Studies of symmetries that give special quantum states the "right to exist"

Hoan Bui Dang

A thesis
presented to the University of Waterloo
in fulfillment of the
thesis requirement for the degree of
Doctor of Philosophy
in
Physics

Waterloo, Ontario, Canada, 2015

© Hoan Bui Dang 2015

I hereby declare that I am the sole author of this thesis. This is a true copy of the thesis, including any required final revisions, as accepted by my examiners.

I understand that my thesis may be made electronically available to the public.

Abstract

In this thesis we study symmetric structures in Hilbert spaces known as symmetric informationally complete positive operator-valued measures (SIC-POVMs), mutually unbiased bases (MUBs), and MUB-balanced states [1–3]. Our tools include symmetries such as the Weyl-Heisenberg (WH) group symmetry, Clifford unitaries, Zauner symmetry, and Galois-unitaries (g-unitaries). In the study of SIC-POVMs, we found their geometric significance as the ''most orthogonal'' bases on the cone of non-negative operators. While investigating SICs, we discovered a linear dependency property of the orbit of an arbitrary vector with the Zauner symmetry under the WH group. In dimension $d = 3$, the linear dependency structures arising from certain special SIC states are identified with the Hesse configuration known from the study of elliptic curves in mathematics. We provide an analytical explanation for linear dependencies in every dimension, and a numerical analysis based on exhaustive numerical searches in dimensions $d = 4$ to 9. We also study the relations among normal vectors of the hyperplanes spanned by the linearly dependent sets, and found 2-dimensional SICs embedded in the Hilbert space of dimension $d = 6$, and 3-dimensional SICs for $d = 9$. A full explanation is given for the case $d = 6$. Another study in the thesis focuses on the roles of g-unitaries in the theory of mutually unbiased bases. G-unitaries are, in general, non-linear operators defined to generalize the notion of anti-unitaries. Due to Wigner's theorem [4], their action has to be restricted to a smaller region of the Hilbert space, which consists of vectors whose components belong to a specific number field. G-unitaries are relevant to MUBs when this number field is the cyclotomic field. In this case, we found that g-unitaries simply permuted the bases in the standard set of MUBs in odd prime-power dimensions. With their action further restricted only to MUB vectors, g-unitaries can be represented by rotations in the Bloch space, just as ordinary unitary operators can. We identify g-unitaries that cycle through all $d + 1$ bases in prime power dimensions $d = p^n$ where n is odd (the problem in even prime power dimensions has been solved using ordinary unitaries). Each of these MUB-cycling g-unitaries always leaves one state in the Hilbert space invariant. We provide a method for calculating these eigenvectors. Furthermore, we prove that when $d = 3 \bmod 4$, they are MUB-balanced states in the sense of Wootters and Sussman [5] and Amburg *et al* [6].

Acknowledgements

First and foremost, I would like to thank my co-supervisor, Prof. Christopher Fuchs, who inspired me to study quantum information and to investigate the SIC problem particularly. Working with Chris, whether at Bell Labs or in the QBism group at Perimeter Institute, has always been an enjoyable and motivating experience: I cannot recall a time walking out of his office without fresh new ideas or inspired thoughts. Despite the circumstance that only allowed us to work remotely with each other in the last years of my PhD program, Chris has always been behind to support me whenever I was in need.

I am deeply grateful to my collaborators, Prof. Ingemar Bengtsson and Dr. Marcus Appleby, for their mentoring and tremendous research support. Being in three different continents means that in order for us to have a discussion via Skype, Marcus would need to get ready at 6am, while Ingemar would have to stay up until midnight. They have meant much more to me than just collaborators, and I cannot thank them enough for the kindness, availability and knowledge they have been providing.

I am very thankful to my supervisor, Prof. Joseph Emerson, for being willing to take me as a student into his research group during the final year of my program and for his support to my research. I would also like to thank all the past and current members of my committee, Prof. Norbert Lutkenhaus, Prof. Debbie Leung, Prof. Lucien Hardy, and Prof. Daniel Gottesman, for their attention and many research comments and suggestions that they have been providing me throughout the course of my PhD. I am very grateful to Prof. William Wootters for his kindness in offering to come a long way from Williamstown (Massachusetts) to be an external examiner in my thesis defense, and for many detailed and helpful comments on this thesis.

My groupmates Matthew Graydon and Gelo Tabia have been my closest friends during my time at Waterloo. We have taken courses and traveled to conferences together. We have discussed physics uncountably many times (not in a set theoretic sense). They have always been available whenever I need help or just someone to talk to. I also want to thank my colleagues Åsa Ericsson, Huangjun Zhu, Kate Blanchfield, and David Andersson for many fruitful research discussions and collaborations.

Finally, nothing that I have accomplished would have been possible without my family. Whether living with me or being thousands of miles away, they always give me their full love, trust, and support. I dedicate this thesis to my family, although I know that nothing I do will be enough to thank them.

My research was financially supported in part by the U.S. Office of Naval Research (Grant No. N00014-09-1-0247), and by the Natural Sciences and Engineering Research

Council of Canada via the Vanier Canada Graduate Scholarship. Research at Perimeter Institute is supported by the Government of Canada through Industry Canada and by the Province of Ontario through the Ministry of Research and Innovation.

In memory of my grandfather, Dr. Hoan Trong Bui (1929-2014), who named me after himself, wishing that whenever I succeed our name will be praised, and whenever I fail we will take the blame together.

Table of Contents

List of Tables

List of Figures

List of Acronyms

MUB	Mutually Unbiased Bases 39, 53, 63
MUS	Minimum Uncertainty State 76, 77
POVM	Positive Operator-Valued Measure 10
SIC-POVM	Symmetric Informationally-Complete Positive Operator-Valued Measure 9
WH	Weyl-Heisenberg 9, 15

List of Notations

d	the dimensionality of the Hilbert space under consideration
ω	d-th root of unity: $\omega = e^{2\pi i/d}$
$\mathbb{Z}_d$	the set of integers modulo d
$\mathbb{F}_d$	the finite field of order d (only when d is a prime power) 92
X	the shift operator 14, 94
Z	the phase operator 14, 94
$D_{\mathbf{u}}$	the displacement operator indexed by $\mathbf{u} = (u_1, u_2) \in \mathbb{Z}_d^2$ or $\mathbb{F}_d^2$ 15, 94
$\Omega(\mathbf{u}, \mathbf{v})$	the symplectic form, or symplectic area 95
$\mathrm{SL}(2, \mathbb{F}_d)$	the special linear group (aka the symplectic group) consisting of 2×2 matrices over the field $\mathbb{F}_d$, whose determinants are 1 42
$\mathrm{GL}(2, \mathbb{F}_d)$	the general linear group consisting of 2×2 matrices over the field $\mathbb{F}_d$, whose determinants are non-zero 42
$\mathrm{GL}_p(2, \mathbb{F}_d)$	the subgroup of $\mathrm{GL}(2, \mathbb{F}_d)$ consisting of matrices whose determinants belong to the subfield $\mathbb{F}_p \subset \mathbb{F}_d$ 47
$\mathrm{ESL}(2, \mathbb{F}_d)$	the extended special linear group consisting of 2×2 matrices over the field $\mathbb{F}_d$, whose determinants are ± 1
$\mathrm{PSL}(2, \mathbb{F}_d)$	the projective special linear group: quotient group of SL obtained by setting SL elements S and S' equivalent if $S = cS'$ for some constant $c \in \mathbb{F}_d$ 42

$\mathrm{PGL}(2,\mathbb{F}_d)$	the projective linear group: quotient group of GL obtained by setting GL elements G and G' equivalent if $G = cG'$ for some constant $c \in \mathbb{F}_d$ 42
$\mathcal{Z}$	the Zauner symplectic matrix $\mathcal{Z} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ 18
$U_{\mathcal{Z}}$	the Zauner unitary 18
S	generally denotes a symplectic matrix in $\mathrm{SL}(2,\mathbb{F}_d)$
U_S	generally denotes a symplectic unitary
G	generally denotes an element of $\mathrm{GL}(2,\mathbb{F}_d)$
U_G	generally denotes a Galois-unitary
Δ	the determinant of a GL element
K	complex conjugation
g_k	the Galois automorphism mapping $\omega \mapsto \omega^k$ 91
Tr	trace of a matrix or a linear operator
tr	field theoretic trace 93
$\mathbb{R}$	the field of real numbers
$\mathbb{Q}$	the field of rational numbers
$\mathbb{C}$	the field of complex numbers
$\mathbb{Q}(\omega)$	the cyclotomic field generated from ω and the rationals 90
$\mathbb{Q}(\omega)^d$	the d-dimensional vector space over the cyclotomic field
$l(x)$	the Legendre symbol 96, 97
Q	the set of quadratic residues consisting of elements of a field that can be written as the square of another non-zero element 96
N	the set of quadratic non-residues consisting of elements of a field that can not be written as the square of any other element 96

Chapter 1

Introduction

''It is only slightly overstating the case to say that physics is the study of symmetry.''

-- Philip Anderson (1972)

1.1 Overview

A symmetry is a property of an object that remains the same under certain transformations. Although this might sound like a purely mathematical concept, symmetries can be found almost everywhere in the world surrounding us. For example, a bicycle has a left-right reflection symmetry: its left half is (mostly) the mirror image of its right half. Without this property, an unbalanced bicycle might be unpleasant to ride. A circular shape has a full rotational symmetry: if someone rotates your round dinner plate about its center by an arbitrary angle while you are away, you will not be able to tell the difference when you come back. Not only have we all made use of this property when we learned how to use a compass in elementary school, or when we played ball games as kids, we are all now living in a world of modern machinery that is largely based on inventions with rotational symmetry, such as wheels and gears. Nature is full of symmetries as well. The bodies of most animals have a bilateral (left-right) symmetry. Flowers often have radially or bilaterally symmetric shapes, which have been found to aid bumble bees in their foraging process [7]. In general, one can find symmetries from a minuscule scale such as in atomic or molecular lattices, all the way to the cosmic scale such as in galaxies that are hundreds of thousands light years in diameter across.

In physics, symmetry plays a fundamental role. Studying physical phenomena can be broken down into two components [8]. The first component is the given initial conditions, which might be very complicated and unpredictable, and therefore they have to be ''given,'' i.e. there is not much we can do but to accept them as they are. The second component consists of rules that capture all the patterns and regularities that are independent of the initial conditions. This is where the physics lies. In other words, when we say we understand the physics of a phenomenon, it means we have figured out what some of these rules are, and the more rules we have found, the more deeply have we understood. In this sense, one major goal of physics is to discover rules of regularities that can be applied to a broad range of phenomena. However, this is a very difficult task, as regularities are often buried under a vast amount of irregularity from the initial conditions. For example, who would have thought that there is a similarity between the elliptic orbits of planets in the Solar system and the falling of an apple? Or who would have thought that electric fields and magnetic fields can be transformed into each other, and how this could start a train of thoughts leading to the explanation of the perihelion precession of Mercury's orbit? This is where symmetry comes to help.

Symmetries in physics, often coming in the form of invariance or equivalence principles, help filter out the irrelevant complications to reveal the regularities at the heart of physical phenomena. For example, the weak equivalence principle (also known as the Galilean equivalence principle, which lays the foundation for theories of gravity) states that the trajectory of a point mass in a gravitational field depends only on its initial position and velocity, and not on its mass or composition. In this example, the principle was deduced from experimental observations by Galileo in the late 16th century. However, as symmetries have become an increasingly powerful tool, it often is the case that symmetries dictate the laws in modern physics and even provide predictions that predate experimental discoveries. For example, Lorentz symmetry formed the backbone of relativity and led to the derivation of Dirac's equation and the prediction of anti-particles. The gauge symmetries underlay the development of electromagnetism, quantum electrodynamics, quantum chromodynamics, and the Standard Model. The symmetry of exchanging identical particles in quantum mechanics classified all elementary particles into bosons or fermions whose behaviors are very distinctive. The list can go on. However, the intimate connection between symmetry and physics is not merely based on historical evidence. It has been rigorously proved that every continuous symmetry of the action of a physical system implies a conserved physical quantity, a result known as Noether's theorem [9]. As Philip Anderson has put it, ''it is only slightly overstating the case to say that physics is the study of symmetry.''

In this thesis, we are interested in the study of symmetries in quantum physics. Quantum theory is considered one of the most successful theories in physics in many different ways:

1) no experiment has ever violated its predictions, 2) the theory has provided the most accurate experimental tests to date, for example the determination of the fine structure constant α with an agreement to one part per billion [10], 3) the theory is applied in most areas of modern physics including condensed matter physics, atomic, molecular and optical physics, particle physics, astrophysics etc., and finally 4) it has a huge impact on today's world, with a wide range of applications such as transistors for computing devices, lasers, light emitting diodes, liquid crystal displays, nuclear magnetic resonance, and magnetic resonance imaging, just to name a few. On the other hand, quantum theory is also considered one of the strangest theories. It has been developed for over a century now, but many questions since its birth are still under debate: what is the nature of the wave function? do wave functions collapse? is the theory non-local because of "spooky action at a distance"? and many more. Indeed, the field of quantum foundations is still an active research area, and many questions have to be answered before quantum theory can be fully comprehended.

During the last few decades, research in quantum foundations has received a boost from developments in the new field of quantum information. Quantum information makes use of special features in quantum theory to help accomplish information-related tasks that are impossible using classical physics. For example, entanglement is used in superdense coding [11] and quantum teleportation [12]. Another example is quantum key distribution [13], which relies on the quantum information-disturbance trade-off to help generate and distribute secure encryption keys. At the same time, quantum information brings tools from information theory into quantum physics, and helps provide us with an information theoretic framework to study quantum theory. An example of this is the quantification of quantum information using von Neumann entropy, which is an analogue of the Shannon entropy used in classical information theory [14].

The research presented in this thesis arises from problems in quantum information involving various symmetric structures in the space of quantum states such as SICs, MUBs, and MUB-balanced states (their definitions will be provided later). These structures display such a high degree of symmetry that makes it seem as though they have no "right to exist," as Amburg *et al* [6] have described MUB-balanced states. Our hopes in investigating these problems are not only to make use of their symmetries to discover new properties and new applications in quantum information, but also to gain a deeper understanding about symmetries in quantum state spaces and quantum theory. The content of the thesis is organized as follows.

1.2 Organization of the thesis

The thesis consists of various studies, from symmetric informationally complete states and linear dependency structures in Weyl-Heisenberg orbits, to the study of Galois-unitaries with applications to the theory of mutually unbiased bases. The results of these studies are organized into two main chapters according the relevant symmetry: Chapter 2 contains results related to the Weyl-Heisenberg symmetry, as well as Clifford unitaries and Zauner symmetry, and Chapter 3 provides the results from a study of Galois-unitary symmetry.

Chapter 2 starts with a historical introduction of the Weyl-Heisenberg group in Section 2.1. We then focus on a class of symmetric structures in the Hilbert space known as SICs in Section 2.2. We provide a brief history of the development of the SIC problem, and an extensive list of SICs' applications and major known results. We discuss group symmetries that are intimately related to SICs such as Weyl-Heisenberg covariance, Clifford group, and Zauner symmetry. We show that SICs form the most orthogonal bases on the cone of non-negative operators. Then, in Section 2.3, we present our results from studies of linear dependencies in Weyl-Heisenberg orbits, which include an analysis in dimension $d = 3$ and the connection to elliptic curves via Hesse configuration, an analytical explanation of linear dependencies in all dimensions where the initial vector is an eigenvector of the Zauner unitary, a detailed numerical report in low dimensions which shows extra linearly dependent relations that cannot be accounted for by our theorem, and a robust construction of ''small SICs'' resulted from the linear dependency structure.

Chapter 3 contains our results from the study of a novel symmetry called Galois-unitary, applied to the theory of mutually unbiased bases. Section 3.1 describes the motivations for our study, including the context in which g-unitaries were first constructed. We first introduce mutually unbiased bases and describe their Clifford-based construction in Section 3.2. We then provide a representation for the general linear group, using Clifford group extended by g-unitary operators in Section 3.3. The treatment is divided into cases, when the dimension $d = p$ is an odd prime, and when $d = p^n$ is an odd prime power. We proved that the representation is faithful if n is odd, and is ''almost'' faithful if n is even. We provide some basic arithmetic of g-unitaries in Section 3.4. In Section 3.5 we describe a type of geometric object called complementarity polytopes and use their symmetry groups to provide a geometric interpretation of g-unitaries. Section 3.6 proposes a scheme to simulate g-unitaries using unitary operators in a larger Hilbert space. The MUB-cycling problem is discuss in Section 3.7, in which we prove that MUB-cyclers exist in every odd prime power dimensions $d = p^n$ where n is odd, and they do not exist when n is even. We also provide a characterization of all MUB-cyclers when they do exist. In Section 3.8, we prove that every MUB-cycler has a unique (up to a phase) eigenvector, and provide

a way to calculate this eigenvector. In Section 3.9, we show that when $d = 3 \bmod 4$, the eigenvectors of MUB-cyclers are MUB-balanced states, that they form a single orbit under the extended Clifford group, and that they are identical to those constructed in Amburg *et al* [6].

Chapter 4 provides a summary of our main results, and suggests a list of open problems and ideas for future investigation.

Appendix A.1 provides an introduction to field theory, which covers the basic concepts used in the thesis such as field extensions, Galois automorphisms, finite fields, cyclotomic fields, etc. Appendix A.2 describes faithful representations of the Clifford group specifically for the case of prime and prime power dimensions.

1.3 List of specific contributions

Results in this thesis that represent my own specific contributions include:

1. Section 2.2.4, published in [1].
2. Sections 2.3.2 to 2.3.4, published in [2].
3. Sections 3.4 and 3.6, from my own research notes.
4. Numerical analysis of g-unitary rotations leading to Section 3.5, published in [3].
5. Lemma 3.4 and Theorem 3.5 in Section 3.7, published in [3].
6. Contribution to the proof of Theorem 3.8 and Lemmas 3.9 to 3.11 in Section 3.8, published in [3].
7. Contribution to the proof of Theorem 3.13 in Section 3.9, published in [3].

Chapter 2

Weyl-Heisenberg group symmetry

Contents

2.1 Historical background

The use of group theory in quantum mechanics dates back to the very early days of the theory. In 1925, Hermann Weyl learned from Born the recent developments in quantum mechanics made by Born, Jordan, and Heisenberg, and he immediately tried his own

approach from the perspective of the representation theory of groups [15]. This work was published in 1927 [16], and further developed in his book [17], in which Weyl used the ray representations of the Abelian group of rotations to develop a quantum formalism that is applicable to both finite and infinite dimensions.

Weyl realized that the canonical commutation relation between the position operator $\hat{q}$ and momentum operator $\hat{p}$ (this is sometimes called the Heisenberg commutation rule, although it first appeared in a paper by Born and Jordan [18, 19])

$$[\hat{q}, \hat{p}] = i \tag{2.1}$$

does not admit finite-dimensional representations (we have set the unit to $\hbar$). In other words, for any dimension d that is finite, there do not exist $d \times d$ matrices Q and P that can satisfy (2.1). One can see that by taking the trace of (2.1) and observing that the left hand side is zero due to the cyclic property of the trace function, while the right hand side is non-zero. Moreover, $\hat{p}$ and $\hat{q}$ are unbounded operators and they are not defined on the whole Hilbert space.

For a finite dimension d, Weyl instead introduced Hermitian matrices P and Q, which are defined by

$$P = \frac{1}{i\alpha} \log X \qquad\qquad Q = \frac{1}{i\beta} \log Z \tag{2.2}$$

so that

$$X = e^{i\alpha P} \qquad\qquad Z = e^{i\beta Q}, \tag{2.3}$$

where X and Z are $d \times d$ unitary matrices satisfying Weyl's commutation relation

$$XZ = \omega^{-1} ZX \qquad\qquad \omega = e^{2\pi i/d}. \tag{2.4}$$

The commutator $[Q, P]$, as one takes the limit $d \to \infty$ while keeping $\alpha\beta = 2\pi/d$, can be calculated to be [20]

$$[Q, P]_{r,s} = i\delta(r - s), \tag{2.5}$$

which recovers Heisenberg commutation relation. For a detailed construction of quantum mechanics in finite dimensions based on Weyl's commutation relation (2.4), we refer the readers to a series of papers by Jagannathan and Santhanam *et al* [20–24]. Here, let us focus on how Weyl constructed unitary X and Z in finite dimensions that satisfy such a commutation relation. The following argument should not be taken as a rigorous mathematical derivation, but should rather be considered as a train of thoughts leading to the construction of the Weyl-Heisenberg group.

Let X and Z be two elements of the group of unitary rotations in a $(d-1)$-dimensional ray space, meaning that they are $d \times d$ unitary matrices. We further assume that they satisfy the following commutation relation

$$XZ = \omega^{-1} ZX, \tag{2.6}$$

where $\omega = e^{2\pi i/d}$ is a primitive d-th root of unity. It follows that

$$X^j Z^k = \omega^{-jk} Z^k X^j \tag{2.7}$$

for all integers j and k. If either j or k is equal to d, then $\omega^{-jk} = 1$ and it follows that X^d commutes with Z and Z^d commutes with X. Under the extra assumption that the representation is irreducible, by Schur's lemma we conclude that

$$X^d = Z^d = \mathbb{1}. \tag{2.8}$$

We can choose a basis in which Z is diagonal and write it in the form

$$Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix}. \tag{2.9}$$

In this basis, X takes the form of a cyclic permutation matrix

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}. \tag{2.10}$$

The two operators X and Z we arrive at are known as the shift and the clock (or phase) operators, respectively. They were introduced by Sylvester in 1882 in the very early days of matrix theory [25]. Here they naturally arise from the construction of a group-based quantum theory built upon Weyl's commutation relation.

The set of operators of the form $\omega^i X^j Z^k$, with i, j and k taking integer values in the range $[0, d-1]$, forms a group under ordinary matrix multiplication. This group is called

the discrete Weyl-Heisenberg (WH) group (to be distinguished from the continuous WH group in infinite dimensions, although we will drop the label ''discrete'' from now on, as it should be clear from the context of the thesis that we are working in finite dimensions only). The group elements

$$D_{j,k} = X^j Z^k \tag{2.11}$$

are called displacement operators (please note that displacement operators may be defined with different phases to suit different situations, and we will make the definition precise when it comes to each situation).

