ell = (c'-a)^3.$$

Likewise, because $\Phi^\dagger\Phi = c'I - C^\dagger C$ we know that $\langle\varphi_j, \varphi_k\rangle = -(c_j \cdot_m c_k)$ for $j \neq k$ and $\langle\varphi_j, \varphi_j\rangle = c' - (c_j \cdot_m c_j) = c' - (c'-a) = a$. Putting these together we can see that for distinct j, k, ℓ we have

$$\Delta(\varphi_j, \varphi_k, \varphi_\ell) = -(c'-a)^3$$

where $c' - a \neq 0$. If $\operatorname{char}\mathbb{F}$ does not divide s we know that Φ is an $(a, b, \frac{s+1}{s}a)$-ETF where $-(c'-a)^3 = -\left(\frac{s+1}{s}a - a\right)^3 = -\frac{a^3}{s^3}$. So if an ETF contains a regular s-simplex, then the triple products of distinct vectors of the simplex would all be equal to $-(c'-a)^3 = -\frac{a^3}{s^3}$. Similar to the real and complex cases, shown by [FJKM18], we will see that simplices are more or less determined by their triple products all being equal in this way, with a few annoying caveats.

Theorem 3.5.7. *Let $\Phi = (\varphi_j)_{j=1}^n$ be an (a,b,c)-ETF for d-dimensional space V over the field $\mathbb{F}_q$, such that $d < n$ and $\operatorname{char}\mathbb{F}_q$ does not divide $s(s+1)$. Then $\kappa \subseteq [n]$ of size $s+1$ gives a regular s-simplex $(\varphi_j)_{j\in\kappa}$ if and only if $a^2 = s^2 b$,*

$$\Delta(\varphi_j, \varphi_k, \varphi_\ell) = -\frac{a^3}{s^3} \neq 0$$

for all distinct $j, k, \ell \in \kappa$, and

$$\sum_{j\in\kappa} \Delta(\varphi_\ell, \varphi_k, \varphi_j) = \frac{s+1}{s} ab$$

for a fixed $\ell \in \kappa$ and all $k \notin \kappa$.

Proof. We have already shown most of the ($\Rightarrow$) direction; so, we will only show the ($\Leftarrow$) direction. Assume that $\Delta(\varphi_j, \varphi_k, \varphi_\ell) = -\frac{a^3}{s^3} \neq 0$ for all distinct $j, k, \ell \in \kappa$. Pick $\alpha \in \mathbb{F}_q^\times$ and $m \in \mathbb{F}_0^\times$ such that $\alpha^\sigma m \alpha = \frac{a}{s}$. Notice that m would be a square depending on if $\frac{a}{s}$ is, and if $\frac{a}{s}$ was a square then we could assume that $m = 1$, otherwise m would be a non-square. Fix some $\ell \in \kappa$ and define $C = \{c_j\}_{j\in\kappa}$ such that $c_\ell = \alpha$ and $c_j = \frac{-1}{m\alpha^\sigma} \langle \varphi_\ell, \varphi_j \rangle$ for all $j \neq \ell$. Notice that

$$c_j^\sigma m c_j = \left\{\begin{matrix} (-1)^2 \frac{s}{a} \langle \varphi_j, \varphi_\ell \rangle \langle \varphi_\ell, \varphi_j \rangle & \text{if } j \neq \ell \\ \alpha^\sigma m \alpha & \text{if } j = \ell \end{matrix}\right\} = \frac{a}{s}$$

and likewise for $j \neq k$

$$c_j^\sigma m c_k = \left\{\begin{matrix} -\langle \varphi_\ell, \varphi_k \rangle & \text{if } j = \ell \\ -\langle \varphi_j, \varphi_\ell \rangle & \text{if } k = \ell \\ \frac{s}{a} \langle \varphi_j, \varphi_\ell \rangle \langle \varphi_\ell, \varphi_k \rangle & \text{otherwise} \end{matrix}\right\} = -\langle \varphi_j, \varphi_k \rangle,$$

where the last line follows from $-\frac{s}{a}\left\langle\varphi_j,\varphi_\ell\right\rangle\left\langle\varphi_\ell,\varphi_k\right\rangle\left\langle\varphi_k,\varphi_j\right\rangle=\frac{a^2}{s^2}=b$. This shows us that

$$\Phi|_\kappa^\dagger\Phi|_\kappa=\frac{s+1}{s}aI-C^\dagger C.$$

Because C is a sequence of constants it is trivially an $(\frac{a}{s},b,\frac{s+1}{s}a)$-ETF, meaning $C^\dagger C$ has one non-zero eigenvalue equal to $\frac{s+1}{s}a$, with corresponding eigenvector $C^\dagger$. From this we can determine that the $\operatorname{rank}(\Phi|_\kappa^\dagger\Phi|_\kappa)=s$. We want to show that $\Phi|_\kappa$ is a Naimark complement of C and so we need to show that $\Phi|_\kappa C^\dagger=0$. We being by computing

$$\Phi|_\kappa C^\dagger=\sum_{j\in\kappa}c_j^\sigma m\varphi_j=\sum_{j\in\kappa}c_j^\sigma mc_\ell\varphi_j,$$

and we will show that $\sum_{j\in\kappa}c_j^\sigma mc_\ell\varphi_j=0$ using the non-degeneracy of $V=\operatorname{im}(\Phi)$. So consider a vector $\varphi_k\in\Phi$ and compute

$$\begin{aligned}\left\langle\varphi_k,\sum_{j\in\kappa}c_j^\sigma mc_\ell\varphi_j\right\rangle&=\sum_{j\in\kappa}c_j^\sigma mc_\ell\left\langle\varphi_k,\varphi_j\right\rangle\\&=c_\ell^\sigma mc_\ell\left\langle\varphi_k,\varphi_\ell\right\rangle-\sum_{j\neq\ell}\left\langle\varphi_k,\varphi_j\right\rangle\left\langle\varphi_j,\varphi_\ell\right\rangle.\end{aligned}$$

This expression is zero if and only if the following is zero

$$\begin{aligned}c_\ell^\sigma mc_\ell\left\langle\varphi_\ell,\varphi_k\right\rangle\left\langle\varphi_k,\varphi_\ell\right\rangle-\sum_{j\neq\ell}\left\langle\varphi_\ell,\varphi_k\right\rangle\left\langle\varphi_k,\varphi_j\right\rangle\left\langle\varphi_j,\varphi_\ell\right\rangle&=\frac{ab}{s}-\sum_{j\neq\ell}\Delta(\varphi_\ell,\varphi_k,\varphi_j)\\&=\frac{ab}{s}-\sum_{j\in\kappa}\Delta(\varphi_\ell,\varphi_k,\varphi_j)+ab\\&=0,\end{aligned}$$

which follows from the initial assumption. □

ETFs with Defiant Characteristics

Now we want to explore the possibility of the characteristic dividing s, which leads to some very different behavior. Consider an (a, b, c)-ETF which contains a regular s-simplex, $\Phi|_\kappa$ which is an (a, b, c')-ETF, which means $\operatorname{char}\mathbb{F} \nmid s+1$. If $\operatorname{char}\mathbb{F}|s$, then we would have $a = 0$ and $b \neq 0$, and so $na = dc$ implies that $c = 0$ or $\operatorname{char}\mathbb{F}|d$. Likewise from $a(c-a) = (n-1)b$ we know that $\operatorname{char}\mathbb{F}|(n-1)$ as $b \neq 0$. Looking at the discriminant we know that

$$\operatorname{discr}(\operatorname{im}\Phi|_\kappa) = (c'-a)(c')^{s+1}\mathbb{F}^{\times 2} = (c')^{s+2}\mathbb{F}^{\times 2} = (c')^{s}\mathbb{F}^{\times 2}.$$

We note c' is intrinsic to the simplex and not the entire frame, meaning it is possible to have an ETF with multiple simplices which have different geometries.

Example 3.5.8. Consider the orthogonal geometry on $\mathbb{F}_3^4$ with the scalar product whose Gram matrix is $\operatorname{diag}(1, 1, 1, 2)$. Notice that $-1 \equiv 2$ is not a square in $\mathbb{F}_3$ so this is an example of an orthogonal geometry that is not the real model. Now consider the frame for $\mathbb{F}_3^4$:

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 \\ 1 & 2 & 1 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \end{bmatrix},$$

where Φ is an $(0, 1, 0)$-ETF of $n = 10$ vectors.

Let $\kappa = \{1, 2, 3, 4\}$. Then $\Phi|_\kappa$ forms a regular 3-simplex which is an $(0, 1, 2)$-ETF with $\operatorname{discr}(\operatorname{im}\Phi|_\kappa) = 2\mathbb{F}^{\times 2}$. Now let $\overline{\kappa} = \{7, 8, 9, 10\}$. Then $\Phi|_{\overline{\kappa}}$ also forms a regular 3-simplex, but this one is a $(0, 1, 1)$-ETF in the real model where $\operatorname{discr}(\operatorname{im}\Phi|_\kappa) = \mathbb{F}^{\times 2}$. In fact there are 30 regular 3-simplices, 15 of which are in the real model and the other 15 which have a non-square discriminant. The 15 simplices which are in the real model, whose indices are shown in (3.8), form a 2-$(10, 4, 2)$ design,

$$\begin{aligned}&\{\{1,2,7,8\},\{1,2,9,10\},\{1,3,5,7\},\{1,3,6,10\},\{1,4,5,9\},\\ &\{1,4,6,8\},\{2,3,5,8\},\{2,3,6,9\},\{2,4,5,10\},\{2,4,6,7\},\\ &\{3,4,7,9\},\{3,4,8,10\},\{5,6,7,10\},\{5,6,8,9\},\{7,8,9,10\}\}\end{aligned} \tag{3.8}$$

Likewise the 15 simplices with non-square discriminant also form a 2-$(10, 4, 2)$ design, whose blocks are shown in (3.9).

$$\begin{aligned}&\{\{1,2,3,4\},\{1,2,5,6\},\{1,3,8,9\},\{1,4,7,10\},\{1,5,8,10\},\\ &\{1,6,7,9\},\{2,3,7,10\},\{2,4,8,9\},\{2,5,7,9\},\{2,6,8,10\},\\ &\{3,4,5,6\},\{3,5,9,10\},\{3,6,7,8\},\{4,5,7,8\},\{4,6,9,10\}\}\end{aligned} \tag{3.9}$$

The Incoherence of a Finite Reality: Equiangular Cocliques

In this section we draw connections between ETFs in orthogonal geometries with real ETFs. There are no real ETFs of $n = 10$ vectors in $\mathbb{R}^4$; however, there is a an ETF of $n = 10$ vectors in an orthogonal geometry on $\mathbb{F}_3^4$ (cf. Example 3.5.8). In this example we also know that in the field extension $\mathbb{F}_{3^2} = \mathbb{F}[x]/(x^2+1)$, 2 becomes a square; so, the orthogonal geometry over $\mathbb{F}_{3^2}^4$ has a square discriminant. In fact, [GIJM22b] showed that there are infinity many dimensions where maximal ETFs over orthogonal geometries are known but it is conjectured, and in some cases it is known that such ETFs don't exist as real ETFs. The requirement that $p > 2n-5$, in Theorem 3.2.12 was not known to be tight, and in the remainder of this section we wish to look at the cases where $d < p < 2n-5$, drawing parallels to the real word.

Here we will continue to explore orthogonal geometries drawing connections to what is known over $\mathbb{R}$. In [Gil18], Gillespie showed that equiangular lines in $\mathbb{R}^d$ with $n = d(d+1)/2$ vectors which saturate the incoherence bound exist if and only if $d = 2, 3, 7, 23$. This gives further evidence that those dimensions are the only dimensions in which there is an ETF of any type with $n = d(d+$

$1)/2$ vectors in $\mathbb{R}^d$, which is the Gillespie conjecture. In this section we wish to complete a similar treatment of equiangular lines which saturate an analogous bound for orthogonal geometries.

Definition 3.5.9. Let Φ be an (a, b)-equiangular system of vectors in a orthogonal geometry V, and fix some β such that $\beta^2 = b$. The set of vectors Φ is β-**incoherent** if $|\Phi| \leq 2$ or $\Delta(\varphi_j, \varphi_k, \varphi_\ell) = \beta^3$ for all distinct j, k, ℓ. We define the β-incoherence number $\mathrm{Inc}_\beta(\Phi)$ to be the size of the largest subset of β-incoherent vectors in Φ. Likewise, Φ is β-**coherent** if $|\Phi| \geq 3$ and $\Delta(\varphi_j, \varphi_k, \varphi_\ell) = -\beta^3$

We note that the choice of β will affect the incoherence number, which we highlight in the following example. Over $\mathbb{R}$, β is chosen to be positive, and incoherent sets are linearly independent. In the finite field setting we will pick β, when possible, so that incoherent sets are linearly independent as well.

Example 3.5.10. Consider $\mathbb{F}_{11}^2$ in the real model with the standard dot product and define

$$\Phi = \begin{bmatrix} 0 & 3 & 8 \\ 1 & 5 & 5 \end{bmatrix} \quad \text{and} \quad \Phi^\dagger \Phi = \begin{bmatrix} 1 & 5 & 5 \\ 5 & 1 & 5 \\ 5 & 5 & 1 \end{bmatrix}.$$

Φ is a $(1, 3, 7)$-ETF. Notice that $5^2 = 3$ and that all three vectors of Φ are a 5-incoherent set as $\Delta(\varphi_1, \varphi_2, \varphi_3) = 5^3 = 4$. However notice also that $6^2 = 3$, But Φ is not a 6-incoherent set. So $\mathrm{Inc}_5(\Phi) = 3$ and $\mathrm{Inc}_6(\Phi) = 2$.

Remark 3.5.11. Assume that Φ is an (a, b)-equiangular system of lines which is also a β-incoherent set. We can construct a second system of n equiangular lines Ψ which is switching equivalent to Φ. First let $\psi_1 = \varphi_1$. Then for each $1 < j \leq n$, let $\psi_j = \varphi_j$ if $\langle \varphi_1, \varphi_j \rangle = \beta$ and let $\psi_j = -\varphi_j$ otherwise. By construction $\Psi = (\psi_j)_{j=1}^n$ is switching equivalent to Φ. Because $\langle \varphi_j, \varphi_k \rangle \langle \varphi_k, \varphi_\ell \rangle \langle \varphi_\ell, \varphi_j \rangle = \beta^3$ for all distinct j, k, ℓ, we know that $\langle \psi_j, \psi_k \rangle \langle \psi_k, \psi_\ell \rangle \langle \psi_\ell, \psi_j \rangle = \beta^3$; so, Ψ is also an incoherent set. Notice also that because $\langle \psi_1, \psi_j \rangle = \beta$ for all $j > 1$ and $\langle \psi_j, \psi_k \rangle \langle \psi_k, \psi_1 \rangle \langle \psi_1, \psi_j \rangle = \beta^3$ we know that $\langle \psi_j, \psi_k \rangle = \beta$ for all distinct j, k. This shows that

Ψ is not only an incoherent set but $\langle \varphi_j, \varphi_k \rangle = \beta$ for all distinct j, k. We will regularly make the assumption that incoherent sets have all scalar products being equal, which is always possible up to switching equivalence.

The definition of incoherent sets comes from the definition of an incoherent set of a two-graph from Section 3.3. Let Φ be an (a, b)-equiangular system of lines, then the coherent triples, with respect to a choice of β are the triples of vectors whose triple products are equal to $-\beta^3$.

Lemma 3.5.12. Let Φ be an (a, b)-equiangular system of lines in a d-dimensional non-isotropic orthogonal space V such that there exists a non-zero $\beta \in \mathbb{F}$ where $\beta^2 = b$, $a \neq \beta$, and Φ is β-incoherent. The vectors of Φ are linearly independent or a minimally dependent set; therefore, $|\Phi| \leq d + 1$.
When $|\Phi| = d + 1$ and $\operatorname{char} \mathbb{F} \nmid d(d-1)$, then $a + d\beta = 0$ and Φ is a regular d-simplex if $a \neq 0$. Furthermore if $\operatorname{char} \mathbb{F} \nmid d(d-1)$ with $a \neq 0$ and $\beta \neq -\frac{a}{d-1}$ then if $|\Phi| = d$ the vectors of Φ are linearly independent. If the parameters also satisfy $\beta^3 \neq -\frac{a^3}{d^3}$ then $|\Phi| \leq d$.

Proof. Assume that $|\Phi| = n$. We will construct a second system of n equiangular lines Ψ which is switching equivalent to Φ as in Remark 3.5.11. In this case, the Gram matrix is $G = \Psi^\dagger \Psi = \beta J + (a - \beta) I$ where J is the all-ones matrix. Notice that the all-ones vector $\mathbb{1}$ is an eigenvector with eigenvalue $a + (n-1)\beta$. Likewise we can consider the vectors whose entries sum to zero, which is an eigenspace of dimension $n - 1$, with eigenvalue $a - \beta \neq 0$ by the initial assumptions. Notice that $\mathbb{1}$ is in the eigenspace of vectors whose entires sum to zero if and only if $\operatorname{char} \mathbb{F}$ divides n. In which case the $\dim(\ker \Psi) \leq \dim(\ker \Psi^\dagger \Psi) \leq 1$. If $\operatorname{char} \mathbb{F}$ does not divide n, then we have a basis for the domain of G in terms of the eigenvectors. This means that $\ker \Psi \leq \ker \Psi^\dagger \Psi \leq \operatorname{span}\{\mathbb{1}\}$ with $\ker \Psi^\dagger \Psi = \operatorname{span}\{\mathbb{1}\}$ if and only if $a + (n-1)\beta = 0$. This means that the vectors of Ψ and therefore the vectors of Φ are linearly independent or form a minimally dependent set when $a + (n-1)\beta = 0$.

