LUNDS
UNIVERSITET

Generalized Bell Measurements and Equiangular Lines

Amanda Wei

Thesis submitted for the degree of Master of Science
Project duration: 8 months
Supervisor: Armin Tavakoli
Department of Physics
Division of Mathematical Physics
Spring 2024

Acknowledgements

I would like to thank first and foremost my supervisor, Armin Tavakoli, for making this research project possible. Thank you for picking out such a fun and interesting problem for me to work on, and for your patience and guidance throughout. Thank you for promoting a lively research environment and for incorporating me into your extended research community by, including but not limited to, introducing me to and involving me in discussions with other researchers who may have been interested in my project. Your dedication to your students and talent for teaching are invaluable.

I thank Gabriele for always finding the time to discuss with me and for answering all the questions I felt were too trivial to go to Armin with, and for having post-meeting meetings to clarify things that I didn't follow during the actual meeting. Thanks for allowing me to return the favor by introducing you to ramen and boba.

I would like to thank Elna and Guglielmo for keeping me company in the examensarbete room and for the afternoon walks. Thanks to the rest of the QIT Scania group including Nicola, Shishir, and Carles for being a fun bunch of people to hang out with outside of working hours including Friday pub.

It goes without saying that I wouldn't be where I am without my mother, father, brother, and Grace. I am endlessly grateful for your presence, patience, and love.

Abstract

This thesis is ultimately concerned with a natural and optimal generalization of the familiar Bell state measurement on four basis states. Measurements in quantum mechanics are interactive processes, meaning the observer actively changes the state they extract information from. Different measurements differ in the degree of the disturbance induced, and in the amount and type of information gained. For example, some measurements result in well-defined post-measurement states while others provide only outcome statistics. The variety of measurements each have unique features enabling all sorts of fine-tuned and tailored manipulations of quantum states.

Another central feature of the Bell state measurement which the generalized measurements inherit is that the measurements are constructed of maximally entangled states. Mathematically, this introduces an interesting restriction of the construction of equiangular lines to the subset of maximally entangled states. Quantum mechanically, this opens the door to unknown yet exciting possibilities for symmetric joint measurements as SIC-POVMs have done for measurements over single qudits.

In this thesis, equiangular sets of the simplest case of bipartite-qubit states are considered and interpreted as generalized Bell measurements. The construction of this generalization borrows techniques from frame theory and builds on the tradition of equiangular lines in real and complex dimensions, so a treatment of the relevant mathematics are presented first. Then a central point of distinction between the generalized Bell measurements and the Bell state measurement is the difference between projective measurements and positive-operator valued ones, so a discussion of measurements in quantum mechanics and entanglement comes next. Finally, explicit constructions are given and studied in the setting of quantum state discrimination. It is found that the generalized five state measurement is comparatively more non-local, or less distinguishable, than the Bell state measurement even with access to two copies. Furthermore, 5-state separable sets and 6-state maximally entangled sets are constructed. Various properties including uniqueness and optimality are also discussed.

Contents

Symbols and Acronyms

$\hat{v}$	Normalized vector v
$\mathbb{Z}$	Set of integers
$\mathbf{1}_d$	All-1's vector in dimension d
J_d	$d \times d$ all-1's matrix
$\mathbb{C}^d$	d-dimensional complex space
$\mathbb{H}^d$	either $\mathbb{R}^d$ or $\mathbb{C}^d$
$\mathbb{R}^d$	d-dimensional real space
$\otimes$	Tensor product
$\sigma_{x,y,z}$	Pauli x,y,z matrices
BSM4	Bell state measurement of 4 outcomes
ETF	Equiangular tight frame
MUB	Mutually Unbiased Basis
POVM	Positive operator-valued measurement
PVM	Projective-valued measurement
SIC	Symmetric informationally complete
SIC-POVM	Symmetric informationally complete positive operator-valued measure

1 Introduction

Entanglement is one of the most surprising predictions to come out of quantum mechanics. Einstein, Podolsky, and Rosen [1] were the first to envision a scenario where two particles in states ψ_1 and ψ_2 are brought to interact for a short while before drifting apart in a joint state Ψ which cannot in general be factorized into pure states of the individual subsystems. They recognized that local measurements of non-commuting observables on the first particle alone would force the wave function of the second particle to 'collapse' to different states, even though they are far away and no longer interacting by the time of measurement. They reason that "...*either* (1) the quantum-mechanical description of reality given by the wave function is not complete *or* (2) when the operators corresponding to two physical quantities do not commute the two quantities cannot have simultaneous reality..." The conclusion from the subsequent analysis accepted the second and rejected the idea that the wave function was a complete quantum state representation. It was Aharanov and Bohm [2] who repackaged the concerns of the authors of [1] into the properties of the singlet state

$$|\Psi^-\rangle_{AB} = \frac{1}{\sqrt{2}}(|01\rangle_{AB} - |10\rangle_{AB}), \tag{1}$$

which is perhaps the more widely recognized symbol of the EPR thought experiment.

The ensuing philosophical discussion about local hidden variables brought us the Bell inequalities [3] which have since experimentally confirmed nonlocality as a truth of nature [4, 5, 6], and the Kocken-Spekker theorem [7, 8, 9] which reject the notion that quantum observables have pre-determined values which are revealed at the time of measurement. So the assumption that the wave function is a complete representation of the state remains undisputed, *and* measurement outcomes do not have pre-determined values before measurement. The false dilemma of [1] is side-stepped by abandoning locality.

The four Bell states

$$\begin{aligned} |\Phi^\pm\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}) \\ |\Psi^\pm\rangle_{AB} &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}) \end{aligned} \tag{2}$$

are perhaps the simplest set of maximally entangled states which span the space of bipartite qubit states.

Much of the concern of the time, which persists until today, centers around the moment of measurement whereupon the states of distant parties collapse randomly and instantaneously. Measurements hold a very special role in the current understanding of quantum mechanics, but they stand in stark contrast to the rest of the unitarity and determinism of quantum theory. Since they are not known to be derivable from the other postulates of quantum mechanics, they are taken to be one themselves. The first measurements formalized in quantum mechanics are projective ones due to von Neumann [10] which project the state onto one of the orthogonal basis states with a certain prescribed probability. A consequence of the projection is that of *repeatability*, where the same measurement made again on the state returns the same result, so any information of the state orthogonal to this projected state is irretrievable.

As an example, a projective measurement of the state $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ projects it to either $|0\rangle$ with probability $|\alpha|^2$ or state $|1\rangle$ with probability $|\beta|^2$. To be consistent with the laws of probability, $|\alpha|^2 + |\beta|^2 = 1$. Suppose Alice and Bob are given a state from the set in (2) and they want to determine which of the basis states they have. To do this, Alice may try to measure her local system in the $\{|0\rangle_A, |1\rangle_A\}$ basis, and Bob may do the same on his part of the composite state. In the end, they will have one of the four outcomes $\{|00\rangle, |01\rangle, |10\rangle, |11\rangle\}$. But then the outcome is just one of the elements of the computational basis, not one of the Bell basis as originally intended! Just as entangled states cannot be described by pure states of each of the individual subsystems, we can construct measurements which cannot be factorized into local measurements on the subsystems. The measurement which projects onto one of the four Bell states is known as a Bell state measurement, or BSM4. It has found central applications in super-dense coding [11], teleportation [12] (and consequently, entanglement swapping [13] and quantum repeaters [14] since they are extensions of the teleporting protocol).

Later it was realized that non-projective measurements offer the possibility to probe the state for information without completely destroying it. Involving non-orthogonal, non-projective measurements, they were shown to surpass projective ones in many quantum information tasks such as state estimation [15], quantum tomography [16, 17], quantum cryptography [18, 19], quantum state discrimination [20, 21], and device-independent quantum information protocols [22, 23]. Achieving performance of these protocols is important for extracting the full computational advantage that quantum mechanics has to offer over classical computing. For example, for tasks like quantum tomography, this means more accurate and efficient characterization of quantum states. For quantum cryptographic applications, better performance means lowering the threshold of detection of the statistical anomalies generated by an eavesdropper, and higher secure key bits generated per qubit used.

But how should such a non-orthogonal measurement be designed? There is only one way to arrange a spanning set of orthogonal measurements up to rotation, but there are many ways to arrange non-orthogonal ones. Perhaps equiangular lines may have something to say about this. Equiangular lines are highly symmetric configurations that go by many names in physics and mathematics: optimal line packings [24], equilateral point sets in elliptic geometry [25], regular 2-graphs [26], SIC-POVMs [27], the list goes on. Of course the optimal measurement will depend on the particular task at hand, but highly symmetric ones seem to make great candidates for optimal general measurements.

We make a note on how such generalized measurements are made in practice. The most common experimental implementation of POVMs are with photonic bits due to the fact that they are fast and non-interacting [28]. In addition, quantum computational gates and operations can be applied easily and accurately to photonic states. There are four degrees of freedom with which the state of a qubit can be encoded with a photon: polarization [29], orbital angular momentum [30], spatial modes [31], and time of arrival [32]. POVMs are often implemented with the help of an ancilla system over which the POVM becomes a projective measurement. With *hyperentanglement* of photonic qubits, the augmentation of the dimension required to make a projective measurement can be achieved by coupling different photonic degrees of freedom. For example, a POVM can be implemented with entangled path and polarization degrees of freedom [29, 33], and spatial modes and orbital angular momentum [34].

We have introduced the central themes of this thesis: entanglement, measurements, and equiangular lines. This work seeks to extend the current understanding of equiangular lines to bipartite Hilbert space, beginning with the simplest case of bipartite qubits. Constructions of equiangular

lines over product and maximally entangled states are presented, and some proofs of optimality are derived. Then, their distinguishability properties are studied under measurements with access to different resources.

In section 2, we discuss redundant bases called frames, which may be more familiar to those approaching the study of equiangular lines from a background in mathematics or signal processing. The advantages of non-orthogonal POVMs are revealed in section 3, where real and complex equiangular lines are discussed. Apart from their application as optimal measurements in quantum mechanics, equiangular lines have had a long history in discrete mathematics, and a condensed version of it is presented in this section also. In section 4, we discuss measurements in quantum mechanics, both projective ones and positive-operator valued ones. Then in section 5, we discuss entanglement and its relationship to local operations. The contributions of this thesis work are presented in section 6, including some equiangular constructions and a discussion of their properties. Finally in section 7, the discussions of entanglement, local operations, and measurements are brought together in the context of quantum state discrimination to optimally discriminate the constructions of section 6 with various kinds of measurements.

It is the intention that the work of this thesis will be the content of a future publication.

1.1 A Note on Notation

Throughout, $\langle \cdot, \cdot \rangle$ will be used to denote the inner product of vectors in $\mathbb{H}^d$ which can stand for either the Euclidean inner product $\mathbb{R}^d$ or the inner product over Hilbert space in $\mathbb{C}^d$. States in bra-ket notation will be reserved for quantum states in Hilbert space.

2 Frames and Welch Bounds

The expansion of a state f in the standard orthonormal basis $\{\hat{e}_i\}_{i=1}^d$ is a very natural and familiar way to uniquely decompose a given state $f \in \mathbb{H}^d$. The standard orthonormal basis contains the minimum number of elements needed to span the full d-dimensional space, a given set of expansion coefficients represent a *unique* state in this basis, and any two elements in the set are orthogonal, making them convenient to make calculations with. Orthogonalizing procedures such as the Gram-Schmidt decomposition of matrices and the prevalence of orthogonal bases in vector and polynomial spaces such as the Hermite and Legendre polynomials make it seem as though orthogonal bases are the end of the story.

However, one may go beyond the standard basis and consider redundant bases called *frames* to represent a given state. We'll consider only discrete frames in finite dimensions. Then we have the following definition of a frame:

Definition 2.1 ([35])**.** A *frame* is defined by a set of $n \in \mathbb{Z}$ vectors $\{x_i\}_{i=1}^n$ and frame bounds $0 < A \leq B < \infty$, for which

$$A||f||^2 \leq \sum_i^n |\langle x_i, f\rangle|^2 \leq B||f||^2 \qquad \forall f \in \mathbb{H}^d \tag{3}$$

This is a *tight frame* when $A = B$, and a *unit-norm frame* when $||x_i||^2 = 1$ for all i. We will only consider unit-norm frames, denoted $\{\hat{x}_i\}_{i=1}^n$. Generally, frame vectors of tight frames will be

normalized so that $A = B = 1$. Then it is a *normalized tight frame*. For brevity, a (n, d)-frame will denote a frame of n lines in $\mathbb{H}^d$ unless it is specified to be real or complex.

The rest of this section will introduce the basics and tools of frame theory and explain how they relate to the equiangular lines we're interested in. We'll find that what frames lack in uniqueness of expansion and orthogonality they make up for with robustness against noisy losses and erasures. With this context we will be more appreciative of the features of equiangular lines, which are a special subset of frames.

2.1 Synthesis, Analysis and Frame Operators

We have the following definitions to describe the action of a frame:

Definition 2.2. [35] For an (n, d)-frame $\{\hat{x}_i\}_{i=1}^n$ and arbitrary state $f \in \mathbb{H}^d$ with frame expansion $(f_1, f_2, ..., f_n) \in \mathbb{H}^n$ where each $f_i = \langle f, \hat{x}_i \rangle$, the $d \times n$ *synthesis operator* is the linear map defined by

$$V : \mathbb{H}^n \longrightarrow \mathbb{H}^d; \quad f \to \sum_i \langle f, \hat{x}_i \rangle \hat{x}_i. \tag{4}$$

In other words, it is a matrix which reconstructs or *synthesizes* the state from the coefficients of the frame expansion. In matrix form, V is the $d \times n$ matrix of the frame vectors $\hat{x}_i$:

$$V = \begin{pmatrix} \hat{x}_1 & \hat{x}_2 & ... & \hat{x}_n \end{pmatrix} \tag{5}$$

Definition 2.3. [35] For an (n, d)-frame $\{\hat{x}_i\}_{i=1}^n$ and arbitrary state $f \in \mathbb{H}^d$, the $n \times d$ *analysis operator* is the linear map

$$V^\dagger : \mathbb{H}^d \longrightarrow \mathbb{H}^n; \quad f \to (\langle f, \hat{x}_1 \rangle, \langle f, \hat{x}_2 \rangle, ..., \langle f, \hat{x}_n \rangle), \tag{6}$$

which maps states from their expansion in the orthonormal basis to their frame expansion

Definition 2.4. For an (n, d)-frame $\{\hat{x}_i\}_{i=1}^n$, the $d \times d$ *frame operator* F is defined by

$$F = VV^\dagger. \tag{7}$$

Finally, we come to the Gram matrix of a frame.

Definition 2.5. For an (n, d)-frame $\{\hat{x}_i\}_{i=1}^n$, the $n \times n$ *Gram matrix* G is a real and symmetric matrix with entries defined by the inner products of the frame vectors:

$$G_{ij} = \langle \hat{x}_i, \hat{x}_j \rangle \tag{8}$$

In terms of the synthesis and analysis operators, $G = V^\dagger V$. It is the adjoint of F. It is positive semi-definite and has 1's along the diagonal.

An important property relating the frame operator and the Gram matrix is that they have the same eigenvalues. Consequently, they have the same rank and trace. This can easily be shown:

$$\begin{aligned} G\vec{v} &= \lambda\vec{v} \\ \implies V^\dagger V\vec{v} &= \lambda\vec{v} \\ \implies VV^\dagger(V\vec{v}) &= \lambda(V\vec{v}) \\ F(V\vec{v}) &= \lambda(V\vec{v}) \end{aligned} \tag{9}$$

If λ is an eigenvalue of G with eigenvector $\vec{v}$, then it is an eigenvalue of F with eigenvector $V\vec{v}$. The humble Gram matrix is used to derive many results throughout, and its power comes from this relationship to the frame operator. It is good to keep this in mind!

2.2 Tight Frames

We have already defined tight frames in passing, but here we elaborate more on some of their properties. Recall that for a tight frame $\{\hat{x}_i\}_{i=1}^n$,

$$A||f||^2 = \sum_i^n |\langle x_i, f\rangle|^2 \quad \forall f \in \mathbb{H}^d, \tag{10}$$

Generally, the frame vectors will be sub-normalized so that $A = 1$. A property which makes tight frames useful in quantum information theory is given in the following theorem.