Besides its structural role in the foundations of quantum mechanics, the WH group has found applications and connections to many other fields of science. For example, in modern mathematics, it naturally appears in the theory of elliptic curves and theta functions [26]. In classical signal processing, WH group is used in the development of adaptive radar and error-correcting codes in communications [27]. In quantum information, this group is also known as the generalized Pauli group, and it has numerous applications, for example in superdense coding [11], quantum error correction [28, 29] and the theory of mutually unbiased bases [1, 30–32]. Its intimate relation to SIC-POVMs will be discussed in the next section.

2.2 Symmetric informationally-complete POVMs

The Weyl-Heisenberg group symmetry plays an indisputable role in the studies of a special class of symmetric structures in quantum state space known as Symmetric Informationally-Complete Positive Operator-Valued Measures (SIC-POVMs), or SICs for short. We will prove a number of results about SICs in this thesis. Moreover, the SIC problem was part of the motivation for the study of linear dependencies in Section 2.3 and g-unitaries in Chapter 3. We devote this section to give an introduction to SIC-POVMs and their relation to the WH group, and to present our result on SICs being the closest to orthonormal bases with respect to a class of orthogonality measures.

2.2.1 Definitions, significances, and the existence problem

There is more than one way to define a SIC-POVM. We start with the one that explains the meaning of its name.

Definition. A set of n Hermitian operators $\{E_i\}_{i=1}^n$ on a d-dimensional Hilbert space is called a Positive Operator-Valued Measure (POVM) if they satisfy

$$E_i \geq 0 \tag{2.12}$$

for all $i = 1, 2, ..., n$ and

$$\sum_i E_i = \mathbb{1}. \tag{2.13}$$

Example. The projection operators $P_i = |i\rangle\langle i|$ of a projective (Von Neumann) measurement, where $|i\rangle$ are states constituting an orthonormal basis in a d-dimensional Hilbert space, form a POVM of d elements.

A POVM $\{E_i\}_{i=1}^n$ can be thought of as a generalized quantum measurement, with n outcomes labeled by i, whose probabilities are given by the Born rule

$$p(i) = \mathrm{Tr}(\rho E_i). \tag{2.14}$$

One can see that condition (2.12) in the definition is to enforce that all the probabilities are non-negative, while condition (2.13), often called the completeness condition, guarantees that they add up to one, as should be the case for a normalized probability distribution.

Definition. A POVM is said to be informationally complete if the unknown measured quantum state ρ is completely specified by the measurement outcome probabilities $p(i)$.

Informational completeness is equivalent to saying that the POVM elements E_i span the space of Hermitian operators regarded as a d^2-dimensional real vector space equipped with the Hilbert-Schmidt inner product

$$\langle H_1, H_2 \rangle = \mathrm{Tr}(H_1 H_2). \tag{2.15}$$

An informationally complete POVM therefore must have a minimum of d^2 elements.

Definition. A SIC-POVM is a POVM with d^2 elements $\{\Pi_i/d\}_{i=1}^{d^2}$, where Π_i are rank-1 projection operators satisfying the symmetric property

$$\mathrm{Tr}(\Pi_i \Pi_j) = \alpha \quad \forall i \neq j \tag{2.16}$$

for some constant α.

Note. We loosely call $\{\Pi_i\}$ a SIC, even though the POVM elements are technically Π_i/d.

There are a few things one can quickly deduce from the definition of SIC-POVMs. First, the value of the constant α can be determined from the dimension of the Hilbert space. From the POVM completeness condition, we have

$$\sum_{i,j=1}^{d^2} \Pi_i \Pi_j = \left(\sum_{i=1}^{d^2} \Pi_i \right)^2 = d^2 \mathbb{1}. \tag{2.17}$$

Taking the trace of both sides and making use of the symmetric property, one finds

$$\alpha = \frac{1}{d+1} \ . \tag{2.18}$$

Secondly, although it is not explicit, the definition of a SIC-POVM implies that it is informationally complete. To see this, we will first show that the operators Π_i are linearly independent. Suppose

$$\sum_i b_i \Pi_i = 0 \tag{2.19}$$

for some set of numbers b_i. Multiplying both sides of the equation by Π_k for some k and then taking the trace, we obtain

$$b_k + \alpha \sum_{i \neq k} b_i = 0. \tag{2.20}$$

On the other hand, Π_i have unit trace as they are rank-1 projectors, so just taking the trace of (2.19) yields

$$\sum_i b_i = 0. \tag{2.21}$$

Given that $\alpha \neq 1$, it follows that

$$b_k = 0 \quad \forall k \tag{2.22}$$

and Π_i are indeed linearly independent. There are d^2 of them, so they span the d^2-dimensional space of Hermitian operators. Thus, the POVM is informationally complete.

If one prefers to work with quantum states rather than with quantum measurements, there is an alternative definition of SIC-POVMs.

Definition. A set of d^2 normalized quantum states $\{|\psi_i\rangle\}_{i=1}^{d^2}$ is called a SIC set if it has a constant overlap between any two distinct states:

$$|\langle \psi_i | \psi_j \rangle| = \frac{1}{\sqrt{d+1}} \quad \forall i \neq j. \tag{2.23}$$

If we define the projection operators $\Pi_i = |\psi_i\rangle\langle\psi_i|$, then they are linearly independent and they span the space of Hermitian operators (following the same argument as before). Therefore the identity matrix can be written as a linear combination

$$\mathbb{1} = \sum_i c_i \Pi_i. \tag{2.24}$$

Using the previous trick of taking the trace of the equation above and taking its trace after multiplying both sides by some Π_k, one can show that $c_k = 1/d$ for all k. So the set $\{\Pi_i/d\}$ is a POVM, and the two definitions of SIC-POVMs are indeed equivalent.

The second definition has a geometrical interpretation. Any vector $|\psi\rangle \in \mathbb{C}^d$ spans a one-dimensional subspace of $\mathbb{C}^d$ called a line, which consists of all vectors of the form $a\,|\psi\rangle$ for any scalar a. If two lines are represented by normalized vectors $|\psi_1\rangle$ and $|\psi_2\rangle$, then the angle θ between the two lines is given by

$$\cos\theta = |\langle\psi_1|\psi_2\rangle|\,. \tag{2.25}$$

This means that the lines represented by vectors in a SIC set have a constant pairwise angle. Such lines are called equiangular lines, and a SIC set therefore is a set of equiangular lines, not just any set but a maximal one (there cannot be more than d^2 elements in the set because of the linear independence and the dimensionality of the space of Hermitian operators). The question is: do SICs exist in every dimension d?

Mathematicians have long been interested in figuring out the largest number of equiangular lines a vector space can admit (let us denote that number by $N(V)$, where V refers to the vector space), and in constructing these maximal sets of equiangular lines.

We start with the simplest type of vector spaces: the real ones $\mathbb{R}^d$. In dimension $d = 2$, one can draw a maximum of 3 equiangular lines on a 2-dimensional plane (imagine the three hands of a watch at 20 minutes past 8 o'clock), so $N(\mathbb{R}^2) = 3$. In three dimensions, $N(\mathbb{R}^3) = 6$ and the 6 equiangular lines can be constructed by connecting antipodal vertices of a regular icosahedron, one of the five Platonic solids. This result, together with $N(\mathbb{R}^4) = 6$, has been known since 1948 in work by Haantjes [33]. Lint and Seidel further investigated the problem, and obtained results in a number of higher dimensions [34]:

$$N(\mathbb{R}^5) = 10, \quad N(\mathbb{R}^6) = 16, \quad N(\mathbb{R}^7) = 28. \tag{2.26}$$

Lemmens and Seidel's paper in 1973 [35] contains some important results about real equiangular lines. One result is Gerzon's theorem, which provides an upper bound for $N(\mathbb{R}^d)$

$$N(\mathbb{R}^d) \leq d(d+1)/2. \tag{2.27}$$

This actually can be seen from the linear independence argument in (2.22) together with the fact that a real $d \times d$ orthogonal matrix is specified by $d(d+1)/2$ real parameters. When the bound is saturated, one can calculate the angle to be

$$\cos\theta = \frac{1}{\sqrt{d+2}}. \tag{2.28}$$

Another key result, mentioned in [35] as P. Neumann's theorem, states that if there exist m equiangular lines in $\mathbb{R}^d$, where $m > 2d$, and if the pairwise angle among them is θ, then $(\cos\theta)^{-1}$ is an odd integer. Together with (2.28), this implies that for $d > 3$, a necessary condition for the bound in (2.27) to be achieved is that $d = a^2 - 2$ for some odd integer a. The converse is not true, for example in dimension $d = 47 = 7^2 - 2$, where it has been proved that the bound cannot be achieved [36].

We will skip the detailed developments of this problem during the last 40 years or so, but we want to note that many dimensions have been investigated, many sets (not necessarily maximal) of real equiangular lines have been constructed, and many improvements have been made to the bounds of $N(\mathbb{R}^d)$ since 1948. However, the exact value for $N(\mathbb{R}^d)$ largely remains unknown even in small dimensions, and as of now in 2015, this is still an on-going line of research [37, 38].

One would have thought that if the problem has been so difficult for the case of real vector spaces, its counterpart in complex vector spaces would be hopeless. Perhaps this is why the problem of complex equiangular lines did not get a lot of attention until much later. Surprisingly, the complex version of the problem seems to be more tractable than the real one. This is just to say that $N(\mathbb{C}^d)$ seems to be of a nice and simple form. Proving so, on the other hand, is a totally different matter and is in fact one of the most challenging open problems in quantum information and algebraic combinatorics.

The upper bound for the number of complex equiangular lines

$$N(\mathbb{R}^d) \leq d^2 \tag{2.29}$$

was proved by Delsarte *et al* in their 1975 paper [39], which also mentioned that the bound can be saturated for $d = 2$ and 3 without giving further details. Hoggar later provided solutions to the complex equiangular lines problem for $d = 2$, 3 and 8 in 1982 [40]. In 1999, Zauner introduced the problem in the context of quantum designs in his PhD thesis [41], in which he conjectured that

$$N(\mathbb{C}^d) = d^2 \tag{2.30}$$

for every dimension d, and gave concrete constructions for dimensions $d = 2$ to 5.

The term SIC-POVM was coined in a paper by Renes *et al* in 2003 [42], in which they constructed SICs numerically all the way up to dimension $d = 45$, thereby adding considerable weight to Zauner conjecture. In addition to its geometric name "complex equiangular lines", SICs are also known as "minimal spherical 2-designs" in studies of quantum t-designs for quantum information theory, and as "equiangular tight frames" in the theory of signal processing for engineering. They have practical applications in quantum tomography [43–49], quantum cryptography and communication [50–58], and radar and classical signal processing [27, 58–61]. In addition, SIC-POVMs play important roles in foundational studies in quantum physics such as the QBist interpretation of quantum mechanics [62–66]. They also have deep mathematical connections to Lie algebras [67, 68], elliptic curves [69, 70], and Galois theory [71]. Despite an enormous amount of research on SIC-POVMs in the recent years [1, 27, 41–95] and strong numerical evidences of their existence (published for every dimension up to $d = 67$ [73]) as well as analytical solutions in many small dimensions ($d = 2$ to 15, 16, 19, 24, 28, 35, and 48 [73–75]), a general analytical construction or an existence proof for all dimensions is still missing.

2.2.2 Weyl-Heisenberg group covariance

One may attempt to find a SIC set by solving the defining system of equations (2.23). But one would quickly realize that this set of non-linear equations is highly over-constrained: including normalization there are a total of d^4 equations, while the number of real parameters needed to describe d^2 vectors in $\mathbb{C}^d$ is $2d^3$. Taking the conjugate symmetry of the inner product into account, the number of equations reduces to $(d^4 + d^2)/2$, but that is still one order in d higher than the number of variables. It seems that the existence of a solution must be a miracle. This is what it means when we say SIC states have no "right to exist" (the expression is borrowed from Amburg *et al* [6], in which they actually talk about MUB-balanced states). However, given strong evidences of SIC states' existence, there is another viewpoint one could take: their existence is not a miracle, but rather an indication of deep underlying symmetries. In fact, one such symmetry has been observed, namely the Weyl-Heisenberg symmetry.

Definition. We define the shift operator X and the phase operator Z by their action on the basis states $\{|x\rangle\}_{x=0}^{d-1}$ in a d-dimensional Hilbert space:

$$X|x\rangle = |x+1\rangle \qquad Z|x\rangle = \omega^x |x\rangle\,, \tag{2.31}$$

where $\omega = e^{2\pi i/d}$ is a primitive d-th root of unity, and the arithmetic inside Dirac's kets is

modulo d. X and Z in matrix form are given in (2.10) and (2.9).

Definition. The Weyl-Heisenberg displacement operators $D_{\mathbf{u}}$, labeled by a two-component vector $\mathbf{u}$, are defined to be

$$D_{\mathbf{u}} \equiv \tau^{u_1 u_2} X^{u_1} Z^{u_2} \qquad\qquad \mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \tag{2.32}$$

where $\tau = -e^{\pi i/d}$ and the two components u_1 and u_2 are integers modulo $\bar{d}$, which is defined to be

$$\bar{d} \equiv \begin{cases} d & \text{if } d \text{ is odd} \\ 2d & \text{if } d \text{ is even.} \end{cases} \tag{2.33}$$

to allow us to conveniently deal with both cases of odd d and even d at the same time [76]. Note that $\tau^{\bar{d}} = 1$, $D_{\mathbf{u}} = D_{\mathbf{v}}$ if and only if $\mathbf{u} = \mathbf{v} \mod \bar{d}$, and $D_{\mathbf{u}}$ are all traceless except when $\mathbf{u} = \mathbf{0} \mod d$.

The particular choice of the phase factors $\tau^{u_1 u_2}$ in the definition above is so that

$$D_{\mathbf{u}}^\dagger = D_{-\mathbf{u}}, \tag{2.34}$$

$$D_{\mathbf{u}} D_{\mathbf{v}} = \tau^{\Omega(\mathbf{u},\mathbf{v})} D_{\mathbf{u}+\mathbf{v}}, \tag{2.35}$$

where

$$\Omega(\mathbf{u}, \mathbf{v}) \equiv u_2 v_1 - u_1 v_2 \tag{2.36}$$

is the symplectic form of $\mathbf{u}$ and $\mathbf{v}$.

Definition. The WH group is defined to be the set of operators

$$\mathcal{W}_d = \{\tau^s D_{\mathbf{u}} : s \in \mathbb{Z}_{\bar{d}}, \mathbf{u} \in \mathbb{Z}_{\bar{d}}^2\}. \tag{2.37}$$

This is a group under matrix multiplication, with the group law given by (2.35). Although $\mathcal{W}_d$ technically has d^3 elements if d is odd or $8d^3$ elements if d is even, if we ignore overall phases of its elements this number reduces to d^2. For example, the Weyl-Heisenberg (WH) orbit of a given quantum state, i.e. a set of states obtained by applying all the displacement operators to the initial state, can only have at most d^2 distinct states because the overall phases of quantum states carry no physical meaning. For this reason, from now on when we consider a WH orbit, we will use $\mathbb{Z}_d^2$ instead of $\mathbb{Z}_{\bar{d}}^2$ to index the displacement operators.

Definition. A SIC set is said to be Weyl-Heisenberg covariant if it is an orbit under the WH group. In other words, it can be written as $\{D_{\mathbf{u}} |\psi\rangle : \mathbf{u} \in \mathbb{Z}_d^2\}$ for some $|\psi\rangle$. Such a state $|\psi\rangle$ is called a Weyl-Heisenberg SIC fiducial.

If we assume WH covariance, the problem of finding a SIC set turns into the problem of finding a single normalized fiducial state $|\psi\rangle$ such that

$$|\langle\psi| D_{\mathbf{u}} |\psi\rangle|^2 = \frac{1}{d+1} \qquad \forall \mathbf{u} \in \mathbb{Z}_d^2 \backslash \{\mathbf{0}\}. \tag{2.38}$$

One can see that the Weyl-Heisenberg symmetry helps reduce the number of equations to the order of d^2. Although the number of (real) variables is now $2d$, and this system of equations is still over-constrained, it significantly simplifies the problem. Almost all known analytical solutions to the SIC problem, as well as all numerical solutions to date [42, 73], are Weyl-Heisenberg covariant, with one exception being the construction in $d = 8$ by Hoggar [40], which is covariant with respect to a 3-fold tensor product of WH groups for $d = 2$. It has even been proved that in prime dimensions, if a SIC set with group covariance exists, the group must be the WH group [89]. It therefore looks as though Weyl-Heisenberg covariance is an intrinsic symmetry of SIC-POVMs.

2.2.3 Clifford unitaries and Zauner symmetry

On top of the Weyl-Heisenberg covariance, another order-3 symmetry on SIC-POVMs was observed by Zauner [41] and later explicitly worked out by Appleby [76]. Before we get there, we first need to define the Clifford group and provide a unitary representation.

Definition. The Clifford group $\mathcal{C}_d$ is defined to be the normalizer of the Weyl-Heisenberg group $\mathcal{W}_d$ within the unitary group $U(d)$. In other words, a unitary operator U belongs to $\mathcal{C}_d$ if and only if

$$U\mathcal{W}_d U^\dagger = \mathcal{W}_d. \tag{2.39}$$

Remark. It should be mentioned that there are several different versions of the Weyl-Heisenberg and Clifford groups. The version that we have just defined is the ordinary one, which can be defined for any dimension d. This ordinary version is relevant to the current chapter when we discuss SICs and linear dependencies in WH orbits. In Chapter 3, we will use another version which is applicable only to odd prime power dimensions, where one takes advantage of finite fields to define a Galoisian variant of the WH group. Corresponding to this Galoisian WH group are two Galoisian variants of the Clifford group: the full and the

restricted one [30], of which we will only use the latter. To avoid confusion, the definitions of the Galoisian WH and Clifford groups are put in Appendix A.2. For now, in this chapter, we use the name WH and Clifford groups to refer to the ordinary version.

Clifford unitaries can be constructed from symplectic matrices [76]. We define the symplectic group $\mathrm{SL}(2,\mathbb{Z}_{\bar{d}})$ to be the set of all 2×2 matrices

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \alpha, \beta, \gamma, \delta \in \mathbb{Z}_{\bar{d}} \tag{2.40}$$

such that $\det(G) = 1 \bmod \bar{d}$. If β has a multiplicative inverse β^{-1} in $\mathbb{Z}_{\bar{d}}$, we can associate S with a unitary U_S defined explicitly by

$$U_S = \frac{e^{i\phi}}{\sqrt{d}} \sum_{x,y=0}^{d-1} \tau^{\beta^{-1}(\alpha y^2 - 2xy + \delta x^2)} \left|x\right\rangle \left\langle y\right|, \tag{2.41}$$

where $e^{i\phi}$ is an arbitrary phase. If β does not admit an inverse, we can always decompose S into a product of two symplectic matrices [76]

$$S = S_1 S_2 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix} \tag{2.42}$$

such that β_1 and β_2 have inverses, and then define $U_S = U_{S_1} U_{S_2}$. Such unitaries U_S with arbitrary overall phases are called symplectic unitaries. They are particularly constructed to satisfy

$$U_S D_{\mathbf{u}} U_S^\dagger = D_{S\mathbf{u}} \tag{2.43}$$

and

$$U_S U_{S'} \doteq U_{SS'} \tag{2.44}$$

for any $S, S' \in \mathrm{SL}(2,\mathbb{Z}_{\bar{d}})$ and $u \in \mathbb{Z}_{\bar{d}}$, where "$\doteq$" means equal up to an overall phase. Clifford unitaries (modulo overall phases) are then products of symplectic unitaries and displacement operators $U_S D_{\mathbf{u}}$.

Every known WH covariant SIC fiducial vector is invariant (ignoring a global phase) under an order 3 Clifford unitary, and conversely, every canonical order 3 Clifford unitary (corresponding to a symplectic matrix of trace -1) has a SIC fiducial as one of its eigenvectors in all dimensions where an exhaustive search has been done [73]. There is a particular choice for an order 3 Clifford unitary that can be conveniently written in the same form in all dimensions, which we call the Zauner unitary.

Definition. The Zauner unitary is defined to be the symplectic unitary $U_{\mathcal{Z}}$ corresponding to the Zauner symplectic matrix $\mathcal{Z}$

$$\mathcal{Z} \equiv \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}. \tag{2.45}$$

One can easily verify that $\mathcal{Z}^3 = \mathbb{1}$ so that $\mathcal{Z}$ is indeed of order 3.

Conjecture (Zauner-Appleby [41, 76])**.** In every d-dimensional Hilbert space, there exists a Weyl-Heisenberg SIC fiducial which is an eigenvector in the largest eigen subspace of the Zauner unitary $U_{\mathcal{Z}}$.

We want to note that in addition to being an extra symmetry for SIC-POVMs on top of the WH covariance, the Zauner symmetry also plays a pivotal role in the study of linear dependencies in Weyl-Heisenberg orbits in Section 2.3.

2.2.4 Analogues to orthonormal bases

While the discussion is still on SIC-POVMs, there is one nice property of them that we would like to introduce, namely they are as close as possible to being an orthonormal basis on the cone of non-negative operators [1].

The set operators acting on d-dimensional vectors in $\mathbb{C}^d$ can be considered as a d^2-dimensional Hilbert space with the Hilbert Schmidt inner product given by

$$\langle A, B\rangle = \mathrm{Tr}(A^\dagger B). \tag{2.46}$$

Let $\{B_i\}_{i=1}^{d^2}$ be an orthogonal basis for this space of operators. One might wonder if it is possible to put some restrictions on B_i. For example, can they all be Hermitian? Or unitary? The answers for both are yes. The Hermitian operators themselves form a d^2-dimensional real vector space with the same inner product as defined in (2.46), so one can have a set of d^2 Hermitian operators H_i that forms an orthogonal basis for the space of Hermitian operators. One can show that this basis spans the whole space of operators by noticing that any operators (not necessarily Hermitian) can be written as

$$A = H_+ - iH_-, \tag{2.47}$$

where

$$H_+ = (A + A^\dagger)/2, \qquad H_- = (iA - iA^\dagger)/2 \tag{2.48}$$

are clearly Hermitian. As for an orthogonal unitary basis, one example is the set of Weyl-Heisenberg displacements operators $\{D_{\mathbf{u}} : \mathbf{u} \in \mathbb{Z}_d^2\}$ defined in (2.32). These displacement operators are orthogonal to each other because for any $\mathbf{u} \neq \mathbf{v}$

$$\langle D_{\mathbf{u}}, D_{\mathbf{v}} \rangle = \mathrm{Tr}(D_{\mathbf{u}}^\dagger D_{\mathbf{v}}) = \tau^{-\Omega(\mathbf{u},\mathbf{v})} \mathrm{Tr}(D_{\mathbf{v}-\mathbf{u}}) = 0. \tag{2.49}$$

However, imposing positive semi-definiteness on an orthogonal basis for the space of operators is impossible, as we will show. Let $\{A_i\}$ be a set of d^2 positive semi-definite operators and assume that A_i are normalized, meaning that $\mathrm{Tr}(A_i^2) = 1$. We would like to quantify the extent to which this set is orthogonal. A natural class of ''orthogonality measures'' is defined by

$$K_t \equiv \sum_{i \neq j} |\langle A_i, A_j \rangle|^t = \sum_{i \neq j} (\mathrm{Tr}(A_i A_j))^t \tag{2.50}$$

for any real number $t \geq 1$. This sum consists of $d^4 - d^2$ terms and it vanishes if and only if A_i are orthogonal to each other. However, as we will see from the following theorem, this can never happen, since K_t is bounded below by a positive number.