Now we wish to explore the maximal case. Assume that $n = d + 1$, which would mean that $a + (n-1)\beta = a + d\beta = 0$. This also means that $a^2 = d^2 b$, and Ψ is a frame for V. Assume that

$\operatorname{char}\mathbb{F}$ neither divides $d = n-1$ nor $d+1 = n$ in which case $\frac{1}{d}a^2 = db$. Likewise for any distinct j, k we have that

$$\sum_{\ell=1}^{n} \Delta(\varphi_j, \varphi_k, \varphi_\ell) = (n-2)\beta^3 + 2ab = (d-1)\beta^3 + -2d\beta^3 = -(d+1)\beta^3 = \frac{d+1}{d}ab.$$

This means that Ψ is an ETF, in particular a regular d-simplex by Theorem 3.4.17 if $a \neq 0$.

To prove the last claim we will first assume that $\operatorname{char}\mathbb{F} \nmid d(d-1)$ and $a \neq 0$. Consider the case where $n = d$ in which case we need only show that $a + (n-1)\beta \neq 0$. Notice that this is equivalent to $\beta \neq -\frac{a}{n-1}$. In this case if $n = d+1$, we would have that Φ is a regular d-simplex from above, but by Theorem 3.5.7, we would have that all triple products would equal $-\frac{a^3}{d^3}$ contradicting out assumption that all triple products equal $\beta^3 \neq -\frac{a^3}{d^3}$. Thus, $n \leq d$. □

A field $\mathbb{F}_q$ with characteristic p has a non-trivial third root of unity when $x^2 + x + 1$ has non trivial roots since $x^3 - 1 = (x-1)(x^2+x+1)$. This is the case when $p \equiv 1 \pmod 3$ or $q = p^{2\ell}$.

As a corollary of Lemma 3.5.12, incoherent sets which are minimally dependent sets are simplices, and can be often easily ruled out.

Corollary 3.5.13. *Let Φ be an (a,b)-equiangular system of n lines in a d-dimensional non-isotropic orthogonal space V where $a \neq 0$ and $a^2 \neq b$. Further let $\beta \in \mathbb{F}$ where $\beta^2 = b \neq 0$. If $\operatorname{char}\mathbb{F} \nmid d$ then*

$$\min(\operatorname{Inc}_\beta(\Phi), \operatorname{Inc}_{-\beta}(\Phi)) \leq d \tag{3.10}$$

Furthermore if $\operatorname{char}\mathbb{F} \nmid (d-1)$ and for β such that $\operatorname{Inc}_\beta(\Phi) = d = \min(\operatorname{Inc}_\beta(\Phi), \operatorname{Inc}_{-\beta}(\Phi))$, then any maximal incoherent set Γ is linearly independent.

Proof. We know that $\operatorname{Inc}_\beta(\Phi) \leq d+1$ and $\operatorname{Inc}_{-\beta}(\Phi) \leq d+1$. We will assume that the first bound is saturated in which case let Γ be $d+1$ vectors of Φ which are β-incoherent. In this case we have that $a + d\beta = 0$, so $a = -d\beta$. If the second bound is saturated there would be a collection of $d+1$ vectors Γ' which are $-\beta$-incoherent. In this case we have that $a - d\beta = 0$, so $a = d\beta$. For

$a = d\beta = -d\beta$ we would need that $a = 0$ which happens if and only if $\operatorname{char}\mathbb{F}$ is 2 or divides d. But from our assumptions, neither is the case. So both bounds cannot be saturated.

Now assume that $\operatorname{char}\mathbb{F} \nmid (d-1)$, $\operatorname{Inc}_\beta(\Phi) = d = \min(\operatorname{Inc}_\beta(\Phi), \operatorname{Inc}_{-\beta}(\Phi))$, and Γ is a maximal β-incoherent set. There are two cases to consider here. First, if $\operatorname{Inc}_{-\beta}(\Phi) = d+1$, then the maximal $-\beta$-incoherent set is a regular d-simplex, meaning $\beta = \frac{a}{d} \neq -\frac{a}{d}$. So, the vectors of Γ are linearly independent. Now assume that $\operatorname{Inc}_\beta(\Phi) = d = \operatorname{Inc}_{-\beta}(\Phi)$. In this case, assume that Γ is a maximal β-incoherent set and Γ' is a maximal $-\beta$-incoherent set, which is also a minimally dependent set. This means that $a-(d-1)\beta = 0$ and therefore $\beta = \frac{a}{d-1} \neq -\frac{a}{d-1}$; so, Γ must be linearly independent. □

We note that the bound in (3.10) does not guarantee linear independence in general when either $\operatorname{Inc}_\beta(\Phi) = d$, or $\operatorname{Inc}_{-\beta}(\Phi) = d$ as highlighted in the following example.

Example 3.5.14. Consider again Example 3.5.8:

$$\Phi = \begin{bmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 2 & 1 & 0 & 0 & 1 & 1 & 2 & 2 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 2 & 1 & 2 \\ 1 & 2 & 2 & 2 & 1 & 2 & 0 & 0 & 0 & 0 \end{bmatrix},$$

where Φ is a $(0,1,0)$-ETF of $n = 10$ vectors for an orthogonal geometry on $\mathbb{F}_3^4$. Computationally we can determine that the first 4 vectors form a maximal set of 1-incoherent vectors. And likewise the last 4 vectors form a maximal -1-incoherence set; however, neither are linearly independent.

Let $\Phi : \mathbb{F}^n \to V$ be an (a,b)-equiangular system of lines in a d-dimension orthogonal space V where $\operatorname{char}\mathbb{F} \nmid d(d-1)$, $a^2 \neq b$ and $a \neq 0$. We will call the bound from (3.10) the **incoherence bound**, and we will denote $\operatorname{Inc}(\Phi) := \min(\operatorname{Inc}_\beta(\Phi), \operatorname{Inc}_{-\beta}(\Phi))$

For the remainder of this section we will be interested in systems of lines with maximal incoherent sets which are also linearly independent. Corollary 3.5.13 guarantees that when the incoherence bound is saturated there exists some β such that if Γ is a maximal β-incoherent set, then Γ is linearly independent.

If Γ is a maximal incoherent subset then by definition for any vector γ not in Γ there exists $\alpha_1, \alpha_2 \in \Gamma$ where $\{\gamma, \alpha_1, \alpha_2\}$ is a coherent triple. We will define two sets

$$\Gamma_i(\gamma) = \{\, \delta \in \Gamma \mid \{\gamma, \alpha_i, \delta\} \text{ is coherent} \,\}$$

for $i = 1, 2$. With Remark 3.5.11 we can assume that this implies that $\langle \gamma, \alpha_1 \rangle = \pm\beta$ and $\langle \gamma, \alpha_1 \rangle = \mp\beta$ and the two sets above can be equivalently defined as

$$\Gamma_1(\gamma) = \{\, \delta \in \Gamma \mid \langle \gamma, \delta \rangle = -\langle \gamma, \alpha_1 \rangle \,\} \quad \text{and} \quad \Gamma_2(\gamma) = \{\, \delta \in \Gamma \mid \langle \gamma, \delta \rangle = -\langle \gamma, \alpha_2 \rangle \,\},$$

or in other words, $\Gamma_1(\gamma)$ and $\Gamma_2(\gamma)$ partition Γ based on the scalar products of elements in Γ with γ, being $\pm\beta$, which are independent of the choice of α_1 and α_2. By convention we label the sets such that $|\Gamma_1(\gamma)| \leq |\Gamma_2(\gamma)|$.

The following three lemmas are generalizations of Theorem 5.4, Theorem 5.6, and a remark in [Tay77] which are used heavily in [Gil18].

Lemma 3.5.15. Let Φ be an (a, b)-equiangular system of n lines in a d-dimensional orthogonal geometry V such that $a^2 \neq b$ and $a \neq 0$. Assume there exists $\Gamma \subseteq \Phi$ that is a maximal β-incoherent set ($|\Gamma| = d$) that is also linearly independent. Then for every γ not in Γ, we have that $|\Gamma_1(\gamma)|$ and $|\Gamma_2(\gamma)|$ are roots of the following equation

$$4x^2 - 4dx + (\rho - 1)^2(d + \rho) \equiv 0$$

where $\rho = a\beta^{-1}$. Furthermore when $\operatorname{char} \mathbb{F} > d$, the smallest integers which are roots are $|\Gamma_1(\gamma)|$ and $|\Gamma_2(\gamma)|$.

Proof. We know that the vectors of Γ for a basis for V; denote them $\varphi_1, \dots, \varphi_d$ and consider the vector $\gamma \notin \Gamma$. As in the proof of Lemma 3.5.12 we may pick a switching equivalent set of vectors $\{\psi_j\}_{j=1}^d$ which are a basis and have pairwise scalar products equal to β by Remark 3.5.11.

We will reorder the vectors of $(\psi_j)_{j=1}^d$, and rescale γ by -1 such that $\varphi_j \in \Gamma_1(\gamma)$ and $\langle \gamma, \psi_j \rangle = \beta$ for $1 \leq j \leq |\Gamma_1(\gamma)| =: r$ and likewise for $\varphi_j \in \Gamma_2(\gamma)$ and $\langle \gamma, \psi_j \rangle = -\beta$ for $r < j \leq d$. Because the vectors $(\psi_j)_{j=1}^d$ are a basis we can write $\gamma = \sum_{j=1}^d b_j \psi_j$. Notice that for $k \leq r$ we have that

$$\langle \gamma, \psi_k \rangle = \sum_{j=1}^d b_j \langle \psi_k, \psi_j \rangle = \sum_{j=1, j\neq k}^d b_j \beta + b_k a = \beta$$

and for $r < k \leq d$

$$\langle \gamma, \psi_k \rangle = \sum_{j=1}^d b_j \langle \psi_k, \psi_j \rangle = \sum_{j=1, j\neq k}^d b_j \beta + b_k a = -\beta.$$

This gives us a system of linear equations, and solving for the b_j's we get

$$b_j = \begin{cases} \dfrac{a\beta + (2d-2r-1)b}{(a+(d-1)\beta)(a-\beta)} \\ \dfrac{(1-2r)b - a\beta}{(a+(d-1)\beta)(a-\beta)} \end{cases} = \begin{cases} \dfrac{2d-2r+\rho-1}{(d+\rho-1)(\rho-1)} & 1 \leq j \leq r \\ -\dfrac{2r+\rho-1}{(d+\rho-1)(\rho-1)} & 1 < j \leq d \end{cases} \tag{3.11}$$

where $\rho = a\beta^{-1}$. We note that under our assumptions $a + (d-1)\beta \not\equiv 0$ and $a - \beta \not\equiv 0$, and so b_j always exists. The rest of the proof follows from the proof in [Tay77]; by expanding we get

$$a = \langle \gamma, \gamma \rangle = \sum_{k=1}^d b_k \langle \gamma, \psi_k \rangle = r b_1 \beta + (r-d) b_d \beta.$$

Then plugging in for b_1 and b_d we get $4r^2 - 4dr + (\rho-1)^2(d+\rho) \equiv 0$, of which r and $d-r$ are roots. □

The next result generalizes Theorem 5.6 of [Tay77], whose proof works in the finite field setting as well.

Lemma 3.5.16. Let Φ be an (a, b)-equiangular system of n lines in a d-dimensional orthogonal geometry V such that $a^2 \neq b$ and $a \neq 0$. Assume there exists $\Gamma \subseteq \Phi$ that is a maximal β-incoherent set ($|\Gamma| = d$) that is also linearly independent. Then for distinct γ and δ not in Γ

$$|\Gamma_1(\gamma) \cap \Gamma_1(\delta)| \equiv |\Gamma_1(\gamma)| - \Delta \tag{3.12}$$

where Δ is either $(\rho - 1)^2/4$ or $(\rho^2 - 1)/4$ and $\rho = a\beta^{-1}$ Furthermore when $\operatorname{char} \mathbb{F} > d$ then $|\Gamma_1(\gamma) \cap \Gamma_1(\delta)|$ is the smallest integer which satisfies (3.12).

Proof. Under the same set up as in Lemma 3.5.15 we will fix two distinct elements $\gamma, \delta \notin \Gamma$ and let $(\psi_j)_{j=1}^{d}$ be switching equivalent to the vectors of Γ such that every pairwise scalar product is β, and we will assume that the vectors are rearranged such that

$$\begin{aligned}\gamma &= \sum_{1\leq j\leq r} b_1\psi_j + \sum_{r<j\leq d} b_d\psi_j \quad \text{and} \\ \delta &= \sum_{1\leq j\leq s} b_1\psi_j + \sum_{s<j\leq r} b_d\psi_j + \sum_{r<j\leq t} b_1\psi_j + \sum_{t<j\leq d} b_d\psi_j.\end{aligned}$$

Notice that due to Lemma 3.5.15 we have that $s + (t - r) \equiv r$ as the size of $\Gamma_1(\gamma)$ is equivalent for all γ, meaning $t \equiv 2r - s$. Similarly, the size of the intersection $|\Gamma_1(\gamma) \cap \Gamma_1(\delta)| = s$ Notice that using the above basis we can determine that

$$\begin{aligned}\langle\gamma, \delta\rangle &= \sum_{1\leq j\leq s} b_1 \langle\gamma, \psi_j\rangle + \sum_{s<j\leq r} b_d \langle\gamma, \psi_j\rangle + \sum_{r<j\leq t} b_1 \langle\gamma, \psi_j\rangle + \sum_{t<j\leq d} b_d \langle\gamma, \psi_j\rangle \\ &= sb_1\beta + (r - s)b_d\beta - (r - s)b_1\beta - (d - (2r - s))b_d\beta \\ &= (2s - r)b_1\beta + (3r - 2s - d)b_d\beta.\end{aligned}$$

Let $\epsilon = \beta^{-1}\langle\gamma, \delta\rangle = \pm 1$. Expanding this and using Lemma 3.5.15 by plugging in for $r^2 = dr - \frac{1}{4}(\rho - 1)^2(d + \rho)$ and the values for b_1 and and b_j from (3.11), we get $s \equiv r + \frac{1}{4}(\rho - 1)(\epsilon - \rho)$ which proves the statement for each choice of ϵ. □

The following result was shown by [Tay77], and the proof uses only that Φ forms a regular two-graph and not any properties of the underlying system of lines.

Lemma 3.5.17. Let Φ be an (a, b)-equiangular system of n lines in a d-dimensional orthogonal geometry V such that $a^2 \neq b$ and $a \neq 0$. Assume there exists $\Gamma \subseteq \Phi$ that is a maximal β-incoherent set ($|\Gamma| = d$) that is also linearly independent. If Φ forms a regular two-graph with parameters (n, ℓ, m) then

$$\sum_{\gamma \in \Phi - \Gamma} |\Gamma_1(\gamma)||\Gamma_2(\gamma)| = \frac{\ell|\Gamma|(|\Gamma| - 1)}{2}.$$

Now that we have a notion of incoherent vectors that matches the behavior of incoherent real lines we can prove equivalent structural results. The first result is a generalization of Theorem 4.9 in [Gil18].

Theorem 3.5.18. *Let Φ be an (a, b)-equiangular system of n lines in a d-dimensional orthogonal geometry V over $\mathbb{F}_q$ such that $a^2 \neq b$, $a \neq 0$, $\operatorname{char} \mathbb{F}_q > d$, and Φ induces a regular two-graph with parameters (n, ℓ, m). Assume also that there exists $\Gamma \subseteq \Phi$ that is a maximal β-incoherent set ($|\Gamma| = d$) that is also linearly independent where $|\Gamma_1(\gamma)| = g_1$ for all γ not in Γ and $g_2 = |\Gamma| - g_1$. If $g_1 \neq g_2$ then $(\Gamma, \mathcal{B}_i)$ is a 2-(d, g_i, λ_i) design for $i = 1, 2$ such that*

$$\mathcal{B}_i = \{\, \Gamma_i(\gamma) \mid \gamma \in \Phi - \Gamma \,\} \quad \textit{and} \quad \lambda_i = \frac{\ell(g_i - 1)}{2g_j} \quad \textit{for } j \neq i.$$

Furthermore, when $n > 2d$, then $(\Gamma, \mathcal{B}_1)$ is a quasi-symmetric 2-$(d, g_1, \lambda_1; s_1, s_2)$ design, where s_1 and s_2 are the smallest integers satisfying

$$s_1 \equiv g_1 - (\rho - 1)^2/4 \quad \textit{and} \quad s_2 \equiv g_1 - (\rho^2 - 1)/4,$$

where $\rho = a\beta^{-1}$. Additionally:

- *If $n = d(d+1)/2$ then $(\Gamma, \mathcal{B}_1)$ is a 4-design;*

- *If* $n = 2d$*,* $(\Gamma, \mathcal{B}_1)$ *is a symmetric* 2-$(d, g_1, \lambda_1; s)$ *with* $s = s_1$ *or* s_2*; and*

- *If* $g_1 = g_2$ *then* $(\Gamma, \mathcal{B}_1 \cup \mathcal{B}_2)$ *is a* 2-$(d, d/2, n - d - \ell)$ *design.*

The proof of this statement is very similar to the proofs in [Gil18], which relies primarily on the fact that Φ gives rise to a regular two-graph.

Proof. As in Remark 3.5.11 we will assume that Γ has all scalar products equalling β. Suppose $|\Gamma| = g$ and fix $\alpha, \beta \in \Gamma$. For all γ not in Γ, where $\{\alpha, \beta, \gamma\}$ is a coherent triple, it would be the case that $\langle \alpha, \gamma \rangle = -\langle \beta, \gamma \rangle$, so $\alpha \in \Gamma_i(\gamma)$ and $\beta \in \Gamma_j(\gamma)$ for $i \neq j$. Likewise for all γ not in Γ whose addition makes $\{\alpha, \beta, \gamma\}$ an incoherent triple we have that the scalar products would be the same so $\alpha, \beta \in \Gamma_i(\gamma)$ for some $i = 1, 2$. For each $i = 1, 2$ we define k_i to be the number of γ not in Γ which makes $\{\alpha, \beta, \gamma\}$ an incoherent triple such that $\alpha, \beta \in \Gamma_i(\gamma)$. Because Φ induced a regular two-graph with parameters (n, ℓ, m) the number of $\gamma \notin \Gamma$ which form coherent triples with α and β is the parameter ℓ and therefore $k_1 + k_2 = n - g - \ell$. By the properties of regular two-graphs outlined in [Gil18], in particular Equation 4.11, we have in addition that $k_1 g_1 + k_2 g_2 = (n - g - \frac{3\ell}{2})g + \ell$.