Theorem 1 ([35]). *The finite sequence $\{\hat{x}_i\}_{i=1}^n$ in $\mathbb{H}^d$ is a tight frame if and only if frame operator $F = VV^\dagger = A\mathbb{I}_d$, where the synthesis and analysis operators $V, V^\dagger$ are defined as in 2.1.*

Proof. From Parseval's identity

$$f = \frac{1}{A}\sum_i^n \langle \hat{x}_i, f\rangle \hat{x}_i \quad \forall f \in \mathbb{H}^d \tag{11}$$

where A is a normalizing factor. Then

$$\begin{aligned} Ff &= VV^\dagger f \\ &= V(\langle \hat{x}_1, f\rangle, \langle \hat{x}_2, f\rangle, ..., \langle \hat{x}_n, f\rangle) \\ &= \sum_i \langle \hat{x}_i, f\rangle \hat{x}_i \end{aligned} \tag{12}$$

where operators V and $V^\dagger$ are as defined in section 2.1. Then, we have that $Ff = Af$, or

$$F = VV^\dagger = A\mathbb{I}_d \tag{13}$$

■

This has the consequence that the rows in the V matrix (equivalently, the columns in $V^\dagger$) are an orthogonal basis for a d-dimensional subspace embedded in $\mathbb{H}^n$.

A special property of tight frames is that every finite normalized tight frame is the orthogonal projection of some orthonormal basis in a higher dimension, and from every finite normalized tight frame, an orthonormal basis in a higher dimension can be obtained. In other words, there exists an $n \times n$ projection operator P which projects onto the column space of the synthesis operator V, so that $\langle P\hat{e}_i, P\hat{e}_j\rangle = \langle \hat{x}_i, \hat{x}_j\rangle$ for orthonormal basis elements $\{\hat{e}_i\}_{i=1}^n \in \mathbb{H}^n$ and finite normalized tight frame $\{\hat{x}_i\}_{i=1}^n \in \mathbb{H}^d$ [35]. This result will sound familiar to physicists who are familiar with Naimark's dilation theorem since tight frames can be interpreted as general quantum measurements and orthogonal bases as projective measurements, but more on this later.

2.3 Equiangular Tight Frames

Finally, we introduce a particularly special frame which are tight frames so they satisfy theorem 1, and the magnitude of the overlap between any pair of states in the set $\{x_i\}_{i=1}^n$ are equal in magnitude:

$$\alpha \equiv \pm\langle x_i, x_j\rangle \qquad \forall i \neq j. \tag{14}$$

Then the states are *equiangular*, and they make an *equiangular tight frame (ETF)*. The synthesis operator of an ETF is special for having orthogonal rows and columns with pairwise equal and minimal overlaps.

2.4 Welch Bounds

We use the *overlap* of two vectors to denote the degree of non-orthogonality of the vectors. The smaller the angle between them, the larger the overlap. Welch [36] was the first to put lower bounds on the maximum of the overlaps of the vectors of any given frame, which we denote $c_{\max}$. Intuitively, the Welch bounds quantify how *well* n frame vectors are able to spread out as evenly as possible in d dimensions. Of course if $n \leq d$, the vectors can be orthogonal, so $c_{\max} = 0$ and the Welch bounds are vacuous.

Theorem 2 (Welch bounds, [37]). *For unit vectors $\{\hat{x}_i\}_{i=1}^n$ in $\mathbb{C}^d$, define $c_{\max} = \max_{i\neq j} |\langle \hat{x}_i, \hat{x}_j\rangle|$. Then,*

$$c_{\max}^{2k} \geq \frac{1}{n-1}\left[\frac{n}{\binom{d+k-1}{k}} - 1\right] \tag{15}$$

The proof will be given for the case $k = 1$, which can be found in [38, 24]. When $k = 1$, equality is reached when the frame is an ETF.

Proof. Since rank $G \leq n - d$, G has at most d non-zero eigenvalues. Let these populate the vector $\vec{\lambda} = (\lambda_1, ..., \lambda_d)$, and define the normalized constant vector $\hat{u} = \frac{1}{\sqrt{d}}\mathbf{1}_d$. Then apply the Cauchy-Schwarz inequality

$$\left(\sum_{i=1}^d u_i\lambda_i\right)^2 \leq \left(\sum_{i=1}^d u_i^2\right)\left(\sum_{i=1}^d \lambda_i^2\right) \tag{16}$$

to obtain

$$\left(\sum_{i=1}^d \lambda_i\right)^2 \leq d\sum_i^d \lambda_i^2, \tag{17}$$

where the left-hand side is $(\mathrm{Tr}\, G)^2 = n^2$. From the Frobenius norm of the Gram matrix G denoted $||G||_F$, we have that

$$||G||_F^2 = \sum_{i=1}^n \lambda_i^2 = \sum_{i,j=1}^n |\langle x_i, x_j\rangle|^2. \tag{18}$$

Substituting (18) into (17),

$$\sum_{i,j=1}^n |\langle x_i, x_j\rangle|^2 \geq \frac{n^2}{d}. \tag{19}$$

Equivalently,

$$\sum_{i\neq j}^n |\langle x_i, x_j\rangle|^2 \geq \frac{n(n-d)}{d} \tag{20}$$

The lower bound is reached when equality is achieved in (17), which occurs when $\vec{\lambda}$ is proportional to $\hat{u}$. In other words, all non-zero eigenvalues of G are equal to some constant, say t. Then, (17) gives $n^2 = d^2t^2$, or $t = \frac{n}{d}$. Recall that F and G have the same eigenvalues so $F = \frac{n}{d}\mathbb{I}$. Equality in this expression is achieved for tight frames. From this, we know in fact that in theorem 1, the constant $A = \frac{n}{d}$. Now, we use the fact that the average of a set of non-negative numbers cannot be greater than the largest in the set, which we label $c^2_{\max}$. This means

$$c^2_{\max} \geq \frac{1}{n(n-1)} \sum_{i \neq j} |\langle x_i, x_j \rangle|^2 \geq \frac{n-d}{d(n-1)}. \tag{21}$$

Finally, we have the Welch bound for $k = 1$.

$$c^2_{\max} \geq \frac{n-d}{d(n-1)}. \tag{22}$$

This is an equality when the maximum overlap is exactly equal to the average, so the lines must be equiangular. The Welch bound is saturated for an ETF. ■

2.5 Applications

Now we are equipped to see why non-orthogonal bases are useful.

Noise
Suppose a source communicates a signal f of length d which is encoded with a normalized tight frame $\{(d/n)\hat{x}_i\}_{i=1}^n$ whose analysis operator is given by V, so $g = V^\dagger f$. Then, g is sent to the receiver. Along the way, the signal is corrupted with noise vector η, so the receiver receives $\hat{g} = Vf + \eta$. We assume the mean of each noise component is centered at zero with variance σ^2, and there is no correlation among noise components. The receiver will try to recover f and their best attempt at a reconstruction will be denoted $\hat{f}$. The objective will be to minimize the difference $||f - \hat{f}||$.

That frame vectors form over-complete bases means that they are linearly dependent, so $\sum_i \eta_i \hat{x}_i = 0$ for non-zero coefficients η_i is possible, and the noise may self-correct. If the frame expansion used in g is a tight frame, then $VV^\dagger = \frac{n}{d}\mathbb{I}$ and the synthesis operator V may be used to optimally reconstruct f. Before doing that, we decompose η into components perpendicular and parallel to the range of V: $\eta = \eta_\perp + \eta_\parallel$. Then,

$$\begin{aligned} \hat{f} &= V\hat{g} = VV^\dagger f + V(\eta_\perp + \eta_\parallel) \\ &= f + V\eta_\parallel. \end{aligned} \tag{23}$$

Due to theorem 44 in [39], we can quantify the reduction of noise in the reconstruction:

$$E(||\eta_\parallel||^2) = \frac{d^2}{n^2} E(||\eta||^2), \tag{24}$$

where $E(X)$ expected value of random variable X. So in this simple example, we get that the mean magnitude of the noise vector squared is reduced by a factor of $(n/d)^2$. For expansion with a general frame, $F = VV^\dagger$ is not the identity so the synthesis operator should not be used for reconstruction. The Moore-Penrose pseudoinverse, defined by $V^+ = (V^\dagger V)^{-1}V^\dagger$ is one potential option in this case [40].

Erasures
Sometimes during transmission, some bits are lost or *erased*. The redundancy of frames offers the possibility to recover the lost information, given the loss is not too great. For even the best (n, d)-frames, erasure of more than $n - d$ components certainly leaves a set which does not span $\mathbb{H}^d$ so it is no longer a frame. However, some frames can do much worse than this. In the worst case, a frame may have one vector which is perpendicular to all others, in which case the erasure of this component means that the information cannot be reconstructed. Thus, intuitively, the best frames that perform the best in the face of erasure are those for which the redundancy of the frame is "spread out as evenly as possible".

An optimal unit-norm, normalized tight frame against m-erasures is defined in [41] as one which minimizes the function

$$F_m(\{\hat{x}_i\}_{i=1}^n) = \max_{||f||\leq 1} \max_{|J|=n-m} \Big|\Big|f - \frac{d}{n}\sum_{i\in J}\langle f, \hat{x}_i\rangle \hat{x}_i\Big|\Big|, \tag{25}$$

where m components are erased. In other words, the optimal frame minimizes the distance between the original signal f and the reconstructed one in the worst case over all signals f and all combinations of m-erasures. It is shown that the normalized tight frame $\{\hat{x}_i\}_{i=1}^n$ which minimizes this function for $m = 2$, also minimizes the maximum overlap of the set

$$\max_{i\neq j} |\langle \hat{x}_i, \hat{x}_j\rangle| \tag{26}$$

over all normalized tight frames. This, as we will see, is satisfied for a tight frame.

3 Equiangular Lines, Real and Complex

A very special class of frames are those which are equiangular. The defining feature of equiangular lines are that every pair of lines in the set $\{\hat{x}_i\}_{i=1}^n$ share a common overlap

$$\langle x_i, x_j\rangle = \pm\alpha \qquad \forall \quad i \neq j \tag{27}$$

Throughout, we let $\mu \equiv |\alpha|^2$ since we are often only interested in the magnitude of the overlap, not the sign. Generally, we are interested in the maximum number of equiangular lines in any given dimension or *maximal sets*, which we denote $n(d)$. Here, we introduce the study of equiangular lines in real and complex dimensions and derive some of the most basic results.

3.1 Equiangular Lines in $\mathbb{R}^d$

First, an example:

Example 1 (Mercedes-Benz Configuration)**.** *The simplest example are the three lines in $\mathbb{R}^2$ which are the antipodes of a regular hexagon with coordinates, given by*

$$\hat{x}_1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad \hat{x}_2 = \begin{pmatrix} -1/2 \\ -\sqrt{3}/2 \end{pmatrix} \quad \hat{x}_3 = \begin{pmatrix} -1/2 \\ \sqrt{3}/2 \end{pmatrix} \tag{28}$$

where $\langle \hat{x}_i, \hat{x}_j\rangle = -1/2$ for all $i \neq j$. and depicted in figure 1.

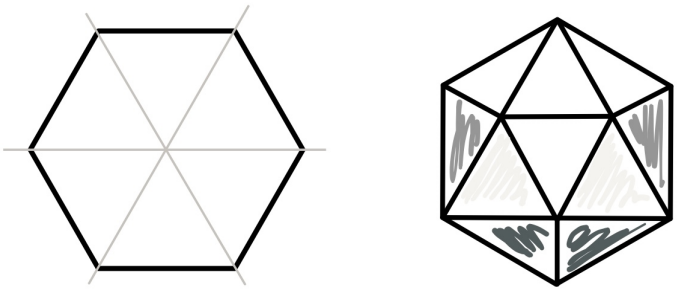

Figure 1: 3 equiangular lines through the diagonals of a hexagon in $\mathbb{R}^2$ (left), and 6 equiangular lines through the diagonals of the regular icosahedron $\mathbb{R}^3$ (right)

3.1.1 A Brief History

Real equiangular lines and the question of maximal sets first showed up in 1948 as equilateral point sets in elliptic geometry [42], where it was shown that $n(3) = n(4) = 6$. In 1966, van Lint and Seidel [25] showed that $n(5) = 10$, $n(6) = 16$, and $n(7) \geq 28$, and revealed the relationship between equiangular lines and graph theory. In 1973, Lemmens and Seidel [43] derived a number of bounds on $n(d)$, including Gerzon's bound $n(d) \leq \binom{d+1}{2}$ and the relative bound. Crucially, their work recognized the number theoretic importance of α, which motivated the investigation into the maximum number of equiangular lines possible for a given angle α in any dimension, $n_\alpha(d)$. They showed that $n_{1/3}(d) = 2(d-1)$ for all $d \geq 15$, and that $n_\alpha(d) > 2d$ if and only if $1/\alpha$ is an odd integer. Subsequent results followed in [44] and [45]. This version of the problem was solved completely in 2022 due to a new result in spectral graph theory which upper bounded the multiplicity of the second largest eigenvalue of the Gram matrix [46].

3.1.2 Gerzon's Absolute Bound

Due to the difficulty of coming up with exact constructions, progress in the field has progressed by deriving progressively tighter upper and lower bounds. Perhaps the most important is the absolute upper bound which is given by the following theorem.

Theorem 3 (Gerzon's bound, [47])**.** *In $\mathbb{R}^d$, there are at most $n(d) = \binom{d+1}{2}$ equiangular lines.*

Refer to appendix B for the proof. In most dimensions, this bound is not met. Saturation of Gerzon's bound is only possible if $d = 2, 3$, or if $d + 2$ is the square of an odd integer [43]. The only known maximal sets are in dimensions $d = 2, 3, 7, 23$ [48], and it remains open whether there are more. However, it has been shown that there exists an infinite number of dimensions satisfying this condition which do not contain maximal sets [49].

3.1.3 Examples

The following examples illustrate but a fraction of the variety of tools of discrete mathematics that have been brought to bear on the construction of real equiangular lines.

Example 2. *In $\mathbb{R}^3$, $n(3) = 6$, and they are lines through the antipodes of a regular icosahedron,*

d	2	3	4	5	6	7-13	14	15	16	17	18	19	20
$N(d)$	3	6	6	10	16	28	28-29	36	40-41	48-50	48-61	72-76	90-96
$1/\alpha$	2	$\sqrt{5}$	$\sqrt{5}, 3$	3	3	3	3,5	5	5	5	5	5	5

Table 1: Table of best known upper and lower bounds on maximum number of equiangular lines $N(d)$ in dimension d, along with known angles of construction. [50]

shown in figure 1.

$$\frac{1}{A}\begin{pmatrix}0\\1\\p\end{pmatrix}, \quad \frac{1}{A}\begin{pmatrix}0\\1\\-p\end{pmatrix}, \quad \frac{1}{A}\begin{pmatrix}-1\\p\\0\end{pmatrix}, \quad \frac{1}{A}\begin{pmatrix}-1\\-p\\0\end{pmatrix}, \quad \frac{1}{A}\begin{pmatrix}p\\0\\1\end{pmatrix}, \quad \frac{1}{A}\begin{pmatrix}-p\\0\\1\end{pmatrix} \tag{29}$$

with $p = \frac{1}{2}(1+\sqrt{5})$, $A = \sqrt{1+p^2}$, *and common overlap* $\alpha = \pm\frac{1}{\sqrt{5}}$.

Example 3 ([51])**.** *In* $\mathbb{R}^8$, *28 equiangular lines come from the set of all possible permutations of*

$$\hat{v} = \frac{1}{\sqrt{24}}(3, 3, -1, -1, -1, -1, -1, -1). \tag{30}$$

They are all orthogonal to $\mathbf{1}_8$, *so the 28 lines span a seven dimensional subspace of* $\mathbb{R}^8$.

Example 4 ([52])**.** *The set of equiangular lines in* $\mathbb{R}^7$ *comes from the Fano plane, a very special incidence structure in combinatorial mathematics. It has seven points and seven lines which are incident with three points each. Every two points lie on a distinct line, and every two lines intersect at exactly one point. See figure 2. One may define an incidence matrix* N *for this structure such*

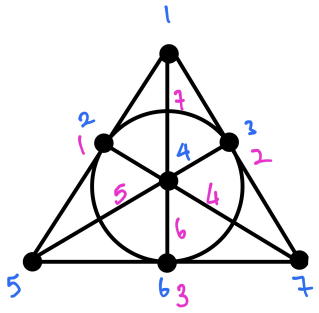

Figure 2: The seven vertices and seven blocks (here represented as lines) of the Fano plane. Blue numbers label the vertices and pink numbers label the blocks in the corresponding incidence matrix in (31). The circle labeled by 7 counts as a line since only the incidence relations are relevant.

that the rows are indexed by the vertices and the columns by the lines. Entry $N_{ij} = 1$ *if line* j *is incident with point* i, *and* 0 *otherwise. The incidence matrix for the Fano plane as indexed in figure 2 is:*

$$N = \begin{pmatrix}1&1&0&0&0&1&0\\1&0&0&1&0&0&1\\0&1&0&0&1&0&1\\0&0&0&1&1&1&0\\1&0&1&0&1&0&0\\0&0&1&0&0&1&1\\0&1&1&1&0&0&0\end{pmatrix} \tag{31}$$

The columns of this matrix produce seven equiangular lines in $\mathbb{R}^7$ whose common overlap equals 1. If one recognizes the scalar product of two columns as the number of points where the corresponding lines are incident, this statement is obvious.