Theorem 2.1. *Let $\{A_i\}_{i=1}^{d^2}$ be a set of d^2 normalized positive semi-definite operators on a Hilbert space of dimension d, and let K_t be defined as in (4.1), then K_t is lower bounded by*

$$K_t \geq \frac{d^2(d-1)}{(d+1)^{t-1}} \tag{2.51}$$

When $t = 1$, the bound is saturated if and only if A_i are rank-1 projectors and $\sum A_i = d\mathbb{1}$. When $t > 1$, the bound is saturated if and only if $\{A_i/d\}$ forms a SIC-POVM.

Proof. We will first prove the inequality for the $t = 1$ case, by making use of a version of the Cauchy-Schwarz inequality (also known as Bouniakowsky inequality [96]):

$$\left(\sum_{i=1}^N x_i^2\right)\left(\sum_{i=1}^N y_i^2\right) \geq \left(\sum_{i=1}^N x_i y_i\right)^2 \tag{2.52}$$

for any $2N$ real numbers x_i and y_i. Particularly, setting $y_i = 1$ leads to

$$\left(\sum_{i=1}^N x_i^2\right) \geq \frac{1}{N}\left(\sum_{i=1}^N x_i\right)^2, \tag{2.53}$$

with equality if and only if $x_1 = x_2 = ... = x_N$.

Since $\mathrm{Tr}(A_i^2) = 1$ by the normalization assumption, the (real and positive) eigenvalues of A_i are no larger than 1, and therefore

$$\mathrm{Tr}(A_i) \geq \mathrm{Tr}(A_i^2) = 1, \tag{2.54}$$

with equality if and only if exactly one eigenvalue of A_i is 1 and the rest are 0, meaning that A_i are rank-1 projectors. Let G be a positive semi-definite operator defined by

$$G = \sum_{i=1}^{d^2} A_i \tag{2.55}$$

It follows that $\mathrm{Tr}(G) \geq d^2$. Applying the inequality (2.53) to the eigenvalues of G we get

$$\mathrm{Tr}(G^2) \geq \frac{1}{d}(\mathrm{Tr}\, G)^2 \geq d^3, \tag{2.56}$$

which implies

$$K_1 \geq d^3 - d^2. \tag{2.57}$$

Equality is obtained if and only if A_i are all rank-1 projectors, and $G = d\mathbb{1}$.

For $t > 1$, if we define a function $f(x) = x^t$, then this is a strictly convex function. We can rewrite K_t as

$$K_t = \sum_{i \neq j} f\left(\mathrm{Tr}(A_i A_j)\right). \tag{2.58}$$

Applying a particular instance of Jensen inequality [97], namely

$$\sum_{i=1}^{N} f(x_i) \geq N f\left(\frac{\sum x_i}{N}\right) \tag{2.59}$$

for any convex function $f(x)$ and any x_i in the domain, with equality (in the case of strict convexity) if and only if x_i are all constant, we obtain

$$\begin{aligned} K_t &\geq (d^4 - d^2) f\left(\frac{\sum_{i \neq j} \mathrm{Tr}(A_i A_j)}{d^4 - d^2}\right) \\ &\geq (d^4 - d^2) f\left(\frac{d^3 - d^2}{d^4 - d^2}\right) \\ &= \frac{d^2(d-1)}{(d+1)^{t-1}}. \end{aligned} \tag{2.60}$$

For this bound to be saturated, equality must take place in both the Jensen inequality and (2.57). This means the d^2 operators A_i must be all rank-1 projectors satisfying $\sum_i A_i = d\mathbb{1}$ and $\mathrm{Tr}(A_i A_j)$ are constant for all $i \neq j$. This is precisely the definition of a SIC-POVM. □

Remark. What we have shown is that on the cone of non-negative operators, there does not exist an orthonormal basis. Furthermore, using K_t as a natural class of "orthogonality measures", we have shown that SIC-POVMs stand out as the "most orthogonal" bases on this cone. We want to note that one of our orthogonality measures, namely K_2, is closely related to the frame potential

$$\Phi = \sum_{i,j} |\langle\psi_i|\psi_j\rangle|^4 \tag{2.61}$$

introduced by Renes *et al* [42] via the simple relation

$$K_2 = \Phi - d^2. \tag{2.62}$$

In [42], the minimization of the frame potential was used to aid the numerical search for SICs, and the bound was proved in the context of frames and spherical t-designs. Here, our proof of the bound relies only on a few well-known elementary inequalities.

2.3 Linear dependencies in Weyl-Heisenberg orbits

The study of linear dependencies in WH orbits [2] stems from an observation that among 9 vectors in any known 3-dimensional SIC set, one can find some sets of 3 vectors that are linearly dependent. This led to our investigation in higher dimensions, where the question we asked was: among d^2 SIC vectors in dimension d, could one find a set of d of them that are linearly dependent? Going through the numerical SICs provided in [73], we found a striking pattern: it seems as though whenever d is divisible by 3, the answer is yes.

Since these are Weyl-Heisenberg covariant SICs, the SIC vectors can be expressed as $D_{\mathbf{p}}|\psi\rangle$, where $D_{\mathbf{p}}$ are the WH displacement operators indexed by $\mathbf{p} = (p_1, p_2) \in \mathbb{Z}_d^2$, and $|\psi\rangle$ is a SIC fiducial vector. If $\{\mathbf{p}_i\}_{i=1}^d$ is a set of d indices $\mathbf{p}_i$ such that the d vectors $D_{\mathbf{p}_i}|\psi\rangle$ are linearly dependent, we call it a "good" p-set. It follows that for any good p-set, there exists a set of coefficients λ_i, which are not simultaneously zero, such that

$$\sum_i \lambda_i D_{\mathbf{p}_i}|\psi\rangle = 0 \qquad \text{or} \qquad L|\psi\rangle = 0, \tag{2.63}$$

where L is defined to be $L = \sum_i \lambda_i D_{\mathbf{p}_i}$. In dimensions d that are divisible by 3, not only have we found many good p-sets, but we have also noticed numerically that in many

cases their corresponding L matrices are of rank $d-1$. This means the null space of L is 1-dimensional, i.e. the matrix equation $Lx = 0$ has a unique solution (up to a phase), which is the SIC fiducial $|\psi\rangle$. If we know what the L matrices are, we could simply solve this matrix equation to obtain the SIC fiducial!

Finding the L matrices requires us to identify good p-sets $\{\mathbf{p}_i\}$ as well as the coefficients λ_i. As it will be shown later in this section, we succeeded in the first task. However, finding λ_i is non-trivial, despite a 3-fold symmetry of theirs that we observe. In fact, it turns out that this approach to the SIC problem cannot work, because the linear dependence property is not unique to SIC fiducials, but is generic to a class of eigenvectors of certain Clifford unitaries, one of which is the Zauner unitary $U_{\mathcal{Z}}$ defined in (2.45).

In this section, we first examine a special SIC set in dimension $d = 3$, which has a connection to elliptic curves via Hesse configuration [69]. We then provide an analytical proof for linear dependencies in the WH orbits of the eigenvectors of the Zauner unitary. We give a detailed report on our numerical study, in which the number of observed linear dependencies is often higher than what can be accounted for from the analytical prediction. And lastly, we show a robust construction of "small SICs" in dimension $d = 2$ and 3 that resulted from this study of linear dependencies.

Remark. Before going into the details of this study, we want to note that the opposite problem, i.e. to find fiducial vectors whose WH orbits contain no linear dependencies, is useful for classical signal processing and it has been solved [98–100].

2.3.1 Dimension $d = 3$ and Hesse configuration

In dimension $d = 3$, there is a continuous family of SICs that can be parameterized by a single parameter [76]. All other known SICs in dimension 3 have been shown to be unitarily equivalent to this family [89]. Explicitly, the 9 vectors of a SIC in this family can be written

in the following form (ignoring normalization factors):

$$\begin{gathered}
\begin{pmatrix} 0 \\ 1 \\ -e^{i\theta} \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -e^{i\theta}\eta \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ -e^{i\theta}\eta^2 \end{pmatrix}, \\
\begin{pmatrix} -e^{i\theta} \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -e^{i\theta}\eta \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} -e^{i\theta}\eta^2 \\ 0 \\ 1 \end{pmatrix}, \\
\begin{pmatrix} 1 \\ -e^{i\theta} \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -e^{i\theta}\eta \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ -e^{i\theta}\eta^2 \\ 0 \end{pmatrix},
\end{gathered} \tag{2.64}$$

where $\eta = e^{2\pi i/3}$ is a third root of unity (we reserve ω for the d-th root of unity in general) and the parameter θ is in the interval $[0, \pi/3]$. One observes that the 3 vectors on each line in (2.64) span a 2-dimensional subspace. Hence, any such SIC contains 3 sets of 3 linearly dependent vectors. However, for certain values of θ, there are additional linear dependencies. One can find these values by putting any 3 vectors from 3 different lines in (2.64) together as a 3×3 matrix and set the determinant of this matrix to zero to obtain

$$e^{3i\theta} = \eta^k \qquad\qquad k = 0, 1, 2. \tag{2.65}$$

Given the range of θ in consideration $[0, \pi/6]$, there are two choices $\theta = 0$ or $2\pi/9$, giving rise to two special SICs that both contain 12 sets of 3 linearly dependent vectors. The SIC corresponding to $\theta = 0$ is ''extra special'' because its fiducial vector

$$|\phi\rangle = \begin{pmatrix} 0 \\ 1 \\ -1 \end{pmatrix} \tag{2.66}$$

is an eigenvector of symplectic unitaries U_S for all $S \in \mathrm{SL}(2, \mathbb{F}_d)$. One can see this by noticing that the density operator can be written as

$$|\phi\rangle\langle\phi| = \mathbb{1} - U_P, \tag{2.67}$$

where the parity operator U_P is the symplectic unitary corresponding to an SL element

$$P = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \tag{2.68}$$

which in turn is the only element (besides the identity element) that commutes with all other elements in SL. If we label the 9 SIC vectors in (2.64) by $|00\rangle, |01\rangle, ..., |22\rangle$, then the linearly dependent relations for the $\theta = 0$ SIC are as follows:

$$\begin{aligned} |00\rangle + |10\rangle + |20\rangle &= 0 \\ |01\rangle + |11\rangle + |21\rangle &= 0 \\ |02\rangle + |12\rangle + |22\rangle &= 0 \end{aligned} \tag{2.69}$$

$$\begin{aligned} |00\rangle + \eta\,|01\rangle + \eta^2\,|02\rangle &= 0 \\ |10\rangle + \eta\,|11\rangle + \eta^2\,|12\rangle &= 0 \\ |20\rangle + \eta\,|21\rangle + \eta^2\,|22\rangle &= 0 \end{aligned} \tag{2.70}$$

$$\begin{aligned} |00\rangle + \quad |11\rangle + \eta\,|22\rangle &= 0 \\ |01\rangle + \eta\,|12\rangle + \quad |20\rangle &= 0 \\ \eta\,|02\rangle + \quad |10\rangle + \quad |21\rangle &= 0 \end{aligned} \tag{2.71}$$

$$\begin{aligned} |00\rangle + \quad |12\rangle + \eta^2\,|21\rangle &= 0 \\ \eta^2\,|01\rangle + \quad |10\rangle + \quad |22\rangle &= 0 \\ |02\rangle + \eta^2\,|11\rangle + \quad |20\rangle &= 0. \end{aligned} \tag{2.72}$$

We note that in Equations (2.69) to (2.72), each linearly dependent relation involves 3 SIC vectors, and each SIC vector appears in 4 relations. If we represent the SIC vectors by 9 points, and draw a ''line'' connecting 3 points if their SIC vectors are linearly dependent, then we obtain a set of 9 points and 12 lines, each line containing 3 points, and each point is contained in 4 lines, as illustrated in Figure 2.1. It was pointed out by Lane Hughston [69] that this was precisely the Hesse configuration [101], often denoted by the configuration $(9_4, 12_3)$ in the language of configurations in geometry.

The Hesse configuration is not realizable in the Euclidean plane. However, it can be realized in the complex projective plane, which was discovered by Hesse in the study of elliptic curves. Particularly, let us consider the following family of cubic curves described by the polynomial equations

$$P(x_1, x_2, x_3) = x_1^3 + x_2^3 + x_3^3 + \lambda x_1 x_2 x_3 = 0 \qquad \lambda \in \mathbb{C}. \tag{2.73}$$

The 3×3 Hessian matrix H consists of second derivatives of P, with its entries given by

$$H_{ij} = \frac{\partial^2 P}{\partial x_i \partial x_j}. \tag{2.74}$$

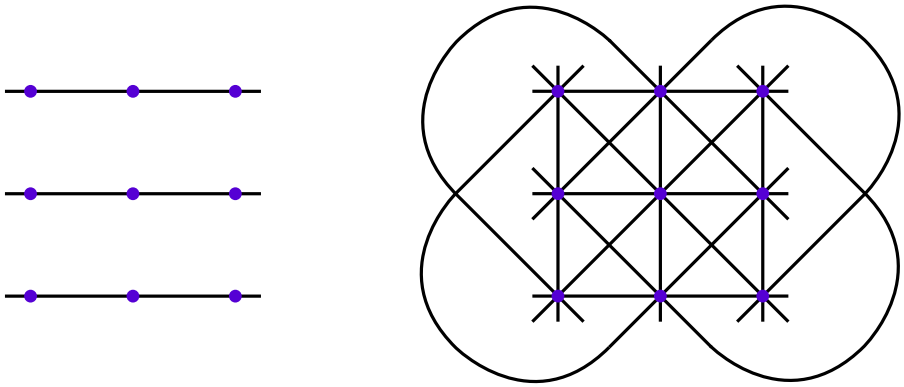

Figure 2.1: The linear dependency structures of a generic 3-dimensional SIC (on the left) and of the special SICs with $\theta = 0$ or $2\pi/9$ (on the right). Each point represents a SIC vector, and points are connected by a line if the corresponding SIC vectors are linearly dependent. The structure to the right, with 9 points and 12 lines, is known as the Hesse configuration.

Points on the curve where the determinant of the Hessian matrix vanishes are called inflection points. This determinant is also a cubic polynomial in the family, and by Bézout's theorem [102], these two cubic curves intersect at 9 points. These 9 inflection points are the same for all values of λ, and they coincide exactly with the 9 vectors of the $\theta = 0$ SIC. Furthermore, there are 4 special (singular) curves in the family corresponding to the cases when $\lambda = \infty$ and $\lambda^3 = -27$:

$$\begin{aligned} &P_0 : x_1 x_2 x_3 = 0 \\ &P_1 : (x_1 + x_2 + x_3)(x_1 + \eta x_2 + \eta^2 x_3)(x_1 + \eta^2 x_2 + \eta x_3) = 0 \\ &P_2 : (x_1 + \eta^2 x_2 + \eta^2 x_3)(x_1 + \eta x_2 + x_3)(x_1 + x_2 + \eta x_3) = 0 \\ &P_3 : (x_1 + \eta x_2 + \eta x_3)(x_1 + \eta^2 x_2 + x_3)(x_1 + x_2 + \eta^2 x_3) = 0 \end{aligned} \tag{2.75}$$

One can see that each of these curves P_i degenerates into 3 projective lines, giving a total of 12 lines. Each of the lines passes through 3 inflection points, and each inflection point belongs to 4 lines. This results in the Hesse configuration. More details on its connection to SICs can be found in [70].

Remark. For each of the 12 linear dependencies in the $\theta = 0$ SIC, the corresponding set of 3 linearly dependent vectors spans a 2-dimensional plane in the Hilbert space, whose normal vector is unique up to a scalar multiplication. These 12 normal vectors form a complete

set of MUBs in dimension $d = 3$ and this observation has been used for a Kochen-Specker inequality [72].

2.3.2 Linear dependencies from Zauner eigenvectors

As we mentioned earlier, the linear dependence property is not a unique feature of SICs. We will now show that linear dependencies can arise in all dimensions in Weyl-Heisenberg orbits of vectors that lie in certain eigenspaces of the Zauner unitary $U_{\mathcal{Z}}$. Known SIC fiducials just happen to be among those vectors.

Recall that by the definition in (2.45), the Zauner symplectic matrix $\mathcal{Z}$ is of order 3. Hence, its symplectic unitary $U_{\mathcal{Z}}$ is also of order 3, for a suitable choice of the phase $e^{i\phi}$ in (2.41). This means that its eigenvalues must be 1, η, or η^2, where $\eta = e^{2\pi i/3}$ is a third root of unity, and $U_{\mathcal{Z}}$ has 3 eigenspaces corresponding to these 3 eigenvalues. If the phase in (2.41) is particularly chosen to be

$$e^{i\phi} = e^{i\pi(d-1)/12}, \tag{2.76}$$

then one finds that [41] the eigenspaces $\mathcal{H}_1$, $\mathcal{H}_\eta$, and $\mathcal{H}_{\eta^2}$ corresponding to the eigenvalues 1, η, and η^2 have dimensions as shown in Table 2.1. In all dimensions d, SIC fiducials are found in $\mathcal{H}_1$, which will be specifically referred to as the Zauner subspace. We want to note that when d is equal to 8 mod 9, additional SIC fiducials are found in the other two eigenspaces as well [73].

	$d = 3k$	$d = 3k + 1$	$d = 3k + 2$
$\dim(\mathcal{H}_1)$	$k + 1$	$k + 1$	$k + 1$
$\dim(\mathcal{H}_\eta)$	k	k	$k + 1$
$\dim(\mathcal{H}_{\eta^2})$	$k - 1$	k	k

Table 2.1: Dimensions of the three eigenspaces $\mathcal{H}_1$, $\mathcal{H}_\eta$, and $\mathcal{H}_{\eta^2}$ of the Zauner unitary $U_{\mathcal{Z}}$ for different dimensions d.

Since Zauner symplectic $\mathcal{Z}$ is of order 3, it generally moves points $\mathbf{p} = (p_1, p_2)$ on the discrete phase space $\mathbb{F}_d^2$ in orbits $\{\mathbf{p}, \mathcal{Z}\mathbf{p}, \mathcal{Z}^2\mathbf{p}\}$ of size 3, which will be referred to as triplets. The exception is when $\mathbf{p}$ is a fixed point of $\mathcal{Z}$, i.e. $\mathcal{Z}\mathbf{p} = \mathbf{p}$, in which case we will call it a singlet. One can easily solve for the fixed points of $\mathcal{Z}$ and find that there are 3 singlets

when d is divisible by 3, and only 1 trivial singlet (the zero vector) otherwise. The singlets are given in Table 2.2. In the Hilbert space, we will use the same terminology to call $D_{\mathbf{p}} |\psi\rangle$ a singlet if $\mathbf{p}$ is a singlet, and to call $\{D_{\mathbf{p}} |\psi\rangle, D_{\mathcal{Z}\mathbf{p}} |\psi\rangle, D_{\mathcal{Z}^2\mathbf{p}} |\psi\rangle\}$ a triplet otherwise.

$d = 3k$	$d \neq 3k$
$\begin{pmatrix}0\\0\end{pmatrix}, \begin{pmatrix}k\\2k\end{pmatrix}, \begin{pmatrix}2k\\k\end{pmatrix}$	$\begin{pmatrix}0\\0\end{pmatrix}$

Table 2.2: Fixed points of the Zauner symplectic $\mathcal{Z}$.

Theorem 2.2. *Let $|\phi\rangle$ be an eigenvector of the Zauner unitary $U_{\mathcal{Z}}$ with eigenvalue λ, and let V be a set of d vectors in the Weyl-Heisenberg orbit of $|\phi\rangle$, i.e. $\{D_{\mathbf{p}} |\phi\rangle : \mathbf{p} \in \mathbb{F}_d^2\}$. Then the vectors in V are linearly dependent if:*

1. *V contains k triplets, or $k-1$ triplets and 3 singlets for the case $d = 3k$,*
2. *V contains k triplets and 1 singlet and $|\phi\rangle \in \mathcal{H}_\eta \cup \mathcal{H}_{\eta^2}$ for the case $d = 3k+1$,*
3. *V contains k triplets and 1 singlet and $|\phi\rangle \in \mathcal{H}_{\eta^2}$ for the case $d = 3k+2$.*

Proof. We start with the case $d = 3k$. If $\mathbf{p}$ is a singlet, then $|\phi\rangle$ and $D_{\mathbf{p}} |\phi\rangle$ lie in the same eigenspace of $U_{\mathcal{Z}}$ because

$$U_{\mathcal{Z}} D_{\mathbf{p}} |\phi\rangle = U_{\mathcal{Z}} D_{\mathbf{p}} U_{\mathcal{Z}}^\dagger U_{\mathcal{Z}} |\phi\rangle = \lambda D_{\mathcal{Z}\mathbf{p}} |\phi\rangle = \lambda D_{\mathbf{p}} |\phi\rangle . \tag{2.77}$$

If $\mathbf{p}$ is in a triplet, we construct 3 new vectors from linear combinations of vectors in the triplet $\{D_{\mathbf{p}} |\phi\rangle, D_{\mathcal{Z}\mathbf{p}} |\phi\rangle, D_{\mathcal{Z}^2\mathbf{p}} |\phi\rangle\}$ as follows:

$$\begin{aligned} |r\rangle &= D_{\mathbf{p}} |\phi\rangle + \quad U_{\mathcal{Z}} D_{\mathbf{p}} |\phi\rangle + \quad U_{\mathcal{Z}}^2 D_p |\phi\rangle \\ |s\rangle &= D_{\mathbf{p}} |\phi\rangle + \eta^2 U_{\mathcal{Z}} D_{\mathbf{p}} |\phi\rangle + \eta\ U_{\mathcal{Z}}^2 D_p |\phi\rangle \\ |t\rangle &= D_{\mathbf{p}} |\phi\rangle + \eta\ U_{\mathcal{Z}} D_{\mathbf{p}} |\phi\rangle + \eta^2 U_{\mathcal{Z}}^2 D_p |\phi\rangle . \end{aligned} \tag{2.78}$$

Given a choice of $\mathbf{p}$, we will refer to vectors constructed in way as r-type, s-type, and t-type respectively. One can straightforwardly verify that

$$U_{\mathcal{Z}} |r\rangle = |r\rangle \tag{2.79}$$

so r-type vectors belong to the eigenspace $\mathcal{H}_1$ of $U_{\mathcal{Z}}$. Similarly, s-type and t-type vectors belong to the other two eigenspace $\mathcal{H}_\eta$ and $\mathcal{H}_{\eta^2}$, respectively. Moreover, (2.78) can be inverted so that any vector in the triplet $\{D_{\mathbf{p}}|\phi\rangle, D_{\mathcal{Z}\mathbf{p}}|\phi\rangle, D_{\mathcal{Z}^2\mathbf{p}}|\phi\rangle\}$ can be written as a linear combination of $|r\rangle, |s\rangle$ and $|t\rangle$:

$$\begin{aligned} D_{\mathbf{p}}|\phi\rangle &= \left(|r\rangle + \quad |s\rangle + \quad |t\rangle\right)/3 \\ U_{\mathcal{Z}} D_{\mathbf{p}}|\phi\rangle &= \left(|r\rangle + \eta \ |s\rangle + \eta^2 |t\rangle\right)/3 \\ U_{\mathcal{Z}}^2 D_{\mathbf{p}}|\phi\rangle &= \left(|r\rangle + \eta^2 |s\rangle + \eta \ |t\rangle\right)/3. \end{aligned} \tag{2.80}$$

Therefore the two sets $\{D_{\mathbf{p}}|\phi\rangle, D_{\mathcal{Z}\mathbf{p}}|\phi\rangle, D_{\mathcal{Z}^2\mathbf{p}}|\phi\rangle\}$ and $\{|r\rangle, |s\rangle, |t\rangle\}$ have exactly the same linear span.