Solving for k_1 and k_2 in the case where $g_1 \neq g_2$ and using Lemma 3.5.17 gives us that $k_1 = \frac{\ell(g_1-1)}{2g_2}$ and $k_2 = \frac{\ell(g_2-1)}{2g_1}$. Notice that these are independent of the choice of α and β, meaning any pair of elements in Γ are contained in k_i of the blocks $\mathcal{B}_i = \{\, \Gamma_i(\gamma) \mid \gamma \notin \Gamma \,\}$, gives us a 2-(g, g_i, k_i) design for $i = 1, 2$. Likewise when $g_1 = g_2$, we have that any pair of elements is contained in $k_1 + k_2 = n - g - \ell$ blocks of $\mathcal{B}_1 \cap \mathcal{B}_2$, giving a 2-$(g, g/2, n - g - \ell)$ design.

Assume that $|\Gamma_1(\gamma)| < |\Gamma_2(\gamma)|$, which is the case if and only if $|\Gamma_1(\gamma)| < d/2$. By Fisher's inequality Lemma 3.3.14, because $|\Gamma_1| < d/2$ we have that $|\mathcal{B}_1| \geq d$. We will consider the case where $n = 2d$ where $|\mathcal{B}_1| = n - |\Gamma| = d$, because each block corresponds to a vector γ not in Γ. From Theorem 1.15 in [CL91], we know that this must also mean that any two distinct block intersections have the same number of points, making $(\Gamma, \mathcal{B}_1)$ a symmetric 2-$(|\Gamma|, |\Gamma_1|, \lambda_1, s)$.

If $n > 2d$ and therefore $|\mathcal{B}_1| > d$, there must be at least two block intersection numbers by Theorem 1.15 in [CL91]. From Lemma 3.5.16 we know that there can only be two block intersection numbers, making $(\Gamma, \mathcal{B}_1)$ a quasi-symmetric 2-$(|\Gamma|, |\Gamma_1|, \lambda_1; s_1, s_2)$ design where s_1 and s_2 are the smallest integers satisfying the following

$$s_1 \equiv g_1 - (\rho - 1)^2/4 \quad \text{and} \quad s_2 \equiv g_1 - (\rho^2 - 1)/4,$$

where $\rho = a\beta^{-1}$ which follows from Lemma 3.5.16.

Finally, consider the special case where $n = d(d+1)/2$. We know that $|\mathcal{B}_1| = n - d = \frac{1}{2}d(d-1)$. Therefore by Proposition 5.6 in [CL91] (and also Proposition 13 in [Neu82]), we have that $(\Gamma, \mathcal{B}_1)$ is a 4-design and therefore also a 3-design. □

3.6 MUBs over Finite Fields

To begin are study of MUBs over finite fields we want to understand the cases in which the exist, mimicking the upper and lower bound we found in the complex setting.

By an exhaustive search over small fields it can be shown the the following cases do not satisfy the lower bound for $\mathcal{M}_6\mathbb{F}_{q^2}$

Proposition 3.6.1. *(Theorem 2.1 [MST21]) for $q \in \{13, 25, 37, 49\}$, $\mathcal{M}_6\mathbb{F}_{q^2} = 2$. With all other $q \leq 53$ achieving $\mathcal{M}_6\mathbb{F}_{q^2} = 3$.*

It also seems as though even in the cases of d being a prime unexpected things happen. Again by exhaustive search it was shown that $\mathcal{M}_7\mathbb{F}_{4^2} = 1$.[Ian: *see more searchs for no char 2.*] It is possible that this is due to the characteristic being 2, but it was also found that $\mathcal{M}_7\mathbb{F}_{17^2} = 2$.

Proposition 3.6.2. *(Proposition 3.1 [MST21]) Let $\mathbb{F}$ with involution σ and $\operatorname{char}\mathbb{F} = p$. Then for any $d \geq 2$ and $p \nmid d$ such that $\mathbb{F}^d$ is a unitary space,*

$$\mathcal{M}_d\mathbb{F}_{q^2} \leq d + 1$$

Proof. The proof is fairly standard and follows the ideas presented in the proofs of the orthoplex bound and Gerzon's bound.

Given an orthonormal basis $\{v_1, \ldots, v_d\}$ for a non-degenerate unitary space for $\mathbb{F}^d$, we will consider the trace-normalized projections $Q_j = v_j v_j^\dagger - d^{-1} I_d$. The projections live in the space L_0 of trace zero self adjoint operators which has dimension $Z(d, \mathbb{F}) - 1$. However this space is often degenerate. However the $d^2 - 1$ dimensional space of trace 0 operators in non-degenerate as long as $\operatorname{tr}(I_d) = d \neq 0$ which is the case when $p \nmid d$. The trace normalized projections have Hermitian scalar products

$$\langle Q_j, Q_k \rangle_F = \langle v_j, v_k \rangle \langle v_k, v_j \rangle - \frac{1}{d}.$$

Following the arguments of Theorem 3.4.13 we can consider the Gram matrix $G = [\langle Q_j, Q_k \rangle_F] = I_d - d^{-1} J_d$ which has eigenvalues 0 and 1, and $\ker G = \operatorname{span}(1^d)$. Because $\sum_k Q_k = 0$ this means that the trace normalized projections span a $d - 1$ dimensional space and any $d - 1$ of them form a basis.

Now consider n MU orthonormal bases $B_1, B_2, \ldots, B_n$. For any two, B_j and B_k where $j \neq k$ we will denote the basis elements as $B_j = (u_1, \ldots u_d)$ and $B_k = (v_1, \ldots v_d)$. Notice that both basis give rise to a collection of d trace normalized projection which span $d - 1$ dimensional spaces: $(Q_j)_{j=1}^d$ and $(P_j)_{j=1}^d$ respectively. For any Q_i and P_j we have that $\langle Q_i, P_\ell \rangle = 0$. This means that each MU orthonormal basis, gives rise to a $d - 1$ dimensional subspace of the non-degenerate $d^2 - 1 = (d-1)(d+1)$ dimensional space of trace zero operators. This means at most $d + 1$ such basis can exist. □

Although the lower bound is not achieved in general, there are many cases in which is is.

Proposition 3.6.3. *(Proposition 3.2 [MST21]) Let $d = \ell^k$ be a prime power, and p a prime distinct from ℓ, and r a positive integer such that $p^r \equiv -1 \pmod{d}$ when d is odd and $p^r \equiv -1 \pmod{4}$ when d is even. Then with $q = p^r$,*

$$\mathcal{M}_d \mathbb{F}_{q^2} \leq d + 1.$$

For a fixed prime power d the set of primes p which satisfy the above condition for some r, has positive Dirichlet density.

Proof. [Ian: *should definitly prove this*] □

Butson type Hadamards and Vanishing Sums of roots of Unity

As we saw in Proposition 3.1.12 the problem of finding n MUBs is equivalent to that of finding $n-1$ MU Hadamard matrices in case U. Furthermore in case U, all Hadamard matrices were Butson Hadamards whose entries were $q+1$ roots of unity. In case U, $\mathbb{F}_{q^2}$ has all of its $q+1$ roots of unity, meaning it also has all of its rth roots of unity, for all $r|(q+1)$. For this reason, the study of Hadamard matrices over finite fields is closely related to the study of roots of unity.

If H is a $BH_q(r,d)$, with $r|(q+1)$, by multiplying every row of H by the appropriate rth root of unity, we can obtain a unitarily equivalent Hadamard where the first column has 1s in every entry. This means the sum of entries of any other columns must be zero. That is

$$\sum_{j=1}^{d} h_{ij} = 0$$

for all $i \geq 2$. Because each h_{ij} is an rth root of unity the question of existence of $BH_q(r,d)$ Hadamards requires the existence of d, rth roots of unity which sum to zero, a vanishing sum. Vanishing sums of roots of unity don't always exist and this can allow us to better understand the cases where no Hadamards exist. To better study vanishing sums of roots of unity we will define the **weight set** $W_p(m)$ to be the set of positive integer n in which there exists a vanishing sum of n, mth roots of unity in $\mathbb{F}_p^{(m)}$, or equivalently in any extension which contains all the mth roots of unity, or simply $\overline{\mathbb{F}_p}$. For a fixed integer m and ζ a primitive mth root of unity and any prime r that divides m we have that $\zeta^{m/r}$ is a primitive rth root of unity, and $\sum_{j=0}^{r-1} \zeta^{jm/r} = 0$ is a vanishing sum of weight r. For this reason and the characteristic of the field we have that for $m = p_1^{a_1} \cdots p_k^{a_k}$ that $p\mathbb{N} + p_1\mathbb{N} + \cdots + p_k\mathbb{N} \subseteq W_p(m)$. This means that in when ever p is odd and q a prime power of p, $6 \in W_p(q+1)$. However this does not tell us about the number of vanishing sums or what they must look like.

For example, consider the field $\mathbb{F}_{11}$ which contains the 5th roots of unity $1, 3, 9, 5$, and 4. In this case we have that $1 + 1 + 9 = 0$ which means the smallest weight in $W_{11}(5)$ is 3 which is not generated by 11 and 5.

Diagonal Equations

If $\mathbb{F}_{p^k}$ contains all of the mth roots of unity meaning $m|p^k-1$, let $d=(p^k-1)/m$, and notice that $(\mathbb{F}_{p^k}^\times)^d$ is the group of mth roots of unity. Therefore vanishing sums of mth roots of unity are equivalent to solutions to the equation $x_1^d+\cdots+x_n^d=0$ which are not all zero. This is an example of a **diagonal equation**, which has historically been studied through the use of Jacobi sums and multiplicative characters.

Let G be a group, a **multiplicative character** is a group homomorphism from G to the complex unit circle. For our purposes we will look at the case where $G=\mathbb{F}_{q^2}^\times$. Each homomorphism, or character λ can then be extended such that $\lambda(0)=1$ if λ is the trivial character, and $\lambda(0)=0$ otherwise. For any character we will define the conjugate character as $\overline{\lambda}(x)=\overline{\lambda(x)}$. That is we just take the complex conjugate.[Ian: *need to define J_0 but i state the result anyway.*

$$\sum_{j_1=0}^{d'}\sum_{j_2=0}^{d'}\cdots\sum_{j_{\ell-1}=0}^{d'} J_0(\lambda^{j_1},\ldots,\lambda^{j_{\ell-1}})$$

]

Jacobi sums are often difficult to work with, and the sum in the previous equation is not know in general, but the next result gives us a range for N the number of solutions to a diagonal equation.

Theorem 3.6.4. *Then number N of solutions to $a_1x_1^{k_1}+\cdots+a_nx_n^{k_n}=0$ in $\mathbb{F}_{q^2}^n$ satisfies*

$$|N-(q^2)^{n-1}|\le M(d_1,\ldots,d_n)(q^2-1)(q^2)^{(n-2)/2}$$

where $d_i=\gcd(k_i,q^2-1)$ and $M(d_1,\ldots,d_n)$ is the number of n-tuples $(j_1,\ldots,j_n)\in\mathbb{Z}^n$ such that $1\le j_i\le d_1-1$ for all i and $\sum_i(j_i/d_i)\in\mathbb{Z}$.

In the specific case of determining how many vanishing sum of 6 root of unity there are we would have the diagonal equation

$$x_1^{q-1}+x_2^{q-1}+x_3^{q-1}+x_4^{q-1}+x_5^{q-1}+x_6^{q-1}=0,$$

where $k = q-1$ and $d = q-1$, and so $M(q-1,\dots,q-1)$ counts the number of integer n tuples $(j_1,\dots,j_n)$, with $1 \le j_i \le q-2$ such that $\sum_i \frac{j_i}{q-1}$ is an integer. We also note that if we are concerned with the sums of roots of unity, that map $x \mapsto x^{q-1}$ is a $q-1$ degree map. So we should divide the total number of solutions by $\prod_i d_i = (q-1)^n$. We can also use an upper bound for $M(q-1,\dots,q_1) \le (q-2)^n$ giving us

$$|N-(q^2)^{n-1}| \le (q-2)^n(q^2-1)(q^2)^{(n-2)/2}$$

$$(q^2)^{n-1}-(q-2)^n(q^2-1)(q^2)^{(n-2)/2} \le N \le (q-2)^n(q^2-1)(q^2)^{(n-2)/2}+(q^2)^{n-1}.$$

Irreducible Cyclotomic Polynomials

More recently [LL96] looked at the reducibility of cyclotomic polynomials and found a bound such that all larger integers where in the weight set. In some sense the factors of a cyclotomic polynomial can tell us about the structure of the roots of unity and their linearly independencies. Over $\mathbb{C}$ every cyclotomic polynomial is irreducible over $\mathbb{Q}$, which also contains no non-trivial mth roots of unity. However this is often not the case for the cyclotomic polynomials over $\mathbb{F}_p$, but when they are irreducible we can recover similar result as in the complex setting.

For any positive integer n, the polynomial x^n-1 defined over a field $\mathbb{F}$ is the monic polynomial which contains all nth roots of unity as its roots. We will denoted $\mathbb{F}^{(n)}$ as its splitting field, which will be called the **nth cyclotomic field** over $\mathbb{F}$, and $E^{(n)}$ will denoted the set of all the nth roots in the cyclotomic field.

Theorem 3.6.5. *(Theorem 2.42 [LN96]) If the characteristic $p \nmid n$ then $E^{(n)}$ forms a cyclic group under multiplication in $\mathbb{F}^{(n)}$. Otherwise if $n = mp^e$ where $p \nmid m$[Ian:* nor *e] then $\mathbb{F}^{(n)} = \mathbb{F}^{(m)}$ and $E^{(n)} = E^{(m)}$ where the roots of x^n-1 are attained with multiplicity p^e*

Through out we will assume that $p \nmid n$, as otherwise we could consider m as in the theorem above. If $p \nmid n$ we will define the n**th cyclotomic polynomial** $\Phi_n(x)$ over a field K, which contains all nth roots of unity, as the polynomials whose roots are the primitive nth roots of unity. For a fixed primitive nth roots of unity $\zeta \in K$, we can write

$$\Phi_n(x) = \prod_{s=1, \gcd(s,n)=1}^{n} (x - \zeta^s).$$

The polynomial Φ_n, when defined, is monic and has coefficients contained in the prime subfield of K, and when $\operatorname{char} K = 0$ the coefficients are contained in $\mathbb{Z}$. The polynomial of all nth roots of unity can then be written as $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Furthermore the splitting field of $x^n - 1$ is the same as the splitting field of Φ_n.

In an arbitrary field $\mathbb{F}$ it is likely the case that $x^n - 1$ does not split into linear factor, $\mathbb{F}$ does not contain all the nth roots of unity. Therefore we will often wish to understand the extensions in which $x^n - 1$ does split, starting with the degree $[\mathbb{F}^{(n)} : \mathbb{F}]$. In the case where $\mathbb{F} = \mathbb{Q}$, and n is a positive integer, the cyclotomic polynomial $\Phi_n(x)$ is always irreducible over $\mathbb{Q}$ and $[\mathbb{F}^{(n)} : \mathbb{F}] = \phi(n)$ where $\phi(n)$ counts the number of positive integers between 1 and n which are coprime with n. Over finite fields the question is very different.

Theorem 3.6.6. *Let $\mathbb{F} = \mathbb{F}_q$ with n a positive integer such that $\gcd(q, n) = 1$ and let d be the smallest positive integer such that $n|(q^d - 1)$. Then $\Phi_n(x)$ factors into $\phi(n)/d$ distinct monic irreducible polynomials over $\mathbb{F}$ of degree d and $[\mathbb{F}^{(n)} : \mathbb{F}] = d$.*

It is generally not the case that $d = \phi(n)$ and in fact a necessary, but not sufficient condition for $d = \phi(n)$ is for $n = 1, 2, 4, p^k, 2p^k$ for some odd prime p and positive integer k, meaning $\Phi_n(x)$ is generally not irreducible.

One case in which $\Phi_n(x)$ is always irreducible over $\mathbb{F}_q$ and $\gcd(q, n) = 1$ is when n is prime. The condition $n|(q^d - 1)$ (assuming $\gcd(q, n) = 1$) can be reinterpreted as asking about the order of q in the group $U(n)$ the group of units of $\mathbb{Z}/n\mathbb{Z}$. When n is prime and q is coprime with n the order of q would always be $\phi(n) = n - 1 = \deg \Phi_n$. In this case $x^n - 1 = (x - 1)\Phi_n(x)$.

When $n = p^m$ is a prime power, $x^n - 1 = (x - 1)\Phi_p \Phi_{p^2}(x) \cdots \Phi_{p^m}(x)$, which splits if and only if $\Phi_{p^m}(x)$ splits. Because p^j is a prime power the group of units $U(p^m)$ is cyclic of order $\phi(p^m) = p^{m-1}(p - 1)$. The order of q in this group is generally very hard to determine. But a well know result tells us that if q generates $U(p^2)$ then it generates $U(p^j)$ for all $j \geq 1$. Meaning if $\Phi_{p^2}(x)$ is irreducible over $\mathbb{F}_q$ then so is $\Phi_{p^j}(x)$ for all $j \geq 1$.