To obtain 28 lines from the seven, we'll furnish them with sign combinations that represent orientations on the Fano plane. From each of the seven columns, four signed vectors are arranged such that two of the three signs cancel out in the inner product of any two of the four vectors, leaving an overlap of magnitude 1. Between two signed vectors obtained from different columns, the original argument for their equiangularity holds. For example, from the first column, we obtain the following four signed vectors:

$$\begin{pmatrix}1\\1\\0\\0\\1\\0\\0\end{pmatrix} \longrightarrow \begin{pmatrix}-1\\+1\\0\\0\\+1\\0\\0\end{pmatrix}, \begin{pmatrix}+1\\+1\\0\\0\\-1\\0\\0\end{pmatrix}, \begin{pmatrix}-1\\-1\\0\\0\\-1\\0\\0\end{pmatrix}, \begin{pmatrix}+1\\-1\\0\\0\\+1\\\\0\end{pmatrix}. \tag{32}$$

For a more systematic treatment of the method of sign determination, refer to [52]. The Fano plane is a simple example of a design in combinatorial design theory, and is not the only one which produces equiangular lines. A much richer equiangular construction is the 276 lines in $\mathbb{R}^{23}$ from the Witt design. A discussion of designs and the Witt design is deferred to appendix A.

More constructions can be found in [47] and [53].

3.2 Equiangular Lines in $\mathbb{C}^d$

Complex equiangular lines, or SICs (symmetric informationally complete) as they have been dubbed by the quantum information community are defined analogously to real equiangular lines, except that the vectors lie in $\mathbb{C}^d$. A striking departure from the real case is that in every dimension studied, a full set of d^2 equiangular lines $\{|x_i\rangle\}_{i=1}^{d^2}$ have been found, with overlaps given by

$$|\langle x_i|x_j\rangle|^2 = \frac{\delta_{ij}d+1}{d+1}. \tag{33}$$

The introduction of SICs to the wider quantum theoretic community is credited to Gerhard Zauner in 1999 [54], (and independently by Renes in 2004 [27]) where he showed that $n(d) \leq d^2$, and conjectured that equality can be reached in every dimension. It remains an open conjecture to this day. By then, he had also made the connection between SICs and the Weyl-Heisenberg group. In 2004, numerical SICs were constructed up to $d = 4$ [55]. By 2010, complete solutions have been found up to $d = 50$ [56] and by 2017, in every dimension up to $d = 151$. In higher dimensions with special symmetries, additional sporadic solutions have been found. Most recently, solutions in seventeen dimensions up to $d = 39604$, each satisfying $d = n^2 + 3 = 4p$ where p is a prime have been found [57]. To get a sense of the magnitude of the problem, finding a solution in $d = 12$ involves a system of 15 polynomial equations in 9 variables, with coefficients with up to 40 digits [58]. The group covariance of SICs under the Weyl-Heisenberg group greatly reduces the problem to one of finding just one vector.

3.2.1 The Weyl-Heisenberg Group

All known equiangular constructions are *group covariant* under the Weyl Heisenberg (WH) group, (except for one in dimension 8). To be group covariant means that a fiducial vector can be chosen so that its orbit under the group generates the full equiangular set. The Weyl-Heisenberg group in dimension d has three generators of order d: the phase (ω), clock (X), and shift (Z) operators which are related by the following:

$$X\omega = \omega X \qquad Z\omega = \omega Z \qquad ZX = \omega XZ \tag{34}$$

where $\omega = e^{2\pi i/d}$. Then up to phase factors, the WH group is the direct product of two cyclic groups $Z_d \times Z_d$, and there are d^2 distinct combinations of X and Z which comprise the group. For a set of orthonormal basis vectors $\{|i\rangle\}_{i=1}^d$ where each vector is defined by its integer label modulo d and Z represented by a diagonal operator, the action of X and Z are given by:

$$X|i\rangle \to |i+1\rangle \qquad Z|i\rangle \to \omega^i|i\rangle. \tag{35}$$

In two dimensions, the clock and shift operators are the Pauli σ_x and σ_z matrices respectively. In $d = 3$, the matrix representation of X and Z is given by

$$X = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 \\ 0 & \omega & 0 \\ 0 & 0 & \omega^2 \end{pmatrix}, \quad \omega = e^{2\pi i/3} \tag{36}$$

Example 5 ([35]). *Four unit vectors in $\mathbb{C}^2$, generated by the application of Pauli-x and Pauli-z operators to a fiducial vector ν: $\{\nu, \sigma_x\nu, \sigma_z\nu, \sigma_x\sigma_z\nu\}$ where*

$$\nu := \frac{1}{\sqrt{6}} \begin{pmatrix} \sqrt{3+\sqrt{3}} \\ e^{\frac{\pi}{4}i}\sqrt{3-\sqrt{3}} \end{pmatrix}, \quad \sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{37}$$

SICs have a lot more to offer than just geometric niceties. This may be hard to see given the numerical solutions which occupy pages and pages of A4 paper, but a closer look at the numbers of the SICs reveal unexpected and deep connections to algebraic number theory. The connection is made possible by the observation that all known fiducial vectors (except in dimension 3) expressed in the standard basis are expressible in radicals [59]. This is not at all obvious since we know from the Abel-Ruffini theorem that even polynomial equations of dimension 5 do not have solutions expressible in terms of a the arithmetic operations $+, -, \times, \div$, and $\sqrt{}$ [60]. Refer to [59] for a treatment aimed at physicists with minimal background in Galois theory. For this reason, even extremely precise numerical solutions (up to 150 digits in some cases [61]) is not enough! Exact expressions are needed to determine the extension field of the SICs, but they have been slower to come by. In 2018, 69 exact solutions were extracted from numerical solutions [62] which was enabled by new results in algebraic number theory.

3.2.2 Applications of Equiangular Lines in Quantum Information Theory

A SIC $\{|x_i\rangle\}_{i=1}^n$ can be made into a sub-normalized POVM of rank-one operators, a SIC-POVM, defined by

$$\Pi = \left\{ \frac{d}{n} |x_i\rangle\langle x_i| \right\}_{i=1}^n \tag{38}$$

where $\mathrm{Tr}(\Pi_i\Pi_j) = \frac{d^2}{n^2}\frac{\delta_{ij}d+1}{d+1}$ and $\sum_i (d/n)|x_i\rangle\langle x_i| = \mathbb{I}$. These are often optimal measurements for many tasks in quantum information theory, for a few main reasons. Broadly speaking, they offer a minimal, tomographically complete basis for sampling, so all the relevant information of the state can be obtained with the least number of measurements due to the symmetry. Furthermore, they feature the largest number of measurement outcomes for an extremal measurement, meaning they cannot be simulated by a combination of other POVMs [63], and they can tolerate the most amount of noise before they become simulable with projective measurements [64]. In other words, their optimal features are unique and are not so easily replicated with other measurements.

A selection of some of their applications is presented here.

Quantum State Tomography (QST)
The objective of quantum state tomography is to reconstruct quantum states from measurements on ensembles of identically prepared states. The d^2 Hermitian matrices obtained from SIC elements $|x_i\rangle \to |x_i\rangle\langle x_i|$ span the full d^2-1 dimensional space of density operators, and this fact is used in the proof of the d^2 upper bound in appendix B. A full SIC-POVM measurement of the d^2 operators is not only *informationally complete* since the full density matrix can be constructed from knowledge of the measurement statistics, it is *minimal* since d^2 is the minimum number of parameters needed to specify a state. Just as how measurement bias can be strategically introduced into the measurement design when prior information is known of the state [65], SIC-POVMs provide the least bias when there is no prior information [15]. In addition, the less redundancy there is among the measurements, the faster the tomography converges [66]. SICs provide a redundant measurement basis which is just enough to provide all the necessary information with the least amount of measurement resources.

Quantum Key Distribution (QKD)
QKD aims to create a shared random bit sequence for two communicating parties which is known by no one else, which they can then use to encrypt and decrypt classical messages. The BB84 protocol [67] was the first QKD protocol and makes use of measurements on two mutually unbiased bases (see appendix A), and is perhaps the most technologically mature quantum information processing application. In principle, its security is guaranteed by the fact that eavesdropper Eve cannot siphon information without creating a statistical disturbance detectable by Alice and Bob. However, the two measurement bases $\pm\hat{z}$ and $\pm\hat{x}$ lie on a single plane of the Bloch sphere, so there is potentially room for a more secure QKD protocol with three mutually unbiased measurement bases which is demonstrated in [68]. Now, eavesdropper Eve would have three measurement bases to choose from, lowering further her chances of going undetected. However, this comes at the cost of 3 exchanged qubits per secure key bit compared to 2 in the BB84 protocol. A more efficient protocol which also takes advantage of the full Bloch sphere space is presented by the Singapore protocol [18], featuring four-outcome SIC-POVMs for both Alice and Bob. A source distributes maximally entangled singlet states to them for which the 16 correlation probabilities $p_{A_iB_j}$ corresponding to the ith measurement setting firing for Alice and the jth for Bob, $i, j \in \{1, 2, 3, 4\}$ can be used to verify the expected outputs of the source. This protocol features a more efficient key rate at 2.41 qubits per key bit compared to the 6-state QKD protocol, and allows for secure key bit generation under much higher levels of noise.

Entanglement Witnesses
SIC-POVMs have been shown to be useful in constructing stronger entanglement detection criteria. One well-known Schmidt number criterion for entanglement detection of a bipartite state is the CCNR criterion for Schmidt numbers. By studying the the statistical correlations among a SIC-POVM measurement instead of those from a projective measurement, entanglement detection

criteria which are strictly stronger than fidelity witness criteria and CCNR criteria can be obtained. [69, 70].

Random number generation from entangled qubits
It is known from [71] that the incompatibility of a Bell inequality violation with a local hidden variable model makes it a candidate for secure device-independent random number generation. Since a SIC-POVM performed on a d-dimensional system allow for d^2 measurement outcomes, in principle $2 \log d$ random bits can be securely generated compared to $\log d$ with projective measurements on the same d-dimensional system.

In [63], the authors derive Bell inequalities that are maximally violated with maximally entangled states and a SIC measurement in Bob's measuring device. Alice possesses two measurement settings which she randomly chooses at each round of the Bell experiment. One implements a SIC-POVM whose outcome a is used for random number generation and the other, which when selected goes towards verifying the violation of the Bell inequality. Then an upper bound on Eve's confidence of Alice's outcome a is derived from the observed violation of the Bell inequality. Eve's uncertainty of Alice's outcome is used to quantify the randomness of Alice's random number generator. From numerical studies, the authors report 2 bits of certified randomness from qubits and more randomness from qutrits with this protocol than any other using projective measurements up to dimension 7.

3.2.3 Equiangular Lines in Experiment

Although SIC-POVMs in principle outperform their projective counterparts in many quantum information tasks including quantum tomography, quantum cryptography, device-independent protocols among others, in practice POVMs are harder to implement. A projective measurement of qubit states can be implemented simply with a polarizing beam splitter, which splits light into two beams of orthogonal polarization states. To implement a POVM, a common technique is to use Naimark's dilation theorem by coupling the system out with an ancilla to augment the system dimension and then making a projective measurement on the whole system.

In the following, some examples of experimental implementations of SIC-POVMs are presented.

In 2006, NMR tomography was performed on the nucleus of ^{1}H with ^{13}C as the ancilla system [72]. They were able to determine the Bloch parameters of the target state from projective measurements on both systems, and report an average fidelity of 0.92

In 2010, an experimental characterization of an optical qutrit state with SIC-POVMs was accomplished using a series of d^2 partial polarizing beam splitters arranged in a loop, each corresponding to an element Π_i of the SIC-POVM. The state after a partial polarization remains mostly undisturbed and is cycled to the next partial polarizer. Crucially, this implementation does not rely on the use of an ancilla. [66]

In 2015, quantum state tomography using SIC-POVMs is performed on qudit states encoded in photonic orbital angular momentum states for dimensions $d = 6$ and $d = 10$, where optimal projective measurements using mutually unbiased bases do not exist [73]. They report reconstruction fidelities in the range of 0.859-0.960 for pure states and 0.818-0.905 for mixed states.

4 Measurements in Quantum Mechanics

As mentioned in the introduction, measurements in quantum mechanics are taken as postulate. From Nielsen and Chuang [74], the postulate of measurements reads:

> Quantum measurements are described by a collection *measurement operators* $\{M_m\}$ acting on the Hilbert space of the system being measured. The index m refers to the possible measurement outcomes. If the state of the quantum system is $|\psi\rangle$ immediately before the measurement then the probability that result m occurs is
>
> $$p(m) = \langle\psi|M_m^\dagger M_m|\psi\rangle \tag{39}$$
>
> and the system state after measurement is
>
> $$\frac{M_m|\psi\rangle}{\sqrt{\langle\psi|M_m^\dagger M_m|\psi\rangle}} \tag{40}$$
>
> where the measurements M_m are complete, $\sum_m M_m^\dagger M_m = \mathbb{I}$.

These conditions ensure consistency with the probabilistic interpretation of the measurements

$$\begin{aligned}\sum_m p(m) &= \sum_m \langle\psi|M_m^\dagger M_m|\psi\rangle \\ &= \langle\psi|\big(\sum_m M_m^\dagger M_m\big)|\psi\rangle \\ &= 1\end{aligned} \tag{41}$$

There are two kinds of measurements in quantum mechanics. In the following sections, we define each and discuss how they relate to each other.

4.1 Projective Valued Measurements (PVM)

The measurements which most are familiar with are projective-valued measurements (PVM) which were first introduced by von Neumann [10]. The measurement, or observable M, is Hermitian with a spectral decomposition $M = \sum_m mP_m$, where each of the P_m satisfy the above conditions in addition to the following:

1. P_m is projective: $P_m^2 = P_m$
2. P_m is orthogonal to all other measurement operators $\mathrm{Tr}(P_iP_j) = d\delta_{ij}$

Expectation values of observable M in state $|\psi\rangle$ are simply given by $\langle\psi|M|\psi\rangle$. Since they are orthogonal, there can be no more than d measurement outcomes which can be a limitation for certain applications such as in random number generation [63] and state discrimination [75]. Projective measurements are also *repeatable*, so once outcome m is obtained from one application of M, an application of M a second time will produce the same measurement outcome. This makes them useful as tools to control decoherence in coupled quantum systems [76, 77]. This is the idea of the quantum Zeno effect [78], which in spirit is the quantum version of "a watched pot never boils." On the other hand, in situations such as those of radiative decay, sufficiently frequent measurement events can accelerate the decay process instead of inhibiting them, which is the *anti*-quantum Zeno effect [79]. In other applications, selective projective measurements are useful for quantum information tasks

where an ensemble of well-defined initial condition states are required [80]. So we see that projective measurements are useful for manipulating certain quantum dynamical processes.

4.2 Positive Operator Valued Measurements (POVM)

Given general measurement $\{M_m\}_{m=1}^n$, we can define new operators $\Pi_m \equiv M_m^\dagger M_m$ which are positive semi-definite operators by construction and satisfy $\sum_m \Pi_m = \mathbb{I}$. Then, we say that the $\{\Pi_m\}_{m=1}^n$ are the POVM elements associated with measurement M. Conversely, given a set of positive semi-definite operators $\{E_m\}_{m=1}^n$ which resolve the identity $\sum_m E_m = \mathbb{I}$, we can reconstruct measurement operators $\{M_m\}_{m=1}^n$ by defining $M_m = \sqrt{E_m}$. But this decomposition is not unique, so unless we know the M_m operators are given, only the measurement outcome statistics are known and the post-measurement state (40) cannot be determined.

PVMs are special cases of POVMs, and this is true when the measurement operators M_m are projection operators:

$$E_m = P_m^\dagger P_m = P_m^2 = P_m. \tag{42}$$

However, it is also true that POVMs are special cases of projective measurements, which is the content of Naimark's dilation theorem.