If V contains k triplets, this gives k-many of each r-,s-, and t-type vector. From Table 2.1 we know that the r-type vectors belong to an eigenspace of dimension $k+1$, the s-type vectors belong to an eigenspace of dimension k, and the t-type vectors belong to an eigenspace of dimension $k-1$. It clearly follows that the k r-type vectors cannot fully span their eigenspace, while the k t-type vectors are overcomplete and therefore linearly dependent.

If V contains $k-1$ triplets and 3 singlets, this gives $(k-1)$-many of each r-,s-, and t-type vector, plus the 3 singlets that belong to the same eigenspace as $|\phi\rangle$. This means there will be $k+2$ vectors among these that belong to the same eigenspace. Since the largest eigenspace of $U_{\mathcal{Z}}$ has dimensionality $k+1$, we obtain linear dependency.

Still sticking to the case $d = 3k$, we want to note that if we further assume $|\phi\rangle \in \mathcal{H}_\eta$, we also obtain linear dependency when V contains $k-1$ triplets and 2 singlets, or $k-2$ triplets and 3 singlets, using the same argument. Assuming $|\phi\rangle \in \mathcal{H}_{\eta^2}$ allows us to extend this linear dependency condition even further, to include cases when V contains $k-3$ triplets and 3 singlets.

In the case $d = 3k+1$, the 3 eigenspaces $\mathcal{H}_1, \mathcal{H}_\eta$ and $\mathcal{H}_{\eta^2}$ have dimensionality $k+1, k$, and k respectively. If $|\phi\rangle \in \mathcal{H}_\eta$, then the singlet together with k s-type vectors give $k+1$ vectors in $\mathcal{H}_\eta$, resulting in linear dependency. If $|\phi\rangle \in \mathcal{H}_{\eta^2}$, the singlet together with k t-type vectors give $k+1$ vectors in $\mathcal{H}_{\eta^2}$, also resulting in linear dependency.

In the case $d = 3k+2$, the eigenspace $\mathcal{H}_{\eta^2}$ has dimensionality k. The k t-type vectors, together with the singlet, form a set of $k+1$ vectors in $\mathcal{H}_{\eta^2}$. Therefore they are linearly dependent.

□

2.3.3 Numerical linear dependencies

Although the results in the previous section provide a significant understanding of how linear dependencies can arise in a WH orbit of an initial vector that is an eigenvector of $U_{\mathcal{Z}}$, they do not account for all the linear dependencies that we observe numerically. In this section, we provide a numerical analysis for linear dependencies in dimensions $d = 4$ to 8, with partial results in $d = 9$. We pay more attention and provide more details for the cases $d = 6$ and 9, as we are interested in dimensions that are divisible by 3 (we know from Theorem 2.2 that in dimensions $d = 3k$ one can obtain linear dependencies from an initial vector in the Zauner subspace $\mathcal{H}_1$, where SIC fiducials are expected to be). Although the additional (cannot be accounted for by Theorem 2.2) linear dependencies in $d = 6$ and 9 do not depend on whether the initial vector is a SIC fiducial or not, there are some interesting orthogonality relationships in the dependency structure that seem to be unique to SICs. Our investigation in $d = 6$ and 9 also led to ''small SICs'', which will be the focus of the next section. In dimension $d = 8$, there are SIC fiducials in $\mathcal{H}_{\eta^2}$, and we observe that these SIC fiducials yield more linearly dependencies than an arbitrary initial vector in $\mathcal{H}_{\eta^2}$. This indicates some similarity to the situation in $d = 3$ that led to the Hesse configuration that we discussed in Section 2.3.1.

In each dimension d that we analyzed, our computer program started with an arbitrary initial vector of each of the eigenspaces of the Zauner unitary $U_{\mathcal{Z}}$, generated the full orbit under the action of the WH group, and then performed an exhaustive search for all subsets of d vectors that are linearly dependent by calculating the determinants of the $d \times d$ matrices formed by these d vectors to a numerical precision of 10^{-15}. For each eigenspace, the procedure was repeated for a small number of arbitrarily chosen initial vectors, to make sure that the results are the same. As for SIC fiducials, we used those given in [73], and when there are more than one Clifford orbit we repeat the calculation with fiducials from each orbit.

We found no distinction between choices of the initial vector, except in dimension $d = 8$ where the SIC fiducial gives rise to 24,935,160 sets of linearly dependent vectors, slightly higher than the generic result shown in Table 2.3. In dimension $d = 7$, the numerical results match our prediction from Theorem 2.2. But in all other cases, there are more numerically observed linear dependencies than what Theorem 2.2 can account for. Table 2.3 shows the number of linearly dependent sets found in WH orbits with generic initial vectors in different eigenspaces of U_Z for dimensions $d = 4$ to 8. We were not able to perform an exhaustive search for dimension 9 or higher.

In dimension $d = 6$ we found 984 numerical linearly dependent sets starting from a generic initial vector in the Zauner subspace. Among these, only 768 sets have the property

	$d=4$	$d=5$	$d=6$	$d=7$	$d=8$
$\mathcal{H}_1$	0	0	984	0	0
	0	0	(768)	0	0
$\mathcal{H}_\eta$	116	0	635,052	5,796	0
	(68)	0	(75,342)	(5,796)	0
$\mathcal{H}_{\eta^2}$	116	6,600	17,903,28	5796	24,756,984
	(68)	(4,200)	-	(5,796)	($\leq$766,080)

Table 2.3: Number of linear dependencies in a WH orbit where the initial vector is arbitrarily taken from each eigenspace of U_Z. The numbers in brackets are the number of sets (or an upper bound in one case) predicted from Theorem 2.2.

that they are invariant under the Zauner unitary, a condition for linear dependency in Theorem 2.2. This leaves 216 sets unaccounted for by our theorem. Interestingly, it is worth noting that these additional 216 sets are instead invariant under an order 6 symplectic unitary $U_{\mathcal{M}}$, where

$$\mathcal{M} = \begin{pmatrix} 3 & 8 \\ 4 & 11 \end{pmatrix}. \tag{2.81}$$

Each of the 36 vectors in the Weyl-Heisenberg orbit lies in 164 different linearly dependent sets, and each of the 984 sets clearly contains 6 vectors. In the language of geometry, we have 36 points and 984 hyperplanes in the complex projective space $\mathbb{CP}^5$, forming the configuration $(36_{164}, 984_6)$.

The 984 linearly dependent sets in dimension $d = 6$ themselves (for an initial vector in the Zauner subspace) can be grouped into orbits under the WH group (note that if a set is linearly dependent, then the set obtained by displacing it with the operator $D_{\mathbf{p}}$ for any $\mathbf{p}$ is also linearly dependent). We counted 27 orbits of length 36, and 1 orbit of length 12. The reason for the short orbit is because it contains sets that are invariant under the subgroup $\{\mathbb{1}, D_{24}, D_{42}\}$. Among these 28 orbits, 22 contain sets that are invariant under $U_{\mathcal{Z}}$, while the other 6 contain sets that are invariant under $U_{\mathcal{M}}$. The results are summarized in Table 2.4, where we have labeled the orbits from 1 to 28, with the first one being the short orbit, and the last 6 (23 to 28) are the ones invariant under $U_{\mathcal{M}}$.

In hope of finding nice structures as in dimension $d = 3$, we also studied the relationship among normal vectors of the 984 5-dimensional hyperplanes corresponding to the linearly dependent sets from Zauner subspace in $d = 6$. We performed an exhaustive search for

Orbit	Length	No. orbits under $U_{\mathcal{Z}}$	No. orbits under $\{\mathbb{1}, D_{24}, D_{42}\}$	No. ON quadruples
1	12	2	2	0
2-10	36	2	1	0
11	36	2	0	9
12-13	36	2	0	0
14-22	36	2	0	0
23-28	36	1	1	0

Table 2.4: Properties of WH orbits of linearly dependent sets with an initial vector in the Zauner subspace $\mathcal{H}_1$ in dimension $d = 6$.

orthogonalities between these vectors. No basis was found, nor was a MUB. However we did find over 20,000 orthogonal triples of normal vectors, i.e. sets of 3 normal vectors that are orthogonal to each other. If we start from a SIC fiducial instead of an arbitrary vector in the Zauner subspace, the linear dependency remains identical. However, in this case we found 216 additional orthogonal triples, and we also found 9 orthogonal quadruples. They all belong to the same orbit (of length 36) under the WH group.

In dimension $d = 9$, starting from an arbitrary vector $|\phi\rangle$ in the Zauner subspace, we found 79,767 sets of 9 linearly dependent vectors in the WH orbit of $|\phi\rangle$, 78,795 of which can be accounted for by Theorem 2.2. This number is too large for us to perform an exhaustive calculation of the scalar products between all pairs of normal vectors as in $d = 6$, but we did find interesting relations among some normal vectors, which will be discussed in the next section. The 79,767 sets can be grouped into orbits under the WH group. We found a total of 987 orbits: 984 of length 81, 2 of length 27, and 1 of length 9. Like in $d = 6$, they can be split into 2 groups: one group of 975 orbits that are exclusively invariant under $U_{\mathcal{Z}}$, and the other group of 12 orbits that are exclusively invariant under $U_{\mathcal{M}}$ (there are 186 orbits that are invariant under both), where $\mathcal{M}$ in odd dimensions $d = 3k$ takes the form

$$\mathcal{M} = \begin{pmatrix} k+1 & k \\ 2k & 2k+1 \end{pmatrix}. \tag{2.82}$$

If we start from a SIC fiducial in $d = 9$, we obtain an identical linear dependency structure. This suggests a distinction between SICs in dimension $d = 3$ and SICs in higher dimensions divisible by 3. The ‘‘special’’ SICs in $d = 3$ give rise to 12 linearly dependent

sets, while others produce only 3. In this sense, no SICs are ''special'' in dimension $d = 6$ and 9. However, we did find one other instance of a SIC fiducial vector giving more linear dependencies than other arbitrary vectors in the same eigenspace. This is the SIC fiducial in $\mathcal{H}_{\eta^2}$ in dimension $d = 8$ (this additional SIC fiducial seems to only exist in dimensions that are equal to 8 mod 9 [73]). In $d = 8$, this particular SIC fiducial exhibit 24,935,160 linearly dependent sets, while a generic vector in $\mathcal{H}_{\eta^2}$ produces 24,756,984 sets. This may be connected to the fact that the SIC has a larger automorphism group than an arbitrary vector in the same eigenspace. Comparing to the case in $d = 3$ where the Hesse configuration arises from the ''special'' SICs, one might ask whether there is a similar connection to elliptic curves in this family of SICs in dimensions $d = 9k + 8$.

2.3.4 Small SICs in dimensions $d = 6$ and 9

In the numerical investigation presented in the previous section, we intentionally left out some interesting observations in dimensions $d = 6$ and 9 for a separate discussion in this section. Among 984 vectors normal to the linear dependent sets generated from an arbitrary vector in the Zauner subspace (not necessarily a SIC fiducial) in $d = 6$, we found 30 sets of 4 normal vectors that form 2-dimensional SICs, i.e. within each set, the overlaps between the vectors are $1/\sqrt{3}$ and the vectors lie in a 2-dimensional subspace. This phenomenon also happens in dimension $d = 9$, where 3-dimensional SICs are found among 79,767 normal vectors. We refer to SICs of this kind as ''small SICs'', as their dimension is smaller than that of the embedding Hilbert space. Attempts to find small SICs in dimension $d = 12$ yielded no positive result so far, but we have not been able to perform an exhaustive search. In this section, we provide an explanation for the small SICs in $d = 6$. Small SICs in $d = 9$ are not yet fully understood.

We observed that every 2-dimensional SIC set found in $d = 6$ can be expressed as an orbit of a vector under the subgroup $\{\mathbb{1}, D_{03}, D_{30}, D_{33}\}$. In other words, the SICs take the form $\{|\psi\rangle, D_{03}|\psi\rangle, D_{30}|\psi\rangle, D_{33}|\psi\rangle\}$, where D_{ij} are the displacement operators defined in (2.32) for dimension $d = 6$. In the following theorem we will prove that for such a set to form a 2-dimensional SIC, $|\psi\rangle$ just needs to be any normalized eigenvector of $U_{\mathcal{Z}}$ that is not in the Zauner subspace. Normal vectors of linearly dependent sets containing 3 singlets in the case the initial vector lies in the Zauner subspace happen to meet this condition, as seen from the proof of Theorem 2.2.

Theorem 2.3. *In dimension $d = 6$, if $|\psi\rangle$ is an eigenvector of $U_{\mathcal{Z}}$, then the 4 vectors $|\psi\rangle, D_{03}|\psi\rangle, D_{30}|\psi\rangle$ and $D_{33}|\psi\rangle$ are equiangular. Furthermore, if $|\psi\rangle \in \mathcal{H}_\eta$ or $|\psi\rangle \in \mathcal{H}_{\eta^2}$, those 4 vectors span a 2-dimensional subspace and therefore constitute a SIC.*

Proof. Let λ be the eigenvalue of $U_{\mathcal{Z}}$ corresponding to $|\psi\rangle$, so that

$$U_{\mathcal{Z}} |\psi\rangle = \lambda |\psi\rangle \qquad |\psi\rangle = \lambda U_{\mathcal{Z}}^{\dagger} |\psi\rangle . \tag{2.83}$$

The first statement of the theorem is true because

$$\langle\psi| D_{\mathbf{p}} |\psi\rangle = \langle\psi| \lambda^* U_{\mathcal{Z}} D_{\mathbf{p}} U_{\mathcal{Z}}^{\dagger} \lambda |\psi\rangle = \langle\psi| D_{\mathcal{Z}\mathbf{p}} |\psi\rangle \tag{2.84}$$

and because the Zauner symplectic matrix $\mathcal{Z}$ simply permutes the three points 03, 30 and 33 in the discrete phase space according to Table 2.5.

$\mathbf{p}$	(0,3)	(3,0)	(3,3)
$\mathcal{Z}\mathbf{p}$	(3,3)	(0,3)	(3,0)

Table 2.5: Cyclic action of $\mathcal{Z}$ on points (0,3), (3,0) and (3,3).

In proving the second statement of the theorem, we make use of a square root of the Zauner unitary. Let $\mathcal{W}$ be the symplectic matrix given by

$$\mathcal{W} \equiv \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix} \qquad \mathcal{W}^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix} = \mathcal{Z} \tag{2.85}$$

Let $U_{\mathcal{W}}$ be the symplectic unitary corresponding to $\mathcal{W}$, with a phase chosen so that

$$U_{\mathcal{W}}^2 = U_{\mathcal{Z}}. \tag{2.86}$$

The structure of the eigenspaces of $U_{\mathcal{Z}}$ and $U_{\mathcal{W}}$ are described in Table 2.6, where $\omega = e^{2\pi i/6}$ and $\eta = e^{2\pi i/3} = \omega^2$. Next, we define three operators R, S and T as follows:

$$\begin{aligned} R &= (D_{03} + D_{30} + D_{33})/\sqrt{3} \\ S &= (D_{03} + \omega^2 D_{30} + \omega^4 D_{33})/\sqrt{3} \\ T &= (D_{03} + \omega^4 D_{30} + \omega^2 D_{33})/\sqrt{3}. \end{aligned} \tag{2.87}$$

Note that $\{|\psi\rangle, D_{03}|\psi\rangle, D_{30}|\psi\rangle, D_{33}|\psi\rangle\}$ and $\{|\psi\rangle, R|\psi\rangle, S|\psi\rangle, T|\psi\rangle\}$ have the same linear span. We will prove that $|\psi\rangle \in \mathcal{H}_\eta$ implies $S|\psi\rangle = 0$ and $R|\psi\rangle = |\psi\rangle$, and that $|\psi\rangle \in \mathcal{H}_{\eta^2}$ implies $T|\psi\rangle = 0$ and $R|\psi\rangle = -|\psi\rangle$. It will immediately follow that the linear span above is 2-dimensional.

Eigenspaces of $U_{\mathcal{Z}}$	$\mathcal{H}_1$ (Zauner)		$\mathcal{H}_\eta$		$\mathcal{H}_{\eta^2}$
Eigenvalue	1		η		η^2
Dimensionality	3		2		1
Eigenspaces of $U_{\mathcal{W}}$	$\mathcal{K}_1$	$\mathcal{K}_{\omega^3}$	$\mathcal{K}_\omega$	$\mathcal{K}_{\omega^4}$	$\mathcal{K}_{\omega^2}$
Eigenvalue	1	ω^3	ω	ω^4	ω^2
Dimensionality	2	1	1	1	1

Table 2.6: Structure of the eigenspaces of $U_{\mathcal{Z}}$ and its squareroot $U_{\mathcal{W}}$, with $\omega = e^{2\pi i/6}$ and $\eta = e^{2\pi i/3} = \omega^2$. Note that $U_{\mathcal{W}}$ is order 6, but it only has 5 eigenvalues (missing ω^5) because the eigenspace corresponding to eigenvalue 1 is degenerate.

From their definitions, one can verify the following properties of R, S and T:

$$S = T^\dagger, \qquad S^2 = T^2 = 0, \qquad R^2 = \mathbb{1}, \tag{2.88}$$

$$ST = \mathbb{1} + R, \qquad TS = \mathbb{1} - R. \tag{2.89}$$

Moreover, $ST/2$ and $TS/2$ are rank-3 projection operators that are orthogonal to each other. One can also verify the following commutation relations between R, S, T and $U_{\mathcal{W}}$:

$$U_{\mathcal{W}} R = R U_{\mathcal{W}}, \qquad U_{\mathcal{W}} S = \omega^4 S U_{\mathcal{W}}, \qquad U_{\mathcal{W}} T = \omega^2 T U_{\mathcal{W}}. \tag{2.90}$$

These equations tell us how R, S and T permute the eigenspaces of $U_{\mathcal{W}}$. For example, if $|\phi\rangle$ is an eigenvector of $U_{\mathcal{W}}$ with eigenvalue ω^2, then $U_W S |\phi\rangle = \omega^4 S U_W |\phi\rangle = S |\phi\rangle$, so $S |\phi\rangle$ is an eigenvector of $U_{\mathcal{W}}$ with eigenvalue 1. A full description of the action of S and T on the eigenspaces of $U_{\mathcal{W}}$ is shown in Figure 2.2 (the action of R is not shown because R commutes with $U_{\mathcal{W}}$ and simply leaves the eigenspaces invariant).

Let $|k_0\rangle$, $|k_1\rangle$, $|k_2\rangle$, $|k_3\rangle$ and $|k_4\rangle$ be non-zero eigenvectors of U_W belonging to the eigenspaces $\mathcal{K}_1$, $\mathcal{K}_\omega$, $\mathcal{K}_{\omega^2}$, $\mathcal{K}_{\omega^3}$ and $\mathcal{K}_{\omega^4}$ respectively. Except for $|k_0\rangle$, the rest of them are unique up to a scalar, because the corresponding eigenspaces are 1-dimensional. As seen from the diagram, we have $S |k_1\rangle = 0$. We are going to prove that $S |k_4\rangle = 0$, so that $S |\psi\rangle = 0$ for any $|\psi\rangle \in \mathcal{H}_\eta$.

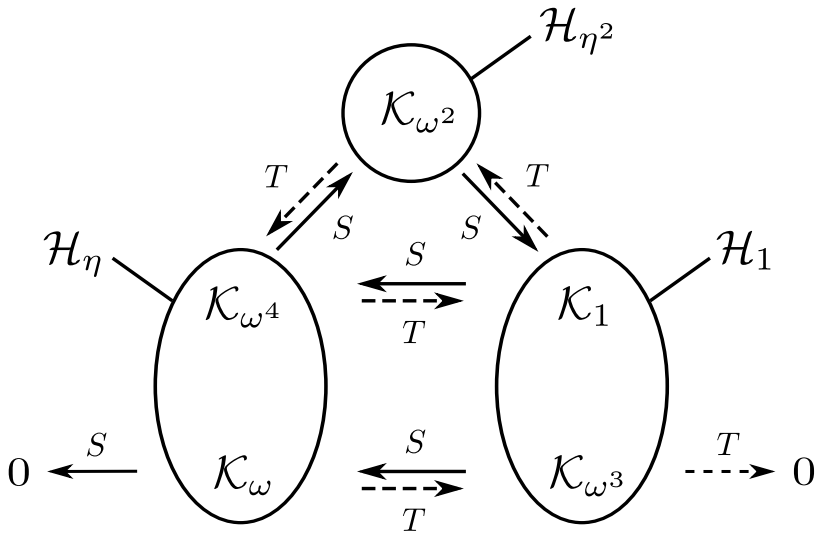

Figure 2.2: Action of S (solid arrow) and T (dashed arrow) on the eigenspaces of U_W. Note that $\mathcal{K}_1$ (2D) and $\mathcal{K}_{\omega^3}$ (1D) span the Zauner subspace $\mathcal{H}_1$ (3D), while $\mathcal{K}_{\omega^4}$ (1D) and $\mathcal{K}_\omega$ (1D) span $\mathcal{H}_\eta$ (2D), and $\mathcal{K}_{\omega^2}$ (1D) is identical to $\mathcal{H}_{\eta^2}$ (1D).