Therefore when $m \geq 2$, $\Phi_{p^m}(x)$ is irreducible over $\mathbb{F}_q$ (where $\gcd(n, q) = 1$) if and only if $q^{p-1} \not\equiv 1 \pmod{p^2}$. In which case $[\mathbb{F}_q^{(n)} : \mathbb{F}_q] = \phi(n)$. This gives two cases for the irreducibility of Φ_{p^j} over $\mathbb{F}_q$. If $q^{p-1} \not\equiv 1 \pmod{p^2}$, then Φ_{p^j} is irreducible. Otherwise Φ_{p^2} splits into p irreducible polynomials of degree $p-1$. For all $j \geq 2$, q is also not a generator of $U(p^j)$. q would have order d dividing $p^{j-1}(p-1)$ and because $q^d \equiv 1 \pmod{p}$ we know that $p-1$ divides d. So Φ_{p^j} is general splits into a prime power number of irreducible factors whose degrees are divisible by $p-1$.

We can also consider the case where $n = 2p^k$ for p and odd prime. A well know results tells us that if g is an odd integer and a generator for $U(p^k)$ then g is also a generator for $U(2p^k)$. So for a field $\mathbb{F} = \mathbb{F}_q$ where q is odd, then ff $q^{p-1} \not\equiv 1 \pmod{p^2}$, q is a generator for $U(p^j)$ and $U(2p^j)$ for all integers $j \geq 1$. In which case $\Phi_{2p^k}(x)$ would be irreducible over $\mathbb{F}_q$.

Using these irreducibility results we get the following result about the non-existence of Butson type Hadamards.

Lemma 3.6.7. Fix a finite field $\mathbb{F}_{q^2}$ where $q = p^\ell$, and a prime $r \neq p$ such that $p^{r-1} \not\equiv 1 \pmod{r^2}$. H is a $d \times d$ Hadamard matrix with entries being r^mth roots of unity only if $d \in \mathbb{N}r + \mathbb{N}p$ and $p \nmid d$.

Proof. By multiplying every row of H by the appropriate rth root of unity, we can assume that the first column of H has 1s in every entry, and the sum of any other column must be zero

$$\sum_{j=1}^{d} h_{ij} = 0$$

with each entry being an r^mth root of unity. Let ζ be a primitive r^mth root unity, and $\alpha = \zeta^{r^{m-1}}$ a primitive rth root of unity. Notice that the field extension $\mathbb{F}_p(\zeta)$ which is contained in $\mathbb{F}_{q^2}$ (as $r^m|(q+1)$) has degree $[\mathbb{F}_p(\zeta) : \mathbb{F}_p] = \deg \Phi_{r^m}(x) = r^{m-1}(r-1)$. Likewise the field extension $\mathbb{F}_p(\alpha)$ has degree $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg \Phi_r(x) = (r-1)$, meaning $[\mathbb{F}_p(\zeta) : \mathbb{F}_p(\alpha)] = r^{m-1}$. Looking at the ith column of H and the vanishing sum of its entries, knowing that the entries are r^mth roots of unity, we can rewrite

$$\sum_{j=1}^{d} h_{ij} = \sum_{k=0}^{r^m-1} \alpha_k \zeta^k = 0$$

where α_k counts the number of times ζ^k appears in the ith row of H. Because the entries $1, \zeta, \ldots, \zeta^{r^{m-1}-1}$ form a $\mathbb{F}_p(\alpha)$ basis for $\mathbb{F}_p(\zeta)$ we can further rearranging this sum by splitting $\zeta^k = z^{nr^{m-1}+\ell}$ where $\zeta^{nr^{m-1}}$ is a rth root of unity and ℓ is between 0 and $r^{m-1} - 1$. This gives us

$$\sum_{k=0}^{r^{m-1}-1} g_k \zeta^k = 0$$

where each g_k is a sum of ℓth roots of unity. Because this is a vanishing sum and $1, \zeta, \ldots, \zeta^{r^{m-1}-1}$ form a basis over $\mathbb{F}_p(\alpha)$, for this sum to be zero each $g_k = 0$, meaning each g_k would need to be a vanishing sum of rth roots of unity. This means that to prove the claim it is enough to show that the claim is true for sums of rth roots of unity.

Consider a vanishing sum of rth root of unity, fix ζ_r a primitive rth root of unity, and rewrite the sum as

$$\sum_{k=0}^{r-1} \alpha_k \zeta_r^k = 0$$

where α_k counts the number of times that ζ_r^k appears in the sum. Using the fact that $\sum_{k=0}^{r-1} \zeta_r^k = 0$ we have that

$$\sum_{k=0}^{r-1} \alpha_k \zeta_r^k = \sum_{k=1}^{r-1} (\alpha_k - \alpha_0) \zeta_r^k.$$

Because $\Phi_r(x)$ is irreducible, $\zeta_r, \zeta_r^2, \ldots, \zeta_r^{r-1}$ are linearly independent over $\mathbb{F}_p$, meaning for this to be a vanishing sum we must have have that $\alpha_k - \alpha_0 = 0$. And so $d \equiv \sum_{k=0}^{r-1} \alpha_k \equiv r\alpha_0 \pmod{p}$. This means as an integer $d \in \mathbb{N}r + \mathbb{N}p$. Furthermore because the first columns of H, which was scaled to be all 1s must have non-zero magnitude, $p \nmid d$. □

In the above theorem we proved the $\subseteq$ direction of the following result.

Theorem 3.6.8. *(Theorem 2.6 [LL96]) Let $m = r^a$ be a prime power where r is distinct from a prime p where $p^{r-1} \not\equiv 1 \pmod{r^2}$. Then $W_p(r^a) = \mathbb{N}r + \mathbb{N}p$.*

Looking at when $r = 2$ and p is a prime greater than 3 we know that d must be sum of multiples of 2 and p. Consider a $d \times d$ Hadamard matrix H with entries being 2nd roots of unity (elements which square to 1) and $d > 2$, scaled as in the previous proof. H would satisfy

$$\sum_{j=1}^{d}(h_{1j} + h_{ij})(h_{1j} + h_{ik}) = \sum_{j=1}^{d}(1 + h_{1j}h_{ik} + h_{ij}h_{1j} + h_{ij}h_{ik}) = d + 0 + 0 + 0 = d$$

for all distinct i and k not equal to 1 or 2. Notice also the term $(h_{1j} + h_{ij})(h_{1j} + h_{ik})$ is congruent to either 0 or 4 as the entries are all either 1 or -1 so d is congruent to a multiple of 4 meaning $d \in \mathbb{N}4 + \mathbb{N}p$.

As a consequence if H were to be a 6×6 Hadamard matrix with entries from $\mathbb{F}_{p^{2\ell}}$, such that $p > 6$ which are r^mth roots of unity where r is a prime different then p, such that $p^{r-1} \neq 1 \pmod{r^2}$, we would have that either $r = 3$ or $r = 2$ and $m > 1$. Unfortunately this does not lead to any immediate non-existence results. In general $q + 1$ is rarely a prime power, and when it is, its a prime power of 2, which this result does not exclude.

Cyclotomic Polynomials with Non-Trivial Roots in $\mathbb{F}_p$

In the previous section we look at the cases where Cyclotomic Polynomials were irreducible, but this is generally not the case, and EVENT worse, cyclotomic polynomials may have linear factors, they might split in the prime subfield.

Example 3.6.9. Over the field $\mathbb{F}_{31}$ the $m = 3$rd roots of unity are 1, 5, and 25 all of which are contained in the prime subfield.

For a finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^{\times}$ is cyclic of order $q - 1$. Meaning when ever $m|(q - 1)$, $\mathbb{F}_q$ will contain all of the mth roots of unity. And more generally if $\gcd(m, q - 1) = m' > 1$ then $\mathbb{F}_q$ will contain the m'th roots of unity which are some but not all of the mth roots of unity.

Theorem 3.6.10. *(Theorem 1.3 [LL96]) Let $K = \mathbb{F}_{p^k}$ and $d = (p^k - 1)/m$ and assume $m \neq 1$ nor $(m, k) = (2, 1)$. Then when ever $n > d$ then $n \in W_p(m)$: that is $[n, \infty)_{\mathbb{Z}} \subseteq W_p(m)$.*

If $q = p^\ell$ is an odd prime power then $q+1$ is even, meaning $\mathbb{N}2 \subseteq W_p(q+1)$. This however still does not tell us about the structure of the vanishing sums which exist. Is may be the case that some multiples of 2 are not contained in $W_p((q+1)/2)$.

Cyclotomic Polynomials with no Non-Trivial Roots in $\mathbb{F}_p$

Looking at vanishing sums of mth root of unity, it may be the case that no mth root of unity is contained in $\mathbb{F}_p$, this is when $\gcd(m, p-1) = 1$. So through out we will consider odd primes p and integers m such that $p \nmid m$ and $\gcd(m, p-1) = 1$. In this case we can look at the polynomial $x^m - 1$ which factors over $\mathbb{F}_p$ as $(x-1)g_1(x)g_2(x)\cdots$ such that each g_i is monic, irreducible and has degree at least 2. Define ℓ to be the minimal degree of the g_is. This gives us the minimal degree field extension $\mathbb{F}_{p^\ell}/\mathbb{F}_p$ which contains a non-trivial mth root of unity. Looking at the cyclotomic polynomial divisors of $x^m - 1$ we can determine that

$$\ell = \min_{n|m}\{d \geq 1 : p^d \equiv 1 \pmod{n}\} = \min_{q|m, q \text{ prime}}\{d \geq 1 : p^d \equiv 1 \pmod{q}\}.$$

Notice that for any integer d such that $p^d \equiv 1 \pmod{q}$ we have that $\gcd(p^d - 1, q) = q$ which also implies $\gcd(p^d - 1, m) \geq 0$. This gives us that

$$\ell = \min\{e : \gcd(p^e - 1, m) \geq 1\}.$$

Let $L = \mathbb{F}_{p^\ell}$ be the smallest field which contains an mth root of unity, and let $m' = \gcd(p^\ell - 1, m)$, in which case L contains all of the m'th roots of unity. Let $H = E^{(m')}$ be the group of m'th roots of unity in L. The degree of this extension tells us about the linear independencies of some of the mth roots of unity, but more importantly it tells us about some of the linear dependence relations which we can utilized to create a vanishing sum. We will define $t = |\operatorname{tr}_{\mathbb{F}_{p^\ell}}(H)|$ where $\operatorname{tr}_{\mathbb{F}_{p^\ell}}(H) = \{\operatorname{tr}_{\mathbb{F}_{p^\ell}}(h) : h \in H\} \subseteq \mathbb{F}_p$ which gives the following result.

Theorem 3.6.11. *(Theorem 5.3 [LL96]) Let ℓ and t be as above and let $n = \lceil \frac{p-1}{t-1} \rceil$. Then if $t > 1$ then $[\ell n, \infty)_{\mathbb{Z}} \subseteq W_p(m') \subseteq W_p(m)$.*

Proof. First we need the following fact, often referred to as the Cauchy-Davenport theorem: For $A, B \subseteq \mathbb{F}_p$ we have that $|A+B| \geq \min\{p, |A|+|B|-1\}$ where $A+B = \{a+b | a \in A, b \in B\}$.

Known that $t > 1$ allows us to consider the size of the set $|T+T| \geq \min\{p, 2t-1\}$. Likewise we wish to consider the size of $|k * T|$, the sum of T k times, and by induction we have that $|k * T| \geq \min\{p, kt-(k-1)\}$, which means for $k * T = \mathbb{F}_p$ we would need $kt-(k-1) \geq p$ which is the case where k is at least n. So $n * T = \mathbb{F}_p$. Meaning for every $j \in \mathbb{N}$ there exists of sum of n elements in T such that $t_1 + \cdots t_n = -j \in \mathbb{F}_p$. By construction each element of T is a sum of ℓ m'th roots of unity, meaning the sum $t_1 + \cdots t_n + j \cdot 1 = 0$ is a sum of $n\ell + j$ roots of unity. □

Notice that the proof of this theorem is actually stronger then the statement itself, in fact it implies that if $-j \in k * \mathrm{tr}_{\mathbb{F}_{p^\ell}}(H)$ we have a vanishing sum of weight $\ell k + j$. And likewise if $-j \in \mathrm{tr}_{\mathbb{F}_{p^\ell}}(H)$ we have a vanishing sum of weight $\ell + j$. So if $0 \in T$ we have a vanishing sum of weight ℓ.

A nice result that needs proof [Ian: *I have the proof somewhere i just need to find it*]

Lemma 3.6.12. $t \geq 2$

Proof. Recall that in the notation presented $L = \mathbb{F}_{p^\ell}$ was the smallest field extension that contained a non-trivial m'th root of unity and also contained all the m'th roots of unity: L is the splitting field of $x^{m'} - 1$. Meaning over $\mathbb{F}_p$ we can factor the polynomial $x^{m'} - 1 = (x-1)g_1(x)g_2(x)\cdots g_r(x)$ such that each g_i is monic, irreducible and has degree ℓ.

For each $g_i(x)$, and α_i one of its roots, we know that $\alpha_i, \alpha_i^p, \ldots, \alpha_i^{p^{\ell-1}}$ are all of the roots of $g_i(x)$. Notice that this means $tr(\alpha_i) = \alpha_i + \alpha_i^p + \cdots + \alpha_i^{p^{\ell-1}} = a_i$ which is independent of the choice of root. Repeating this for all r irreducible factors of $x^{m'} - 1$ we get

$$T = \{tr(1), a_1, \ldots, a_r\} = \{\ell, a_1, \ldots, a_r\}$$

which has possible duplicates.

An important observation is that the sum of all the m'th roots of unity is zero, which follows from the $x^{m'-1}$ coefficient, in $x^{m'}-1=\prod_{i=0}^{m'-1}(x-\zeta^i)$ being zero where ζ is a primitive m'th root of unity. From the above construction of T we get that $1+\sum_{i=1}^r a_i=0$. Notice that if $a_j=\ell$ for all j we would have that $1+r\ell\equiv 0$. However because $m=1+r\ell$ this is not possible meaning $|T|\geq 2$. We can also see that $|T|\leq 1+r$. □

This previous result gives a the following

Theorem 3.6.13. *(Theorem 5.6 [LL96]) Let $K=\mathbb{F}_{p^k}$ be a field containing all mth roots of unity. Assume that $\gcd(p-1,m)=1$ then $[d',\infty)_{\mathbb{Z}}\subseteq[d,\infty)_{\mathbb{Z}}\subseteq W_p(m')\subseteq W_p(m)$ except when $d'=p-1$ or $p=2$, $d'=3$ and $m'=5$, in which case $[d'+1,\infty)_{\mathbb{Z}}\subseteq[d+1,\infty)_{\mathbb{Z}}\subseteq W_p(m')\subseteq W_p(m)$.*

Proof. First notice that $L=\mathbb{F}_{p^\ell}\subseteq K$, where ℓ is defined above. Let G be the group of all mth roots of unity in K, and H the m' roots of unity in L. This means that $H=L^\times\cap G$ and $d=(p^k-1)/m=[K^\times:G]$ and likewise $d'=(p^\ell-1)/m'=[L^\times:H]=[L^\times G:G]$ where the last equality follows from the second isomorphism theorem. Because $G\leq L^\times G\leq K^\times$ we have that $d'|d$. We also know that $m'|m$ by definition of ℓ. Define the integer s such that $d'=s(p-1)$ this would mean that

$$s=(p^{\ell-1}+\cdots+p+1)/m'$$

First we will consider the case where $d'=p-1$ meaning $s=1$. We will show that $[p,\infty)_{\mathbb{Z}}\subseteq W_p(m')$. Notice that because $d'=[L^\times:H]=p-1$ and $H\cap F_p=\{1\}$ (follows from the assumptions) we know that $L^\times=H\mathbb{F}_p^\times$ which follows from counting orders and $HF_{p-1}^\times\leq L^\times$.

This means for any α a primitive m'th root of unity we have that $\alpha-1=b^{-1}\alpha^i$ which rearranges as $b\cdot\alpha=\alpha^i+b\cdot 1$ associating b as an integer between 1 and $p-1$. We can also consider the vanishing sum $p\cdot 1=b\cdot 1+(p-b)\cdot 1=0$ which by by multiplying by α and using the previous equation we get the vanishing sum $\alpha^i+b\cdot 1+(p-b)\cdot\alpha=0$ with weight $p+1$. Notice that by multiplying by α again we get the vanishing sum $\alpha^{i+1}+\alpha^i+b\cdot 1+(p-b)\cdot\alpha^2=0$ which has weight $p+2$. we can repeat this to get sums of weight $p+i$ for all $i\geq 1$.

Now we will consider the case where $s > 1$. Except for possible $p = 2$ and $\ell = 4, 6, 8, 9$ we get that $s \geq \ell$, which we will prove in the next Lemma. But this give us that $d' = s(p-1) \geq \ell(p-1)$ And from before we we know that $[\ell n, \infty)_{\mathbb{Z}} \subseteq W_p(m') \subseteq W_p(m)$. And from the fact that $t \geq 2$ we can conclude that $n \leq p-1$ so $\ell n \leq \ell(p-1) \leq d'$ proving the result for all but $p = 2$ and $\ell = 4, 6, 8, 9$. Which we will omit. □

Lemma 3.6.14. If $s > 1$ then $s \geq \ell$, except possible when $p = 2$ and $\ell = 4, 6, 8, 9$

Proof. We will consider two cases, first when ℓ is prime, and then when ℓ is composite.