Theorem 4 ([64]). *For an n-outcome POVM $\{\Pi_i\}_{i=1}^n$ on $\mathcal{H}$, and pure state $|\phi\rangle\langle\phi|$ on $\mathcal{H}'$ where $\dim \mathcal{H} = \dim \mathcal{H}' = d$, there exists an nd-outcome PVM $\{P_i\}_{i=1}^{nd}$ on $\mathcal{H} \otimes \mathcal{H}'$ such that*

$$\mathrm{Tr}(\rho \Pi_i) = \mathrm{Tr}((\rho \otimes |\phi\rangle\langle\phi|) P_i) \quad \forall i = 1, ..., n \tag{43}$$

We see that measurements on the augmented system produce the statistics of the POVM, so POVMs are also the projections of projective measurements onto a subspace. When the dimension of the ancilla system and the original system are each d, the full system is d^2-dimensional and a projective measurement can measure d^2 outcomes, which is just enough to fix $d^2 - 1$ parameters in the density matrix. [64].

5 Entanglement

Quantum mechanics cannot be fully appreciated without considering multipartite states, since it is there that the most intuitively confronting, philosophically confounding yet experimentally irrefutable predictions of the theory come to light. Namely, stronger-than-classical correlations of simultaneous measurements of distant particles become possible. This is the content of Bell's 1964 paper [3] which brought the debate over local hidden variables [1] within the realm of experimental verification. In the following decades, better and better experiments demonstrated time after time that quantum mechanics, and in fact any post-quantum theory must be nonlocal [4, 81, 82, 83]. Since the first Bell inequality was published in the 1964 paper, many more variations have come out, but they all essentially predict upper bounds on the observable correlations between the inputs and outputs of distant measurement devices when constrained to local classical resources only. Locality here is defined by independence of the distant party in each round in the sampling. In addition, the inequalities are all maximally violated by the sharing of a maximally entangled state. However, the relationship between non-locality and entanglement is not so linear, as we shall see later. For now, a more in depth treatment of entanglement is in order.

Throughout this thesis we will only be concerned with bipartite states, but in general, multi-partite states can be classified into those which are separable, and those which are not. Separable pure states are those which can be expressed as a tensor product of pure states in each subspace

$$|\psi\rangle = |\psi_1\rangle \otimes |\psi_2\rangle \otimes ... \otimes |\psi_n\rangle \tag{44}$$

for an n-partite system in $\mathcal{H}^{\otimes n}$, where each $|\psi_i\rangle$ is the quantum state in the ith system. Those which cannot be expressed in this form are entangled states. We will see in this section that entanglement is fundamentally a quantum mechanical phenomenon.

Consider the maximally entangled singlet state from before:

$$|\psi^-\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B). \tag{45}$$

A measurement which reveals the state of system A to be in state $|0\rangle$ simultaneously collapses the state of system B to state $|1\rangle$. If A measures $|1\rangle$, then B will observe $|0\rangle$. This effect is observable if the roles of A and B are reversed, in any basis they measure, and regardless of how far apart systems A and B are. In recent decades, this feature of quantum mechanics has found a home as a resource in quantum information theory. Efforts to quantify entanglement and to understand the possible manipulations and transformations via protocols for entanglement swapping, entanglement distillation, and teleportation, among others, have driven much of the understanding. In this section, we discuss briefly measures of entanglement and their fundamental connection to local operations. Then, we will discuss maximally entangled states and some properties which facilitate the construction of bipartite equiangular sets.

5.1 The Schmidt Decomposition

The Hilbert space of a bipartite state is $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$. An arbitrary pure state $|\psi\rangle \in \mathcal{H}$ has spanning orthogonal bases $\{|i\rangle_A\}$ in $\mathcal{H}_A$ and $\{|i\rangle_B\}$ which spans $\mathcal{H}_B$. Then for non-negative and real *Schmidt coefficients* λ_i satisfying $\sum_i \lambda_i^2 = 1$, there exists a *Schmidt decomposition* given by [74]

$$|\psi\rangle = \sum_i^k \lambda_i |i\rangle_A |i\rangle_B. \tag{46}$$

We define the *Schmidt rank* $r(|\psi\rangle\langle\psi|)$ to be the number k of terms required in the decomposition of state $|\psi\rangle$. In other words, the Schmidt rank $r(\rho) \geq 1$ counts the number of superpositions of product states needed to produce the state. Separable pure states have no entanglement and have rank one, so a basis can always be found so the state is a product state.

A generalization of the Schmidt rank exists to characterize the degree of entanglement for mixed states and is the *Schmidt number* [84].

5.2 Entanglement Measures and LOCC

We can define a nice measure of entanglement E_S from the Schmidt rank given by

$$E_S(\rho) = r(\rho) - 1. \tag{47}$$

Then it satisfies the following two properties which we require a general entanglement measure E to satisfy [85]:

$$\begin{aligned} &1.\ \rho \text{ is separable} \iff E(\rho) = 0 \\ &2.\ E(\rho) \geq E(\Lambda_M(\rho)), \quad \Lambda_M(\rho) \equiv \frac{M\rho M^\dagger}{\mathrm{Tr}(M\rho)} \qquad \forall M \in \mathrm{LOCC}_X(A:B) \end{aligned} \tag{48}$$

The first statement is straightforward and says that $E(\rho) = 0$ when there is no entanglement. Since $r(\rho) = 1$ for a separable state, E_S satisfies the first condition. The second statement says that entanglement cannot increase under the class of LOCC_X operations. How this set is defined determines the properties of the entanglement measure. For example, let LOCC_{LI} be the set of all local invertible (LI) operations, which includes the set of local unitary operations. These operations change the Schmidt coefficients in the Schmidt decomposition, but leave the Schmidt rank invariant. This can be easily seen:

$$T_1 \otimes T_2 |\phi_r\rangle = \sum_i^r \lambda_i U_1 |i\rangle_A \otimes U_2 |i\rangle_B \tag{49}$$

The idea of a maximally entangled state depends on the entanglement measure. If ρ is the maximally entangled state for a general entanglement measure E, the state $T_1 \otimes T_2\ \rho$ is not maximally entangled according to E. However, if the entanglement measure is defined over the set of all local invertibles, then we have from the definition that for a maximally entangled state ρ_S,

$$E(\rho) \geq E(\Lambda_T(\rho)) \geq E(\Lambda_T^{-1}\Lambda_T(\rho)) = E(\rho) \tag{50}$$

So maximally entangled states can be transformed into each other via local invertible transformations, and the notion of a maximally entangled state is well-defined. These entanglement measures are called *universal entanglement measures*. Since we have shown in (49) that local invertible operations do not change the Schmidt rank, it is a universal entanglement measure [84]. Entanglement measures which are not universal but more useful for particular tasks in quantum information theory are *operational measures*.

If we allow the LOCC class to include local projections LOCC_{LP}, then the resulting entanglement measure is a monotone of the Schmidt rank, since projections map state $|\phi_r\rangle \to |\phi_{r-1}\rangle$ and we've shown that the entanglement increases with the Schmidt number [85].

All this is to show that entanglement in defined relative to the definition of local operations.

5.3 Maximally Entangled States

> Another way of expressing the peculiar situation is: the best possible knowledge of a whole does not necessarily include the best possible knowledge of all its parts, even though they may be entirely separate and therefore virtually capable of being 'best possibly known,' i.e., of possessing, each of them, a representative of its own... I would not call that one but rather the characteristic trait of quantum mechanics, the one that enforces its entire departure from classical lines of thought. -Schrödinger, 1935 [86]

Beyond Schmidt ranks and entanglement measures, an important qualitative property of maximally entangled states is that local states, obtained by tracing out the other part, contain no information at all; locally, they the parts are in maximally mixed states. All the state information is encoded in

the correlation between the two distant parts. This is the peculiarity about entangled states which Schrödinger points out in the above excerpt from [86]. Given many copies of the same bipartite state $|\psi\rangle$, Alice and Bob learn nothing of the state from making local measurements. In any basis they measure, they will obtain the two outcomes with 50-50 probability. Only when they come together and compare their measurement results will they be able to deduce the state. That Alice and Bob do not learn anything from their nonlocal correlations until they communicate classically is how they evade jail time for faster-than-light communication.

Mathematically, this is expressed by the fact that the partial trace of the maximally entangled pure state with respect to any of the subsystems is $|\phi_{AB}\rangle$ the maximally mixed state. The partial trace is the quantum analog of taking the marginal probability distribution of a probability distribution of two random variables, where the probabilities over one are summed over to obtain a probability distribution depending only on one variable. The partial trace over system B of ρ_{AB} produces a reduced density matrix in system A, and is given by

$$\mathrm{Tr}_B[\rho_{AB}] = \sum_i (\mathbb{I}_A \otimes_B \langle i|)\rho_{AB}(\mathbb{I}_A \otimes |i\rangle_B). \tag{51}$$

A similar expression is true for tracing out system A.

5.3.1 Equiangular Lines over Maximally Entangled States

In the space of maximally entangled bipartite states, we make use of the fact that all maximally entangled states can be obtained from another by a unitary matrix in $SU(2)$, since these operations preserve entanglement as shown earlier. For convenience, we let our "base state" be the first Bell state $|\Phi^+\rangle$, so any other maximally entangled state can be obtained from the application of elements of $SU(2)$.

$$|\phi\rangle = U_1 \otimes U_2 |\Phi^+\rangle, \tag{52}$$

The $SU(2)$ unitaries are parameterized by the Lie algebra $\mathfrak{su}(2)$ to Lie group correspondence:

$$U = e^{i\alpha \hat{v}\cdot\vec{\sigma}} \tag{53}$$

where α is the rotation angle, $\hat{v}$ is a unit Bloch vector, and $\vec{\sigma} = (\sigma_x, \sigma_y, \sigma_z)$ where σ_i are the usual Pauli matrices:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{54}$$

If we expand the matrix exponential and use the fact that the square of any Pauli matrix is the identity, we get a very simple expression for an arbitrary $SU(2)$ unitary:

$$U = \cos\alpha + i \sin\alpha (\hat{v}\cdot\vec{\sigma}). \tag{55}$$

We can further simplify the expression (52) due to a feature of operators which are applied to maximally entangled states:

$$U \otimes \mathbb{I}_d |\phi^+\rangle = \mathbb{I}_d \otimes U^{\mathsf{T}} |\phi^+\rangle, \tag{56}$$

where $|\phi^+\rangle$ may be replaced with any maximally entangled state.

To show this, insert the tensor identity element $\sum_{j,k}(|j\rangle_A|k\rangle_B)(\langle j|_A\langle k|_B)$ into the expression in

(52):

$$\begin{aligned}(U \otimes \mathbb{I}_2)|\Phi^+\rangle &= (U \otimes \mathbb{I}_2)\frac{1}{\sqrt{2}}\sum_{i=0}^{1}|i\rangle_A|i\rangle_B \\ &= \frac{1}{\sqrt{2}}\sum_{i,j,k=0}^{1}|j\rangle_A|k\rangle_B\langle j|_A\langle k|_B[(U \otimes \mathbb{I}_2)|i\rangle_A|i\rangle_B] \\ &= \frac{1}{\sqrt{2}}\sum_{i,j=0}^{1}|j\rangle_A|i\rangle_B\langle j|_A U|i\rangle_A \\ &= \frac{1}{\sqrt{2}}\sum_{i,j=0}^{1}U_{ji}|j\rangle_A|i\rangle_B \\ &= \frac{1}{\sqrt{2}}\sum_{j=0}^{1}|j\rangle_A\Big(\sum_i U_{ji}|i\rangle_B\Big) \\ &= (\mathbb{I}_2 \otimes U^{\mathsf{T}})|\Phi^+\rangle\end{aligned} \tag{57}$$

so letting $U \equiv U_1 U_2^{\mathsf{T}}$, (52) can be rewritten

$$|\phi\rangle = U \otimes \mathbb{I}|\Phi^+\rangle. \tag{58}$$

With this, we derive the following formula for the inner product of a pair of maximally entangled two qubit states $|\phi_i\rangle = U_i|\Phi^+\rangle$, $|\phi_j\rangle = U_j|\Phi^+\rangle$:

$$\begin{aligned}|\langle\phi_i|\phi_j\rangle|^2 &= \left|\frac{1}{2}\langle\Phi^+|U_i^\dagger U_j \otimes \mathbb{I}|\Phi^+\rangle\right|^2 \\ &= \left|\frac{1}{2}\mathrm{Tr}(U_i^\dagger U_j)\right|^2.\end{aligned} \tag{59}$$

5.4 Constructions in $\mathbb{C}^2 \otimes \mathbb{C}^2$

The construction of equiangular lines in two-qubit systems is facilitated by the following angle-preserving isomorphism from unit vectors in $\mathbb{R}^4$ to matrices in $SU(2)$:

$$\hat{v} = v_t e_1 + v_x e_2 + v_y e_3 + v_z e_4 \leftrightarrow u = v_t i\mathbb{I} + v_x\sigma_x + v_y\sigma_y + v_z\sigma_z, \tag{60}$$

where $\{\hat{e}_i\}_{i=1}^4$ are the standard orthonormal basis vectors. It can be verified that values of scalar products of arbitrary vectors $\hat{v}_i$, $\hat{v}_j$ in $\mathbb{R}^4$ are preserved under the mapping to the Hilbert-Schmidt inner products of the matrices. If vectors $\hat{v}_1, \hat{v}_2 \in \mathbb{R}^4$ map respectively to $u_1, u_2 \in SU(2)$, then

$$\hat{v}_1 \cdot \hat{v}_2 = \frac{1}{2}\mathrm{Tr}(u_1^\dagger u_2). \tag{61}$$

Then, the problem is reduced to finding equiangular lines in $\mathbb{R}^4$ and then mapping them to unitaries in $SU(2)$ which define the corresponding maximally entangled states via (58). Such a simple parameterization of unitary matrices does not exist for qutrits and beyond, so constructing equiangular lines in higher dimensions becomes quite a bit more difficult!

6 Results

Here, we present some equiangular constructions in $\mathbb{C}^2 \otimes \mathbb{C}^2$, which are the results of this thesis work.

6.1 5 State Constructions

6.1.1 Product State ETF

The set $\{U_i \otimes V_i|00\rangle\}_{i=1}^5$ forms an ETF of 5 product states at $\mu = 1/16$ where the $U_i \otimes V_i$ are given by

$$\begin{aligned}
U_1 \otimes V_1 &= \mathbb{I} \otimes \mathbb{I} \\
U_2 \otimes V_2 &= \left(\cos\frac{2\pi}{5}\mathbb{I} + i\sin\frac{2\pi}{5}\sigma_x\right) \otimes \left(\cos\frac{4\pi}{5}\mathbb{I} + i\sin\frac{4\pi}{5}\sigma_x\right) \\
U_3 \otimes V_3 &= \left(\cos\frac{3\pi}{5}\mathbb{I} + i\sin\frac{3\pi}{5}\sigma_x\right) \otimes \left(\cos\frac{\pi}{5}\mathbb{I} + i\sin\frac{\pi}{5}\sigma_x\right) \\
U_4 \otimes V_4 &= \left(\cos\frac{\pi}{5}\mathbb{I} - i\sin\frac{\pi}{5}\sigma_x\right) \otimes \left(\cos\frac{2\pi}{5}\mathbb{I} - i\sin\frac{2\pi}{5}\sigma_x\right) \\
U_5 \otimes V_5 &= \left(\cos\frac{\pi}{5}\mathbb{I} + i\sin\frac{\pi}{5}\sigma_x\right) \otimes \left(\cos\frac{2\pi}{5}\mathbb{I} + i\sin\frac{2\pi}{5}\sigma_x\right)
\end{aligned} \tag{62}$$

The local sets $\{U_i\}_{i=1}^5$ and $\{V_i\}_{i=1}^5$ themselves cannot be equiangular, since the maximum number of lines in $\mathbb{C}^2$ is 4. However, they each form tight frames, so

$$\begin{aligned}
\sum_{i=1}^{5} U_i|0\rangle\langle 0|U_i^\dagger &= \frac{5}{2}\mathbb{I} \\
\sum_{i=1}^{5} V_i|0\rangle\langle 0|V_i^\dagger &= \frac{5}{2}\mathbb{I}.
\end{aligned} \tag{63}$$