Suppose otherwise, that $S|k_4\rangle \neq 0$. It has to be the case that $S|k_0\rangle = 0$, because otherwise $S|k_0\rangle$ will be a non-zero vector in the 1-dimensional eigenspace $\mathcal{K}_{\omega^4}$, which implies $S|k_0\rangle = \alpha|k_4\rangle$ for some $\alpha \neq 0$, and therefore $S|k_4\rangle = \alpha^{-1}S^2|k_0\rangle = 0$, contradicting the assumption that $S|k_4\rangle \neq 0$. Since $S|k_4\rangle$ is a non-zero vector in the 1-dimensional eigenspace $\mathcal{K}_{\omega^2}$, we must also have $S|k_4\rangle = \beta|k_2\rangle$ for some $\beta \neq 0$, and therefore $S|k_2\rangle = \beta^{-1}S^2|k_4\rangle = 0$. So from the assumption that $S|k_4\rangle \neq 0$, we deduce that $0 = S|k_1\rangle = S|k_2\rangle = S|k_0\rangle$, which implies $0 = TS|k_1\rangle = TS|k_2\rangle = TS|k_0\rangle$, which in turn means that TS is orthogonal to the 4-dimensional subspace spanned by $\mathcal{K}_1$, $\mathcal{K}_\omega$ and $\mathcal{K}_{\omega^2}$. This contradicts the fact that $TS/2$ is a rank-3 projection operator.

Thus, we conclude that $S|k_4\rangle = 0$, and that $S|\psi\rangle = 0$ for any $|\psi\rangle \in \mathcal{H}_\eta$. The identity $R|\psi\rangle = |\psi\rangle$ immediately follows from $0 = TS|\psi\rangle = (\mathbb{1} - R)|\psi\rangle$. Note that $T|\psi\rangle \neq 0$ (because TS is orthogonal to ST) is a non-zero vector in $\mathcal{H}_1$. $T|\psi\rangle$ is not proportional to $|\psi\rangle$ because $T|\psi\rangle$ lies in $\mathcal{H}_1$ and $|\psi\rangle$ lies in $\mathcal{H}_\eta$. Therefore $|\psi\rangle$, $R|\psi\rangle$, $S|\psi\rangle$ and $T|\psi\rangle$ indeed span a 2-dimensional subspace.

It is a similar reasoning that leads to $T|k_2\rangle = 0$, which implies that $T|\psi\rangle = 0$ and

$R|\psi\rangle = -|\psi\rangle$ for any $|\psi\rangle \in \mathcal{H}_{\eta^2}$. We conclude that $\{|\psi\rangle, R|\psi\rangle, S|\psi\rangle, T|\psi\rangle\}$ spans a 2D subspace whenever $|\psi\rangle \in \mathcal{H}_\eta \cup \mathcal{H}_{\eta^2}$, thus proving the second statement of the theorem. □

We have provided an analytical explanation for why 2-dimensional small SICs occur in dimension $d = 6$. Unfortunately, this argument cannot be applied to explain the 3-dimensional small SICs found in $d = 9$. If one tries to use the construction described in the proof of Theorem 2.3 for the case $d = 9$, one would obtain 9 vectors which do not span a 3-dimensional subspace and whose overlaps are not constant (even though they only take two different values). The construction also fails to produce SICs in dimensions 12 and 15. We summarize the situation in Table 2.7, which shows the dimensionality of the subspace spanned by the $d^2/9$ vectors obtained using the construction in Theorem 2.3 for different eigenspaces of $U_{\mathcal{Z}}$ from which $|\psi\rangle$ is chosen.

	$d = 6$	$d = 9$	$d = 12$	$d = 15$
$\mathcal{H}_1$	4	8	12	15
$\mathcal{H}_\eta$	2	7	8	15
$\mathcal{H}_{\eta^2}$	2	6	8	10

Table 2.7: Dimensions of the spans of the orbits of $|\psi\rangle$ under the subgroup generated by D_{03} and D_{30} in higher dimensions for three eigenspaces of $U_{\mathcal{Z}}$ that $|\psi\rangle$ is chosen from.

Nevertheless, the fact remains that in dimension $d = 9$, instead of choosing a vector in $\mathcal{H}_\eta$ or $\mathcal{H}_{\eta^2}$ and following the construction in the proof of Theorem 2.3, if one starts from an initial vector $|\psi\rangle$ in the Zauner subspace (not necessarily a SIC fiducial), then one can always find 3-dimensional SICs among the normal vectors to the linearly dependent sets generated by $|\psi\rangle$. We have found 4 such small 3-dimensional SICs (there could possibly be more). Upon an inspection of the triple products, we noticed that all of these are unitarily equivalent to the "most exceptional" SIC, whose WH fiducial vector is $(0, 1, -1)/\sqrt{2}$ [66]. This construction is robust in the sense that the resulting small SICs are always the same, regardless of the choice of the initial vector $|\psi\rangle \in \mathcal{H}_1$. If this phenomenon repeats in higher dimensions it might open up an intriguing possibility that one might be able to get a constructive proof of SIC existence in this way. We did not succeed in finding small SICs in dimension $d = 12$, but an exhaustive search was out of computational power's reach.

Chapter 3

Galois-unitary symmetry

Contents

3.1 Motivations

In contrast to the previous chapter where our study was based on an almost 90-year-old group symmetry, in this chapter we focus on a novel symmetry, which is a generalization of anti-unitary symmetry.

Quantum physicists are very familiar with unitary transformations. One of the postulates in quantum mechanics states that the evolutions of quantum states are described by unitary transformations. All physical transformations must therefore be unitary. Unitary operators are defined to be operators that preserve the inner product between any two vectors in a Hilbert space:

$$\langle Ux, Uy\rangle = \langle x, y\rangle, \tag{3.1}$$

and therefore they also preserve the transition probabilities:

$$|\langle Ux, Uy\rangle| = |\langle x, y\rangle|\,. \tag{3.2}$$

Anti-unitary operators $\bar{U}$ are defined to satisfy

$$\langle \bar{U}x, \bar{U}y\rangle = \langle x, y\rangle^*, \tag{3.3}$$

where * represents complex conjugation. Although anti-unitaries are unphysical and less frequently seen, they also play important roles in physics, such as in representing time-reversal symmetry [4] and in entanglement theory [103]. One can clearly see from the definition that they also preserve transition probabilities. Together with unitaries, they form the only transformations of quantum states that have this probability preserving property, a milestone result from 1931 known as Wigner's theorem [4].

In a restricted region of a Hilbert space, however, it is possible to have symmetries beyond those of unitary or anti-unitary character. Such transformations were recently constructed by Appleby *et al* [71] to aid the search of SIC-POVMs. They are named Galois-unitaries (or g-unitaries for short), for they are unitary operators composed with Galois automorphisms of a chosen number field extension. The motivation under the construction of g-unitaries stems from an observation by Scott and Grassl [73] that every known analytical SIC fiducial (except the continuous family in dimension $d = 3$) can be

expressed in terms of radicals, implying that the corresponding Galois group is solvable. In Appleby *et al* [71], SIC fiducials were found to be eigenvectors of a family of g-unitaries. It was hoped that the additional g-unitary symmetry, on top of WH covariance and Zauner symmetry, would help reveal the solution for the SIC problem. Despite significant progresses, the SIC problem remains unsolved.

On the other hand, one notices that the Galois groups of cyclotomic field extensions (see Appendix A.1 for a review of Galois groups and cyclotomic fields) are quite simple. This is relevant to Mutually Unbiased Bases (to be defined in the next section) since all the components of standard MUB vectors indeed belong to a cyclotomic field. As we will see in Section 3.2, Clifford unitaries simply move one MUB vector to another and permute the bases according to Möbius transformations. However, not all permutations on the bases can be realized by Clifford unitaries. This is where g-unitaries come in to provide some of the missing symmetries. Started out as a toy model for SICs, our study of the roles of g-unitaries in the theory of mutually unbiased bases [3] led to a number of new findings. By extending the Clifford group with g-unitaries, we were able to solve the MUB-cycling problem in odd prime-power dimensions (see Section 3.7). We also provided a construction for a distinguished class of quantum states known as MUB-balanced states (see Section 3.9). Although our construction relies on a different technique, namely the g-unitary symmetry, it yields identical results to the construction by Amburg *et al* [6].

We want to note that g-unitay operators are not unitary in general, and therefore cannot be physically realized. However, it is possible to simulate them using unitary operators in a larger Hilbert space. We propose such a simulation scheme in Section 3.6.

3.2 Mutually unbiased bases

In a d-dimensional Hilbert space, two orthonormal bases $\{e_i\}$ and $\{e'_i\}$ are called Mutually Unbiased Basess (MUBs) if

$$\left|\langle e_i|e'_j\rangle\right| = \frac{1}{\sqrt{d}} \tag{3.4}$$

for any $i, j = 0, 1, ..., d-1$. One can see that if a quantum state is completely specified from the measurement outcome probabilities in one basis (i.e. it is one of the basis vectors), then the outcome probabilities from the measurement in the other basis must be a uniform distribution. This is very much like measuring with the position and momentum operators, where learning the precise location of a particle erases all information about its momentum and vice versa. Mutually unbiased bases can therefore be considered as a finite-dimensional

analogue of complementary observables. They play important roles not only in foundational studies such as complementarity in quantum mechanics [104], but also in areas in quantum information such as quantum state estimation [105] and quantum cryptography [13] (we have provided only a few milestone references).

If the Hilbert space has d dimensions, there can be at most $d+1$ bases that are mutually unbiased to each other [105]. These are said to form a complete (or full) set of MUBs, and we will use the acronym MUBs to refer to such a complete set only. It has been shown by Ivonovic [106] that complete sets of MUBs can be constructed in prime dimensions. This construction was later generalized to prime power dimensions by Wootters and Fields [105]. The existence of complete sets of MUBs in general is still an open question. Even in the lowest non-prime-power dimension $d = 6$, although it has been found unlikely that a complete set of MUBs could exist, a non-existence proof has not been reached despite numerous research efforts [107–113].

There are many known techniques for constructing a complete set of MUBs, for example by finding maximal Abelian subgroups of the Weyl-Heisenberg group, by taking the eigenbases of unitary operators constructed from the shift operator X and the clock operator Z, by using Hadamard matrices, and by taking the WH orbit of an Alltop fiducial [32]. Here we describe a Clifford-based construction [30], which produces the same set of MUBs that originally appeared in Wootters and Fields' paper [105]. We will refer to this particular set as the standard set of MUBs. All MUBs in the thesis are implicitly understood as standard sets of MUBs, unless specifically noted otherwise.

We now restrict ourselves to the case $d = p^n$ is an odd prime power. Making use of the existence of the finite field $\mathbb{F}_d$ when d is a prime power, one can provide a faithful unitary representation U_S of symplectic matrices $S \in \mathrm{SL}(2, \mathbb{F}_d)$. We will appeal to the particular representation described by (A.41) in Appendix A.2 (see [30] for more details). Note that this is the representation for the restricted Galoisian Clifford group, which is not the same as the ordinary Clifford group used in Chapter 2.

Consider the following $d+1$ matrices in $\mathrm{SL}(2, \mathbb{F}_d)$

$$\begin{aligned} S_b &= \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \quad \text{for} \quad b \in \mathbb{F}_d \\ S_\infty &= \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \quad \text{for} \quad b = \infty. \end{aligned} \tag{3.5}$$

If we transform the standard basis by the symplectic unitaries U_{S_b} we will obtain $d+1$ bases in a full set of MUB. More explicitly, let $|v\rangle$ denote the standard basis vectors, and

let us define

$$|b, v\rangle = U_{S_b} |v\rangle \tag{3.6}$$

for all $b \in \mathbb{F}_d \cup \{\infty\}$ and $v \in \mathbb{F}_d$, then the claim is that $|b, v\rangle$ are $d(d+1)$ vectors in a complete set of MUBs, where b labels the bases, and v labels the vectors within each basis. To see why, let us first note that for any symplectic matrix

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \det(S) = 1 \tag{3.7}$$

with $\beta \neq 0$, it directly follows from (A.41) that

$$|\langle v| U_S |v'\rangle| = \frac{1}{\sqrt{d}} \tag{3.8}$$

for all standard basis vectors $|v\rangle$ and $|v'\rangle$. One can verify that for any $b, b' \in \mathbb{F}_d \cup \{\infty\}$ and $b \neq b'$, the β-entry of $S_b^{-1} S_{b'}$ is non-zero, therefore

$$\begin{aligned} |\langle b, v|b', v'\rangle| &= \left|\langle v| U_{S_b}^\dagger U_{S_{b'}} |v'\rangle\right| \\ &= \left|\langle v| U_{S_b^{-1}} U_{S_{b'}} |v'\rangle\right| \\ &= \left|\langle v| U_{S_b^{-1} S_{b'}} |v'\rangle\right| \\ &= \frac{1}{\sqrt{d}} \end{aligned} \tag{3.9}$$

so that the two bases b and b' are indeed mutually unbiased.

We would like to point out that it also directly follows from the representation in (A.41) that when $\beta = 0$, U_S simply permutes vectors in the standard basis and adds phases to them. In general (for any value of β), for any symplectic S in the form given by (3.7) one can explicitly work out the action of U_S on the MUB vectors $|b, v\rangle$ to be [30]

$$U_S |b, v\rangle \doteq \begin{cases} \left|\frac{\alpha b+\beta}{\gamma b+\delta}, \frac{v}{\gamma b+\delta}\right\rangle & \text{if } b \neq \infty, \gamma b + \delta \neq 0 \\ |\infty, -\gamma v\rangle & \text{if } b \neq \infty, \gamma b + \delta = 0 \\ \left|\frac{\alpha}{\gamma}, \frac{v}{\gamma}\right\rangle & \text{if } b = \infty, \gamma \neq 0 \\ |\infty, \delta v\rangle & \text{if } b = \infty, \gamma = 0 \end{cases} \tag{3.10}$$

where "$\doteq$" means "equals up to a phase". One now sees the reason behind the use of the symbol ∞: it allows us to summarize the permuting actions of U_S on the bases by the Möbius transformation [114]

$$b \quad \rightarrow \quad \frac{\alpha b + \beta}{\gamma b + \delta}. \tag{3.11}$$

Remark. The faithful unitary representation we have is for symplectic matrices $S \in \mathrm{SL}(2, \mathbb{F}_d)$, which have $\det S = \alpha\delta - \beta\gamma = 1$. However, a general Möbius transformation only requires that $\alpha\delta - \beta\gamma \neq 0$, which is the requirement for the general linear group $\mathrm{GL}(2, \mathbb{F}_d)$. Note that if we scale α, β, γ and δ by a constant factor, the Möbius transformation in (3.11) remains the same. Möbius transformations are therefore represented by the quotient group of GL, where any two elements G and G' in GL are considered equivalent if they are related by $G' = cG$ for some constant $c \in \mathbb{F}_d$. This is called the projective general linear group $\mathrm{PGL}(2, \mathbb{F}_d)$. In a similar manner, the special linear group $\mathrm{SL}(2, \mathbb{F}_d)$ gives rise to the projective special linear group $\mathrm{PSL}(2, \mathbb{F}_d)$, which is a proper subgroup of PGL. The orders of these groups are provided in Table 3.1.

Notation	Name	Order
$\mathrm{GL}(2, \mathbb{F}_d)$	general linear group	$d(d-1)(d^2-1)$
$\mathrm{PGL}(2, \mathbb{F}_d)$	projective general linear group	$d(d^2-1)$
$\mathrm{SL}(2, \mathbb{F}_d)$	special linear group	$d(d^2-1)$
$\mathrm{PSL}(2, \mathbb{F}_d)$	projective special linear group	$d(d^2-1)/2$

Table 3.1: The orders of the general linear group and its various subgroups.

We observe that if an element G in $\mathrm{GL}(2, \mathbb{F}_d)$

$$G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \det(G) \neq 0 \tag{3.12}$$

has determinant $\det(G) = \Delta$ which is a quadratic residue in $\mathbb{F}_d$, meaning that $\Delta = x^2$ for some non-zero $x \in \mathbb{F}_d$, we can write G as

$$G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} = x \begin{pmatrix} \alpha x^{-1} & \beta x^{-1} \\ \gamma x^{-1} & \delta x^{-1} \end{pmatrix} = xS, \tag{3.13}$$

where S is clearly an element of $\mathrm{SL}(2, \mathbb{F}_d)$. Since G and S in the above expression are equivalent, they correspond to the same element in PGL. Therefore, elements in GL whose

determinants are quadratic residues do not add to PGL beyond the contribution from SL. But elements whose determinants are quadratic non-residues do. The message here is that symplectic unitaries permutes MUB bases according to Möbius transformations, but not all Möbius transformations can be realized by these permutations. We will later see that Galois-unitaries come in to help supply the missing transformations (all of them in certain cases, and some of them in other cases).

3.3 The Clifford group extended by g-unitaries

We again want to remind that throughout this chapter, we exclusively use the term Clifford group to refer to the restricted Galoisian Clifford group [30], as opposed to the ordinary version used in the previous chapter. The symplectic group $\mathrm{SL}(2,\mathbb{F}_d)$ is one key ingredient in the construction of the Clifford group. In Appendix A.2 we describe a faithful unitary representation of $\mathrm{SL}(2,\mathbb{F}_d)$. Here, the question of interest is: is it possible to extend this representation to also include all linear transformations G in the discrete phase space that have determinant $\Delta = \det(G) \neq 1$? According to (A.33), such a transformation scales the symplectic area by a factor of Δ. In order for the group law in (A.31) to hold, the representation of G should also transform $\omega \mapsto \omega^{\Delta}$, otherwise it will not be an automorphism of the Weyl-Heisenberg group. This is where Galois automorphisms come into the picture (see Appendix A.1.2 for an introduction to Galois automorphisms), as they do precisely what we need:

$$g_\Delta : \omega \mapsto \omega^{\Delta}. \tag{3.14}$$

In the special case when $\Delta = \det(G) = -1$, G is called an anti-symplectic matrix in $\mathrm{ESL}(2,\mathbb{F}_d)$, and it is represented by an anti-unitary transformation, i.e. an ordinary unitary transformation following complex conjugation. The Clifford group extended by these anti-unitaries is called the extended Clifford group, which was well studied in [76].

We now consider the case when G is an arbitrary element of $\mathrm{GL}(2,\mathbb{F}_d)$, i.e. a 2×2 matrix with determinant $\Delta \neq 0$ (so that it is invertible) over the field $\mathbb{F}_d$. Although it is possible to analyze the most general case of odd prime power dimensions right away, we would like to start with the simpler case when $d = p$ is an odd prime to explain the core concepts first, then add the technical complications of the general case $d = p^n$ later.

3.3.1 In odd prime dimensions

Let the dimension $d = p$ be an odd prime, and let G be any element in $\mathrm{GL}(2, \mathbb{F}_d)$

$$G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{3.15}$$

where $\alpha, \beta, \gamma, \delta \in \mathbb{F}_d$ and $\Delta \equiv \det(G) \neq 0$. We can always decompose G into

$$G = SK_\Delta, \tag{3.16}$$

where, for any $x \in \mathbb{F}_d$, we define $K_x \in \mathrm{GL}(2, \mathbb{F}_d)$ to be

$$K_x \equiv \begin{pmatrix} 1 & 0 \\ 0 & x \end{pmatrix}, \tag{3.17}$$

and

$$S = GK_\Delta^{-1} = \begin{pmatrix} \alpha & \beta\Delta^{-1} \\ \gamma & \delta\Delta^{-1} \end{pmatrix} \tag{3.18}$$

Note that S has determinant 1, so $S \in \mathrm{SL}(2, \mathbb{F}_d)$ and can be represented by the unitary U_S given in (A.35). The matrix K_Δ has determinant Δ and will be represented by the Galois automorphism g_Δ:

$$K_\Delta = \begin{pmatrix} 1 & 0 \\ 0 & \Delta \end{pmatrix} \quad \rightarrow \quad g_\Delta : \omega \mapsto \omega^\Delta. \tag{3.19}$$

Therefore G can now be represented by a Galois-unitary (or g-unitary for short) U_G:

$$G = SK_\Delta \quad \rightarrow \quad U_G \equiv U_S g_\Delta. \tag{3.20}$$

This concept of a g-unitary was introduced in [71] as a generalization to an anti-unitary transformation, which can be realized by first applying complex conjugation, and then applying a unitary transformation. Similarly, to realize a g-unitary, one first applies a Galois automorphism, and then performs a unitary transformation.

It is worth emphasizing that U_G is not a unitary operator except when $\det(G) = 1$. It is not even a linear operator in general, so it cannot be expressed in a matrix form. The action of U_G on a vector in the Hilbert space is

$$U_G |\psi\rangle = U_S g_\Delta(|\psi\rangle), \tag{3.21}$$

where $g_\Delta(|\psi\rangle)$ denotes the vector obtained by applying g_Δ to the components of $|\psi\rangle$ in the standard basis.

Furthermore, g-unitaries are only defined to act on vectors (or matrices) whose components belong to the cyclotomic field $\mathbb{Q}(\omega)$. Because of this restriction, we have to verify that these added Galois automorphisms can act on the whole Clifford group. Looking at the representation in (A.35) one might ask whether the overall factor $e^{i\phi}/\sqrt{p}$ is in the cyclotomic field. Let us recall the Gaussian sum [115]

$$\sum_{x=0}^{p-1} \omega^{x^2} = \sum_{x\in Q} \omega^x - \sum_{x\in N} \omega^x = \begin{cases} \sqrt{p} & \text{if } p = 4k+1 \\ i\sqrt{p} & \text{if } p = 4k+3. \end{cases} \tag{3.22}$$

It follows that the factors $e^{i\phi}/\sqrt{p}$ in (A.35) belong to the cyclotomic field, and therefore so do the entries of the symplectic unitaries U_S. We are now allowed to use symplectic unitaries along with the Galois automorphisms of the cyclotomic field extension to represent $\mathrm{GL}(2,\mathbb{F}_d)$. This representation is faithful, as shown in the following lemma.