First if ℓ is prime, we will show the stronger statement that $\ell \leq q$ for any prime divisor of s. By definition of s we have that when $q|s$ that $p^{\ell-1} + \cdots + p + 1 \equiv 0 \pmod{q}$. And because $d' = s(p-1)$ we have that $(p^{\ell-1} + \cdots + p + 1)(p-1) \equiv p^{\ell} - 1 =\equiv 0 \pmod{q}$. Because q is prime p in the multiplicative group $\mathbb{F}_q^\times$ is either equivalent to the identity or has order ℓ which is also prime. If $p \equiv 1 \pmod{q}$ then $p^{\ell-1} + \cdots + p + 1 \equiv \ell \cdot 1 \equiv 0 \pmod{q}$ so $\ell = p$. In the other case if p has order ℓ, we would have that $\ell | q-1$. In either case $\ell \leq q \leq s$

Now consider the case where $\ell = qt$ where q is the smallest prime divisor of ℓ and $t > 1$. Notice that by construction of ℓ we know that $\gcd(p^t, m) = 1$. Notice that the roots of $x^t - 1$ are the tth roots of unity and $x^\ell - 1$ the ℓth roots of unity. And because $t|\ell$ the tth roots are also ℓth roots so $(x^t - 1)|(x^\ell - 1)$ and $(p^t - 1)|(p^\ell - 1)$. By definition of s and the fact that $s(p-1) = (p^\ell - 1)/m'$ we can write $s(p-1) = (p^\ell - 1)/m' = (p^t - 1)a/m'$ and because $\gcd(p^t - 1, m) = 1$ and $m'|m$ we know that a/m' is an integer. So $s = (p^t - 1)a/(m'(p-1)) \geq (p^t - 1)/(p-1)$.

Now we will use the fact that $p^x \geq (p-1)x^2 + 1$ for all integers $x \geq 2$, except when $p = 2$ and $x = 2, 3, 4$.

This allows us to conclude that $s \geq (p^t - 1)/(p-1) \geq t^2 \geq qt = \ell$ in all but maybe the mentioned cases. □

3.6.1 Future Work: More on MUBs and Vanishing Sums of Roots of Unity

WARNING UNEDITED FROM HERE TO THE END OF CHAPTER

As mentioned previously the proof of Theorem 3.6.11 implied more then what wen have used so far. Recall that in the notation presented $L = \mathbb{F}_{p^\ell}$ was the smallest field extension that contained a non-trivial m'th root of unity and also contained all the m'th roots of unity: L is the splitting field of $x^{m'} - 1$. Meaning over $\mathbb{F}_p$ we can factor the polynomial $x^{m'} - 1 = (x-1)g_1(x)g_2(x)\cdots g_r(x)$ such that each g_i is monic, irreducible and has degree ℓ.

Some observations if $|T| = 2$ then $T = \{\ell, -1\}$. And so we can create a vanishing sum of weight $\ell + 1$. If $|T| = 3$ then $\ell \in T$ and there exists a, b such that $a + b \equiv -1$. Of which there are p solutions, possibly with one being 0.

It should also be noted that when $0 \in T$ this means that a m'th root of unity is in the kernel of the trace map. elements in the kernel of the trace have the form $\beta^p - \beta$ for some $\beta \in L$. The non-zero element in the kernel of the trace are defined by the variety $0 = 1 + x^{p-1} + \cdots + x^{p^{\ell-1}-1}$. Using that map $x \mapsto x^{d'}$ any solution β to $0 = 1 + x^{d'(p-1)} + \cdots + x^{d'(p^{\ell-1}-1)}$ would mean that $\beta^{d'}$ would be in the kernel of trace and a m'th root of unity.

Also in the sense explored above this means that the corresponding irreducible $g_j(x)$ the $x^{\ell-1}$ coefficient is zero. [Ian: *figure out when* $0 \in T$]

Trying to prove a lower bound

Here we want to find the smallest non-zero element of $W_p(m)$. Based on computer search it seems to me that the smallest non-zero weight is greater then or equal to the minimum of ℓ or p, when $s > 1$. when $s = 1$ it does appear that you get weights which are less then both p and ℓ.

Example 3.6.15. Here are cases where the conjecture breaks, all of which are when s=1 p, m, ell, m', d', t, s, n_min, conj holds 5, 781, 5, 781, 4, 5, 1, 3, 0 5, 5467, 5, 781, 4, 5, 1, 3, 0 7, 2801, 5, 2801, 6, 7, 1, 3, 0

The are the smallest examples

What does this mean really? Well from the above we had the following result and consequences

Theorem 3.6.16. *(5.3) Let ℓ and t be as above and let $n = \lceil \frac{p-1}{t-1} \rceil$. Then $[\ell n, \infty)_{\mathbb{Z}} \subseteq W_p(m') \subseteq W_p(m)$.*

Proof. This proof used the Cauchy-Davenport theorem to $T \subseteq \mathbb{F}_p$. [Ian:

Theorem 3.6.17. *For* $A, B \subseteq \mathbb{F}_p$ *we have that* $|A+B| \geq \min\{p, |A|+|B|-1\}$ *where* $A+B = \{a+b | a \in A, b \in B\}$

Proof. omitted □

] Here we must assume that $t > 1$ This allows us to consider the size of the set $|T+T| \geq \min\{p, 2t-1\}$. Likewise we wish to consider the size of $|k*T|$, the sum of T k times, and by induction we have that $|k*T| \geq \min\{p, kt-(k-1)\}$, which means for $k*T = \mathbb{F}_p$ we would need $kt-(k-1) \geq p$ which is the case where k is at least n. So $n*T = \mathbb{F}_p$. Meaning for every $j \in \mathbb{N}$ there exists of sum of n elements in T such that $t_1 + \cdots t_n = -j \in \mathbb{F}_p$. By construction each element of T is a sum of ℓ m'th roots of unity, meaning the sum $t_1 + \cdots t_n + j \cdot 1 = 0$ is a sum of $n\ell + j$ roots of unity. □

Notice that if $-j \in |k*T|$ we have a vanishing sum of weight $k\ell + j$. And likewise if $-j \in T$ we have a vanishing sum of weight $\ell + j$. So if $0 \in T$ we have a vanishing sum of weight ℓ.

We want to show that this is in general the best you can ever do. But before that we should understand what these examples look like. again I am going to reiterate some of the notation and ideas we want.

Fix p prime and m a positive integer, such that $\gcd(p-1, m) = 1$. Let ℓ be the smallest positive integer such that $\gcd(p^\ell - 1, m) = m' > 1$. Define also $d' = (p^\ell - 1)/m'$. And assume that $d' \neq p-1$ in $\mathbb{F}_p$ the polynomial $x^{m'} - 1$ factors as

$$x^{m'} - 1 = (x-1)g_1(x) \cdots g_r(x)$$

where each $g_j(x)$ is monic and irreducible of degree exactly equal to ℓ. $x^{m'} - 1$ splits completely in $L = F_{p^\ell}$. For any m'th root of unity $\alpha \neq 1$, let $g_j(x)$ be its minimal polynomial, the irreducible factor of $x^{m'} - 1$ of which it is a root. The roots of $g_j(x)$ are $\alpha, \alpha^p, \ldots, \alpha^{p^{l-1}}$ where $tr(\alpha) = \alpha + \alpha^p + \cdots + \alpha^{p^{l-1}} \in \mathbb{F}_p$.

So the question to ask is what is the minimal number of m'th roots of unity which sum to an element of $\mathbb{F}_p$?

Because $L = \mathbb{F}_{p^\ell} = \mathbb{F}_p[x]/(g_j(x))$

Idea: Show that the only Linear Dependence of root of unity which the same minimal polynomial are just summing them all together.

Really what i want to show: any $\ell - 1$ roots of unity are linearly independent.

How? well we can look at diagonal equations, showing that there are zero solutions to $a_1x_1^{d'} + a_2x_2^{d'} + \cdots + a_{\ell-1}x_{\ell-1}^{d'} = 0$. 6.36 in the book says that

$$q^{\ell-2} - M(d_1, \ldots, d_{\ell-1})(q-1)q^{(\ell-3)/2} \leq N \leq q^{\ell-2} + M(d_1, \ldots, d_{\ell-1})(q-1)q^{(\ell-3)/2}$$

where $q = p^\ell$, maybe sub $d' = s(p-1)$ where $s > 1$.[Ian: *this probably wont give me what i want.*]

instead we should use 6.33 in the book which says

$$N = q^{\ell-2} + \sum_{(j_1,\ldots,j_{\ell-1})\in T} \overline{\lambda}_1^{j_1}(a_1)\cdots\overline{\lambda}_{\ell-1}^{j_{\ell-1}}(a_{\ell-1})J_0(\lambda_1^{j_1}, \ldots \lambda_{\ell-1}^{j_{\ell-1}})$$

I dont understand this. so we will just dump a ton of relevantish results. If $\ell - 1 > d'$ then we are guaranteed to have a vanishing sum of $\leq \ell - 1$, m'th roots of unity. [Ian: *notice in the cases where $s = 1$ this means $d' = p - 1$*]

Also notice that we can simplify this problem to assume $a_j = 1$ for all j then we are looking for average values of the $J_0(\lambda_1^{j_1}, \ldots \lambda_{\ell-1}^{j_{\ell-1}})$. refer to page 205 for the definition of this.[Ian: *6.43 might explain why the s=1 case is bad*]

MISC NOTES

Conjecture 3.6.18. FALSE Assuming $s > 1$ (defined below) The smallest non-zero element of $W_p(m)$ is greater then or equal to the minimum of ℓ or p. MAYBE PLEASE BE TRUE?? IDK i should see if this is true for a boatload of examples. wouldn't be hard to test.[Ian: *do this lol*]

Proof. THIS IS FALSE AS WRITTEN. But maybe there is somethign salvagable here? idk

p, m, ell, m', d', t, s, n_min, conj holds

11, 3221, 5, 3221, 50, 11, 5, 3, 0

Let a be a generator of $\mathbb{F}_{11^5}^\times$ then the roots of unity which sum to zero are 1, $6 * a^4 + 5 * a^3 + 6 * a^2 + 4 * a + 7$, $5 * a^4 + 6 * a^3 + 5 * a^2 + 7 * a + 3$.

They have trace 5, 6 and 0 respectively. nothing else out of the ordinary

□

Chapter 4

Future Work: Algorithms for Finding Frames: Alternating Projections

So far we have discussed many things. many many thing. Probably many more then i wish we had. But yet here we are and we have one more thing to discuss, which hopefully turns into a paper, and then would be a long thing to finish discussing.

In this section we wish to understand better the structure of tight frames to create algorithms to numerically find them. The set of $d \times N$ α-tight frames.

$$\mathscr{X}_\alpha = \{X \in \mathbb{C}^{d\times N} | XX^* = \alpha I_d\}$$

[Ian: *switch notation to match what ive been doing throughout.*]

4.1 Alternating Projections

The basic question behind alternating projections is given a random $d \times n$ matrix, what is the closest $d \times n$ matrix which is a tight frame. And likewise given a random $d \times n$ matrix we can ask what is the closest $d \times n$ matrix whose columns are equiangular. The hope is that by repeatedly asking and alternating which of these questions we ask, we will eventually converge on a $d \times n$ matrix whose columns are an ETF.

First we will consider the set of $d \times N$ c-tight frames which we will denote as

$$\mathscr{X}_c = \{\Phi \in \mathbb{C}^{d\times N} | \Phi\Phi^* = cI_d\}.$$

Then we will consider a set $\mathscr{S} \subseteq \mathbb{C}^{d\times N}$ that possess some structural property/And we will ask how to find a matrix in $\mathscr{S}$ that is closest to $\mathscr{X}_\alpha$, and hopefully there will be some overlap between the sets.

Often it is easier to just work with Gram matrices instead of the frames these selves. From a rank d, $n \times n$ Gram matrix we can always recover a (non-unique) $d \times n$ frame with a cholesky decomposition or various different matrix decompositions. In this case we can rewrite the set of c-tight as a set of Gram matrices coming from c-tight frame which we will denote

$$\mathscr{G}_\alpha = \{G \in \mathbb{C}^{N \times N} | G = G^*, \mathrm{spec}(G) = (\alpha, \ldots, \alpha, 0, \ldots, 0)\},$$

where $\mathrm{spec}(G)$ is the sequence of eigenvalues of G.

Alternating problems will then ask the same question as before, this time considering a structure set which we will denote $\mathscr{H}$ to play the role of $\mathscr{S}$. This is an example of a wider family of problems called inverse eigenvalue problems as $\mathscr{G}_\alpha$ is defined by a spectral constraint.

An Algorithmic Outline

The algorithm behind alternating projection is very simples, its general structure requires that we have two sets $\mathscr{A}$ and $\mathscr{B}$, both subsets of $\mathbb{C}^{d \times N}$ or $\mathbb{C}^{N \times N}$, that are defined by some constraints, assumed to be spectral and structural respectively. We will assume that one set is closed and the other compact.[Ian: *why?*]

Algorithm 1 Alternating Projections Template

Input: Matrix A_1 and number of iterations J
Output: A matrix $A \in \mathscr{A}$ and a matrix $B \in \mathscr{B}$.

```
1: $j = 0$
2: while $j \leq J$ do
3:     $B_j \in \arg\min_{B \in \mathscr{B}} \|B - A_j\|_F$
4:     $A_{j+1} \in \arg\min_{A \in \mathscr{A}} \|A - B_j\|_F$
5: end while
6: Return $A = A_{j+1}$ and $B = B_j$
```

In a very literal sense, lines 3 and 4 are projections, or maybe more accurately they are idempotent. The resulting elements A_j and B_j may not be unique. Implementations of these steps, called matrix nearness problems, are the bread and butter of this method: Generally this results in a "differential calculus problem".

Projections onto $\mathscr{X}_c$

Proposition 4.1.1. *Let Φ be an arbitrary $d \times N$ matrix with singular value decomposition $\Phi = U\Sigma V^*$. Then cUV^* is a c-tight frame with minimum distance to Φ. If Φ started with full rank then cUV^* would be the unique nearest tight frame.*

Proof. proof omitted. □

Under the Gram matrix perspective we have a similar statement

Proposition 4.1.2. *Assume G is a $n \times n$ hermitian matrix, with spectral decomposition $G = U\Lambda U^*$, with the eigenvalues of Λ arranged in a algebraically weakly decreasing order. Then $cU(I_d \oplus 0)U^*$ is the Gram matrix of a c-tight frame that is closest to G. G is unique if $\lambda_d > \lambda_{d+1}$, meaning there is no ambiguity what is are top d eigenvalues.*

Projections onto Structurally Specifed Sets

Now we may consider some structural properties, lets say we want to find tight frames with specific squared column norms $c_1, \dots, c_n$. In this case we can define

$$\mathscr{S} = \{S \in \mathbb{C}^{d \times N} | \left\| s_n \right\|^2 = c_n\}$$

If $Z = (z_j)$ is a matrix, then S is the nearest matrix with squared column norms $c_1, \dots, c_n$ where

$$s_n = \begin{cases} c_n u_n & s_n = \vec{0} \\ \\ c_n z_n / \left\| z_n \right\| & s_n \neq \vec{0} \end{cases}$$

Likewise we may want to consider the geometric property of minimal coherence, these would be Equiangular tight frames (under some other assumptions, blah blah blah) if they exist.

Welch Bound is a thing.

Let G be an $n \times n$ matrix [Ian: *blah blah blah the closest matrix with coherence bounded by the welch bound*] is the matrix H where

$$h_{jk} = \begin{cases} g_{jk} & |g_{jk}| \leq \mu \\ \mu g_{jk}/|g_{jk}| & \text{otherwise} \end{cases}$$

4.2 Packing in Grassmannians

Frames can be thought of as packings in projective spaces, where their vectors represent the line in which they span. ETFs are an example of a nice packings: being solutions to an optimization problem: that of minimizing the coherence. More formally we can rephrase this question about optimal packing in terms of riemannian geometry. Consider the space $\mathbb{C}^d$ and consider the lines through the origin, which form the projective space $\mathbb{CP}^{d-1}$, which is a Riemannian manifold. Being a Riemannian manifold there is intrinsic notion of distance, that of geodesic distance. Let ℓ_1, ℓ_2 be lines in $\mathbb{C}^d$ represented by the unit vectors v_1, v_2 respectively. The geodesic distance between the lines is then

$$d(\ell_1, \ell_2) = \theta$$

where θ is the acute angle between the lines. This follows from the fact that $|v_1^* v_2|^2 = \cos^2 \theta$. An optimal packing of lines could then be understood to be a collection of lines, or points in projective space, whose minimal pair wise angle, or distance, is maximized. This is equivalent to minimizing the maximum modulus of the inner product between unit vector representatives.

In this section we will consider packings in Grassmannian manifolds. In a similar vain we can consider an optimal packing to be those which maximize the pair wise distance coming from the underlying geodesic distance from the riemannian manifold. However this will not be the only notion of distance we will wish to consider.

Distance in Grassmannians

As discussed, frames are packings of lines or 1-dimensional subspaces in $\mathbb{C}^d$. And as an good mathematician would do we can begin to count: we may consider packings of 2-dimensional subspaces, or planes in $\mathbb{C}^d$, or even k-dimensional subspaces. The collection of all k-dimensional subspaces in $\mathbb{C}^d$ is called a Grassmannian.

Definition 4.2.1. The collection of all k-dimensional subspaces of $\mathbb{C}^d$ is called a Grassmannian and is denoted

$$Gr(k, \mathbb{C}^d) = \{U \subseteq \mathbb{C}^d | \dim U = k\}$$

By representing any point, or subspace, U in $Gr(k, \mathbb{C}^d)$ as a orthonormal basis of $\mathbb{C}^d$ with the first k basis elements forming a basis for U and the remaining $d-k$ forming a basis for the orthogonal compliment of U, we can determine that

$$Gr(k, \mathbb{C}^d) \cong \frac{U(d)}{U(k) \times U(d-k)}$$

which also implies that $Gr(k, \mathbb{C}^d) \cong Gr(d-k, \mathbb{C}^d)$.