6.1.2 Maximally Entangled ETF (BSM5)

To make things simpler, we make the following assignments:

$$\begin{aligned}
a = \cos\frac{2\pi}{5} &= \frac{-1+\sqrt{5}}{4}, \quad b = \sin\frac{2\pi}{5} = \sqrt{\frac{5+\sqrt{5}}{8}} \\
c = \cos\frac{4\pi}{5} &= -\frac{1+\sqrt{5}}{4}, \quad d = \sin\frac{4\pi}{5} = \sqrt{\frac{5-\sqrt{5}}{8}},
\end{aligned} \tag{64}$$

and we make use of the isomorphism in (60). We generate six equiangular lines in $\mathbb{R}^4$ by repeated application of the generator

$$G = \begin{pmatrix} a & -b & 0 & 0 \\ b & a & 0 & 0 \\ 0 & 0 & c & -d \\ 0 & 0 & d & c \end{pmatrix} \tag{65}$$

to the fiducial $\frac{1}{\sqrt{2}}(1,0,1,0)$. Since $G^5 = \mathbb{I}$, this construction generates a five-state ETF:

$$\hat{u}_1 = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\0\\1\\0\end{pmatrix} \quad \hat{u}_2 = \frac{1}{\sqrt{2}}\begin{pmatrix}a\\b\\c\\d\end{pmatrix} \quad \hat{u}_3 = \frac{1}{\sqrt{2}}\begin{pmatrix}a\\-b\\c\\-d\end{pmatrix} \quad \hat{u}_4 = \frac{1}{\sqrt{2}}\begin{pmatrix}c\\-d\\a\\b\end{pmatrix} \quad \hat{u}_5 = \frac{1}{\sqrt{2}}\begin{pmatrix}c\\d\\a\\-b\end{pmatrix} \tag{66}$$

These are mapped to $SU(2)$ unitaries which produce the ETF in $\mathbb{C}^2 \otimes \mathbb{C}^2$.

$$\begin{aligned}
|\phi_1\rangle &= |\Phi^+\rangle \\
|\phi_2\rangle &= \frac{1}{2}\Big[(a+c)|\Phi^+\rangle + (a-c)|\Psi^-\rangle + i\big[(b-d)|\Phi^-\rangle - (b+d)|\Psi^+\rangle\big]\Big] \\
|\phi_3\rangle &= \frac{1}{2}\Big[(a+c)|\Phi^+\rangle + (a-c)|\Psi^-\rangle + i\big[-(b-d)|\Phi^-\rangle + (b+d)|\Psi^+\rangle\big]\Big] \\
|\phi_4\rangle &= \frac{1}{2}\Big[(a+c)|\Phi^+\rangle - (a-c)|\Psi^-\rangle - i\big[(b+d)|\Phi^-\rangle + (b-d)|\Psi^+\rangle\big]\Big] \\
|\phi_5\rangle &= \frac{1}{2}\Big[(a+c)|\Phi^+\rangle - (a-c)|\Psi^-\rangle + i\big[(b+d)|\Phi^-\rangle + (b-d)|\Psi^+\rangle\big]\Big]
\end{aligned} \tag{67}$$

where we have applied $U_1^\dagger \otimes \mathbb{I}$ to all states $U_i \otimes \mathbb{I}|\phi^+\rangle$ so that the unitary on state $i = 1$ is just the identity with Bloch vector $(0,0,0)$. The Bloch vectors of the other four states form a regular tetrahedron as shown in figure 3. The rotation angle α about the Bloch vector is the same for all states, but this value can take on one of four values $\alpha = \arccos(\frac{1}{4}) + \frac{n\pi}{4}$, $n = 1,2,3,4$.

Although the five equiangular lines in $\mathbb{R}^4$ are group covariant, there seems to be no such group relation among the maximally entangled states which can be seen from the fact that the five corresponding unitaries do not include inverses for any of the elements. The ETF in the Bloch sphere is shown in figure 3.

6.1.3 Uniqueness of Equiangular Tight Frames

Supposing Gram matrices G_1 and G_2 represent two ETFs with common overlap $|\alpha|$, they must both have characteristic polynomial $\lambda^{n-d}(\lambda - n/d)^d$. This is because we know that rank G = rank F, and for for ETFs, the rank is d. So G_1 and G_2 both have eigenvalue 0 with multiplicity $n-d$. Because the frame operator is proportional to the identity $F = c\mathbb{I}$, all other eigenvalues are equal to some constant c with multiplicity d. The trace of the Gram matrix is fixed to Tr $G = n$, so $n = c \times d$ and the eigenvalue is $c = n/d$ with multiplicity d.

So G_1 and G_2 have the same characteristic polynomial, meaning they are related by a sequence of index permutations and multiplications of rows and corresponding columns by -1. We know this because [25] determined that there are 16 distinct classes distinguished by their characteristic polynomials, and all Gram matrices within a class can be obtained from each other by these operations. The compositions of such unitary operations is of course, unitary, so G_1 and G_2 are related by a unitary transformation.

Thus, all ETFs (including the 5-state ETF in $\mathbb{R}^4$ and, therefore, the corresponding bipartite qubit ETF) are unique up to unitary equivalence.

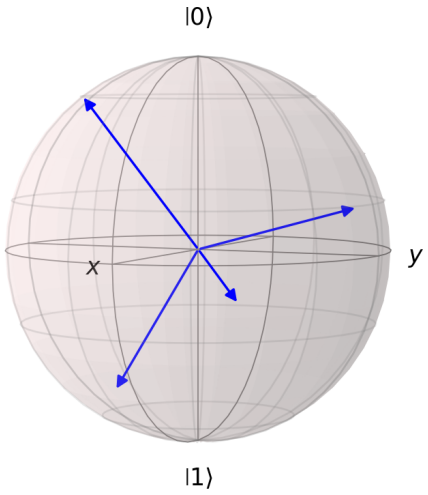

Figure 3: Bloch vector representation of the unitary matrices which form a set of 5 equiangular lines in $\mathbb{C}^2 \otimes \mathbb{C}^2$ when applied to the first Bell state $|\Phi^+\rangle$. The first state is the identity matrix which is represented at the origin of the Bloch sphere. The other four form a regular tetrahedron, which is a $(4, 3)$ real ETF.

6.2 6 State Constructions

6.2.1 Maximally Entangled Equiangular Set from the Regular Icosahedron

Looking at table 1, we notice that the maximum number of equiangular lines in $\mathbb{R}^3$ is the same as that in $\mathbb{R}^4$, so we may embed the three dimensional equiangular set in $\mathbb{R}^4$, and make the mapping to $\mathbb{C}^2 \otimes \mathbb{C}^2$ with (60) to obtain 6 maximally entangled equiangular lines. Then, the equiangular set in $\mathbb{R}^4$ comes from the 6 diagonals of the regular icosahedron in (29) with an extra zero in the fourth dimension appended to each vector. The states they map to are given by

$$\begin{aligned} |\phi_1\rangle &= \frac{1}{A}(|\Psi^+\rangle - ip|\Psi^-\rangle) & |\phi_2\rangle &= \frac{1}{A}(|\Psi^+\rangle + ip|\Psi^-\rangle) \\ |\phi_3\rangle &= \frac{1}{A}(-i|\Phi^+\rangle + p|\Psi^+\rangle) & |\phi_4\rangle &= \frac{1}{A}(-i|\Phi^+\rangle - p|\Psi^+\rangle) \\ |\phi_5\rangle &= \frac{1}{A}(ip|\Phi^+\rangle - i|\Psi^-\rangle) & |\phi_6\rangle &= \frac{1}{A}(-ip|\Phi^+\rangle - i|\Psi^-\rangle) \end{aligned} \tag{68}$$

6.2.2 Optimal Maximally Entangled Equiangular Set

From the discussion of frames and erasures, we find that the 6 equiangular lines constructed in the previous section are not the most optimal since they are all orthogonal in the fourth dimension. We show that the Welch bound cannot be reached for $n = 6$ in the next section, but we can reach

$\mu = 1/9$. The states producing this optimal set are given by

$$\begin{aligned}
|\psi_1\rangle &= |\Phi^+\rangle \\
|\psi_2\rangle &= -\frac{1}{3}|\Phi^+\rangle + i\frac{2\sqrt{2}}{3}|\Phi^-\rangle \\
|\psi_3\rangle &= \frac{1}{3}|\Phi^+\rangle - i\frac{\sqrt{2}}{6}|\Phi^-\rangle - i\sqrt{\frac{5}{6}}|\Psi^+\rangle \\
|\psi_4\rangle &= \frac{1}{3}|\Phi^+\rangle + i\frac{\sqrt{2}}{3}|\Phi^-\rangle + i\sqrt{\frac{2}{15}}|\Psi^+\rangle + 2\sqrt{\frac{2}{15}}|\Psi^-\rangle \\
|\psi_5\rangle &= \frac{1}{3}|\Phi^+\rangle + i\frac{\sqrt{2}}{3}|\Phi^-\rangle - i\sqrt{\frac{2}{15}}|\Psi^+\rangle - 2\sqrt{\frac{2}{15}}|\Psi^-\rangle \\
|\psi_6\rangle &= \frac{1}{3}|\Phi^+\rangle - i\frac{\sqrt{2}}{6}|\Phi^-\rangle + i\frac{3}{\sqrt{30}}|\Psi^+\rangle - \frac{4}{\sqrt{30}}|\Psi^-\rangle
\end{aligned} \tag{69}$$

The proof that $\mu = 1/9$ really is the smallest overlap squared value for $n = 6$ states for bipartite qubit states is given in appendix C.

6.2.3 No 6-State ETF Proof

From the Gram matrix, of an equiangular set $\{\hat{x}_i\}_{i=1}^n$ with common overlap $\pm\alpha$, the following matrix may be defined:

$$S = \frac{1}{\alpha}(G - \mathbb{I}), \tag{70}$$

This real and symmetric matrix has ± 1 on all off-diagonal entries, and 0's along the diagonal. We will show that from theorem 12 and corollary 13 in [87], when $d < n - 1$ and $n \neq 2d$, the following quantities must be integers for there to exist an ETF of n lines in $\mathbb{R}^d$:

$$\lambda_1 = \sqrt{\frac{d(n-1)}{n-d}} \qquad \lambda_2 = \sqrt{\frac{(n-1)(n-d)}{d}}. \tag{71}$$

For $n = 6$ and $d = 4$, $\lambda_1 = \sqrt{10}$ and $\lambda_2 = \sqrt{5/2}$ so there can be no ETF. Due to the isomorphism (60), there can be no ETF of 6 states for bipartite qubit states either.

An informal motivation for why this theorem is true follows. Recall that $G = V^\dagger V$ and $F = VV^\dagger$ have the same eigenvalues. For an ETF, the eigenvalues for both are 0 with multiplicity $n - d$, and n/d with multiplicity d. The characteristic polynomial of matrix S belongs to the ring of integer polynomials $\mathbb{Z}[x]$, since all of its entries are integers. It is well known that complex conjugate roots of a polynomial with real coefficients come in pairs. A similar statement is true for irrational roots of polynomials with integer or rational coefficients. For example, the polynomial $f(x) = x^2 - 2$ has coefficients in the ring of integers, and there are two conjugate roots $\pm\sqrt{2}$. So the fact that $n \neq 2d$ ensures that the two eigenvalues with multiplicities d and $n-d$ cannot be conjugate pairs of any kind.

In brief, the eigenvalues of G belong to the same field as do the coefficients of the characteristic polynomial given that $n \neq 2d$, and they are all integers.

7 Quantum State Discrimination (QSD)

Due to the description of general quantum states as superpositions of orthogonal basis states, unless two bipartite states $|\phi_0\rangle$ and $|\phi_1\rangle$ are orthogonal, applying a measurement on either state generally produces non-zero probabilities to observe either state. This makes correctly differentiating quantum states harder than determining the outcome of a coin toss. For a given state $|\phi_i\rangle$ with prior probability p_i from the set $\{p_i, |\phi_i\rangle\}$, how can you design measurements of the state to optimize your chances of guessing correctly? For differentiating two states, it is known that the minimum probability of error in discrimination is given by the Helström bound [88]:

$$P_{err} = \frac{1}{2}\left(1 - \sqrt{1 - 4p_0p_1|\langle\phi_0|\phi_1\rangle|^2}\right). \tag{72}$$

Suppose you in Sweden and your best friend in New York have been distributed two parts of a bipartite state from $\{p_i, \rho_{AB}\}$. Provided that you can only make rotations and measurements on your half of the bipartite state and communicate with a classical channel, how can you cooperate with them to optimize your guessing probability then? This is the task of quantum state discrimination. It is through this task that the relationship between entanglement and nonlocality can be probed with more nuance. As we'll see, there are entirely orthogonal product sets which are nonetheless LOCC indistinguishable, and at the same time there are orthogonal sets of maximally entangled states which are LOCC distinguishable but become indistinguishable when one is replaced by a product state [88]. For some states, the distinguishability even depends on who makes the first measurement [89]. So the relationship between entanglement and nonlocality is not as linear as it may seem at first.

7.1 Applications of Quantum State Discrimination

7.1.1 Taking Advantage of Indistinguishability

Terhal et. al. [90] put this local indistinguishability of entangled states to use with a bit-hiding protocol. In this protocol, a hider has a reservoir of each of the four Bell states, and encodes a bit b into state $\rho_0^{(n)}$ for the $b = 0$ bit and $\rho_1^{(n)}$ for $b = 1$. n quantifies the degree of security of the protocol. To hide each bit, a set of n randomly chosen Bell states are distributed to Alice and Bob. If the number of singlet states $|\psi^-\rangle$ is even, then the hidden bit is $b = 0$. If odd, then $b = 1$. They demonstrate that the probabilities of successful determination, $p_{0|0}$ and $p_{1|1}$, satisfy

$$-\delta \leq p_{0|0} + p_{1|1} - 1 \leq \delta. \tag{73}$$

They show that $\delta = 1/2^{n-1}$, so as the number of Bell states per hidden bit grows, $p_{0|0}$ and $p_{1|1}$ are squeezed closer and closer to a 50-50 distribution, so less and less information of the bit can be obtained with LOCC. Of course, if Alice and Bob have a quantum channel or have access to global measurements, they can measure each Bell state one by one and count the number of singlet states. If they share sufficient prior entanglement, Alice can teleport her Bell states to Bob and he can also count the singlet states one by one by making global measurements on the whole bipartite state. From this example, we can see that it is useful to be able to determine for the security of the bit-hiding how much information the adversarial parties Alice and Bob can gain from the states they are given access to different resources.

7.1.2 No-Cloning, No-Signaling, and Quantum State Discrimination

A fundamental result in quantum information theory is the no-cloning theorem, which says that arbitrary, non-orthogonal quantum states cannot be perfectly replicated. A common justification for this is due to the linearity of quantum operators [91]. Suppose that for two possible orthogonal states $|\uparrow\rangle_A, |\downarrow\rangle_A \in \mathcal{H}_A$ and arbitrary initial state $|0\rangle_B \in \mathcal{H}_B$, there exists a unitary evolution U acting on $\mathcal{H}_A \otimes \mathcal{H}_B$ which has the effect

$$\begin{aligned} U|\uparrow_A 0_B\rangle &= |\uparrow_A\uparrow_B\rangle \\ U|\downarrow_A 0_B\rangle &= |\downarrow_A\downarrow_B\rangle \end{aligned} \tag{74}$$

As it is a perfect cloner, it should also replicate any superposition of the two. However, we find that

$$\begin{aligned} U(\alpha|\uparrow\rangle_A + \beta|\downarrow\rangle_A)|0\rangle_B &= \alpha|\uparrow_A\uparrow_B\rangle + \beta|\downarrow_A\downarrow_B\rangle \\ &\neq (\alpha|\uparrow_A\rangle + \beta|\downarrow\rangle_A)(\alpha|\uparrow_B\rangle + \beta|\downarrow\rangle_B) \end{aligned} \tag{75}$$

so the linear operator cannot clone arbitrary states. Known orthogonal states, however, can be cloned. As such, only orthogonal states are distinguishable. It is known that measurements on a single copy of a quantum state can only provide partial information of the full state. A full determination of the state requires a reservoir of identically prepared states over which statistical averages are taken over different observables. [92]. So provided a perfect quantum cloning machine, Bob can produce the ensemble he needs to make a perfect state determination. It can also be understood to be that given state $|\psi\rangle$ ($|\phi\rangle$), Bob can obtain the state $|\psi\rangle^{\otimes n}$ ($|\phi\rangle^{\otimes n}$) with his cloning machine. In the limit that $n \to \infty$, the states become orthogonal and can be perfectly distinguished with a projective measurement. So we see that the no-cloning theorem and the state-discrimination problem are closely related to each other.

In [93], no-cloning is shown to be a restriction of any theory which accepts both nonlocality and no-signaling (i.e. no superluminal signaling). Naturally, one would expect that no-signaling and no-cloning are also fundamentally related. Indeed, in [94], the problem of QSD is incorporated into a communication scenario, and it is shown that in fact that the no-signaling constraint of the semidefinite program is a tight bound on optimal QSD.