Lemma 3.1. *Let the dimension $d = p$ be an odd prime and let G_1 and G_2 be any two elements of $\mathrm{GL}(2,\mathbb{F}_d)$. It then holds that*

$$U_{G_1} U_{G_2} = U_{G_1 G_2}. \tag{3.23}$$

Proof. Explicitly, let

$$G_1 = \begin{pmatrix} \alpha_1 & \beta_1 \\ \gamma_1 & \delta_1 \end{pmatrix} \qquad G_2 = \begin{pmatrix} \alpha_2 & \beta_2 \\ \gamma_2 & \delta_2 \end{pmatrix}, \tag{3.24}$$

and let us write them in the same form as (3.16):

$$G_1 = S_1 K_1 \qquad G_2 = S_2 K_2. \tag{3.25}$$

Note that K_1 and K_2 are short notations for K_{Δ_1} and K_{Δ_2}. Then we can write

$$G_1 G_2 = S_1 K_1 S_2 K_2 = S_1 (K_1 S_2 K_1^{-1}) K_1 K_2, \tag{3.26}$$

where

$$K_1 S_2 K_1^{-1} = \begin{pmatrix} \alpha_2 & \beta_2 \Delta_1^{-1} \\ \gamma_2 \Delta_1 & \delta_2 \end{pmatrix}, \tag{3.27}$$

is symplectic and is therefore represented by a symplectic unitary $U_{K_1S_2K_1^{-1}}$. On the other hand, in the g-unitary representation we have

$$U_{G_1}U_{G_2} = U_{S_1}g_1(U_{S_2}g_2) = U_{S_1}g_1(U_{S_2})g_1g_2, \tag{3.28}$$

where g_1 and g_2 are short notations for g_{Δ_1} and g_{Δ_2}. From (3.22) it follows that

$$g_1(e^{i\phi}/\sqrt{p}) = \begin{cases} e^{i\phi}/\sqrt{p} & \text{if } \Delta_1 \in \mathbf{Q} \\ -e^{i\phi}/\sqrt{p} & \text{if } \Delta_1 \in \mathbf{N} \end{cases} \tag{3.29}$$

In addition to the fact that $l(-\beta\Delta_1^{-1}) = l(-\beta)l(\Delta_1^{-1})$, which equals to $l(-\beta)$ if $\Delta_1 \in \mathbf{Q}$, and $-l(-\beta)$ if $\Delta_1 \in \mathbf{N}$, and in view of the representation given in (A.35), we obtain

$$g_1(U_{S_2}) = U_{K_1S_2K_1^{-1}}. \tag{3.30}$$

Given that the representation of SL is faithful, (3.28) can be rewritten as

$$U_{G_1}U_{G_2} = U_{S_1}U_{K_1S_2K_1^{-1}}g_1g_2 = U_{S_1(K_1S_2K_1^{-1})K_1K_2} = U_{G_1G_2} \tag{3.31}$$

as desired.

□

Remark. We want to remind that the action of g-unitaries is restricted to vectors in the Hilbert space whose components belong to the cyclotomic field $\mathbb{Q}(\omega)$. Although this set is dense within the Hilbert space, one should not be tempted to play the usual trick of taking limits because these transformations are not continuous, as will be demonstrated below. The good news, however, is that this restricted subset of the Hilbert space g-unitaries can act on includes all MUB vectors, since the components of the standard basis vectors are in the field, and since every other MUB vector can be obtained from the standard basis by a Clifford unitary, whose entries are also in the field. It also includes all vectors that can be obtained from the standard basis by applying a larger set of transformations known as the Clifford hierarchy, which is large enough for universal quantum computation [116].

The Hilbert space norm is preserved by g-unitaries only if it is rational, which need not always be the case. This means that g-unitaries are wildly discontinuous. As an example, let us consider the g-unitary consisting of only the Galois automorphism $g_2 : \omega \mapsto \omega^2$ in dimension $d = 5$, and its action on the (unnormalized) vector

$$|\psi\rangle = \begin{pmatrix} \omega^2+\omega^3 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} \quad \to \quad g_2(|\psi\rangle) = \begin{pmatrix} \omega^4+\omega \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}. \tag{3.32}$$

Both of these are real vectors. So they can be approximated by rational vectors, which are left invariant by the g-unitary. However $|\psi\rangle$ has clearly been moved quite a distance in the Hilbert space by g_2.

G-unitaries do, however, preserve a norm that is the product of the scalar product of two vectors with all its $d-2$ Galois conjugates [117]. In mathematics this is called the field norm. It is unknown whether the field norm has any physical meaning in this case.

3.3.2 In odd prime power dimensions

Now that the concept of g-unitaries has been explained, we move on to the general case of odd prime power dimensions $d = p^n$. In this case, complications come from the fact that the finite field $\mathbb{F}_d$ of order d no longer contains only ordinary integers like the prime field $\mathbb{Z}_p$. Materials on finite fields (see Appendix A.1.4) and on the Galoisian Weyl-Heisenberg and Clifford groups in odd prime power dimensions (see Appendix A.2.2) will be assumed.

We start with the first complication that the definition of a g-unitary U_G in (3.20) no longer makes sense in general. This is because one cannot define the Galois automorphism $g_x : \omega \mapsto \omega^x$ for all elements $x \in \mathbb{F}_d$: one can only raise ω to a power which is an integer, not an abstract element of a finite field. In order to still use (3.20), we now have to impose a restriction on G, namely its determinant Δ must belong to the ground field $\mathbb{F}_p$ (i.e. integers mod p). All such G form a subgroup that we will denote by $\mathrm{GL}_p(2, \mathbb{F}_d)$.

Definition. $\mathrm{GL}_p(2, \mathbb{F}_d)$ is defined to be the subgroup of $\mathrm{GL}(2, \mathbb{F}_d)$ consisting of 2×2 matrices whose (non-zero) determinants are in the ground field $\mathbb{F}_p$.

We can now safely use (3.20) to define U_G for any $G \in \mathrm{GL}_p(2, \mathbb{F}_d)$. Hence the case of prime power dimensions (where the power $n > 1$) differs from the prime dimensional case in that the g-extended Clifford group only includes a proper subgroup of GL. Another difference is that we should now use the more general formula (A.41) for the unitary representation U_S of a symplectic S:

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \to \quad U_S = \begin{cases} l(\alpha) \sum_{x \in \mathbb{F}_d} \omega^{\mathrm{tr}(\alpha\gamma x^2/2)} |\alpha x\rangle \langle x| & \text{if } \beta = 0 \\ h(\beta) \sum_{x,y \in \mathbb{F}_d} \omega^{\mathrm{tr}(\frac{\delta x^2 - 2xy + \alpha y^2}{2\beta})} |x\rangle \langle y| & \text{if } \beta \neq 0, \end{cases} \tag{3.33}$$

where we have defined $h(x) = (-i)^{-n(p+3)/2} l(-x)/\sqrt{d}$.

The main result of this section is the faithfulness of the above representation described by the following theorem.

Theorem 3.2. *Let the dimension $d = p^n$ be an odd prime power, where n is odd, and let G_1 and G_2 be any two elements of $\mathrm{GL}_p(2, \mathbb{F}_d)$. Then it holds that*

$$U_{G_1} U_{G_2} = U_{G_1 G_2}. \tag{3.34}$$

Proof. The proof is similar to the proof of Lemma 3.1, so we will not repeat the set-up here. The only thing we need to do is to re-verify (3.30):

$$g_1(U_{S_2}) = U_{K_1 S_2 K_1^{-1}}. \tag{3.35}$$

First, recall the basic fact that $\mathbb{F}_p = \{x \in \mathbb{F}_d : x^p = x\}$. Let θ be a primitive element of $\mathbb{F}_d$. One can then show that

$$\theta_p \equiv \theta^{1+p+\cdots+p^{n-1}} \tag{3.36}$$

belongs to $\mathbb{F}_p$ by verifying that $\theta_p^p = \theta_p$, and that θ_p is a primitive element of $\mathbb{F}_p$. We can then write $\Delta_1 = \theta_p^u$, and $g_1 = g_{\theta_p}^u$, for some integer $0 \leq u \leq p-2$. Note that Δ_1 is a quadratic residue in $\mathbb{F}_p$ if and only if u is even.

Since $h(\beta)^2$ is rational while $h(\beta)$ is irrational, and since g_{θ_p} generates the Galois group, we must have

$$g_{\theta_p}\left(h(\beta)\right) = -h(\beta), \tag{3.37}$$

which implies

$$g_{\Delta_1}\left(h(\beta)\right) = (-1)^u h(\beta). \tag{3.38}$$

As n is odd, we can use Lemma 1 in [30] to write

$$g_{\Delta_1}\left(h(\beta)\right) = h(\Delta_1 \beta). \tag{3.39}$$

Since $l(\alpha)$ is either 1, -1, or 0, and is therefore rational, it is invariant under g_{Δ_1}. Thus

$$g_{\Delta_1} U_{S_2} = \begin{cases} l(\alpha) \sum_{x \in \mathbb{F}_d} \omega^{\mathrm{tr}(\Delta_1 \alpha \gamma x^2/2)} \left|\alpha x\right\rangle \left\langle x\right| & \text{if } \beta = 0 \\ h(\Delta_1 \beta) \sum_{x,y \in \mathbb{F}_d} \omega^{\mathrm{tr}\left(\frac{\Delta_1(\delta x^2 - 2xy + \alpha y^2)}{2\beta}\right)} \left|x\right\rangle \left\langle y\right| & \text{if } \beta \neq 0, \end{cases} \tag{3.40}$$

which validates (3.35).

□

Remark. It can be seen from the proof above that when n is even, we have $U_{G_1} U_{G_2} = \pm U_{G_1 G_2}$. The representation in this case is therefore ‘‘close to faithful’’ in a sense.

3.4 Arithmetic of g-unitaries

This section provides some basic arithmetic of g-unitaries. The derivations are straightforward, but they might help readers better understand how to handle these non-linear g-unitary operators. In any case, it would be useful to have a list of formulae that we can readily use in later calculations. Throughout this section we will always use the notation U_G to refer to the g-unitary representing an element $G \in \mathrm{GL}_p(2, \mathbb{F}_d)$

$$G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \qquad \alpha, \beta, \gamma, \delta \in \mathbb{F}_d \qquad \Delta \equiv \det(G) \in \mathbb{F}_p \backslash \{0\}, \tag{3.41}$$

and decompose U_G into a Galois automorphism g_Δ followed by a symplectic unitary U_S

$$U_G = U_S g_\Delta, \tag{3.42}$$

where $S = GK_{\Delta^{-1}}$ is an element of $\mathrm{SL}(2, \mathbb{F}_d)$, with K_Δ being a matrix of determinant Δ as defined in (3.17). Where there is no ambiguity, we will drop the subscript Δ and write g for the Galois automorphism for short. It should also be noted that if we omit the parentheses specifying what g acts on, it should be understood that g acts on everything to its right in the expression, for example:

$$g_1 A g_2 B = g_1(A g_2(B)) = g_1(A) g_1 g_2(B). \tag{3.43}$$

3.4.1 Action on vectors and matrices

We know how a Galois automorphism g_Δ transforms a number in the cyclotomic field $\mathbb{Q}(\omega)$: it replaces every p-th root of unity ω by ω^Δ in that number's decomposition into powers of ω. For a matrix (or a vector), we require all its entries (or components) in the standard basis to be in the cyclotomic field in order to define the action of a Galois automorphism on it. When this condition is met, the action is defined entry-wise:

$$(g(A))_{j,k} = g(A_{j,k}). \tag{3.44}$$

Accordingly, the action of a g-unitary on a matrix (or a vector) A is:

$$U_G A = U_S g(A). \tag{3.45}$$

3.4.2 Composition and power

Let U_{G_1} and U_{G_2} be two g-unitaries. We want to find out the resulting action of applying them one after another. Since these are operators, it is the safest practice to apply them to an arbitrary matrix A

$$\begin{aligned} U_{G_1}U_{G_2}A &= U_{S_1}g_1U_{S_2}g_2A \\ &= U_{S_1}g_1(U_{S_2}g_2(A)) \\ &= U_{S_1}g_1(U_{S_2})g_1(g_2(A)), \end{aligned} \tag{3.46}$$

and remove A in the end to get

$$U_{G_1}U_{G_2} = U_{S_1}g_1(U_{S_2})g_1g_2. \tag{3.47}$$

Similarly, the composition of more than two g-unitaries is given by

$$U_{G_1}U_{G_2}\cdots U_{G_k} = U_{S_1}g_1(U_{S_2})g_1g_2(U_{S_3})\cdots g_1g_2...g_k. \tag{3.48}$$

Setting all g-unitaries identical in the previous equation results in the power formula

$$U_G^k = U_Sg(U_S)\cdots g^{k-1}(U_S)g^k. \tag{3.49}$$

If the dimension d is a prime number, we have (by Fermat's little theorem)

$$\Delta^{d-1} = 1 \pmod{d}. \tag{3.50}$$

This means $g_\Delta^{d-1} : \omega \mapsto \omega^{\Delta^{d-1}} = \omega$ is the identity mapping, and therefore

$$U_G^{d-1} = U_Sg(U_S)\cdots g^{d-2}(U_S) \tag{3.51}$$

is an ordinary unitary.

3.4.3 The inverse

The inverse of a g-unitary $U_G = U_Sg$ is given by

$$U_G^{-1} = g^{-1}U_S^{-1} = g^{-1}(U_S^{-1})g^{-1}, \tag{3.52}$$

where the inverse of a Galois automorphism g_Δ is given by

$$g_\Delta^{-1} = g_{\Delta^{-1}}, \tag{3.53}$$

so that $g_\Delta g_\Delta^{-1} = g_\Delta^{-1} g_\Delta$ is the identity mapping. One can prove (3.52) by verifying that $U_G^{-1} U_G = U_G U_G^{-1} = \mathbb{1}$.

When the power n is odd, the representation of U_G is faithful (see Theorem 3.2) and another expression for the inverse of U_G is

$$U_G^{-1} = U_{G^{-1}}, \tag{3.54}$$

because $U_G U_{G^{-1}} = U_{GG^{-1}} = \mathbb{1}$.

3.4.4 Conjugate transposition and the adjoint

Since the action of a Galois automorphism g on a vector or matrix A is defined entry-wise, it commutes with the transposition on A. Meanwhile, the Galois group for the cyclotomic extension is abelian, therefore g also commutes with all other Galois automorphisms in the group including the complex conjugation. This means

$$(g(A))^\dagger = g(A^\dagger). \tag{3.55}$$

The conjugate transposition of $U_G A$, where A is a matrix or a vector over the cyclotomic field $\mathbb{Q}(\omega)$, can be calculated as follows:

$$\begin{aligned} (U_G A)^\dagger &= (U_S g(A))^\dagger \\ &= (g(A))^\dagger U_S^\dagger \\ &= g(A^\dagger) U_S^\dagger, \end{aligned} \tag{3.56}$$

or in Dirac notation, when applied to state vectors:

$$(U_G \left|\psi\right\rangle)^\dagger = g(\left\langle\psi\right|) U_S^\dagger. \tag{3.57}$$

Definition. As in [71], we define the adjoint of a g-unitary U_G to be the unique operator $U_G^\dagger$ such that

$$\langle U_G x, y\rangle = g(\langle x, U_G^\dagger y\rangle) \qquad \forall x, y \in \mathbb{Q}(\omega)^d. \tag{3.58}$$

This is a natural generalization from the case of anti-linear operators [71], where their adjoints are defined so that $\langle Lx, y\rangle = (\langle x, L^\dagger y\rangle)^*$, with * denoting complex conjugation. It turns out that the adjoint of a g-unitary U_G is exactly its inverse, since

$$\begin{aligned} g\langle x, U_G^{-1} y\rangle &= g\langle x, g^{-1} U_S^\dagger y\rangle \\ &= g\left(\left\langle x\right|\right) g(g^{-1} U_S^\dagger \left|y\right\rangle) \\ &= g\left(\left\langle x\right|\right) U_S^\dagger \left|y\right\rangle \\ &= \langle U_G x, y\rangle. \end{aligned} \tag{3.59}$$

If $d = p^n$ and n is odd, we further have

$$U_G^\dagger = U_G^{-1} = U_{G^{-1}}. \tag{3.60}$$

3.4.5 Conjugate action on matrices and displacement operators

Let A be an arbitrary $d \times d$ matrix over the cyclotomic field $\mathbb{Q}(\omega)$. Its conjugation by a g-unitary U_G is given by

$$U_G A U_G^{-1} = U_S g(A) U_S^{-1}, \tag{3.61}$$

which can be verified straightforwardly.

Next, we are going to calculate the conjugation of a displacement operator $D_{\mathbf{p}}$ by U_G. We will show that

$$U_G D_{\mathbf{p}} U_G^{-1} = D_{G\mathbf{p}}. \tag{3.62}$$

We first need to know how a Galois automorphism acts on $D_{\mathbf{p}}$. From the explicit form of the shift and the phase operator, one can see that

$$g_\Delta(X) = X \qquad g_\Delta(Z) = Z^\Delta, \tag{3.63}$$

which implies

$$\begin{aligned} g_\Delta(D_{\mathbf{p}}) &= g(\omega^{\frac{p_1 p_2}{2}}) g(X^{p_1}) g(Z^{p_2}) \\ &= \omega^{\frac{\Delta p_1 p_2}{2}} X^{p_1} Z^{\Delta p_2} \\ &= D_{K_\Delta \mathbf{p}}. \end{aligned} \tag{3.64}$$

Therefore

$$\begin{aligned} U_G D_{\mathbf{p}} U_G^{-1} &= U_S g D_{\mathbf{p}} g^{-1} U_S^{-1} \\ &= U_S g(D_{\mathbf{p}}) g(g^{-1} U_S^{-1}) \\ &= U_S D_{K_\Delta \mathbf{p}} U_S^{-1} \\ &= D_{S K_\Delta \mathbf{p}} \\ &= D_{G\mathbf{p}}. \end{aligned} \tag{3.65}$$

Conjugations of phase point operators $A_{\mathbf{p}}$ used in the discrete Wigner function can be similarly calculated. Recall their definition

$$A_{\mathbf{p}} = D_{\mathbf{p}} A_0 D_{\mathbf{p}}^\dagger, \tag{3.66}$$

where

$$A_0 = \frac{1}{d}\sum_{\mathbf{p}} D_{\mathbf{p}}. \tag{3.67}$$

It is clear that A_0 is left invariant by the conjugation:

$$U_G A_0 U_G^{-1} = \frac{1}{d}\sum_{\mathbf{p}} D_{G\mathbf{p}} = A_0. \tag{3.68}$$

Other phase point operators $A_{\mathbf{p}}$ are transformed into

$$\begin{aligned} U_G A_{\mathbf{p}} U_G^{-1} &= (U_G D_{\mathbf{p}} U_G^{-1})(U_G A_0 U_G^{-1})(U_G D_{\mathbf{p}}^{\dagger} U_G^{-1}) \\ &= D_{G\mathbf{p}} A_0 D_{G\mathbf{p}}^{\dagger} \\ &= A_{G\mathbf{p}}. \end{aligned} \tag{3.69}$$

3.5 Geometric interpretation

3.5.1 Complementarity polytopes

In this section we would like to introduce a class of geometrical objects closely related to MUBs that can help explain the role of g-unitaries from a geometrical perspective. These are called complementarity polytopes and they have been well studied in [118]. The space under consideration here is called the Bloch space, which will be defined shortly.

We start from the set of $d \times d$ Hermitian matrices of unit trace. This set includes all quantum states represented by density matrices, and it also contains matrices that are not quantum states, namely those that are not positive semidefinite. For any element H in the set, we define the Hermitian traceless matrix $\dot{H}$ by

$$\dot{H} = H - \mathbb{1}/d. \tag{3.70}$$

We obtain the set of all traceless Hermitian matrices. This new set is clearly closed under addition and multiplication by real scalars. It therefore forms a real vector space, with the zero element (the origin) corresponding to the maximally mixed state $\mathbb{1}/d$, as can be seen from (3.70).

Definition. The aforementioned vector space will be referred to as the Bloch space. A point (which can also be considered as a vector) $\dot{H}$ in the Bloch space corresponds to a Hermitian operator H of unit trace on the Hilbert space via equation (3.70). The density operators on the Hilbert space form a convex body in the Bloch space, which will be called the Bloch body.

Considered as a real vector space, the Bloch space has dimensionality equal to the number of real parameters needed to describe a d by d traceless Hermitian matrix, which can be worked out to be $d^2 - 1$. The Bloch body, restricted by positive semidefiniteness, is also $(d^2 - 1)$-dimensional. For example, for the qubit case ($d = 2$), the Bloch body of quantum states is a 3-dimensional ball, which is commonly called the Bloch ball. In higher dimensions, the Bloch body is no longer a ball.

Next, we use the standard Hilbert-Schmidt inner product to define a dot product for two vectors $\dot{H}_1$ and $\dot{H}_2$ in the Bloch space by

$$\dot{H}_1 \cdot \dot{H}_2 \equiv \frac{1}{2} \operatorname{Tr}(\dot{H}_1 \dot{H}_2) = \frac{1}{2} \left(\operatorname{Tr}(H_1 H_2) - \frac{1}{d} \right). \tag{3.71}$$

The Bloch space therefore can be thought of as a $(d^2 - 1)$-dimensional Euclidean space, with the Euclidean distance between any two points $\dot{H}_1$ and $\dot{H}_2$ given by

$$D(\dot{H}_1, \dot{H}_2) = \sqrt{\frac{1}{2} \operatorname{Tr} \left(\dot{H}_1 - \dot{H}_2 \right)^2} = \sqrt{\frac{1}{2} \operatorname{Tr} \left(H_1 - H_2 \right)^2} \ . \tag{3.72}$$

Remark. Pure quantum states are the extreme points of the Bloch body. They all lie on the surface of a sphere of radius $\sqrt{(d-1)/2d}$ centered at the origin. However, not every point on this sphere corresponds to a quantum state, except when $d = 2$, in which case the sphere is called the Bloch sphere and it consists entirely of pure states, while the interior of the Bloch ball consists of all mixed states.

We also want to note that if H_1 and H_2 are density matrices of two MUB vectors in two distinct bases, then the vectors $\dot{H}_1$ and $\dot{H}_2$ in the Bloch space are orthogonal to each other, as their dot product can be seen to vanish.