Grassmannian, being a generalization of projective spaces, are them selves Riemannian manifolds, and hence have a intrinsic notion of distance coming from the geodesics. For any two points in a Grassmannian, two k-dimensional subspaces S and T of $\mathbb{C}^d$ we can represent them by choices of matrices, X and Y whose columns are orthonormal bases for S and T respectively. The collection of all such matrices form equivalence classes $[X]$ and $[Y]$. Any two representatives are related by unitary transformations on the subspaces.

Proposition 4.2.2. *Let X, Y be $n \times k$ matrices, whose columns are orthonormal, which represent equivalence classes $[X], [Y] \in Gr(k, \mathbb{C}^n)$. Then the geodesic distance is*

$$d([X],[Y]) = \sqrt{\sum_{i=1}^{k} \theta_i^2}$$

where $\cos(\theta_i)$ are the singular values of X^*Y.

We will not provide a full proof of this statement but instead we will give some intuition.

Consider the matrix X^*Y which encodes to inner product between the bases of the two spaces. A singular value decomposition would then give us $U\cos(\Theta)V^*$ where U is a unitary on the space spanned by the columns of X and likewise V is a unitary of the space spanned by the columns of Y. This means $[X] = [XU]$ and $[Y] = [YV]$. Using the representatives XU and YV we can notice that $(XU)^*YV = \cos(\theta)$ is a diagonal matrix, with entries being the cosines of the angles between bases elements. Under these representatives we can interpret the geodesic as rotations of the basis elements. These angles are called **principal angles**. This means that the geodesic distance is the 2-norm of the principal angles. We may further assume that each such angle represents the acute angles, and the angles are ordering weakly increasing.

The principal angles represent distance in a way proportional to arc-length. However we may also wish to consider a distance more similar to that of a chordal distance. Notice that we can consider the Grassmannian in a different way, by an embedding in $\mathbb{C}^{d\times d}$ by associated with each subspace S a orthogonal projection onto that subspace, $\Pi_S := X^*X$ which X is a matrix whose columns form a orthonormal basis for S. Notice that Π_S is independent of the choice of X. This means the Grassmannian $Gr(k, \mathbb{C}^d)$ is equivalent to the collection of orthogonal projections of rank k: $\{\Pi : \Pi^* = \Pi, \Pi^2 = \Pi, tr(\Pi) = k\} \subseteq \mathbb{C}^{d\times d}$. Notice that $\frac{1}{\sqrt{k}}\Pi$ has Frobenious norm $\left\|\frac{1}{\sqrt{k}}\Pi\right\|_F = 1$ and so lives on a sphere. The metric, or distance, induced by the Frobenious norm, is then exactly that of the chordal distance with respect to this sphere. That is the chordal distance would be

$$\|\Pi_S - \Pi_T\|_F = \sqrt{2k - 2tr(\Pi_S\Pi_T)} = \sqrt{2k - 2tr((XY^*)^*(XY^*))}$$

Definition 4.2.3. Let X, Y be $n \times k$ matrices, whose columns are orthonormal, which represent equivalence classes $[X], [Y] \in Gr(k, \mathbb{C}^n)$. Then the chordal distance is

$$d_c([X], [Y]) = \sqrt{k - tr((XY^*)^*(XY^*))}$$

where $\cos(\theta_i)$ are the singular values of X^*Y

The chordal distance can also be expressed in terms of the principal angles in the following way

Proposition 4.2.4. *Let X, Y be $n \times k$ matrices, whose columns are orthonormal, which represent equivalence classes $[X], [Y] \in Gr(k, \mathbb{C}^n)$. Then the chordal distance is*

$$d_c([X],[Y]) = \sqrt{\sum_{i=1}^{k} \sin(\theta_i)^2}$$

where $\cos(\theta_i)$ are the singular values of X^*Y.

Proof. citation 15 of this: here. □

Other distance in which we may consider are the **Spectral distance** and **Fubini-Study Distance**. which i will define later. In the same where $k = 1$ are 4 of the distance are equivalent up to a monotonicly increasing transformation.

Optimal Packings in Grassmannians

As in the case of packings of lines, we wish to consider the cases where a packing of k-dimensional subspaces is optimal in that it maximized the minimum pair wise distance, with respect to any of the above distance.

A packing of a Grassmannian, is a collection of n k-dimensional subspaces of $\mathbb{C}^d$: $(U_1, \ldots, U_n)$ represented by a collection of n (non-unique) $d \times k$ matrices $(X_1, \ldots, X_n)$, with orthonormal columns, whose span $spanX_j = U_j$. This gives us a $d \times kn$ matrix $X = \begin{bmatrix} X_1 | \ldots | X_n \end{bmatrix}$ which can also be viewed as a $d \times k \times n$ tensor. What does this give me? IDK ask nate maybe.

The corresponding Gram matrix $G = X^*X$ is a $k \times k$ block matrix where the blocks $G_{mn} = X_m^* X_n$.

Optimal Packings with Respect to Chordal Distance

An optimal packing with respect to the chordal distance is a packing such that

$$\min_{i \neq j} d_c([X_i], [X_j])$$

is maximize. Notice that this is equivalent to minimizing

$$\max_{i \neq j} tr((X_i X_j^*)^*(X_i X_j^*)) = \max_{i \neq j} \left\| X_i X_j^* \right\|_F .$$

A lower bound for this quantaty can...

4.3 Quaternionic ETFS numerically

[Ian: *do stuff here*]

Chapter 5

Future Work: A Superposition of Frame Theory and its Application to Quantum Information Theory

Through this paper so far we have often made claims vaguely of the form

"…is of particular interest in quantum computing as …which we will discuss in Chapter 5."

Well now it is Chapter 5.

[Ian: *this section need a lot of work but for now i will copy some paper to check out when i get around to doing that work*]

5.1 Quantum mechanics

Frame theory and design theory can play a fundamental role in understanding quantum information and in particular quantum state tomography. In this chapter we wish to briefly introduce the postulates of quantum mechanics and draw connections to frame theory. For a more in-depth overview we point to these books [**see onedrive books you know the ones**]

Quantum Systems

Based on experimental evidence([**i am not familar with the source but have been told there is one**]), any closed system is modeled by a complex Hilbert space $\mathcal{H}$, with the unit vectors describing the systems states. Hence forth we will use the notation of $|\psi\rangle$ to denote a vector of $\mathcal{H}$. To model a single qubit with the physical states of 0 and 1, we would have a 2-dimensional complex Hilbert space: $\mathbb{C}^2$ where

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \text{ and } |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

being the physical states and any unit vector in their span representing a super position of the two states. This perspective tells us that for a system modeled by a finite N dimensional hilbert space, the state space is $\mathbb{CP}^{N-1}$.

Alternatively a system can be described by its density matrices: positive semi-definite, hermitian matrices with trace 1. Many authors will include hermitian as part of the definition of a positive semi-definite matrix. A density matrix ρ is said to be a pure state if $\rho = |\psi\rangle\langle\psi|$ for some unit vector $|\psi\rangle \in \mathcal{H}$. Otherwise ρ is called a mixed state.

Both perspective give an equivalent foundation for quantum mechanics, but the density matrix formulation is often more convenient for the situations we will be interested in. In some sense the density matrix formulation is an ensemble version of the unit vector formulation where we can represent the situation where a system is in the state $|\psi_j\rangle$ with probability p_j over some index set for j, as the density matrix $\rho = \sum_{j=1}^{\ell} p_j |\psi_j\rangle\langle\psi_j|$. It is important to note however that different ensembles of states may give rise to the same density matrices.

Proposition 5.1.1. *Let ρ be a density matrix then the following are equivalent:*

(a) *ρ is a pure state*

(b) $\operatorname{tr}(\rho^2) = 1$

(c) $\rho^2 = \rho$

(d) $\operatorname{rank}(\rho) = 1$

Proof. This is an easy proof that ill do later. □

In general, any density matrix will satisfy $\operatorname{tr}(\rho^2) \leq 1$.

The state space of a combination of independent systems can be modeled by the tensor product of the different systems. A system involving two qubits is the combination of two systems of one qubit: $\mathbb{C}^4 = \mathbb{C}^2 \otimes \mathbb{C}^2$, and the state of the first qubit being 0 and the second 1 would be represented by the unit vector $|01\rangle = |0\rangle|1\rangle := |0\rangle \otimes |1\rangle$.

Quantum Measurements

Quantum system are often in a superposition of states: the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ being in a super position of the states $|0\rangle$ and $|1\rangle$. Interpreting the coefficients, $|\alpha|^2$ is the probability that the state $|\psi\rangle$ is measured to be $|0\rangle$ and $|\beta|^2$ is the probability that the state $|\psi\rangle$ is measured to be $|1\rangle$. Once a system is measured the state collapses according to the measurement device used. Often we will wish to measure a state with respect to the computational basis: $|0\rangle, |1\rangle$, in which cases the probabilities can be easily computed from the coefficients, but this is not required, and in fact a state can be measure with respect to many different outcomes, more than even the dimension of the underlying space $\mathcal{H}$.

Quantum measuring devices can be modeled by a collection of measurement operators $\{M_m\}_{m\in\Sigma}$ where Σ represents the set of outcomes we are measuring for. The measurement operators must satisfy the completeness condition

$$\sum_{m\in\Sigma} M_m^\dagger M_m = I.$$

Given a state $|\psi\rangle$, likewise a density matrix ρ, that we wish to measure, the probability of measuring the outcome m is

$$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle = \operatorname{tr}(M_m^\dagger M_m \rho).$$

And if we get the outcome m the resulting state after the measurement collapses to

$$\frac{M_m|\psi\rangle}{\sqrt{p(m)}} \text{ or as a density matrix } \frac{M_m \rho M_m^\dagger}{p(m)}.$$

projective Measurements

Measuring a state with respect to the computational basis is a special case of the above definition, with the measurement operators being $M_0 = |0\rangle\langle 0|$ and $M_1 = |1\rangle\langle 1|$. In this case the measurement operators are projection matrices onto the states $|0\rangle$ and $|1\rangle$ which are orthogonal. This special case is an example of a projective measurement, and requires that the outcome of the measurement corresponds to orthogonal subspaces of $\mathcal{H}$, which may not always be possible.

[Ian: *include example of distiguishing states.*]

POVMs

Often measuring a system is only done after the conclusion of an experiment, meaning the resulting state is not important and only the probabilities of measuring each outcome are needed. In these cases if we had a measurement device modeled by the measurement operators $\{M_m\}_{m\in\Omega}$ we could instead consider the operators $\{E_M = M_m^\dagger M_m\}_{m\in Omega}$ which are positive semi-definite, and satisfy the completeness condition $\sum_{m\in\Omega} E_m = I$. Such a collection of operators is called a Positive-Operator Values measurement(POVM). In the special case where $\mathrm{rank}(E_m) = 1$, then E_m would be a scaled projection matrix. For a POVM the Probability of measuring the outcome m is

$$p(m) = \langle\psi|E_m|\psi\rangle = \mathrm{tr}(E_m\rho).$$

If instead we started with a POVM $\{E_m\}_{m\in Omega}$ we can always recover, non-uniquely, a collection of of measurement operators, using a Cholesky decomposition. In some sense POVMs represent equivalence classes of measurement operators such that the resulting probabilities are equal. Through out we will always assume that the Hilbert space $\mathcal{H}$ is d-dimensional and that Ω is finite and we will denote the outcomes as $\Omega = \{1, 2, \dots, n\}$.

POVMs have many advantages compared to Projective measurements, in that they do not require the outcomes to correspond to orthogonal subspaces, and they can include more outcomes than the dimension of the space. Both of these are highlighted in the following examples

Example 5.1.2. Alice prepares a qubit $|\psi\rangle$, either as $|0\rangle$ or $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and sends the qubit to bob, who wishes to distinguish the two possibility. It is not possible to design a projective measurement devices to achieve this task, and in fact it is not possible to achieve this task with certainty: but a POVM can at the very least ensure that a miss-reading is not possible. Consider the POVM operators

$$E_1 = \frac{\sqrt{2}}{1+\sqrt{2}}|1\rangle\langle 1|, \quad E_1 = \frac{\sqrt{2}}{1+\sqrt{2}}(|0\rangle - |1\rangle)(\langle 0| - \langle 1|), \quad E_3 = I - E_1 - E_2.$$

These three operators form a POVM. If $|\psi\rangle = |0\rangle$ then notice that the probabilities to measure the three outcomes corresponding to the three operators are

$$p(1) = 0, \quad p(2) = \frac{\sqrt{2}}{1+\sqrt{2}}, \quad p(3) = \frac{1}{1+\sqrt{2}}$$

Likewise if $|\psi\rangle = |+\rangle$ then notice that the probabilities to measure the three outcomes are

$$p(1) = \frac{\sqrt{2}}{1+\sqrt{2}}, \quad p(2) = 0, \quad p(3) = \frac{1}{1+\sqrt{2}}.$$

Notice that this means if we measure the state and get outcome 1 we know for certain that $|\psi\rangle$ was in the state $|+\rangle$ and likewise if we measure outcome 2 we would know for certain that $|\psi\rangle$ was in the state $|0\rangle$. It is only outcome 3 that we would not know the original state, and the experiment would need to be repeated

Definition 5.1.3. A POVM $\{E_m\}_{m=1}^{n}$ is called informationally complete if the probabilities for each outcome are distinct on the set of density matrices. In other words: A POVM $\{E_m\}_{m\in\Omega}$ is called informationally complete if the linear map $\mathcal{A}$ which maps a density matrix ρ to the vector of probabilities $(p(m))_{m\in\Omega} = (\mathrm{tr}(E_m\rho))_{m\in\Omega}$, is injective on the set of density matrices.

Theorem 5.1.4. *A POVM $\{E_m\}_{m\in\Omega}$ is informationally complete if and only if the real span of its operators $\mathrm{span}_{\mathbb{R}}\{E_m\}$ contains every Hermitian operator*

Proof. There is something to show here but i wont do that yet □

This is really telling us that an informationally complete POVMs are examples of real frames for the space of Hermitian operators. The rank of the space of $d \times d$ Hermitian operators, as a real vector space, is d^2, meaning any informationally complete POVM for a d-dimensional Hilbert space must have at least d^2 operators.

An important class of informationally complete POVMS, which we will explore in depth later, come from maximal complex ETFs.

Proposition 5.1.5. *Let $\Psi = (\psi)_{j=1}^{d^2} \subseteq \mathbb{C}^d$ be a collection of unit norm vectors which form an ETF, meaning $|\langle \psi_j \,|\, \psi_k \rangle| = \frac{1}{\sqrt{d+1}}$ for $j \neq k$ and $\Psi\Psi^* = dI$. In this case for each j construct $E_j = \frac{1}{d}|\psi_j\rangle\langle\psi_j|$. The collection $\{E_j\}_{j=1}^{d^2}$ for a informationally complete POVM.*

Proof. I assume the proof is basically the same as Gerzon's where we are looking at the Gram matrix of the E_js with respect to the hilbert-schmidt IP and what not. I wont do it now but I will assume it to be true. □

Not every maximal ETF gives rise to a distinct POVM: multiplication of the frame vectors by unimodulars gives rise to the same POVMs.

Proposition 5.1.6. *prove that claim here*

Proof. ok □

[Ian: *Also what examples of info compelte POVMS dont come from frames? or maybe fusion frames?*] We will continue to expand this connection with frames and POVMs in the follow section

[Ian: *talk about MUBs here too*]

Entanglement

The density matrix formulation is particularly helpful in understanding entanglement which we highlight in the example below

Example 5.1.7. Let $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ be the superposition of two qubits as either 00 or 11. Notice that this is an example of entanglement: if the first qubit is measured to be 0, the second must also be 0. Entanglement can also be seen mathematically: if we wish to isolate each qubit, we would need to decompose the vector $|\psi\rangle$ as a tensor product: $|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$, but this is not possible, as the states are not independent, they are entangled.

With the density matrix formulation we would have the density matrix

$$\rho = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)\frac{1}{\sqrt{2}}(\langle 00| + \langle 11|)$$

which we are also unable to split as the tensor product of two 2×2 density matrices. However the density matrix formulation can can still allow us isolate the qubits individually as mixed states. Intuitively, if we had the first qubit we would not be able to think of it as an equal super position of $|0\rangle$ and $|1\rangle$, because its state is dependent on the second qubit. Instead we can think about the first qubit as an ensemble of states, that is with probability $1/2$ it is $|0\rangle$ and probability $1/2$ it is $|1\rangle$. This suggests we can model this qubit as the density matrix $\rho_1 = \frac{1}{2}|0\rangle\langle 0| + \frac{1}{2}|1\rangle\langle 1| = \frac{1}{2}I$.

To formalize this we need to use a partial trace.

Definition 5.1.8. Given two finite-dimensional hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$, the Partial trace over $\mathcal{H}_B$ is the unique map $\operatorname{tr}_B : L(\mathcal{H}_A \otimes \mathcal{H}_B) \to L(\mathcal{H}_A)$ such that for any $f \in L(\mathcal{H}_A)$ and $g \in L(\mathcal{H}_B)$

$$\operatorname{tr}_B(f \otimes g) = \operatorname{tr}(g) f$$

In the case of density matrices, this tells us how to split a composite system where the subsystems are not entangled. If ρ_A represents the state of system A and ρ_B the state of system B, such that the states are not entangled, the composition of the two states would be $\rho_A \otimes \rho_B$ and taking a partial trace over $\mathcal{H}_B$, tracing out system B, we would recover

$$\operatorname{tr}_B(\rho_A \otimes \rho_B) = \operatorname{tr}(\rho_B)\rho_A = \rho_A.$$

The partial trace is then the unique map on the space of all operators $L(\mathcal{H}_A \otimes \mathcal{H}_B)$ that respects this property.