The rest of this section will discuss various measurements and provide some particularly interesting examples of QSD. Then we will take a look at the distinguishability of the above constructions.

7.2 Measures of Successful Discrimination

Suppose Alice and Bob are separated in space and share a composite state which is drawn from the ensemble $\{p_i, \rho_i\}_i^N$, where $\rho_i = |\phi_i\rangle\langle\phi_i|$. Their task will be to devise a measurement strategy of measurements $\{E_a\}$ with outcomes labelled by a to best determine which state they are given. To do this, they use the following expression to quantify their success rate P_{win}:

$$P_{\text{win}} = \frac{1}{N}\sum_i \text{Tr}(\rho_i E_a) = \frac{1}{N}\sum_i \langle\phi_i|E_a|\phi_i\rangle G(i|a) \tag{76}$$

where $\text{Tr}(\rho_i\, E_a) = \langle\phi_i|E_a|\phi_i\rangle$ is the probability that they observe measurement outcome a given state $\rho_i = |\phi_i\rangle\langle\phi_i|$, and post-processing strategy $G(i|a)$ is the probability that Alice and Bob choose state i given the observation of measurement a. Summing over index i gives P_{win}, the total probability that Alice and Bob guess state i given the measurement outcome when they are given state $|\phi_i\rangle$.

Optimal measurements optimize (76) over all measurements $\{E_i\}$ and guessing strategies $G(i|a)$. We impose the constraint $\sum_i G(i|a) = 1$ which just says that that for a given measurement outcome a, the probabilities of choosing one of the states in the set must sum to one. Then maximizing over the guessing strategy G means

$$\max_G \sum_{i,a} \langle\phi_i|E_a|\phi_i\rangle G(i|a) = \sum_a \max_G \left[\sum_i \langle\phi_i|E_a|\phi_i\rangle G(i|a) \right] \tag{77}$$

where the sum in the big brackets is a convex combination of the measurement probabilities. It is known that convex combinations of linear functions find their maxima at extremal points, so the optimal guessing strategy is a deterministic one. It is straightforward to show that given state ρ from ensemble $\{p_i, \rho_i\}_i^n$, the maximum success rate for Alice and Bob to determine the state is d/n. To show this,

$$\frac{1}{n}\sum_a \mathrm{Tr}(E_a\rho) \leq \frac{1}{n}\sum_a \lambda_{\max}\mathrm{Tr}(\rho) \leq \frac{1}{n}\sum_a \mathrm{Tr}(E_a) = \frac{1}{n}\mathrm{Tr}(\sum_a E_a) = \frac{1}{n}\mathrm{Tr}(\mathbb{I}) = \frac{d}{n} \tag{78}$$

Where the first inequality follows from choosing ρ to be in the eigenstate of E_a with the largest eigenvalue. The second inequality holds because a positive semi-definite operator E_a only has non-negative eigenvalues so the sum of all of them must be greater than or equal to its maximum eigenvalue.

7.3 Global Measurements

7.3.1 Global Entangled Measurements

The most powerful measurements are of course those which can be performed jointly on both parts of the system with entangled measurements, meaning that the states $|\psi_i\rangle$ in measurements $\{|\psi_i\rangle\langle\psi_i|\}_{i=1}^n$ are entangled. Any orthonormal basis of maximally entangled states can be perfectly distinguished with such global measurements, and the set of 5 maximally entangled equiangular set can be distinguished with 4/5 success rate. This follows from (78). This is the generalization of BSM4 to non-projective, non-orthogonal measurements.

7.3.2 PPT Measurements

For a multi-partite state to be separable, it is necessary (and sufficient for $2 \otimes 2$ and $2 \otimes 3$ systems) that the partial transpose of the density operator with respect to any partition are also positive semi-definite density operators. For example, for bipartite state ρ_{AB}, we may define T to be the transpose operator and $\mathbb{I} \otimes T$ to be the partial transpose operator leaving A invariant and transposing system B. Applied to state $\rho_{m\mu,n\nu}$ where Latin letters index system A and Greek letters index system B, we have

$$(\mathbb{I} \otimes T)\rho_{m\mu,n\nu} = \rho_{m\nu,n\mu} \tag{79}$$

This criterion follows from the fact that T is a positive operator, but not completely positive so $T \otimes I$ may or may not be, depending on the state ρ_{AB} it is applied to. In fact if ρ_{AB} is separable, then the independent action of the transpose on system A or B given by $(\mathbb{I} \otimes T)\rho_{AB}$ is still positive semi-definite. If ρ_{AB} is non-separable, then $(\mathbb{I} \otimes T)\rho_{AB}$ may or may not be positive semi-definite. So all separable measurements are necessarily PPT, but there exist states which are separable but not PPT [95]. This strict inclusion can be used to derive albeit weak upper bounds on the distinguishability of separable and LOCC measurements.

7.3.3 Separable Measurements

A separable measurement $\Pi = \{\Pi_1, \Pi_2, ..., \Pi_n\}$ where $\sum_i \Pi_i = \mathbb{I}$ is one where each Π_i operating on Hilbert space $\mathcal{H} = \mathcal{H}_A \otimes \mathcal{H}_B$ can be expressed as a convex combination of product operators [95]:

$$\Pi_i = \sum_j P_j \otimes Q_j \tag{80}$$

where P_j and Q_j are positive semi-definite operators. Separable measurement operators are separable, so they are also PPT. Global separable measurements cannot produce entanglement where there was none initially. Set $Sep(X : Y)$ is a compact, closed convex set so optimizations can be easily performed with convex optimization. A sample optimization problem statement

$$\begin{aligned} \text{maximize: } & \sum_i p_i \text{Tr}(\rho_i \Pi_i) \\ \text{satisfying: } & \sum_i \Pi_i = \mathbb{I}_{X\otimes Y} \\ & \Pi_i \in Sep(X : Y) \quad \forall i \end{aligned}$$

7.4 LOSR and LOCC Measurements

Now we turn to LOCC measurements. If the measurement outcome of $\{\Pi_a\}_a^n$ applied to state ρ is a, then the post-measurement state is

$$\rho \to \frac{\Pi_a \rho \Pi_a^\dagger}{\text{Tr}(\Pi_a \rho \Pi_a^\dagger)} \tag{81}$$

After one round of LOCC, Alice has made measurement A_{a_1} with outcome a_1, communicated this classically to Bob, and subsequently Bob has made a measurement $B_{b_1|a_1}$ on his state conditioned on the result Alice sent him. After two rounds, state ρ becomes

$$\rho \to \frac{\big(A_{a_1} \otimes B_{b_1|a_1}\big)\rho\big(A_{a_1}^\dagger \otimes B_{b_1|a_1}^\dagger\big)}{\text{Tr}\big((A_{a_1} \otimes B_{b_1|a_1})\rho(A_{a_1}^\dagger \otimes B_{b_1|a_1}^\dagger)\big)} \tag{82}$$

$$\to \frac{\big(A_{a_2|b_1,a_1}A_{a_1} \otimes B_{b_2|a_2,b_1,a_1}B_{b_1|a_1}\big)\rho\big(A_{a_2|b_1,a_1}^\dagger A_{a_1}^\dagger \otimes B_{b_2|a_2,b_1,a_1}^\dagger B_{b_1|a_1}^\dagger\big)}{\text{Tr}\big((A_{a_1} \otimes B_{b_1|a_1})\rho(A_{a_1}^\dagger \otimes B_{b_1|a_1}^\dagger)\big)}. \tag{83}$$

Already, after just two rounds, the expressions for the states become quite cumbersome. The LOCC class includes all strategies involving an infinite number of measurement and communication rounds, it is clear to see that characterizing and optimizing over the full class of LOCC measurements is a hopelessly difficult thing to do. Moreover, the full class of LOCC protocols is not a closed set [96]. For this reason, the class of separable measurements is useful for providing tighter upper bounds on LOCC since all LOCC measurements can be expressed as a separable measurement in the form given in (80), but not the other way around. See section 7.5 for examples of this. Given an arbitrary measurement operator in the form of (80), it is generally difficult to tell if this can be decomposed into an LOCC sequence [97].
The class of LOCC measurements can be further classified into the following variations:

- One-way LOCC ($\text{LOCC}_\to$): classical communication is limited to one pre-determined direction

- N-round LOCC (LOCC_N): finite number of LOCC rounds
- unbounded LOCC: infinite rounds are allowed

The relationships between LOCC, SEP, PPT and global entangled measurements are given by [96]

$$\text{LOCC} \subset \text{SEP} \subset \text{PPT} \subset \text{GLOBAL} \tag{84}$$

In [98], an algorithm is proposed to implement an arbitrary separable measurement when it exists. In the absence of an exact LOCC implementation, the measurement statistics of a separable measurement can always be simulated by an LOCC measurement [99]. To get a sense of the diversity of operations which are LOCC, we note that well-known protocols such as quantum teleportation, quantum key distribution and entanglement distillation are all carried out with LOCC operations.

Finally, we can restrict the communication capabilites of Alice and Bob so that now they are restricted to local operations and shared randomness. This is abbreviated as LOSR.

7.4.1 Distinguishing Bell States with LOCC

For illustration purposes and for later comparison with the distinguishability of BSM5, we study the distinguishability of the four Bell states (85) under LOCC. The four states are stated again here:

$$\begin{aligned} |\Phi^{\pm}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle_{AB} \pm |11\rangle_{AB}) \\ |\Psi^{\pm}\rangle_{AB} &= \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}) \end{aligned} \tag{85}$$

With global measurements, the four Bell states can be perfectly discriminated since they are orthogonal. The measurement they make is $\{|\Phi^{\pm}\rangle\langle\Phi^{\pm}|, |\Psi^{\pm}\rangle\langle\Psi^{\pm}|\}$. Restricted to LOCC with one-copy only, Alice and Bob have a success rate of 50%, due to the fact that in any basis they measure, they always project out one bit of information. For instance, if they both measure in the $\hat{z}$ basis, they will obtain either $\{|00\rangle, |11\rangle\}$ from which they conclude either $|\Phi^{\pm}\rangle$ or $\{|01\rangle, |10\rangle\}$ from which they conclude either $|\Psi^{\pm}\rangle$.

With two copies, Alice and Bob can perfectly identify the state. To do so, they both measure in $\hat{z}$ on one copy, with which they narrow the possibilities down to the same two options from before. Then they make $\hat{x}$ on the other to distinguish the remaining two. In fact, the protocol they use to perfectly distinguish the four states did not require any communication so they are able to do so with LOSR only.

We collect some well-known results about distinguishing product and maximally entangled states with LOCC:

- Any two orthogonal pure or entangled states can be distinguished with LOCC [100].
- Any two non-orthogonal pure or entangled state can be optimally distinguished with LOCC. This means an LOCC measurement can do as well as a separable one [101].
- Any three orthogonal states can be perfectly distinguished with LOCC iff two are product [89].
- Any three linearly independent pure quantum states can be locally distinguished with non-zero probability [102].

- At most d states can be distinguished in $\mathbb{C}^d \otimes \mathbb{C}^d$ with LOCC [103].

7.5 Special Sets

Here we describe some highly-cited constructions which have demonstrated that entanglement is not necessary for LOCC to fail to discriminate quantum states. The implication is that nonlocality exists in the absence of entanglement so they are separate phenomena.

7.5.1 Peres and Wootter's Qu-Trine States

In 1991, Peres and Wootters constructed the first product states of two qubits for which LOCC measurements could not do as well as a global measurement [21]. Later, Wootters demonstrated that a separable measurement could do just as well as global measurements, but LOCC remained sub-optimal [104]. The qu-trine states from the construction are reproduced here from (28)

$$|\psi_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad |\psi_1\rangle = \begin{pmatrix} -1/2 \\ -\sqrt{3}/2 \end{pmatrix} \quad |\psi_2\rangle = \begin{pmatrix} -1/2 \\ \sqrt{3}/2 \end{pmatrix} \tag{86}$$

Alice and Bob are each given a part of one of three product states $|\psi_i\rangle \otimes |\psi_i\rangle$ for $i = 0, 1, 2$. With LOCC measurements, they are tasked to determine which one they have been given. By means Monte Carlo simulations of various measurement strategies, they were able to show that an information gain of 1.262 bits was optimally obtainable from an LOCC measurement whereas 1.369 bits is possible from a global measurement. Chitambar and Hsieh [97] showed that the distinguishing power of the qutrine states are ordered as follows

$$\text{LOCC}_{\rightarrow} \subset \text{LOCC} \subset \text{GLOBAL SEP} = \text{GLOBAL ENT} \tag{87}$$

7.5.2 Nonlocality without Entanglement

Nine orthogonal, product $2 \otimes 3$ states were presented in a celebrated paper demonstrating nonlocality in the absence of entanglement. The unnormalized states are given by

$$\begin{aligned} |\psi_1\rangle &= |1\rangle \otimes |1\rangle & |\psi_2\rangle &= |0\rangle \otimes |0+1\rangle \\ |\psi_3\rangle &= |0\rangle \otimes |0-1\rangle & |\psi_4\rangle &= |2\rangle \otimes |1+2\rangle \\ |\psi_5\rangle &= |2\rangle \otimes |1-2\rangle & |\psi_6\rangle &= |1+2\rangle \otimes |0\rangle \\ |\psi_7\rangle &= |1-2\rangle \otimes |0\rangle & |\psi_8\rangle &= |0+1\rangle \otimes |2\rangle \\ |\psi_9\rangle &= |0-1\rangle \otimes |2\rangle \end{aligned} \tag{88}$$

It is known that orthogonality of a set of states is necessary for perfect distinguishability, but these states demonstrate that it is not sufficient. It is for the very simple reason that the product states, with the components in both systems taken together, form an orthogonal set so they are distinguishable by an observer with access to global separable measurements. However, the nine local states observed by Alice and Bob in their local systems $\{|0\rangle, |1\rangle, |2\rangle, |1+2\rangle, |1-2\rangle, |0+1\rangle, |0-1\rangle\}$ are not orthogonal, since nine states cannot be orthogonal in $\mathbb{C}^3$. Each local set *completes* the orthogonality of the other's. So Alice and Bob, who locally do not have access to the full orthogonal set, can only perform local operations and measurements on their totally indistinguishable states. Refer to [105] for the full proof.

7.6 Distinguishability of the 5-State Bell Measurement

All numerical results in this section regarding the distinguishability of the states in section 6 were obtained with Mathematica.

One Copy For LOSR, we optimize the expression

$$P_{\text{win}} = \frac{1}{5}\sum_i \text{Tr}\big((A_a \otimes B_b)\rho_i\big)G(i|a,b) \tag{89}$$

over measurements A_a, B_b, and guessing strategy $G(i|a,b)$. For one-way LOCC, we optimize

$$P_{\text{win}} = \frac{1}{5}\sum_i \text{Tr}\big((A_a \otimes B_{b|a})\rho_i\big)G(i|a,b) \tag{90}$$

Where now Bob's choice of measurement depends on the outcome of Alice's. The operators A_a and B_b associated respectively with measurement outcomes a and b are parameterized by

$$\begin{aligned} A_{0,1} &= \frac{1}{2}(\mathbb{I} \pm \vec{a}\cdot\vec{\sigma}) \\ B_{0,1} &= \frac{1}{2}(\mathbb{I} \pm \vec{b}\cdot\vec{\sigma}) \end{aligned} \tag{91}$$

Then we find that one-way LOCC and LOSR achieve the same success rate at 0.39365.

Two Copies If Alice and Bob are distributed two copies of the maximally entangled state to measure and are permitted global measurements on the two qubits they receive, optimal measurements and guessing strategies yields a success rate of 0.7539 for one-way LOCC and 0.7298 for LOSR.

7.7 Distinguishability of 5 Product State ETF

For the 5 product state ETF defined by the unitaries in (62), a separable measurement with subnormalized measurement operators formed from the equiangular states themselves achieves the optimal value $P_{\text{win}}^{\text{SEP}} = 0.8$. An optimal success rate of 0.6906 was obtained for one-way LOCC, and 0.6195 for LOSR.

8 Conclusions

In this thesis we extended the discussion of highly symmetric state configurations in real and complex dimensions to the state space of maximally entangled states. As equiangular lines are really a special class of frames, many of the tools from frame theory are useful in deriving results for equiangular lines (namely, the cospectrality of the Gram and frame operators). In addition, the study of frames provides helpful context and perspective with which one can better appreciate the features of equiangular lines. A brief introduction to real and complex equiangular lines was given to highlight the areas of discrete mathematics that the problem has found connections to, since constructing them from solving polynomial equations alone is prohibitively difficult.