In the Bloch space, one can construct a regular $(d^2 - 1)$-dimensional simplex, consisting of d^2 vertices labeled by $\dot{A}_{\mathbf{u}}$, where the index $\mathbf{u} = (u_1, u_2) \in \mathbb{F}_d^2$ can take d^2 values. Since the dihedral angle of a regular n-simplex is $\cos^{-1}(n^{-1})$ (see [119] for the first general proof, or [120] for a more elementary calculation), the vertices $\dot{A}_{\mathbf{u}}$ can be chosen so that

$$\dot{A}_{\mathbf{u}} \cdot \dot{A}_{\mathbf{v}} = \begin{cases} \frac{d^2-1}{2d} & \text{if } \mathbf{u} = \mathbf{v} \\ \frac{-1}{2d} & \text{if } \mathbf{u} \neq \mathbf{v}, \end{cases} \tag{3.73}$$

or equivalently in the Hilbert space

$$\mathrm{Tr}(A_{\mathbf{u}}A_{\mathbf{v}}) = \begin{cases} d & \text{if } \mathbf{u} = \mathbf{v} \\ 0 & \text{if } \mathbf{u} \neq \mathbf{v}. \end{cases} \tag{3.74}$$

Eventually, $A_{\mathbf{u}}$ will be identified with Wootters' phase point operators for odd prime dimensions [121], or kernel operators [122] and displaced parity operators [123] in the more general case of odd prime power dimensions. But for now we simply use them to define a regular simplex in the Bloch space. We center the simplex at the origin by imposing the condition

$$\sum_{\mathbf{u}} \dot{A}_{\mathbf{u}} = 0 \quad \Leftrightarrow \quad \sum_{\mathbf{u}} A_{\mathbf{u}} = d\mathbb{1}. \tag{3.75}$$

Each facet (a hyperplane containing $d^2 - 1$ vertices) of the simplex that does not contain vertex $\dot{A}_{\mathbf{u}}$ for some $\mathbf{u}$ consists of all points $\dot{M}$ such that $\mathrm{Tr}(A_{\mathbf{u}}M) = 0$.

What we have so far is a regular simplex centered at the origin created from d^2 vertices in the Bloch space. We are now going to impose a combinatorial structure on it, using what is called a finite affine plane. From now on, we will assume that the dimension $d = p^n$ is a prime power, because that is when affine planes are guaranteed to exist.

Definition. A finite affine plane of order d consists of d^2 points grouped into subsets that are called lines. The grouping is done in such a way that any two points belong to a unique line, and for every point not belonging to a line there exists a parallel line (two lines are called parallel if they are disjoint subsets of points) containing that point.

The existence or non-existence of affine planes in general is an open problem. However, there are some cases for which it has been solved. Bruck-Ryser theorem states that if $d = 1$ or 2 mod 4, and d is not the sum of two squares, then affine planes of order d cannot exist [124]. The existence for $d = 10$ has also been ruled out [125, 126]. Here, we are interested in the case $d = p^n$ is a prime power, when it is known that affine planes exist and that they have the following properties [127]:

1. Each line contains exactly d points.
2. Each point belongs to exactly $d + 1$ lines.
3. There are $d + 1$ sets of d parallel lines, which totals to $d(d + 1)$ lines.

The sets of parallel lines in the last property mentioned above will be called pencils of lines, or just pencils for short. An easy way to visualize a finite affine plane is by associating it with the vector space $\mathbb{F}_d^2$ (see Figure 3.1 for an example when $d = 3$). Although this coordinatization is not required for the construction of affine planes in general, we choose to stick with it here. Particularly, we will use the index $b \in \{\mathbb{F}_d \cup \infty\}$ to label the $d + 1$

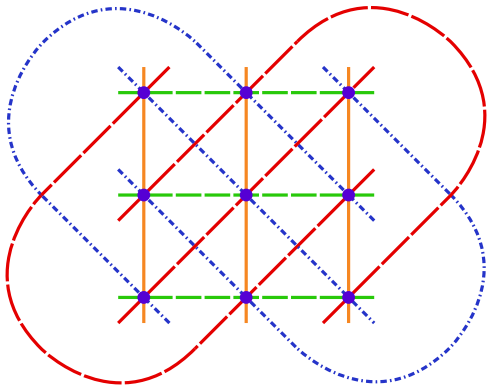

Figure 3.1: Example of an affine plane of order 3 with 9 points and 12 lines. The points are positioned by their coordinates in $\mathbb{Z}_3^2$. The lines are grouped into 4 pencils, each containing 3 parallel lines marked by the same color. The orange pencil (solid lines) is labeled by ∞ since they have a "slope" of ∞.

pencils, where the symbol ∞ refers to the pencil of "vertical" lines. Lines in the b-th pencil are labeled by the index $v \in \mathbb{F}_d$, and are denoted by l_v^b (the reason behind this labeling is that the line l_v^b will later be made to correspond to the v-th MUB vector in the b-th basis). The affine plane's points are labeled by $\mathbf{u} = (u_1, u_2) \in \mathbb{F}_d^2$.

We associate each line in the affine plane with an operator $P_v^{(b)}$ defined to be the average of all phase point operators $A_\mathbf{u}$ associated with points on that line:

$$P_v^{(b)} = \frac{1}{d} \sum_{\mathbf{u} \in l_v^b} A_\mathbf{u}. \tag{3.76}$$

One can verify that $P_v^{(b)}$ is a Hermitian matrix of unit trace, so it corresponds to a point in the Bloch space. In view of (3.75) and the fact that there are $d + 1$ lines intersecting at each point, we can invert the above equation to get

$$A_\mathbf{u} = \sum_{l_v^b \ni \mathbf{u}} P_v^{(b)} - \mathbb{1}, \tag{3.77}$$

which contains a summation of all operators $P_v^{(b)}$ representing lines going through the point $\mathbf{u}$ represented by $A_{\mathbf{u}}$. Using the properties of the affine plane, we can then derive

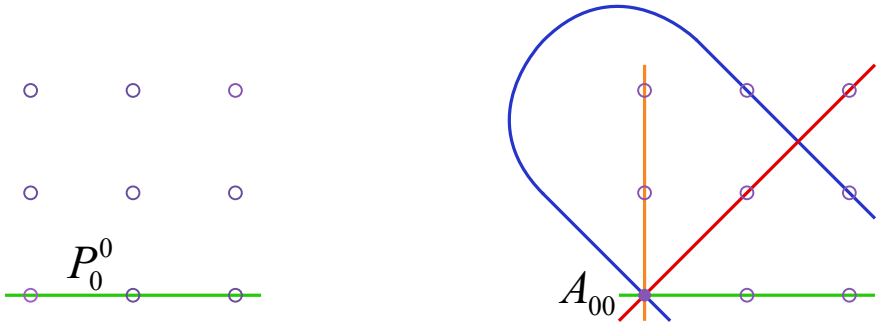

Figure 3.2: Illustrations of line operators and phase point operators for $d = 3$. To the left, the operator $P_0^{(0)}$ corresponding to the line is given by the equation $P_0^{(0)} = (A_{00} + A_{10} + A_{20})/3$. To the right, the intersection point of four lines corresponds to the phase point operator $A_{00} = P_0^{(0)} + P_0^{(1)} + P_0^{(2)} + P_0^{(\infty)} - \mathbb{1}$. Note that both the lines and the points in the affine plane correspond to points in the Bloch space.

$$\mathrm{Tr}\left(P_{v_1}^{(b_1)} P_{v_2}^{(b_2)}\right) = \begin{cases} 1 & \text{if } b_1 = b_2 \text{ and } v_1 = v_2 \text{ (identical lines)} \\ 0 & \text{if } b_1 = b_2 \text{ and } v_1 \neq v_2 \text{ (parallel lines, no common point)} \\ \frac{1}{d} & \text{if } b_1 \neq b_2 \text{ (intersecting lines, one common point).} \end{cases} \tag{3.78}$$

This means that any pencil of d parallel lines (in the affine plane) forms a regular simplex spanning a $(d-1)$-dimensional hyperplane in the Bloch space. There are $d+1$ of these hyperplanes. They are orthogonal to each other and they span the whole Bloch space.

If we take the convex hull of $d(d+1)$ vertices $\dot{P}_v^{(b)}$ in the Bloch space, we obtain what is called a complementarity polytope [118]. One can construct complementarity polytopes in all Euclidean spaces of dimension $d^2 - 1$ for an arbitrary d by splitting the space into $d+1$ totally orthogonal $(d-1)$-dimensional subspaces, placing a regular simplex centered at the origin in each subspace, and taking the convex hull. The special advantage when d is a prime power is that we are able to make use of the combinatorics of an affine plane to inscribe it in a regular simplex. In fact, the phase point operator simplex (whose vertices are the $\dot{A}_{\mathbf{u}}$) is not the only simplex we can inscribe the complementarity polytope into. It is just one out of d^{d-1} possibilities. Let us consider a vector $\vec{v} = (v_0, v_1, ..., v_{d-1}, v_\infty)$ with

$d+1$ components v_b, which are elements of $\mathbb{F}_d$. There are d^{d+1} such vectors. For each $\vec{v}$ we define a generalized phase point operator

$$A_{\vec{v}} \equiv \sum_b P^{(b)}_{v_b} - \mathbb{1}. \tag{3.79}$$

The difference between this equation and (3.77) is that here no assumption is made about the lines labeled by b and v_b, whereas the lines in (3.77) are required to intersect at the point $\mathbf{u}$. If we do this for each $\vec{v}$, we obtain d^{d+1} generalized phase point operators $A_{\vec{v}}$. They clearly have unit trace, and for any vectors $\vec{v}$ and $\vec{v}'$ they satisfy

$$\mathrm{Tr}\left(A_{\vec{v}} A_{\vec{v}'}\right) = \sum_b \mathrm{Tr}\left(P^{(b)}_{v_b} P^{(b)}_{v'_b}\right) - 1. \tag{3.80}$$

The d^{d+1} vectors $\vec{v}$ can be grouped into d^{d-1} groups, each containing d^2 vectors, in such a way that any two vectors $\vec{v}$ and $\vec{v}'$ within a group agree at exactly one component (this is a non-trivial combinatorial problem, see section 4 in [128] for how to do it). One can see from the previous equation that for any $\vec{v}$ and $\vec{v}'$ belonging to the same group

$$\mathrm{Tr}(A_{\vec{v}} A_{\vec{v}'}) = \begin{cases} d & \text{if } \vec{v} = \vec{v}' \\ 0 & \text{if } \vec{v} \neq \vec{v}'. \end{cases} \tag{3.81}$$

So the points $\dot{A}_{\vec{v}}$ in each group form the vertices of a regular (d^2-1)-simplex, much like the phase point operators $\dot{A}_{\mathbf{u}}$ do in (3.74), resulting in d^{d-1} simplices. Moreover, we have

$$\mathrm{Tr}\left(A_{\vec{v}} P^{(b)}_v\right) = \begin{cases} 1 & \text{if the } b\text{-th component of } \vec{v} \text{ is } v \\ 0 & \text{otherwise.} \end{cases} \tag{3.82}$$

This means for each $A_{\vec{v}}$ and two associated parallel hyperplanes defined by the two equations $\mathrm{Tr}\left(A_{\vec{v}} H\right) = 0$ and $\mathrm{Tr}\left(A_{\vec{v}} H\right) = 1$, every vertex $\dot{P}^{(b)}_v$ of the complementarity polytope must lie on one of the two hyperplanes. The complementarity polytope is therefore confined with between all such pairs of hyperplanes, hence circumscribed by each of the d^{d-1} simplices. We have an illustration for $d = 2$ (see Figure 3.3), as the Bloch space in this case is 3-dimensional.

3.5.2 The symmetry group of the complementarity polytope

Recall from the geometrical meaning of (3.78) that a complementarity polytope consists of $d+1$ simplices, each of which spans a $(d-1)$-dimensional hyperplane, and that these

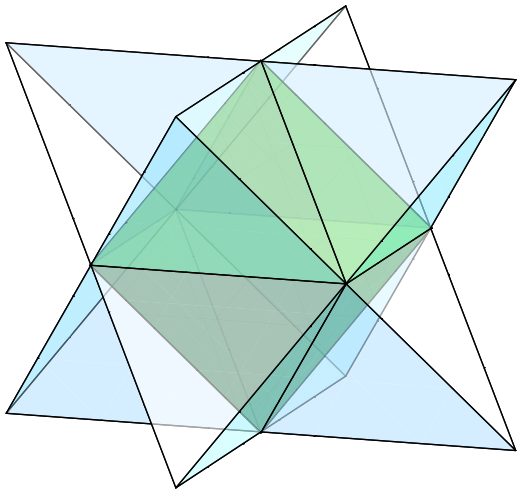

Figure 3.3: When $d = 2$, the Bloch space has $2^2 - 1 = 3$ dimensions and the Bloch body consisting of all quantum states is a 3-dimensional ball. The complementarity polytope (green) is inscribed in $2^{2-1} = 2$ simplices. It is a regular octahedron with $2 \cdot 3$ vertices and 2^3 facets.

hyperplanes are all orthogonal to each other. The symmetry group of the complementarity polytope is therefore

$$S_{d+1} \times S_d \times S_d \times \cdots \times S_d \subset O(d^2 - 1), \tag{3.83}$$

where S_d is the group of all permutations of the vertices of a $(d-1)$-dimensional simplex, and S_{d+1} is the group of all permutations of $d+1$ orthogonal $(d-1)$-dimensional planes. However, we want to impose an extra condition on the complementarity polytope, namely that its vertices must correspond to pure quantum states. This means the polytope is inscribed in the convex Bloch body of quantum states. This might sound like a hard task, but when d is a prime power, a full set of MUBs exists and this could be done by letting $P_v^{(b)}$ be the density matrix of the standard MUB vector r in the MUB basis z:

$$P_v^{(b)} = |e_v^{(b)}\rangle\langle e_v^{(b)}|. \tag{3.84}$$

From Wigner's theorem [4], we know the symmetry group of the Bloch body of quantum states, ignoring anti-unitaries for the moment, is

$$U(d)/U(1) \subset SO(d^2 - 1). \tag{3.85}$$

Since Clifford unitaries simply transform one MUB vector into another, we deduce that the intersection of the two symmetry groups in (3.83) and (3.85) contains the Clifford group

(ignoring overall phases), which, when d is a prime power, can be written as

$$\mathrm{SL}(2,\mathbb{F}_d) \ltimes \mathbb{F}_d^2. \tag{3.86}$$

If we include anti-unitaries, this will lead to the extended Clifford group [30]

$$\mathrm{ESL}(2,\mathbb{F}_d) \ltimes \mathbb{F}_d^2. \tag{3.87}$$

On the other hand, from the combinatorics of an affine plane, we know that the complementarity polytope can be inscribed into a regular simplex, whose symmetry group is S_{d^2}. The intersection of the symmetry group of the polytope and that of the simplex can be identified by noticing that it must take points to points and lines to lines on the affine plane. Its elements are therefore affine transformations, and the group is isomorphic to

$$\mathrm{GL}(2,\mathbb{F}_d) \ltimes \mathbb{F}_d^2. \tag{3.88}$$

This is not quite the same as the result in (3.87) that we obtain by considering symmetries of the complementarity polytope that also preserve the inscribed body of quantum states. When d is a prime ($d > 3$), it is g-unitaries that provide all of the extra symmetries. When d is a prime power, g-unitaries provide only some of the extra transformations, namely those belonging to the subgroup $\mathrm{GL}_p(2,\mathbb{F}_d)$ of $\mathrm{GL}(2,\mathbb{F}_d)$, as a g-unitary U_G is only defined for G with $\det(G) \in \mathbb{F}_p$.

Thus, we come to the conclusion on the geometrical interpretation of g-unitaries: when their action is restricted to the standard MUB vectors, they are simply rotations in the Bloch space, just like ordinary unitaries. However, unlike unitary operators, which are rotations on the whole Bloch body, first of all g-unitaries do not apply to all quantum states. Then, even on the domain that they do apply, namely $\mathbb{Q}(\omega)^d$, they are not rotations on the whole domain due to their wildly discontinuous nature. This interpretation therefore has a very limited scope.

Remark. Further to the discussion at the end of Section 3.2, we want to note that in odd prime dimensions the projective group PGL is a subgroup of the group S_{d+1} in (3.83), which permutes the $(d-1)$-dimensional hyperplanes corresponding to the bases of the MUB. Let us recall that elements of GL whose determinant is a quadratic residue do not add anything to PGL beyond the contribution from SL, as seen from (3.13). When $d = 3 \bmod 4$, element -1 of the field $\mathbb{F}_d$ is a quadratic non-residue, so the full set of projective transformations can be obtained from the extended symplectic group represented by unitary and anti-unitary operators. When $d = 1 \bmod 4$, -1 is a quadratic residue, and we need to include general

g-unitaries to obtain the full set of projective transformations. In prime power dimension $d = p^n$, we only obtain all the projective transformations from g-unitaries when n is odd.

Lastly, we want to note that when the vertices of the complementarity polytope are associated with the standard MUB vectors as in (3.84), there is a special choice for the phase point operators that takes a rather simple form. When d is odd, one of them is the parity operator

$$A_0 = \frac{1}{d} \sum_{\mathbf{v} \in \mathbb{F}_d^2} D_{\mathbf{v}}, \tag{3.89}$$

and the others are simply obtained by acting on the parity operator with the WH group's displacement operators

$$A_{\mathbf{u}} = D_{\mathbf{u}} A_0 D_{\mathbf{u}}^{-1} = \sum_{\mathbf{v} \in \mathbb{F}_d^2} \omega^{\Omega(\mathbf{u},\mathbf{v})} D_{\mathbf{v}}. \tag{3.90}$$

3.6 Simulating g-unitaries using unitaries

Quantum mechanics teaches us that physical transformations must be unitary: a non-unitary operator cannot be implemented in any physical system. But that is not to say that it cannot be simulated in a physical system. Simulations of unphysical transformations can be useful in fundamental studies in physics, and have in fact been experimentally realized, for example to study Majorana's equation where anti-unitaries are involved [129, 130]. The key technique used in these papers is to separate the real and the imaginary parts of a quantum state and embed them in a larger Hilbert space. It is worth going through their simulation of an anti-unitary for a qubit, as it will help make the idea transparent. Then, we will propose a scheme for simulating g-unitaries in any odd prime power dimension.

Let $\bar{U}$ be an anti-unitary, which can always be written as

$$\bar{U} = UK, \tag{3.91}$$

where U is an ordinary 2×2 unitary and K stands for complex conjugation. Let

$$|\psi\rangle = \begin{pmatrix} a_1 + ib_1 \\ a_2 + ib_2 \end{pmatrix} \tag{3.92}$$

be a quantum state expressed as a vector in the standard basis, where a_1, a_2, b_1, b_2 are real numbers. The action of $\bar{U}$ on $|\psi\rangle$ is then

$$\bar{U}|\psi\rangle = UK|\psi\rangle = U \begin{pmatrix} a_1 - ib_1 \\ a_2 - ib_2 \end{pmatrix} = U|\psi\rangle_{\text{re}} - iU|\psi\rangle_{\text{im}}. \tag{3.93}$$

If we embed $|\psi\rangle$ into a Hilbert space twice as large using the following mapping $\mathcal{T}$

$$\begin{pmatrix} a_1 + ib_1 \\ a_2 + ib_2 \end{pmatrix} \quad \xrightarrow{\mathcal{T}} \quad \begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{pmatrix}, \tag{3.94}$$

applying the unitary operator $(\sigma_z \otimes U)$, where σ_z is a Pauli matrix, to obtain

$$\begin{pmatrix} U & 0 \\ 0 & -U \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ b_1 \\ b_2 \end{pmatrix} = \begin{pmatrix} U|\psi\rangle_{\text{re}} \\ -U|\psi\rangle_{\text{im}} \end{pmatrix}, \tag{3.95}$$

and finally applying the inverse of the embedding mapping to go back to the original Hilbert space

$$\begin{pmatrix} U|\psi\rangle_{\text{re}} \\ -U|\psi\rangle_{\text{im}} \end{pmatrix} \quad \xrightarrow{\mathcal{T}^{-1}} \quad U|\psi\rangle_{\text{re}} - iU|\psi\rangle_{\text{im}}, \tag{3.96}$$

we will get the same result as if we have used $\bar{U}$ to act on $|\psi\rangle$. Therefore the unphysical anti-unitary $\bar{U}$ can be effectively simulated by the unitary operator $(\sigma_z \otimes U)$ in a larger embedding space.

Let us now make the generalization to g-unitaries. Let $d = p^n$ be an odd prime power dimension. Let G be an element of $\mathrm{GL}_p(2, \mathbb{F}_d)$ and let U_G be its corresponding g-unitary written in the usual form

$$U_G = U_S g_\Delta, \tag{3.97}$$

where U_S is unitary, and $\Delta = \det(G) \in \mathbb{F}_p$. The Galois automorphism g_Δ can be thought of as a permutation on the set $\{1, \omega, ..., \omega^{p-1}\}$ leaving 1 invariant and mapping ω^k to $\omega^{\Delta k}$. We will denote this $p \times p$ permutation matrix by σ_Δ. For any vector $|\psi\rangle \in \mathbb{Q}(\omega)^d$, we can embed it into a dp-dimensional vector space over the rational field $\mathbb{Q}$ using the embedding

mapping $\mathcal{T}$ defined as follows:

$$|\psi\rangle = \begin{pmatrix} q_0^{(1)} + q_1^{(1)}\omega + ... + q_{p-1}^{(1)}\omega^{p-1} \\ q_0^{(2)} + q_1^{(2)}\omega + ... + q_{p-1}^{(2)}\omega^{p-1} \\ \vdots \\ q_0^{(d)} + q_1^{(d)}\omega + ... + q_{p-1}^{(d)}\omega^{p-1} \end{pmatrix} \quad \longrightarrow \quad \mathcal{T}\left(|\psi\rangle\right) = \begin{pmatrix} q_0^{(1)} \\ \vdots \\ q_0^{(d)} \\ \vdots \\ q_{p-1}^{(1)} \\ \vdots \\ q_{p-1}^{(d)} \end{pmatrix}, \tag{3.98}$$

where $q_j^{(k)}$ are rational numbers and $q_{p-1}^{(1)} = q_{p-1}^{(2)} = ... = q_{p-1}^{(d)} = 0$ (we leave them in the expression as we need to keep track of ω^{p-1} terms).