Proposition 5.1.9. *The defining property in 5.1.8 defines a unique map that respects quantum measurements. [Ian:* write out what this means and prove it i guess.*]*

Proof. □

Given a basis $e_1, \dots, e_d$ for $\mathcal{H}_A$ and $f_1, \dots, f_s$ for $\mathcal{H}_B$, the elements $e_j \otimes f_k$ form a basis for $\mathcal{H}_A \otimes \mathcal{H}_B$. A linear operator on this space could be represented as a matrix M with respect to this basis such that $M = (M_{k\ell,ij})$ where the $M_{k\ell,ij}$ entry is in the row corresponding to the $e_k \otimes f_\ell$ basis element and is in the column corresponding to the $e_i \otimes f_j$ basis element. The partial trace over $\mathcal{B}$ with respect to this choice of basis is then the $d \times d$ matrix

$$\mathrm{tr}_B(M) = (\sum_{j=1}^{s} M_{kj,ij})_{k,i}$$

and like wise tracing out system A would give

$$\mathrm{tr}_A(M) = (\sum_{i=1}^{d} M_{j\ell,ij})_{k,i}.$$

[Ian: *I think. i am guessing here*] [Ian: *there is another helpful way to write this which i may include. but this is nice if you write out the matrix*]

Example 5.1.10. Considering again the state in the previous example where $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\rho = |\psi\rangle\langle\psi|$. We can use the partial trace to trace out the second qubit. The density matrix corresponding to the first qubit would then be $\rho_1 = \mathrm{tr}_2(|\psi\rangle\langle\psi|) = \frac{1}{2}I$, which agrees with the intuition from the previous example.

Quantum Channels

Quantum states evolve with respect to the Schrödinger equation

$$i\bar{h}\frac{d|\psi\rangle}{dt} = H|\psi\rangle$$

where H is a Hamiltonian. In the previous sections we have discussed that the quantum state space for a closed system can be modeled as a complex projective space. The Schrödinger equation tells us that in fact, quantum state spaces are homogeneous manifolds with an action by the lie group of unitary operators. The Schrödinger equation tells us that the corresponding lie algebra is that of the skew hermitian matrices, which exponential to the unitary group.[Ian: *I think i am slightly wrong here. but i dont know how*]

More concretely if $|\psi_1\rangle$ describes a closed system at time t_1, and $|\psi_2\rangle$ the system at time t_2, the two states are related by some unitary U such that $|\psi_2\rangle = U|\psi_1\rangle$. Under the density matrix formulation, if ρ_1 describes a system at time t_1, and ρ_2 the system at time t_2, then the two states are related by some unitary U such that $\rho_2 = U\rho_1 U^\dagger$. Furthermore any unitary can be realized as some evolution of a closed system.[Ian: *something something do i have to consider anti-unitaries?*]

By allowing a system to be open, either by considering unitary operations acting on a larger space, or in measuring a system, we will encounter more general maps representing the evolution of a system, which we will call quantum channels.

Definition 5.1.11. Consider a linear map $\Psi : L(\mathcal{H}_A) \to L(\mathcal{H}_B)$ from the operators of the state space $\mathcal{H}_A$ to the operators of the state space $\mathcal{H}_B$. Ψ is a quantum channel if it satisfies the following

(CP) Ψ is completely positive: meaning $I_n \otimes \Psi$ is positive for all $n \in \mathbb{Z}^{>0}$

(TP) Ψ is trace preserving: meaning $\mathrm{tr}(\Psi\rho) = \mathrm{tr}(\rho)$

Notice that a unitary would be an example of a quantum channel. A theorem by Choi says if $\dim(\mathcal{H}_A) = n$ and $\dim(\mathcal{H}_B) = m$ then any completely positive linear map can be decomposed such that

$$\Psi(A) = \sum_{j=1}^{N} K_j A K_j^\dagger$$

for some $N < nm$ and a collection of operators $\{K_j\}_{j=1}^N$, called Kraus operators which satisfy a completeness condition $\sum_{j=1}^N K_j^\dagger K_j = I$ if and only if Ψ is trace preserving. The minimum number of Kraus operators N is called the Kraus rank. It is common to take this result as the definition of a quantum channel. Some authors who have studied the connection between design theory and quantum information, as we will do in section **??**, call quantum channels **entanglement breaking maps**, and call the entanglement breaking rank the

Example 5.1.12. Quantum measurements are examples of quantum channels. Consider a collection of quantum measurement operators $\{M_m\}_{m\in\Omega}$. We can use these as the Kraus Operators of a quantum channel Φ by defining

$$\Phi(\rho) = \sum_{m \in \Omega} M_m \rho M_m^\dagger = \sum_{m \in \Omega} p(m) \frac{M_m \rho M_m^\dagger}{p(m)}$$

which is the ensemble state that is equal to $\frac{M_m \rho M_m^\dagger}{p(m)}$, the result if the measurement outcome is m, with probability $p(m)$.

Quantum operators also describe the interactions of systems with the environment or with other systems. For example if a system is not perfectly closed

Example 5.1.13. Here we will construct a quantum channel that introduces noise into a system, through interactions with the environment. Let $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ represent the state of a single qubit in which we are interested in, and fix $|e\rangle$ to be a single qubit representing the environment. In this case we are interested in the state $|e\rangle|\psi\rangle$ which represents the larger system consisting of the two qubits. If we assume that these two qubits form a closed system, any operation of the entire system will be that of a unitary action on the $|e\rangle \otimes |\psi\rangle$. Consider the unitary

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

which will act on the entire system as $CNOT(|e\rangle \otimes |\psi\rangle)$. Notice that when $|e\rangle = |0\rangle$, then the resulting state is unchanged: $CNOT(|e\rangle \otimes |\psi\rangle) = |e\rangle \otimes |\psi\rangle$. If $|e\rangle = \sqrt{p}|0\rangle + \sqrt{1-p}|1\rangle$, then the initial state is

$$|e\rangle \otimes |\psi\rangle = \alpha\sqrt{p}|00\rangle + \beta\sqrt{p}|01\rangle + \alpha\sqrt{1-p}|10\rangle + \beta\sqrt{1-p}|11\rangle$$

and after applying the unitary $CNOT$ the resulting state is

$$CNOT(|e\rangle \otimes |\psi\rangle) = \alpha\sqrt{p}|00\rangle + \beta\sqrt{p}|01\rangle + \beta\sqrt{1-p}|10\rangle + \alpha\sqrt{1-p}|11\rangle$$

which in general can not be decomposed as a tensor product of the states of the individual qubits, meaning to analyze the second qubit we will need to use the density matrix formulation and a partial trace to trace out the first qubit. If we look at the density matrix we would have

$$\rho = (\alpha\sqrt{p}|00\rangle + \beta\sqrt{p}|01\rangle + \beta\sqrt{1-p}|10\rangle + \alpha\sqrt{1-p}|11\rangle)(\alpha\sqrt{p}|00\rangle + \beta\sqrt{p}|01\rangle + \beta\sqrt{1-p}|10\rangle + \alpha\sqrt{1-p}|$$

$$= \begin{bmatrix} \alpha^2 p & \alpha\beta p & \alpha\beta\sqrt{p}\sqrt{1-p} & \alpha^2\sqrt{p}\sqrt{1-p} \\ \alpha\beta p & \beta^2 p & \beta^2\sqrt{p}\sqrt{1-p} & \alpha\beta\sqrt{p}\sqrt{1-p} \\ \alpha\beta\sqrt{p}\sqrt{1-p} & \beta^2\sqrt{1-p}\sqrt{p} & \beta^2(1-p) & \alpha\beta(1-p) \\ \alpha^2\sqrt{p}\sqrt{1-p} & \alpha\beta\sqrt{1-p}\sqrt{p} & \alpha\beta(1-p) & \alpha^2(1-p) \end{bmatrix}$$

and taking a partial trace, tracing out the first qubit, will give us

$$\rho_2 = \begin{bmatrix} \alpha^2 p + \beta^2(1-p) & \alpha\beta p + \alpha\beta(1-p) \\ \alpha\beta p + \alpha\beta(1-p) & \beta^2 p + \alpha^2(1-p) \end{bmatrix}$$

If we wanted to measure this state with respect to the computational basis we could use the measurement operators defined in section idk to get that

$$p(0) = \alpha^2 p + \beta^2(1-p) \text{ and } p(1) = \beta^2 p + \alpha^2(1-p)$$

This process is a model of a noisy channel that takes in a pure state $|\psi\rangle\langle\psi|$ and maps it to the density matrix ρ_1 that represents a bit flip parameterized by p. This also highlights a unique difficulty in quantum computing: noise is continuous rather than discrete as it is in the classical setting.

5.2 Framed by Quantum Measurements

[Ian: *Talk about quantum designs, or i guess weighted projective designs.*]

Now that we have discussed the basic of quantum mechanics, we will expand on the role of POVMs and their connection to frame theory and design theory.

A paper by Scott(paper here) formulated a mean-squared error associated with a POVM $\{E_j\}$ and showed that on pure states, the mean-squared error was minimized if and only if $\mathrm{rank}(E_j) = 1$ for each j and if the POVM operators formed a weighted projective 2-design. Furthermore, in the case of a minimal weighted projective 2-design, that is when $n = d^2$, the weights are equal.

Projective t-Designs

The standard definition of a projective t-designs is a collection of points, which corresponds to a collection of pure states, that satisfy the **exact cubature rule**, for a specific class of homogeneous functions. In general a collection of functions $\mathcal{F} = \{f : D \to C\}$, which are integrable with respect to some normalized measure μ, and a finite collection of points $\{d_j\}_j = 1^n$, satisfy the exact cubature rule if for any function in $\mathcal{F}$: integrating with respect to the measure is the same as averaging the function over the n points. That is they satisfy

$$\frac{1}{n}\sum_{j=1}^{n} f(d_j) = \int_D f(x)d\mu \text{ for all } f \in \mathcal{F}.$$

A projective t-design is a special case of this exact cubature rule for phase invariant monomials over the state space: $\mathcal{F} = \mathrm{Hom}_d(t)$ which are the function $\mathbb{C}^d \to \mathbb{C}$ spanned by the monomial that map $(z_1, \ldots, z_d) \mapsto z_1^{\alpha_1} \cdots z_d^{\alpha_d} \overline{z}_1^{\beta_1} \cdots \overline{z}_d^{\beta_d}$ such that $t = \sum_{j=1}^d \alpha_j = \sum_{j=1}^d \beta_j$. Projective t-designs are then collection of unit vectors of $\mathbb{C}^d$ that satisfy the exact cubature rule with the functions of $\mathrm{Hom}_d(t)$, along with the normalized Haar measure, the unique measure invariant under the unitary action. Throughout we will denote $S(\mathbb{C}^d)$ to be the set of all unit vectors of $\mathbb{C}^d$.

Definition 5.2.1. A (rank-one) complex projective t-design for $\mathbb{C}^d$ is a collection $\{\psi_j\}_{j=1}^n$ of unit vector of $\mathbb{C}^d$ that satisfy the exact cubature rule

$$\frac{1}{n}\sum_{j=1}^{n} f(\psi_j) = \int_{S(\mathbb{C}^d)} f(x)d\mu(x) \text{ for all } f \in \mathrm{Hom}_d(t)$$

The exact cubature rule is equivalent to the following formulations

Proposition 5.2.2. *For a collection of vectors $\{\psi_j\}_{j=1}^n$ in $S(\mathbb{C}^d)$ the following are equivalent*

(a) $\frac{1}{n}\sum_{j=1}^{n} f(\psi_j) = \int_{S(\mathbb{C}^d)} f(x)d\mu(x)$ *for all* $f \in$ *Hom*$_d(t)$

(b) $\frac{1}{n}\sum_{j=1}^{n} |\psi^{\otimes t}\rangle\langle\psi^{\otimes t}| = \binom{d+t-1}{t}^{-1}\Pi_d^{(t)}$

(c) $\frac{1}{n^2}\sum_{j=1}^{n}\sum_{k=1}^{n} |\langle\psi_j \,|\, \psi_k\rangle|^{2t} = \binom{d+t-1}{t}^{-1}$

where $\Pi_d^{(t)} : (\mathbb{C}^d)^{\otimes t} \to (\mathbb{C}^d)^{\otimes t_{sym}}$ *is the orthogonal projection onto* $(\mathbb{C}^d)^{\otimes t_{sym}}$*. Likewise*

An important observation here is that condition (b) from prop ?? means that a projective t-designs is a tight frame for $(\mathbb{C}^d)^{\otimes t}_{\text{sym}}$ which has dimension $\binom{d+t-1}{t}$. Condition (c) is related to the frame potential of this frame.

[Ian: *why do projective 2 designs have lower bound $n >= d^2$? Its becasue of frame condition*]

The third condition is a average of the moduli of inner products, [Ian: *motivate via min/maxing: and in order to minimize the maximum of this average we would need ... but like correct, for t=1?*]. This motivates the first connection between t-designs ($t \geq 2$) and ETFs. First we will say that a collection of vectors $\{\psi_j\}$ is **equiangular** if $|\langle\psi_j \,|\, \psi_k\rangle|^2$ is constant for all $j \neq k$. This is equivalent to

$$|\{|\langle\psi_j \,|\, \psi_k\rangle| : j \neq k\}| = 1$$

In the case of a design, this means the degree is 1.[4]. ←$\boxed{\text{I}}$

Proposition 5.2.3. *Consider a collection of vectors $\Psi = \{\psi_j\}_{j=1}^n$ in $S(\mathbb{C}^d)$:*

[4] Ian: *based on definition from zauner's thesis*

- *If Ψ is a projective 2-design then $n \geq d^2$, and in the case of equality Ψ is equiangular.*

- *If Ψ is equiangular then $n \leq d^2$, and in the case of equality Ψ is a projective 2-design.*

Therefore in the case equality, when $n = d^2$, Ψ is an ETF if and only if Ψ is a projective 2-design.

In the case where $n = d^2$ we will say Ψ is a **tight** projective 2-design.

Just as in section 1, we can reformulate projective t-designs in terms of density matrices.

[Ian: *The standard definition of PSD requires a matrix to be hermitian. But when do other condition imply hermitian? From wikipidea: A square matrix A is Hermitian if and only if it is unitarily diagonalizable with real eigenvalues. If we consider rank 1 projections: it has real eigenvalues and is unitarily diagnolizable!*]

Proposition 5.2.4. *A collection of rank-one density*[5] *matrices $\{\rho_j\}_{j=1}^n$ induces a (rank-one) projective t-design if it satisfies one of the following equivalent conditions*

- $\frac{1}{n}\sum_{j=1}^n f(\rho_j) = \int_{S(\mathbb{C}^d)} f(|x\rangle\langle x|)d\mu(x)$ *for all $f \in Hom_d(t)$*

- $\frac{1}{n}\sum_{j=1}^n \rho_j^{\otimes t} = \binom{d+t-1}{t}^{-1}\Pi_d^{(t)}$

- $\frac{1}{n^2}\sum_{j=1}^n \sum_{k=1}^n \operatorname{tr}(\rho_j\rho_k)^t = \binom{d+t-1}{t}^{-1}$

Where $Hom_d(t)$ are the function $\mathbb{C}^{d\times d} \to \mathbb{C}$ spanned by degree t monomials on the entires of the matrices.

With this perspective 1-design are collections of rank-one density matrices where the average of any entry is equal to the average over all pure states, or all rank-one projection matrices. A 2-design is then when the second moments are equal: the variances and covariances being equal. A general t-design is then indicating equality up to the t-th moment. Throughout we will refer to collections of rank-one density matrices that satisfy prop **??** as being a projective t-designs and ignore the fact that they induce multiple distinct, but equivalent, projective 2-designs.

[5] Ian: *the paper i am going off of only requires the mats to be projections and doesnt care about hermitian. Does this matter? idk*

More generally we can allow for weighted averages of the rank-one density matrices in the definition of a design.

Definition 5.2.5. A collection of rank-one density matrices $\{\rho_j\}_{j=1}^n$ and a corresponding collection of positive weights $\{w_j\}_{j=1}^n$ is called a rank-one weighted projective t-design if

$$\sum_{j=1}^n w_j \rho_j^{\otimes t} = \binom{d+t-1}{t}^{-1} \Pi_d^{(t)} \text{ and } \sum_{j=1}^n w_j = 1$$

[Ian: *need to show that $n <= d^2$ and equality gives weights $= 1/n$*]

Proposition 5.2.6. *Consider a collection of vectors $\Psi = \{\psi_j\}_{j=1}^n$ in $S(\mathbb{C}^d)$ and weights $\{w_j\}_{j=1}^n$: If Ψ is a weighted projective 2-design then $n \geq d^2$, and in the case of equality the weights are equal and $w_j = \frac{1}{n}$.*

Proof. [Ian: *prove this at some point*] □

POVMs as Projective 2-designs

Now that we have introduced projective 2-designs we will connect them back to POVMs, showing that POVMs that minimize a mean-squared error over pure states, form weighted projective 2-designs, and therefore the minimal such POVMs form projective 2-designs which are equivalently ETFs.