Then we discussed measurements and the distinction between projective measurements and non-projective POVMs. Throughout the thesis, the comparison between orthogonal projective bases and non-orthogonal ones is a running theme. For measurements of maximally entangled states, the

famous Bell state measurement is used to distinguish the four maximally entangled Bell states. But what is the most optimal extension of BSM4 to non-orthogonal measurements? Can we achieve a perfect informationally complete measurement as can be done in complex dimensions? The answer, we found, is no. In fact, only 6 equiangular lines of maximally entangled states can be found, and only 5 equiangular lines of maximally entangled states can be constructed to create a quantum measurement of maximally entangled states. But equiangular lines over maximally entangled states may do better in quantum information tasks such as bit hiding, a protocol which was described in the text for BSM4 since we have shown that the 5 equiangular lines are much less distinguishable locally compared to BSM4, even with two copies.

However, it is well known that qubit systems are often exceptions compared to their bipartite counterparts in higher dimensions. This we have already suspected since only for bipartite qubit states is there an isomorphism of states to vectors in $\mathbb{R}^4$ due to the happy coincidence that the Pauli matrices square to the identity. It would be interesting to see what mathematical tools can be used to cleverly construct equiangular lines in higher dimensions of maximally entangled states.

9 Outlook

Equiangular lines in real and complex dimensions have enjoyed decades of research and applications to classical and quantum information processing tasks which exploit their great symmetries. Applications of discrete structures from geometry, combinatorial design theory, spectral graph theory and group theory have been the inspiration for many equiangular constructions. A natural next step then is to extend this work to higher dimensions. How many equiangular lines can be constructed in $\mathbb{C}^d \otimes \mathbb{C}^d$ for $d > 2$? Are there absolute upper bounds that can be derived analogous to those for real and complex equiangular lines? What discrete structures can be used to systematically construct equiangular lines? Under what circumstances can equiangular lines in $\mathbb{C}^2 \otimes \mathbb{C}^2$ be reduced to equiangular lines in real or complex dimensions?

Although the questions above are interesting in their own right it is also interesting to wonder where equiangular lines can find applications in quantum information processing or elsewhere. A natural place to look for applications is where the BSM4 is already useful, such as in teleportation and entanglement swapping. Frankly, the applications for such maximally entangled equiangular lines is still unclear. But if the breadth and depth of the applications of real and complex equiangular lines is any indication, it is worth the effort to think on this more.

10 References

[1] A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10), 1935.

[2] D. Bohm and Y. Aharonov. Discussion of experimental proof for the paradox of Einstein, Rosen, and Podolsky. *Physical Review*, 108(4), 1957.

[3] J. S. Bell. On the Einstein Podolsky Rosen paradox. *Physics Physique Fizika*, 1(3), 1964.

[4] A. Aspect, J. Dalibard, and G. Roger. Experimental test of Bell's inequalities using time-varying analyzers. *Phys. Rev. Lett.*, 49(25), 1982.

[5] B. Hensen et al. Loophole-free Bell inequality violation using electron spins separated by 1.3 kilometres. *Nature*, 526(7575), 2015.

[6] J. Handsteiner et al. Cosmic Bell Test: Measurement Settings from Milky Way Stars. *Physical Review Letters*, 118(6), 2017.

[7] S. Kochen and E. Specker. The Problem of Hidden Variables in Quantum Mechanics. *Indiana University Mathematics Journal*, 17(1), 1967.

[8] Y. F. Huang et al. Experimental Test of the Kochen-Specker Theorem with Single Photons. *Physical Review Letters*, 90(25), 2003.

[9] D. Vincenzo et al. Experimental implementation of a Kochen-Specker set of quantum tests. *Physical Review X*, 3(1), 2013.

[10] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, 2018.

[11] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on Einstein-Podolsky- Rosen states. *Physical Review Letters*, 69(20), 1992.

[12] C. H. Bennett et al. Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels. *Physical Review Letters*, 70(13), 1993.

[13] B. Yurke and D. Stoler. Einstein-Podolsky-Rosen effects from independent particle sources. *Physical Review Letters*, 68(9), 1992.

[14] B. K. Behera, S. Swarnadeep, A. Das, and P. K. Panigrahi. Demonstration of entanglement purification and swapping protocol to design quantum repeater in IBM quantum computer. *Quantum Information Processing*, 18(4), 2019.

[15] D. Petz and L. Ruppert. Efficient quantum tomography needs complementary and symmetric measurements. *Reports on Mathematical Physics*, 69(2), 2012.

[16] D. Petz and L. Ruppert. Optimal quantum-state tomography with known parameters. *Journal of Physics A: Mathematical and Theoretical*, 45(8), 2012.

[17] J. Nunn, B. J. Smith, G. Puentes, I. A. Walmsley, and J. S. Lundeen. Optimal experiment design for quantum state tomography: Fair, precise, and minimal tomography. *Physical Review A - Atomic, Molecular, and Optical Physics*, 81(4), 2010.

[18] E. Berthold-Georg et al. Efficient and robust quantum key distribution with minimal state tomography. arXiv:quant-ph/0412075v4, 2008.

[19] C. H. Bennett. Quantum cryptography using any two nonorthogonal states. *Physical Review Letters*, 68(21), 1992.

[20] A. Peres. How to differentiate between non-orthogonal states. *Physics Letters A*, 128(1-2), 1988.

[21] A. Peres and W. K. Wooters. Optimal Detection of Quantum Information. *Phys. Rev. Lett.*, 66(9), 3 1991.

[22] A. Acín, S. Pironio, T. Vértesi, and P. Wittek. Optimal randomness certification from one entangled bit. *Physical Review A*, 93(4), 2016.

[23] E. S. Gómez et al. Device-Independent Certification of a Nonprojective Qubit Measurement. *Physical Review Letters*, 117(26), 2016.

[24] T. Strohmer and R. W. Heath. Grassmannian frames with applications to coding and communication. *Applied and Computational Harmonic Analysis*, 14(3), 2003.

[25] J. H. van Lint and J. J. Seidel. Equilateral point sets in elliptic geometry. *Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen: Series A: Mathematical Sciences*, 69(3):335–348, 1966.

[26] S. Waldron. On the construction of equiangular frames from graphs. *Linear Algebra and Its Applications*, 431(11), 2009.

[27] J. M. Renes. Spherical-code key-distribution protocols for qubits. *Physical Review A - Atomic, Molecular, and Optical Physics*, 70(5 A), 2004.

[28] N. Peters et al. Precise creation, characterization and manipulation of single optical qubits. *Quantum Information and Computation*, 3(SPEC. ISS.), 2003.

[29] Y. Y. Zhao, N. K. Yu, P. Kurzyński, G. Y. Xiang, C. F. Li, and G. C. Guo. Experimental realization of generalized qubit measurements based on quantum walks. *Physical Review A - Atomic, Molecular, and Optical Physics*, 91(4), 2015.

[30] D. O. Akat'ev et al. Multiqudit quantum hashing and its implementation based on orbital angular momentum encoding. *Laser Physics Letters*, 19(12), 2022.

[31] N. J Cerf, M. Bourennane, A. Karlsson, and N. Gisin. Security of quantum key distribution using d-level systems. *Physical Review Letters*, 88(12), 2002.

[32] R. T. Thew, A. Acín, H. Zbinden, and N. Gisin. Bell-type test of energy-time entangled qutrits. *Physical Review Letters*, 93(1), 2004.

[33] Z. Hou et al. Deterministic realization of collective measurements via photonic quantum walks. *Nature Communications*, 9(1), 2018.

[34] J. Singh, Arvind, and S. K. Goyal. Implementation of discrete positive operator valued measures on linear optical systems using cosine-sine decomposition. *Physical Review Research*, 4(1):013007, 1 2022.

[35] S. Waldron. An introduction to finite tight frames. In *Applied and Numerical Harmonic Analysis*, number 9780817648145. 2018.

[36] L. R. Welch. Lower Bounds on the Maximum Cross Correlation of Signals. *IEEE Transactions on Information Theory*, 20(3), 1974.

[37] S. Datta, S. Howard, and D. Cochran. Geometry of the Welch bounds. *Linear Algebra and Its Applications*, 437(10), 2012.

[38] S. Waldron. Generalized Welch Bound Equality Sequences are Tight Frames. *IEEE Transactions on Information Theory*, 49(9), 2003.

[39] O. Oktay. *Frame Quantization Theory and Equiangular Tight Frames.* PhD thesis, University of Maryland, College Park, 2007.

[40] V. K. Goyal, J. Kovačević, and J. A. Kelner. Quantized Frame Expansions with Erasures. *Applied and Computational Harmonic Analysis*, 10(3), 2001.

[41] R. M. Gray. Quantization Noise Spectra. *IEEE Transactions on Information Theory*, 36(6), 1990.

[42] J. Haantjes. Distance geometry. Curvature in abstract metric spaces. *Proc. Kon. Ned. Akad. v. Wetenseh*, 50, 1947.

[43] P. W.H. Lemmens and J. J. Seidel. Equiangular lines. *Journal of Algebra*, 24(3), 1973.

[44] A. Neumaier. Graph representations, two-distance sets, and equiangular lines. *Linear Algebra and Its Applications*, 114-115(C), 1989.

[45] B. Bukh. Bounds on equiangular lines and on related spherical codes. *SIAM Journal on Discrete Mathematics*, 30(1), 2016.

[46] Z. Jiang, J. Tidor, Y. Yao, S. Zhang, and Y. Zhao. Equiangular lines with a fixed angle. *Annals of Mathematics*, 194(3), 2021.

[47] G. Greaves. Equiangular Lines: Mini-course. Lecture notes. Centre de recherches mathematiques, Universite de Montreal, Aug. 2022.

[48] I. Balla, F. Dräxler, P. Keevash, and B. Sudakov. Equiangular lines and spherical codes in Euclidean space. *Inventiones Mathematicae*, 211(1), 2018.

[49] E. Bannai. On tight spherical designs. *Journal of Combinatorial Theory, Series A*, 26(1), 1979.

[50] G. Greaves, J. H. Koolen, A. Munemasa, and F. Szöllosi. Equiangular lines in Euclidean spaces. *Journal of Combinatorial Theory. Series A*, 138, 2016.

[51] C. Godsil and G. Royle. *Algebraic Graph Theory.* Springer-Verlag, New York, 2001.

[52] B. C. Stacey. Maximal sets of equiangular lines. arXiv:quant-ph/2008.13288, 2020.

[53] J. C. Tremain. Concrete constructions of real equiangular line sets. arXiv:math.MG/0811.2779, 2008.

[54] G. Zauner. Quantum designs: Foundations of a noncommutative design theory. *International Journal of Quantum Information*, 9(1), 2011.

[55] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6), 2004.

[56] A. J. Scott and M. Grassl. SIC-POVMs: A new computer study. *J. Math. Phys.*, 51, 2010.

[57] I. Bengtsson, M. Grassl, and G. McConnell. Sic-povms from stark units: Dimensions $n^2+3 = 4p$, p prime. arXiv:quant-ph/2403.02872, 2024.

[58] M. Grassl. Computing equiangular lines in complex space. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, volume 5393 LNCS, 2008.

[59] M. Appleby, S. Flammia, G. McConnell, and J. Yard. SICs and Algebraic Number Theory. *Foundations of Physics*, 47(8), 2017.

[60] P. Ramond. The abel–ruffini theorem: Complex but not complicated. *The American Mathematical Monthly*, 129(3):231–245, March 2022.

[61] M. Grassl and A. J. Scott. Fibonacci-Lucas SIC-POVMs. *Journal of Mathematical Physics*, 58(12), 2017.

[62] N Appleby, T. Y. Chien, S. Flammia, and S. Waldron. Constructing exact symmetric informationally complete measurements from numerical solutions. *Journal of Physics A: Mathematical and Theoretical*, 51(16), 2018.

[63] A. Tavakoli, M. Farkas, D. Rosset, J. D. Bancal, and J. Kaniewski. Mutually unbiased bases and symmetric informationally complete measurements in Bell experiments. *Science Advances*, 7(7), 2021.

[64] M. Oszmaniec, L. Guerini, P. Wittek, and A. Acín. Simulating Positive-Operator-Valued Measures with Projective Measurements. *Physical Review Letters*, 119(19), 2017.

[65] S. Olivares and M. G.A. Paris. Quantum estimation via the minimum Kullback entropy principle. *Physical Review A - Atomic, Molecular, and Optical Physics*, 76(4), 2007.

[66] Z. E. D. Medendorp et al. Experimental characterization of qutrits using symmetric informationally complete positive operator-valued measurements. *Physical Review A - Atomic, Molecular, and Optical Physics*, 83(5), 2011.

[67] C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. *Theoretical Computer Science*, 560(P1), 2014.

[68] D. Bruß. Optimal eavesdropping in quantum cryptography with six states. *Physical Review Letters*, 81(14), 1998.

[69] A. Tavakoli and S. Morelli. Enhanced Schmidt number criteria based on correlation trace norms. arXiv:quant-ph/2402.09972, Feb. 2024.

[70] J. Shang, A. Asadian, H. Zhu, and O. Gühne. Enhanced entanglement criterion via symmetric informationally complete measurements. *Physical Review A*, 98(2), 2018.

[71] S. Pironio et al. Random numbers certified by Bell's theorem. *Nature*, 464(1021), 2010.

[72] J. Du et al. Realization of entanglement-assisted qubit-covariant symmetric- informationally-complete positive-operator-valued measurements. *Phys. Rev. A*, 74(4), 2006.

[73] N. Bent et al. Experimental realization of quantum tomography of photonic qudits via symmetric informationally complete positive operator-valued measures. *Phys. Rev. X*, 5(4), 2015.

[74] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. 2011.

[75] D. Dieks. Overlap and distinguishability of quantum states. *Physics Letters A*, 126(5-6), 1988.

[76] D. B. R. Dasari et al. Anti-Zeno purification of spin baths by quantum probe measurements. *Nature Communications*, 13(1), 2022.

[77] Y. S. Patil, S. Chakram, and M. Vengalattore. Measurement-Induced Localization of an Ultracold Lattice Gas. *Physical Review Letters*, 115(14), 2015.

[78] B. Misra and E. C.G. Sudarshan. The Zeno's paradox in quantum theory. *Journal of Mathematical Physics*, 18(4), 1976.

[79] A. G. Kofman and G. Kurizki. Acceleration of quantum decay processes by frequent observations. *Nature*, 405(6786), 2000.

[80] I. B. Djordjevic. Quantum Mechanics Fundamentals. *Quantum Information Processing, Quantum Computing, and Quantum Error Correction*, pages 31–95, 1 2021.

[81] M. A. Rowe, D. Kielpinski, V. Meyer, C. A. Sackett, W. M. Itano, C. Monroe, and D. J. Wineland. Experimental violation of a Bell's inequality with efficient detection. *Nature*, 409(6822), 2001.

[82] M. Ansmann et al. Violation of Bell's inequality in Josephson phase qubits. *Nature*, 461(7263), 2009.

[83] B. Hensen et al. Loophole-free Bell test using electron spins in diamond: Second experiment and additional analysis. *Scientific Reports*, 6, 2016.

[84] B. M. Terhal and P. Horodecki. Schmidt number for density matrices. *Physical Review A - Atomic, Molecular, and Optical Physics*, 61(4), 2000.

[85] J. Sperling and W. Vogel. The Schmidt number as a universal entanglement measure. *Physica Scripta*, 83(4), 2011.

[86] E. Schrödinger. Discussion of Probability Relations between Separated Systems. *Mathematical Proceedings of the Cambridge Philosophical Society*, 31(4), 1935.

[87] M. A. Sustik et al. On the existence of equiangular tight frames. *Linear Algebra and Its Applications*, 426(2-3), 2007.

[88] S. M. Barnett and C. Sarah. Quantum State Discrimination. *Adv. Opt. Photon.*, 1(2):238–278, 2009.

[89] J. Walgate and L. Hardy. Nonlocality, asymmetry, and distinguishing bipartite states. *Phys. Rev. Lett.*, 89(14), 2002.

[90] B. M. Terhal, D. P. DiVincenzo, and D. W. Leung. Hiding bits in bell states. *Physical Review Letters*, 86(25), 2001.

[91] W. K. Wootters and W. H. Zurek. A single quantum cannot be cloned. *Nature*, 299(5886), 1982.

[92] J. Bae and A. Acín. Asymptotic quantum cloning is state estimation. *Physical Review Letters*, 97(3), 2006.

[93] L. I. Masanes, A. Acin, and N. Gisin. General properties of nonsignaling theories. *Physical Review A - Atomic, Molecular, and Optical Physics*, 73(1), 2006.

[94] J. Bae, W. Y. Hwang, and Y. D. Han. No-signaling principle can determine optimal quantum state discrimination. *Physical Review Letters*, 107(17), 2011.

[95] M. Horodecki, P. Horodecki, and R. Horodecki. Separability of mixed states: Necessary and sufficient conditions. *Physics Letters, Section A: General, Atomic and Solid State Physics*, 223(1-2), 1996.

[96] E. Chitambar, D. Leung, L. Mančinska, M. Ozols, and A. Winter. Everything You Always Wanted to Know About LOCC (ButWere Afraid to Ask). *Communications in Mathematical Physics*, 328(1), 2014.

[97] E. Chitambar and M. H. Hsieh. Revisiting the optimal detection of quantum information. *Physical Review A*, 88(2), August 2013.

[98] S. M. Cohen. When a quantum measurement can be implemented locally, and when it cannot. *Physical Review A - Atomic, Molecular, and Optical Physics*, 84(5), 2011.

[99] J. Wartrous. *The Theory of Quantum Information*. Cambridge University Press, 2018.

[100] J. Walgate, A. J. Short, L. Hardy, and V. Vedral. Local distinguishability of multipartite orthogonal quantum states. *Physical Review Letters*, 85(23), 2000.

[101] S. Virmani, M. F. Sacchi, M. B. Plenio, and D. Markham. Optimal local discrimination of two multipartite pure states. *Physics Letters, Section A: General, Atomic and Solid State Physics*, 288(2), 2001.

[102] S. Bandyopadhyay and J. Walgate. Local distinguishability of any three quantum states. *Journal of Physics A: Mathematical and Theoretical*, 42(7), 2009.

[103] M. Nathanson. Distinguishing bipartitite orthogonal states using LOCC: Best and worst cases. *Journal of Mathematical Physics*, 46(6), 2005.

[104] W. K. Wootters. Distinguishing unentangled states with an unentangled measurement. *International Journal of Quantum Information*, 4(1), 2006.

[105] C. H. Bennett et al. Quantum nonlocality without entanglement. *Physical Review A - Atomic, Molecular, and Optical Physics*, 59(2), 1999.

[106] C. Godsil and G. Royle. Generalized Polygons and Moore Graphs. In *Algebraic Graph Theory*, chapter 5, pages 94–97. Springer-Verlag, New York, 2001.

[107] D. E. Taylor. Regular 2-graphs. *Proc. London Math. Soc.*, s3-35(2):257–274, 1977.

[108] I. Bengtsson and K. Zyczkowski. *Geometry of Quantum States: An Introduction to Quantum Entanglement*. Cambridge University Press, 2006.

[109] C. Godsil. Quantum Geometry: MUB's and SIC-POVM's. Presentation slides. University of Waterloo, Dec. 2009.

[110] J. H. van Lint and J.J. Seidel. Equilateral point sets in elliptic geometry. *Indagationes Mathematicae (Proceedings)*, 69, 1966.

A Related Discrete Structures

A.1 Combinatorial Designs

t-designs form an important class of incidence structures in combinatorial mathematics. A $t-(v,k,\lambda_t)$ design consists of a set $\mathcal{P}$ of v *points* and a collection of *blocks* $\mathcal{B}$ of k-point subsets such that any set of t points lies in precisely λ_t blocks [106]. The Fano plane from section 4 is such a $2-(7,3,1)$ design. It consists of 7 points and 7 blocks which each contain 3 points. Any two points belong only to one block.

Equiangular Lines from the Witt Design
The Witt design, *one of the most remarkable structures in all of combinatorics* [51], is a fruitful source of equiangular lines in many dimensions. It is a $4-(23,7,1)$ design, so it has 23 points arranged in blocks of 7 points such that any four of them appear only once in the block set. To construct the incidence matrix N of the Witt design, begin with the polynomial

$$p(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1 \in \mathbb{F}_2[x] \tag{92}$$

where $\mathbb{F}_2[x]$ is the polynomial ring with coefficients in the field of integers modulo 2. Then, identify the point set with $\mathcal{P} = \{x_i\}_{i=1}^{23}$, and define polynomial set $\mathcal{S} = \{p(x)^i \mod x^{23}-1\}$, the set of powers of $p(x)$ modulo $x^{23}-1$. Then the blocks $\mathcal{B} \subset \mathcal{S}$ are the polynomials in $\mathcal{S}$ with exactly 7 non-zero coefficients. So a block (polynomimal $p(x) \in \mathcal{B}$) contains point x^i if it has a non-zero coefficient in $p(x)$. Then the incidence matrix as defined in 4 is a 23×253 matrix. From this, the Seidel matrix of 276 equiangular lines in $\mathbb{R}^{23}$ is given by

$$S = \begin{pmatrix} J_{23} - \mathbb{I}_{23} & J_{23\times 253} - 2N \\ J_{253\times 23} - 2N^{\mathsf{T}} & N^{\mathsf{T}}N - 5\mathbb{I}_{253} - 2J_{253} \end{pmatrix}. \tag{93}$$

It can be confirmed that this is a 276×276 matrix. From the principal submatrices of S, 176 lines in $\mathbb{R}^{22}$ [43], 126 lines in $\mathbb{R}^{21}$ [43], and 90 lines in $\mathbb{R}^{20}$ [107] have been found, among others.

A.2 Mutually Unbiased Bases (MUBs)

Another class of discrete structures that are often mentioned together with SICs are mutually unbiased bases (MUBs). A pair of orthonormal bases $\{e_i\}_{i=1}^d$ and $\{f_j\}_{j=1}^d$ in $\mathbb{C}^d$ are mutually unbiased if

$$|\langle e_i | f_j \rangle|^2 = \frac{1}{d} \qquad \forall i,j \tag{94}$$

MUBs have deep connections to complementarity and incompatible observables in quantum mechanics. Perhaps the most familiar example of complementarity is that of measurements in position

and momentum featured in the formula

$$|\langle x|p\rangle|^2 = \frac{1}{2\pi}. \tag{95}$$

When a full set exists, they are the optimal choice for measurement bases in quantum state tomography with projective measurements, since the information produced by measurements in each of the bases are not redundant. One of their first applications in quantum information theory was in the BB84 quantum key distribution protocol [67], where they are optimal for the detection of eavesdropping third parties. They were also used in the improvement to the BB84 protocol [68], where three MUBs were used instead of two. The difficulty with MUBs is that it is often difficult to find complete sets. In any dimension d, $d+1$ is an absolute upper bound on the number of MUBs and in prime dimensions, this upper bound can be met. But this is not true in general, and where maximal sets cannot be found, SICs are the next highly symmetric alternative to consider. See chapter 12 of [108] for more.

B Proofs of Various Upper Bounds

Each of the proofs are similar in spirit; a one-to-one mapping is made from the n hypothetical equiangular lines to a set of matrix or polynomial set which is necessarily orthogonal. Then, the dimension of this orthogonal set bound the maximum number of equiangular lines.

B.1 In $\mathbb{R}^d$: Gerzon's Bound

Proof that the maximum number of lines in $\mathbb{R}^d$ is $\binom{d+1}{2}$ [47].

Proof. For equiangular set $\{u_i\}_{i=1}^N$, define degree 2 homogeneous polynomials

$$f_i(\vec{x}) = \langle u_i, x\rangle^2 - \alpha^2\langle x, x\rangle \tag{96}$$

for arbitrary vector $x \in \mathbb{R}^d$, for each equiangular line u_i. This is the space of degree 2 polynomials of the d variables in the vector x. So the dimension of this space is $\binom{d}{2} + d = \binom{d+1}{2}$. This is true because $\binom{d}{2}$ counts the number of degree-2 monomials of the form $x_i x_j$ when $i \neq j$, but we also need to count the d terms when $i = j$ —hence, the additional d. We will show that the set $\{f_i\}_{i=1}^N$ are linearly independent. First, we note that

$$\begin{aligned} f_i(u_j) &= \langle u_i, u_j\rangle^2 - \alpha^2\langle u_j, u_j\rangle = \alpha^2 - \alpha^2 = 0 \\ f_i(u_i) &= \langle u_i, u_i\rangle^2 - \alpha^2\langle u_i, u_i\rangle = 1 - \alpha^2 \end{aligned} \tag{97}$$

Now suppose

$$c_1 f_1(x) + c_2 f_2(x) + ... + c_n f_n(x) = 0. \tag{98}$$

Replace $x = u_i$ so from (97), $c_i f_i(u_i) = c_i(1-\alpha^2) = 0$ which implies $c_i = 0$. So, the functions f_i are linearly independent and $N(d) \leq \binom{d+1}{2}$. ■

B.2 In $\mathbb{C}^d$

Proof that the maximum number of lines in $\mathbb{C}^d$ is d^2 [109].

Proof. Suppose we have a set of unit n equiangular lines $\{x_i\}$, so that

$$|\langle x_i|x_j\rangle| = \alpha \quad i \neq j \tag{99}$$

To each x_i, we assign a $d \times d$ projection matrix $X_i = x_i x_i^\dagger$ to each of the vectors. This is a Hermitian matrix and can be checked easily. This set of Hermitian matrices is spanned by d^2 basis matrices

$$\{E_{ii}\} \cup \{E_{jk} + E_{kj}, i(E_{jk} - E_{kj})\} \tag{100}$$

since the basis matrices should be Hermitian. Then, by counting arguments, the space of Hermitian matrices is spanned by d^2 elements. So if we show that the set $\{X_i\}$ are linearly independent, then there can be no more than d^2 of them. To do this, we first show:

$$\begin{aligned} \mathrm{Tr}(X_i X_j) &= \mathrm{Tr}(x_i x_i^\dagger x_j x_j^\dagger) \\ &= \langle x_i, x_j\rangle \mathrm{Tr}(x_i x_j^\dagger) \\ &= |\langle x_i, x_j\rangle|^2 \end{aligned} \tag{101}$$

This equals 1 if $i = j$ and α^2 if $i \neq j$. If there is some set of non-trivial coefficients c_i such that

$$\sum c_i X_i = 0, \tag{102}$$

then the matrices are linearly dependent. We define matrix $Y_j = X_j - \alpha^2 I_d$, and take the Hilbert-Schmidt inner product

$$\begin{aligned} \mathrm{Tr}(Y_j^\dagger X_i) &= \mathrm{Tr}(X_j^\dagger X_i - \alpha^2 X_i) \\ &= |\langle x_i|x_j\rangle|^2 - \alpha^2 \end{aligned} \tag{103}$$

This now equals 0 if $i \neq j$, and $1 - \alpha^2$ if $i = j$. Now if we substitute the linear combination in (102), we have

$$\begin{aligned} 0 &= \mathrm{Tr}(Y_j^\dagger \sum_i c_i X_i) \\ &= \sum_i c_i \mathrm{Tr}(Y_j^\dagger X_i) \\ &= c_i(1 - \alpha^2) \end{aligned} \tag{104}$$

The sum becomes just a single term, since from (103), the contributions are zero if $i \neq j$. And since the X_i are projection operators, they have eigenvalues 0 and 1, so c_i is not negative. And we choose the vectors to be non-orthogonal, so $a > 0$, and therefore $c_i = 0$ must be true. Therefore, the set $\{X_i\}$ must be linearly independent, and can be no more than d^2 matrices. ■

C Optimal Configuration of 6 Equiangular Lines of Bipartite Qubit States

Recall that for a set of n equiangular lines in $\mathbb{R}^d$ with Gram matrix G, $\mathrm{rank}(G) \leq d$. Recall also that G has ones along the diagonal and $\pm\alpha$ on all the off-diagonal entries. This means that we want to find sign combinations for the 15 entries above the diagonal (since G is symmetric the

lower half will automatically be determined) and α which satisfy the two conditions. Then, we will find that the characteristic polynomial divides λ^{n-d}, and all other roots are positive. But 2^{15} is a lot of sign combinations to go through, and even more difficult if we have to find the best α for each!

To simplify the problem, use the fact that multiplying a row or column of a matrix by a constant c also scales the determinant of the matrix by c. Then if we simultaneously multiply row i and column i of $G - \lambda\mathbb{I}$ by -1, $\det(G - \lambda\mathbb{I})$ is unchanged. Luckily for us, spectral graph theorists have already noticed this, and have classified all such matrices whose characteristic polynomials (and spectrum) are left invariant after multiplication of their rows and corresponding columns by -1, or what they call *switching operations*. (The graph theoretical representation of this operation motivates the name). The 16 switching equivalent classes for $n = d$ along with their graphical representations are shown in table 4.1 of [110]. With the help of Mathematica, we find that the 16 characteristic polynomials corresponding to the plots in order from left to right are

$$
\begin{aligned}
p_1(\alpha,\lambda) &= (\lambda - 5\alpha - 1)(\lambda + \alpha - 1)^5 \\
p_2(\alpha,\lambda) &= (\lambda - \alpha - 1)(\lambda + \alpha - 1)^3(\lambda^2 - 2(1+\alpha)\lambda - 11\alpha^2 + 2\alpha + 1) \\
p_3(\alpha,\lambda) &= (\lambda + \alpha - 1)^3(\lambda^3 - 3(1+\alpha)\lambda^2 + 3(1 + 2\alpha - 3\alpha^2)\lambda + 19\alpha^3 + 9\alpha^2 - 3\alpha - 1) \\
p_4(\alpha,\lambda) &= (\lambda + \alpha - 1)(\lambda^2 - 2\lambda - 5\alpha^2 + 1)(\lambda^3 - (3+\alpha)\lambda^2 + (3 + 2\alpha - 9\alpha^2)\lambda + \alpha^3 + 9\alpha^2 - \alpha - 1) \\
p_5(\alpha,\lambda) &= (\lambda - \alpha - 1)^2(\lambda + \alpha - 1)(\lambda + 3\alpha - 1)(\lambda^2 - 2(1+\alpha)\lambda - 7\alpha^2 + 2\alpha + 1) \\
p_6(\alpha,\lambda) &= (\lambda - 3\alpha - 1)^2(\lambda + \alpha - 1)^3(\lambda + 3\alpha - 1) \\
p_7(\alpha,\lambda) &= (\lambda - \alpha - 1)(\lambda^2 - 2\lambda - 5\alpha^2 + 1)(\lambda^3 - (3-\alpha)\lambda^2 - (9\alpha^2 + 2\alpha - 3)\lambda - \alpha^3 + 9\alpha^2 + \alpha - 1) \\
p_8(\alpha,\lambda) &= ((\lambda - 1)^2 - \alpha^2)^2((\lambda - 1)^2 - 13\alpha^2) \\
p_9(\alpha,\lambda) &= (\lambda - \alpha - 1)(\lambda - 3\alpha - 1)(\lambda + \alpha - 1)(\lambda + 3\alpha - 1)(\lambda^2 - 2\lambda - 5\alpha^2 + 1) \\
p_{10}(\alpha,\lambda) &= (\lambda - \alpha - 1)(\lambda + \alpha - 1)(\lambda^4 - 4\lambda^3 + (6 - 14\alpha^2)\lambda^2 + (28\alpha^2 - 4)\lambda + 29\alpha^4 - 14\alpha^2 + 1) \\
p_{11}(\alpha,\lambda) &= (\lambda - \alpha - 1)^3(\lambda - 3\alpha - 1)(\lambda + 3\alpha - 1)^2 \\
p_{12}(\alpha,\lambda) &= (\lambda - \alpha - 1)(\lambda - 3\alpha - 1)(\lambda + \alpha - 1)^2(\lambda^2 + 2(\alpha - 1)\lambda - 7\alpha^2 - 2\alpha + 1) \\
p_{13}(\alpha,\lambda) &= (\lambda - \alpha - 1)(\lambda^2 - 2\lambda - 5\alpha^2 + 1)(\lambda^3 + (\alpha - 3)\lambda^2 - (2\alpha + 9 - 3)\lambda - \alpha^3 + 9\alpha^2 + \alpha - 1) \\
p_{14}(\alpha,\lambda) &= (\lambda - \alpha - 1)^3(\lambda^3 + 3(\alpha - 1)\lambda^2 - 3(3\alpha^2 + 2\alpha - 1)\lambda - 19\alpha^3 + 9\alpha^2 + 3\alpha - 1) \\
p_{15}(\alpha,\lambda) &= (\lambda - \alpha - 1)^3(\lambda + \alpha - 1)(\lambda^2 + 2(\alpha - 1)\lambda - 11\alpha^2 - 2\alpha + 1) \\
p_{16}(\alpha,\lambda) &= (\lambda - \alpha - 1)^5(\lambda + 5\alpha - 1)
\end{aligned}
\tag{105}
$$