Bibliography

[ABDF17] Marcus Appleby, Ingemar Bengtsson, Irina Dumitru, and Steven Flammia. “DIMENSION TOWERS OF SICS. I. ALIGNED SICS AND EMBEDDED TIGHT FRAMES”. In: *J. Math. Phys* 58.11 (2017). 108

[AFF11] DM Appleby, Steven T Flammia, and Christopher A Fuchs. “The Lie algebraic significance of symmetric informationally complete measurements”. In: *J. Math. Phys.* 52.2 (2011). 80, 82

[Axl24] Sheldon Axler. *Linear algebra done right*. Fourth. Undergraduate Texts in Mathematics. Springer, Cham, 2024, pp. xvii+390. ISBN: 978-3-031-41025-3; 978-3-031-41026-0. DOI: 10.1007/978-3-031-41026-0. 42

[Bar23] Jacob L. Barnett. *Locality and Exceptional Points in Pseudo-Hermitian Physics*. 2023. arXiv: 2306.04044 [quant-ph]. 36

[BBRV02] Somshubhro Bandyopadhyay, P. Oscar Boykin, Vwani Roychowdhury, and Farrokh Vatan. “A new proof for the existence of mutually unbiased bases”. In: vol. 34. 4. Quantum computation and quantum cryptography. 2002, pp. 512–528. DOI: 10.1007/s00453-002-0980-7. 63

[BE98] Ulrich Brehm and Boumediene Et-Taoui. “Congruence criteria for finite subsets of complexprojective and complex hyperbolic spaces”. In: *manuscripta mathematica* 96.1 (May 1998), pp. 81–95. ISSN: 1432-1785. DOI: 10.1007/s002290050055. 80

[BFMW13] Afonso S. Bandeira, Matthew Fickus, Dustin G. Mixon, and Percy Wong. “The road to deterministic matrices with the restricted isometry property”. In: *J. Fourier Anal. Appl.* 19.6 (2013), pp. 1123–1149. ISSN: 1069-5869. DOI: 10.1007/s00041-013-9293-2. 1, 42

[BLRTT09] Bernhard G. Bodmann, My Le, Letty Reza, Matthew Tobin, and Mark Tomforde. "Frame theory for binary vector spaces". In: *Involve* 2.5 (2009), pp. 589–602. ISSN: 1944-4176,1944-4184. DOI: 10.2140/involve.2009.2.589. 4

[CFMPS13] Peter G. Casazza, Matthew Fickus, Dustin G. Mixon, Jesse Peterson, and Ihar Smalyanau. "Every Hilbert space frame has a Naimark complement". In: *J. Math. Anal. Appl.* 406.1 (2013), pp. 111–119. ISSN: 0022-247X,1096-0813. DOI: 10.1016/j.jmaa.2013.04.047. 49, 51, 95

[CL91] P. J. Cameron and J. H. van Lint. *Designs, graphs, codes and their links*. Vol. 22. London Mathematical Society Student Texts. Cambridge University Press, Cambridge, 1991, pp. x+240. ISBN: 0-521-41325-7; 0-521-42385-6. DOI: 10.1017/CBO9780511623714. 87, 90, 106, 123, 124

[Cra86] Henry Crapo. "Orthogonality". In: *Theory of Matroids*. Ed. by Neil White. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 1986, pp. 76–96. ISBN: 978-0-521-09202-9. DOI: 10.1017/CBO9780511629563.008. 36, 41

[CW16] Tuan-Yow Chien and Shayne Waldron. "A characterization of projective unitary equivalence of finite frames and applications". In: *SIAM J. Discrete Math.* 30.2 (2016), pp. 976–994. ISSN: 0895-4801,1095-7146. DOI: 10.1137/15M1042140. 78, 80, 82, 83, 85, 86

[DBBA13] Hoan Bui Dang, Kate Blanchfield, Ingemar Bengtsson, and D. M. Appleby. "Linear dependencies in Weyl–Heisenberg orbits". In: *Quantum Information Processing* 12.11 (Nov. 2013), pp. 3449–3475. ISSN: 1573-1332. DOI: 10.1007/s11128-013-0609-6. 108

[DF04] David S. Dummit and Richard M. Foote. *Abstract algebra*. Third. John Wiley & Sons, Inc., Hoboken, NJ, 2004, pp. xii+932. ISBN: 0-471-43334-9. 7, 10, 13, 14

[DL98] Xingde Dai and David R. Larson. "Wandering vectors for unitary systems and orthogonal wavelets". In: *Mem. Amer. Math. Soc.* 134.640 (1998), pp. viii+68. ISSN: 0065-9266. 95

[EZ01] Thomas Ericson and Victor Zinoviev. *Codes on Euclidean spheres*. Vol. 63. North-Holland Mathematical Library. North-Holland Publishing Co., Amsterdam, 2001, pp. xiv+549. ISBN: 0-444-50329-3. 60

[Fej65] L. Fejes Tóth. "Distribution of points in the elliptic plane". In: *Acta Math. Acad. Sci. Hungar.* 16 (1965), pp. 437–440. ISSN: 0001-5954. DOI: 10.1007/BF01904849. 1, 42

[FHS17] Christopher A. Fuchs, Michael C. Hoang, and Blake C. Stacey. "The SIC Question: History and State of Play". In: *Axioms* 6.3 (2017). DOI: 10.3390/axioms6030021. 1, 42

[FIS97] Stephen H. Friedberg, Arnold J. Insel, and Lawrence E. Spence. *Linear algebra*. Third. Prentice Hall, Inc., Upper Saddle River, NJ, 1997, pp. xiv+557. ISBN: 0-13-233859-9. 30, 32

[FJKM18] Matthew Fickus, John Jasper, Emily J. King, and Dustin G. Mixon. "Equiangular tight frames that contain regular simplices". In: *Linear Algebra Appl.* 555 (2018), pp. 98–138. ISSN: 0024-3795,1873-1856. DOI: 10.1016/j.laa.2018.06.004. 80, 106, 110

[FJM18] Matthew Fickus, John Jasper, and Dustin G. Mixon. "Packings in real projective spaces". In: *SIAM J. Appl. Algebra Geom.* 2.3 (2018), pp. 377–409. ISSN: 2470-6566. DOI: 10.1137/17M1137528. 55

[FM16] Matthew Fickus and Dustin G. Mixon. *Tables of the existence of equiangular tight frames*. 2016. arXiv: 1504.00253 `[math.FA]`. 58

[GIJM22a] Gary R. W. Greaves, Joseph W. Iverson, John Jasper, and Dustin G. Mixon. “Frames over finite fields: basic theory and equiangular lines in unitary geometry”. In: *Finite Fields Appl.* 77 (2022), Paper No. 101954, 41. ISSN: 1071-5797,1090-2465. DOI: 10.1016/j.ffa.2021.101954. 4, 66–69, 72, 74, 75, 78, 92, 93, 95, 97, 98, 100

[GIJM22b] Gary R. W. Greaves, Joseph W. Iverson, John Jasper, and Dustin G. Mixon. “Frames over finite fields: equiangular lines in orthogonal geometry”. In: *Linear Algebra Appl.* 639 (2022), pp. 50–80. ISSN: 0024-3795,1873-1856. DOI: 10.1016/j.laa.2021.11.024. 4, 5, 66, 67, 75–77, 90, 93, 104, 105, 107, 114

[Gil18] Neil I Gillespie. “Equiangular lines, incoherent sets and quasi-symmetric designs”. In: *arXiv preprint arXiv:1809.05739* (2018). 3, 58, 106, 114, 119, 122, 123

[GP77] P. X. Gallagher and R. J. Proulx. “Orthogonal and unitary invariants of families of subspaces”. In: *Contributions to algebra (collection of papers dedicated to Ellis Kolchin)*. Academic Press, New York-London, 1977, pp. 157–164. ISBN: 0-12-080550-2. 80, 86

[GR01] Chris Godsil and Gordon Royle. *Algebraic graph theory*. Vol. 207. Graduate Texts in Mathematics. Springer-Verlag, New York, 2001, pp. xx+439. ISBN: 0-387-95241-1; 0-387-95220-9. DOI: 10.1007/978-1-4613-0163-9. 3, 58

[Gro02] Larry C. Grove. *Classical groups and geometric algebra*. Vol. 39. Graduate Studies in Mathematics. American Mathematical Society, Providence, RI, 2002, pp. x+169. ISBN: 0-8218-2019-2. DOI: 10.1090/gsm/039. 16, 18, 26

[Gur21] Robert M. Guralnick. “On the singular value decomposition over finite fields and orbits of $\mathrm{GU} \times \mathrm{GU}$”. In: *Indag. Math. (N.S.)* 32.5 (2021), pp. 1083–1094. ISSN: 0019-3577,1872-6100. DOI: 10.1016/j.indag.2021.01.006. 32

[HJ13] Roger A. Horn and Charles R. Johnson. *Matrix analysis*. Second. Cambridge University Press, Cambridge, 2013, pp. xviii+643. ISBN: 978-0-521-54823-6. 36

[HL00] Deguang Han and David R. Larson. “Frames, bases and group representations”. In: *Mem. Amer. Math. Soc.* 147.697 (2000), pp. x+94. ISSN: 0065-9266,1947-6221. DOI: 10.1090/memo/0697. 49

[Hug07] Lane Hughston. *$d = 3$ SIC-POVMs and Elliptic Curves*. Perimeter Institute, Seminar Talk, http://pirsa.org/07100040/. Oct. 2007. 108

[IKM21] Joseph W. Iverson, Emily J. King, and Dustin G. Mixon. “A note on tight projective 2-designs”. In: *J. Combin. Des.* 29.12 (2021), pp. 809–832. ISSN: 1063-8539,1520-6610. DOI: 10.1002/jcd.21804. 4, 67

[Ivo81] I D Ivonovic. “Geometrical description of quantal state determination”. In: *Journal of Physics A: Mathematical and General* 14.12 (Dec. 1981), p. 3241. DOI: 10.1088/0305-4470/14/12/019. 63

[Jac53] Nathan Jacobson. “Bilinear Forms”. en. In: *Lectures in Abstract Algebra: II. Linear Algebra*. Ed. by Nathan Jacobson. Graduate Texts in Mathematics. New York, NY: Springer, 1953, pp. 136–171. ISBN: 978-1-4684-7053-6. DOI: 10.1007/978-1-4684-7053-6_5. 16, 18, 26, 79

[JK25] Ian Jorquera and Emily J. King. *On the Structure of Frames and Equiangular Lines over Finite Fields and their Connections to Design Theory*. 2025. arXiv: 2505.12175 [math.CO]. 4

[JKM19] John Jasper, Emily J. King, and Dustin G. Mixon. *Game of Sloanes: Best known packings in complex projective space*. 2019. arXiv: 1907.07848 [math.MG]. 55

[Kin19] Emily J King. “2-and 3-covariant equiangular tight frames”. In: *2019 13th International conference on Sampling Theory and Applications (SampTA)*. IEEE. 2019, pp. 1–4. 101

[Kin25] Emily J. King. *k-Homogeneous Equiangular Tight Frames*. 2025. arXiv: 2505.00160 [math.FA]. 36

[KM25] Emily J King and Dustin G Mixon. “The impossibility of extending the Naimark complement”. arXiv:2504.09534. 2025. 51, 95

[LL00] T. Y. Lam and K. H. Leung. “On vanishing sums of roots of unity”. In: *J. Algebra* 224.1 (2000), pp. 91–109. ISSN: 0021-8693,1090-266X. DOI: 10.1006/jabr.1999.8089. 65

[LL96] T. Y. Lam and K. H. Leung. “Vanishing sums of mth roots of unity in finite fields”. In: *Finite Fields Appl.* 2.4 (1996), pp. 422–438. ISSN: 1071-5797,1090-2465. DOI: 10.1006/ffta.1996.0025. 6, 128, 131–133, 135

[LN96] Rudolf Lidl and Harald Niederreiter. *Finite Fields*. 2nd ed. Encyclopedia of Mathematics and its Applications. Cambridge: Cambridge University Press, 1996. ISBN: 978-0-521-39231-0. DOI: 10.1017/CBO9780511525926. 7, 128

[LS73] P. W. H. Lemmens and J. J. Seidel. “Equiangular lines”. In: *J. Algebra* 24 (1973), pp. 494–512. ISSN: 0021-8693. DOI: 10.1016/0021-8693(73)90123-3. 58, 106

[MD14] Ahmed Medra and Timothy N. Davidson. “Flexible codebook design for limited feedback systems via sequential smooth optimization on the Grassmannian manifold”. In: *IEEE Trans. Signal Process.* 62.5 (2014), pp. 1305–1318. ISSN: 1053-587X. DOI: 10.1109/TSP.2014.2301137. 1, 42

[MQKF13] Dustin G. Mixon, Christopher J. Quinn, Negar Kiyavash, and Matthew Fickus. “Fingerprinting with equiangular tight frames”. In: *IEEE Trans. Inform. Theory* 59.3 (2013), pp. 1855–1865. ISSN: 0018-9448. DOI: 10.1109/TIT.2012.2229781. 1, 42

[MST21] Gary McConnell, Harry Spencer, and Afaq Tahir. “Evidence for and against Zauner’s MUB conjecture in $\mathbb{C}^6$”. In: *Quantum Inf. Comput.* 21.9-10 (2021), pp. 721–736. ISSN: 1533-7146. 5, 64, 124, 125

[MW24] Daniel McNulty and Stefan Weigert. *Mutually Unbiased Bases in Composite Dimensions – A Review*. 2024. arXiv: 2410.23997 [quant-ph]. 63, 64

[Neu43] M. A. Neumark. “On a representation of additive operator set functions”. In: *C. R. (Doklady) Acad. Sci. URSS (N.S.)* 41 (1943), pp. 359–361. 49, 95

[Neu82] A. Neumaier. “Regular sets and quasi-symmetric 2-designs”. In: *Combinatorial Theory*. Ed. by Dieter Jungnickel and Klaus Vedder. Berlin, Heidelberg: Springer Berlin Heidelberg, 1982, pp. 258–275. ISBN: 978-3-540-39380-1. 124

[Oxl11] James Oxley. *Matroid theory*. Second. Vol. 21. Oxford Graduate Texts in Mathematics. Oxford University Press, Oxford, 2011, pp. xiv+684. ISBN: 978-0-19-960339-8. DOI: 10.1093/acprof:oso/9780198566946.001.0001. 36, 40, 41

[PP72] Martin H. Pearl and Alan I. Penn. “Normal matrices with entries from an arbitrary field of characteristic $\neq$ 2”. In: *J. Res. Nat. Bur. Standards Sect. B* 76B (1972), pp. 119–143. ISSN: 0022-4340. 35

[Ran55] R. A. Rankin. “The closest packing of spherical caps in n dimensions”. In: *Proc. Glasgow Math. Assoc.* 2 (1955), pp. 139–144. ISSN: 2040-6185,2051-2104. 57, 60

[RBSC04] Joseph M. Renes, Robin Blume-Kohout, A. J. Scott, and Carlton M. Caves. “Symmetric informationally complete quantum measurements”. In: *J. Math. Phys.* 45.6 (2004), pp. 2171–2180. ISSN: 0022-2488. DOI: 10.1063/1.1737053. 1, 42

[Sei76] J. J. Seidel. “A survey of two-graphs”. In: *Colloquio Internazionale sulle Teorie Combinatorie (Roma, 1973), Tomo I*. Accad. Naz. Lincei, Rome, 1976, pp. 481–511. 104

[SH03] Thomas Strohmer and Robert W. Heath Jr. “Grassmannian frames with applications to coding and communication”. In: *Appl. Comput. Harmon. Anal.* 14.3 (2003), pp. 257–275. ISSN: 1063-5203. 1, 42

[STDH07] Mátyás A. Sustik, Joel A. Tropp, Inderjit S. Dhillon, and Robert W. Heath Jr. “On the existence of equiangular tight frames”. In: *Linear Algebra Appl.* 426.2-3 (2007), pp. 619–635. ISSN: 0024-3795,1873-1856. DOI: 10.1016/j.laa.2007.05.043. 3, 58

[Str07] Nate Strawn. “Geometry and Constructions of Finite Frames”. MA thesis. Texas A&M University, May 2007. 86

[Tay77] D. E. Taylor. “Regular 2-graphs”. In: *Proc. London Math. Soc. (3)* 35.2 (1977), pp. 257–274. ISSN: 0024-6115,1460-244X. DOI: 10.1112/plms/s3-35.2.257. 87, 119, 120, 122

[TZ59] Olga Taussky and Hans Zassenhaus. “On the similarity transformation between a matrix and its transpose”. In: *Pacific J. Math.* 9 (1959), pp. 893–896. ISSN: 0030-8730,1945-5844. 36

[VS66] J. H. Van Lint and J. J. Seidel. “Equilateral point sets in elliptic geometry”. In: *Indagationes Mathematicae, Proc. Koninkl. Ned. Akad. Wetenschap. Ser. A* 69.3 (1966), pp. 335–34. 78

[Wal09] Shayne Waldron. “On the construction of equiangular frames from graphs”. In: *Linear Algebra Appl.* 431.11 (2009), pp. 2228–2242. ISSN: 0024-3795,1873-1856. DOI: 10.1016/j.laa.2009.07.016. 104

[Wal20] Shayne Waldron. “Tight frames over the quaternions and equiangular lines”. arXiv:2006.06126. 2020. 80

[Wel74a] L. Welch. “Lower Bounds on the Maximum Cross Correlation of Signals”. In: *IEEE Trans Inf Theory* 20.3 (May 1974), pp. 397–399. ISSN: 0018-9448. DOI: 10.1109/TIT.1974.1055219. 1, 42

[Wel74b] L. Welch. “Lower bounds on the maximum cross correlation of signals (Corresp.)” In: *IEEE Transactions on Information Theory* 20.3 (1974), pp. 397–399. DOI: 10.1109/TIT.1974.1055219. 57

[Wil09] James B. Wilson. “Decomposing p-groups via Jordan algebras”. In: *J. Algebra* 322.8 (2009), pp. 2642–2679. ISSN: 0021-8693,1090-266X. DOI: 10.1016/j.jalgebra.2009.07.029. 16, 18

[Zau11] G. Zauner. “Quantum designs: foundations of a noncommutative design theory”. In: *Int. J. Quantum Inf.* 9.1 (2011), pp. 445–507. ISSN: 0219-7499. DOI: 10.1142/S0219749911006776. 3

[Zau99] G. Zauner. “Quantendesigns - Grundzüge einer nichtkommutativen Designtheorie”. English translation in International Journal of Quantum Information (IJQI) 9 (1), 445–507, 2011. PhD thesis. University Wien (Austria), 1999. 3

[Zhu15] Huangjun Zhu. “Super-symmetric informationally complete measurements”. In: *Ann. Physics* 362 (2015), pp. 311–326. ISSN: 0003-4916. DOI: 10.1016/j.aop.2015.08.005. 101