It can be seen that by applying the unitary operator $(\sigma_\Delta \otimes U_S)$ on $\mathcal{T}\left(|\psi\rangle\right)$ and then applying $\mathcal{T}^{-1}$ to get back to the d-dimensional vector space $\mathbb{Q}(\omega)^d$, we obtain

$$\mathcal{T}^{-1}\big(\left(\sigma_\Delta \otimes U_S\right)\mathcal{T}\left(|\psi\rangle\right)\big) = U_S g_\Delta(|\psi\rangle). \tag{3.99}$$

This means that the action of U_G can be simulated by the unitary $(\sigma_\Delta \otimes U_S)$ in the embedding space using the embedding mapping $\mathcal{T}$ as defined.

Remark. We have shown that in principle it is possible to simulate a g-unitary by a physical unitary operator in a larger Hilbert space. In practice, however, this is extremely difficult to implement because the embedding mapping $\mathcal{T}$ is highly discontinuous: given 2 complex numbers that are very close to each other, the rational coefficients in their cyclotomic expansions can be vastly different.

3.7 The MUB-cycling problem

Definition. Given a full set of MUB, a MUB-cycler is an operator whose repeated actions on any single basis generate all other bases in succession.

Note. Although technically a MUB-cycler is an operator acting on MUB bases in the Hilbert space, we also call an element $G \in \mathrm{GL}(2, \mathbb{F}_d)$ a MUB-cycler if its representation U_G is a MUB-cycler.

In even prime power dimensions, unitary MUB-cyclers have been constructed [5, 131]. In odd prime power dimensions it has been shown that there is no Clifford unitary MUB-cycler [30]. However, if the dimension equals 3 mod 4, there are MUB-cycling anti-unitaries [30]. Now that we have a notion of Galois-unitaries, we want to see whether they enable us to solve the MUB cycling problem in cases where ordinary unitary and anti-unitary operators fail. The quick answer is yes: in odd prime power dimension $d = p^n$ where the exponent n is odd, there exist g-unitaries that cycle through the MUBs. In this section we will provide a construction for all such operators. For even n we will disprove their existence. These results will come clear from the theorems to follow.

3.7.1 Suborder and 3 types of GL elements

We first want to introduce the notion of the suborder of a GL element. There are $d+1$ bases in a full set of MUBs in a prime power dimension d. In order for a projective permutation of the bases to cycle through all of them, we need an element of PGL (see Section 3.2) with order $d+1$, or equivalently an element of GL with an "effective order" of $d+1$, by which we mean that we only care about its permutation on the bases and neglect its action on individual vectors within each basis. To explain this more precisely let us consider an element $G \in \mathrm{GL}(2, \mathbb{F}_d)$ and its m-th power expressed as:

$$G = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}, \; G^m = \begin{pmatrix} \alpha_m & \beta_m \\ \gamma_m & \delta_m \end{pmatrix}. \tag{3.100}$$

It follows from the expression for the Möbius transformation (3.11) that U_{G^m} takes the basis labelled by $b = 0$ to basis $b' = \beta_m/\delta_m$ if $\delta_m \neq 0$, and to basis $b' = \infty$ if $\delta_m = 0$. So if $\beta_m = 0$, basis $b = 0$ will be brought back to itself if repeatedly acted on by U_G for m times. We can now define the suborder of G as follows.

Definition. The suborder m of G is the smallest positive integer for which $\beta_m = 0$.

Remark. The suborder m of G need not be equal to the order of G because although U_{G^m} brings a MUB basis back to itself, it might permute the vectors within the basis. In general, m is a factor of the order of G (hence the name suborder). Following Lemma 3.4, we will see that the smallest positive integer m for which G^m is proportional to the 2×2 identity matrix is an equivalent definition of the suborder.

What we can say about the suborder of a GL element turns out to depend crucially on the nature of its eigenvalues. Let G be an element of $\mathrm{GL}(2, \mathbb{F}_d)$ with trace t and determinant

$\Delta \neq 0$. The eigenvalues of G are roots of the characteristic polynomial $x^2 - tx + \Delta = 0$ and are given by

$$\lambda_\pm = (t \pm \sqrt{t^2 - 4\Delta})/2 \ . \tag{3.101}$$

If $t^2 - 4\Delta$ is zero or a quadratic residue, i.e. it has a non-zero square root in $\mathbb{F}_d$, then $\lambda_\pm$ belong to the field $\mathbb{F}_d$. Otherwise, the eigenvalues do not belong to $\mathbb{F}_d$, but they are still well-defined and they can be included in the extension field $\mathbb{F}_{d^2}$. To deal with these cases, it is convenient to classify GL elements into three types, as summarized in Table 3.2.

Type	Definition in terms of t and Δ	Equivalent definition
1	$t^2 - 4\Delta$ is a quadratic residue	$\lambda_\pm \in \mathbb{F}_d, \lambda_+ \neq \lambda_-$
2	$t^2 - 4\Delta$ is a quadratic non-residue	$\lambda_\pm \notin \mathbb{F}_d, \lambda_+ \neq \lambda_-$
3	$t^2 - 4\Delta = 0$	$\lambda_\pm = t/2 \in \mathbb{F}_d$

Table 3.2: A classification of GL elements into three types, among which only type 2 can include MUB-cyclers, as will be seen in the next section.

3.7.2 Constructing MUB-cyclers

Throughout this section we assume that the dimension d is a prime power of the form $d = p^n$, where p is an odd prime number.

Lemma 3.3 (Cayley-Hamilton theorem [132] for 2×2 matrices)**.** *If A is a 2×2 matrix of trace t and determinant Δ, then*

$$A^2 = tA - \Delta I, \tag{3.102}$$

where I is the 2×2 identity matrix.

Proof. One can explicitly calculate A^2 to verify that the lemma is true. □

Lemma 3.4. *If A is a 2×2 matrix with trace t and determinant Δ, then it holds, for any integer $m \geq 1$, that*

$$A^m = s_m A - s_{m-1}\Delta I, \tag{3.103}$$

where the sequence $\{s_m\}$ is defined by the recurrence relation

$$s_{m+1} = ts_m - \Delta s_{m-1}, \tag{3.104}$$

with $s_0 = 0$ *and* $s_1 = 1$. *Equivalently,* s_m *can be calculated by*

$$s_m = \begin{cases} (\lambda_+^m - \lambda_-^m)/(\lambda_+ - \lambda_-) & \text{if } \lambda_+ \neq \lambda_- \\ m\lambda_+^{m-1} & \text{if } \lambda_+ = \lambda_- \end{cases} \tag{3.105}$$

where $\lambda_\pm$ *are roots of the characteristic polynomial* $x^2 - tx + \Delta$.

Proof. We will prove the lemma by induction. Let us first note that (3.105) is equivalent to

$$s_m = \sum_{i=0}^{m-1} \lambda_+^{m-1-i}\lambda_-^i \ . \tag{3.106}$$

By definition, $s_2 = ts_1 - \Delta s_0 = t = \lambda_+ + \lambda_-$, therefore (3.106) holds for $m = 1$ and $m = 2$. Suppose (3.106) holds for $m = 1, 2, ...,$ up to $m = k$, then

$$\begin{aligned} s_{k+1} = ts_k - \Delta s_{k-1} &= (\lambda_+ + \lambda_-)\sum_{i=0}^{k-1} \lambda_+^{k-1-i}\lambda_-^i - \lambda_+\lambda_- \sum_{i=0}^{k-2} \lambda_+^{k-2-i}\lambda_-^i \\ &= \sum_{i=0}^{k-1} \lambda_+^{k-i}\lambda_-^i + \sum_{i=0}^{k-1} \lambda_+^{k-1-i}\lambda_-^{i+1} - \sum_{i=0}^{k-2} \lambda_+^{k-1-i}\lambda_-^{i+1} \\ &= \sum_{i=0}^{k-1} \lambda_+^{k-i}\lambda_-^i + \left(\sum_{i=1}^{k} \lambda_+^{k-i}\lambda_-^i - \sum_{i=1}^{k-1} \lambda_+^{k-i}\lambda_-^i \right) \\ &= \sum_{i=0}^{k-1} \lambda_+^{k-i}\lambda_-^i + \lambda_-^k = \sum_{i=0}^{k} \lambda_+^{k-i}\lambda_-^i \ , \end{aligned} \tag{3.107}$$

which implies that it also holds for $m = k + 1$, and consequently, for all $m \geq 1$.

Equation (3.103) obviously holds for $m = 1$. Lemma 3.3 implies that it also holds for $m = 2$. Suppose it holds for $m = 1, 2, ...,$ up to $m = k$, then

$$\begin{aligned} A^{k+1} = A^k A &= (s_k A - s_{k-1}\Delta I)A \\ &= s_k A^2 - s_{k-1}\Delta A \\ &= s_k(tA - \Delta I) - s_{k-1}\Delta A \\ &= (s_k t - s_{k-1}\Delta)A - s_k \Delta I \\ &= s_{k+1}A - s_k \Delta I \ , \end{aligned} \tag{3.108}$$

which implies that it also holds for $m = k + 1$, and consequently, for all $m \geq 1$. □

Remark. If A takes the form $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, we can explicitly rewrite Eq. (3.103) as

$$A^m = \begin{pmatrix} s_m\alpha - s_{m-1}\Delta & s_m\beta \\ s_m\gamma & s_m\delta - s_{m-1}\Delta \end{pmatrix}, \tag{3.109}$$

from which it can be seen that if $\beta \neq 0$ (for a non-zero determinant, we can always force $\beta \neq 0$ using the canonical form in (3.126) near the end of this section) the suborder of A is the smallest positive integer m for which $s_m = 0$. For such m, A^m is proportional to the identity matrix.

Theorem 3.5. *Let G be an element of $\mathrm{GL}(2, \mathbb{F}_d)$ with determinant Δ.*

1. *If G is of type 1, then G has suborder of at most $d-1$.*
2. *If G is of type 2, then G has suborder of at most $d+1$ and satisfies*
$$G^{d+1} = \Delta I \qquad (I \text{ is the } 2\times 2 \text{ identity matrix}). \tag{3.110}$$
3. *If G is of type 3, then G has suborder of at most d.*

Proof. Let $\lambda_\pm$ be the eigenvalues of G, based upon which we define the sequence $\{s_m\}$ just as in Lemma 3.4. Although $\lambda_\pm$ might not be in the field $\mathbb{F}_d$, the sequence $\{s_m\}$ always is, as seen from the recursive definition in (3.104). Lemma 3.4 implies that if $s_m = 0$ for some m, then $G^m = -s_{m-1}\Delta I$, and therefore the suborder of G is at most m. Let us now consider specific cases. Facts about finite fields (see Section A.1.4) will be used implicitly.

1. If G is of type 1, then the eigenvalues $\lambda_\pm$ are in $\mathbb{F}_d$, so
$$\lambda_+^{d-1} = \lambda_-^{d-1} = 1\ , \tag{3.111}$$
$$s_{d-1} = (\lambda_+^{d-1} - \lambda_-^{d-1})/(\lambda_+ - \lambda_-) = 0\ , \tag{3.112}$$
and therefore G has suborder of at most $d-1$.
2. If G is of type 2, to include $\lambda_\pm$ we create an extension field $\mathbb{F}_{d^2}$ from the base field $\mathbb{F}_d$ and the generator $j \equiv \sqrt{t^2 - 4\Delta}$. Since $(j^d)^2 = (t^2-4\Delta)^d = t^2 - 4\Delta = j^2$, we have

$j^d = \pm j$. Because j is not in the field $\mathbb{F}_d$ we cannot have $j^d = j$, and it therefore must be the case that $j^d = -j$. As d is odd we have:

$$\lambda_\pm^d = \frac{(t \pm j)^d}{2^d} = \frac{t \pm j^d}{2} = \frac{t \mp j}{2} = \lambda_\mp \ . \tag{3.113}$$

We then use (3.105) to derive

$$s_d = (\lambda_+^d - \lambda_-^d)/(\lambda_+ - \lambda_-) = -1 \ , \tag{3.114}$$

$$s_{d+1} = \frac{\lambda_+^{d+1} - \lambda_-^{d+1}}{\lambda_+ - \lambda_-} = \frac{\lambda_+\lambda_- - \lambda_-\lambda_+}{\lambda_+ - \lambda_-} = 0 \ , \tag{3.115}$$

and therefore

$$G^{d+1} = s_{d+1}G - s_d\Delta I = \Delta I \ . \tag{3.116}$$

It follows that G has suborder of at most $d+1$.

3. If G is of type 3, then $\lambda_\pm = t/2$. It follows from (3.105) that $s_d = d\lambda_+^{d-1} = 0$, so G has suborder of at most d.

□

Lemma 3.6. *Let $G \in \mathrm{GL}_p(2, \mathbb{F}_d)$, i.e. an element $\mathrm{GL}(2, \mathbb{F}_d)$ whose determinant Δ is in the prime field $\mathbb{F}_p$. Let $\bar{\theta}$ be a primitive element of $\mathbb{F}_{d^2}$ (therefore $\theta = \bar{\theta}^{d+1}$ is a primitive element of $\mathbb{F}_d$). Note that $(d-1)/(p-1)$ is an integer, so we can define $\eta \in \mathbb{F}_{d^2}$ as*

$$\eta \equiv \bar{\theta}^{(d-1)/(p-1)} \ . \tag{3.117}$$

Then G is of type 2 if and only if it has eigenvalues η^r and η^{dr}, for some integer r in the range $0 < r < (p-1)(d+1)$ that is not a multiple of $(d+1)/2$.

Proof. Assume that G is of type 2, and let $\lambda_\pm \notin \mathbb{F}_d$ be its eigenvalues. Following (3.113), we have $\lambda_\pm^d = \lambda_\mp$, so we may write

$$\lambda_+ = \bar{\theta}^k \qquad\qquad \lambda_- = \bar{\theta}^{dk} \tag{3.118}$$

for some integer $1 \le k \le d^2 - 1$. The assumption that $\lambda_\pm$ are not elements of $\mathbb{F}_d$ implies that k is not a multiple of $d+1$. The fact that $\Delta \in \mathbb{F}_p$ means

$$\bar{\theta}^{pk(d+1)} = \Delta^p = \Delta = \bar{\theta}^{k(d+1)} \ , \tag{3.119}$$

or equivalently

$$\bar{\theta}^{k(p-1)(d+1)} = 1 \ , \tag{3.120}$$

implying that $(d-1) \mid k(p-1)$. Let $r = k(p-1)/(d-1)$, then r is an integer in the range $0 \leq r \leq (p-1)(d+1)$. The eigenvalues can then be re-written as

$$\lambda_+ = \eta^r \qquad\qquad \lambda_- = \eta^{dr} \ . \tag{3.121}$$

The requirement that $\lambda_+ \notin \mathbb{F}_d$ means

$$\eta^r = \bar{\theta}^{r(d-1)/(p-1)} \notin \mathbb{F}_d \ , \tag{3.122}$$

which is true if and only if $r(d-1)/(p-1)$ is not a multiple of $(d+1)$, which in turn is equivalent to r not being a multiple of $(d+1)/2$ because $\gcd((d-1)/(p+1), d+1) = 2$.

Conversely, if G has eigenvalues of the form $\lambda_+ = \eta^r$ and $\lambda_- = \eta^{dr}$, where r is not a multiple of $(d+1)/2$, then $\lambda_\pm$ are not in the field $\mathbb{F}_d$, and G is therefore of type 2. One can further verify that its trace is in $\mathbb{F}_d$ and its determinant is in $\mathbb{F}_p$ by defining

$$t \equiv \eta^r + \eta^{dr} \qquad\qquad \Delta \equiv \eta^{(d+1)r} \tag{3.123}$$

and using the facts $\eta^{d^2} = \eta$ and $\eta^{(d+1)p} = \eta^{d+1}$ to check that

$$t^d = t \qquad\qquad \Delta^p = \Delta \ . \tag{3.124}$$

□

Remark. With Lemma 3.6, all type-2 elements of $\mathrm{GL}_p(2, \mathbb{F}_d)$ are now characterized by an integer r, via their eigenvalues. In the next theorem, we will pin down exactly which values of r correspond to MUB-cyclers when they exist.

Theorem 3.7. *Let $G \in \mathrm{GL}_p(2, \mathbb{F}_d)$ be of type 2 and let the integer r be as in the statement of Lemma 3.6.*

1. *When n is even, G has suborder of at most $(d+1)/2$.*
2. *When n is odd, G has suborder $d+1$ if and only if $\gcd(r, d+1) = 1$.*

Proof. Let $\lambda_\pm$ be the eigenvalues of G and the sequence s_m be as defined in Lemma 3.4. We recall that the suborder of G is the smallest positive integer m for which $s_m = 0$, which in this case is equivalent to $\lambda_+^m = \lambda_-^m$, as G is of type 2 and its eigenvalues are distinct.

1. When n is even, $(d-1)/(p-1) = 1 + p + \ldots + p^{n-1}$ is an even integer, so $(d-1)/2$ is a multiple of $(p-1)$. It then follows from (3.120) that

$$\bar{\theta}^{k(d-1)(d+1)/2} = 1 \ , \tag{3.125}$$

which implies $\lambda_+^{(d+1)/2} = \lambda_-^{(d+1)/2}$, or $s_{(d+1)/2} = 0$. Therefore G has suborder of at most $(d+1)/2$ and cannot be a MUB-cycler.

2. When n is odd, $(d-1)/(p-1)$ is an odd integer. It follows from this, and the fact that $\gcd(d+1, d-1) = 2$, that $(d-1)/(p-1)$ is co-prime to $d+1$. We have $\lambda_+^m = \lambda_-^m$ if and only if $\eta^{m(d-1)r} = 1$, which in turn is true if and only if $mr(d-1)/(p-1)$ is a multiple of $d+1$. Therefore G has suborder $d+1$ if and only if r is co-prime to $d+1$.

□

In summary, in this section we have proved the non-existence of MUB-cyclers when the exponent n is even. When n is odd, we have identified all MUB-cycling elements in $\mathrm{GL}(2, \mathbb{F}_d)$ according to the characteristics of their eigenvalues. Lastly, we want to provide an explicit form for these MUB-cyclers. The proof in the Appendix of [114] can be extended to show that for any element in $G \in \mathrm{GL}(2, \mathbb{F}_d)$ with trace t and determinant Δ, where $t^2 - 4\Delta \neq 0$, there exists $S \in \mathrm{SL}(2, \mathbb{F}_d)$ such that

$$G = SG_cS^{-1} \qquad G_c = \begin{pmatrix} 0 & -\Delta \\ 1 & t \end{pmatrix}, \tag{3.126}$$

where we call G_c the canonical form of G. Therefore, an element of $\mathrm{GL}(2, \mathbb{F}_d)$ is a MUB-cycler if and only if it is conjugate to G_0^r where

$$G_0 = \begin{pmatrix} 0 & -\eta^{(d+1)} \\ 1 & \eta + \eta^d \end{pmatrix} \ , \tag{3.127}$$

η is defined as in (3.117), and r is an integer co-prime to $d+1$. Note that the order of G_0 is $(p-1)(d+1)$ because this is the smallest integer r such that η^r and η^{dr}, the eigenvalues of G_0^r, are both equal to 1.

Remark. It follows that anti-symplectic MUB-cyclers exist if and only if the dimension $d = 3 \pmod 4$, a fact already shown in [30]. This is because G_0^r is anti-symplectic if and only if $\eta^{r(d+1)} = -1$, which is true if and only if r is an odd multiple of $(p-1)/2$. If $d = 1 \pmod 4$ then $(p-1)/2$ is even, so no multiple of $(p-1)/2$ is co-prime to $d+1$. But if $d = 3 \pmod 4$ one can see that $(p-1)/2$ is co-prime to $d+1$, implying that $G_0^{r(p-1)/2}$ is an anti-symplectic MUB-cycler for every r co-prime to $d+1$.

3.8 Eigenvectors of MUB cyclers

One can always find eigenvalues and eigenvectors of an ordinary unitary operator by diagonalizing it. However when it comes to g-unitaries, the situation is tricker. When dealing with g-unitaries, one has to be extra careful because much of our intuition about ordinary unitaries can fail for g-unitaries. For example, a scalar multiplication of an eigenvector of a g-unitary can change its eigenvalues, resulting in the possibility of a g-unitary having infinitely many eigenvalues (see the example below). Or in other cases, a g-unitary might not have any eigenvector at all (see the example below). We will start this section with an example of anti-unitaries, and then proceed to the analysis of the eigenvectors of a special kind of g-unitaries, namely the MUB-cyclers.

Example. Let U_A be an anti-unitary over the complex field $\mathbb{C}$, which can be expressed as $U_A = UK$, where U is a unitary and K denotes complex conjugation. We notice that $U_A^2 = UKUK = U\bar{U}$, where $\bar{U}$ denotes the complex conjugate of U, is a unitary. Let $|\phi\rangle$ be an eigenvector of U_A with the eigenvalue λ:

$$U_A |\phi\rangle = \lambda |\phi\rangle \ . \tag{3.128}$$

It then follows that

$$U_A^2 |\phi\rangle = UK\lambda |\phi\rangle = \lambda^* UK |\phi\rangle = |\lambda|^2 |\phi\rangle \ . \tag{3.129}$$

Since U_A^2 is unitary, $|\lambda|^2$ must be of modulus 1, and therefore $\lambda = e^{i\theta}$ is a phase. There are two things that follow from this. First of all, let $e^{i\phi}$ be any phase, then

$$U_A(e^{i\phi} |\phi\rangle) = e^{-i\phi}\lambda |\phi\rangle = e^{i(\theta-2\phi)} e^{i\phi} |\phi\rangle \tag{3.130}$$

so $e^{i\phi} |\phi\rangle$ is an eigenvector of U_A with eigenvalue $e^{i(\theta-2\phi)}$. This means that U_A has a continuum of eigenvalues, whose eigenvectors only differ by an overall phase, and that we can ensure the eigenvalue is 1 by adjusting the phase. Secondly, since $|\lambda|^2$ is real and positive, we must have $|\lambda|^2 = 1$. Therefore $|\phi\rangle$ is an eigenvector of the unitary U_A^2 with unit eigenvalue. If U_A^2 does not have any eigenvalue equal to 1, then U_A cannot have any eigenvector at all. For a concrete example in $\mathbb{C}^2$ consider the anti-unitary $U_A = UK$ where

$$U = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \ , \quad U_A^2 = U\bar{U} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \ . \tag{3.131}$$

The eigenvalues of U_A^2 are $\pm i$, therefore U_A has no eigenvector.

Wigner has characterized the eigenvectors of anti-unitaries [133]. It is not straightforward to generalize his results to g-unitaries. However, by restricting ourselves to a special kind of g-unitaries, namely those that have the MUB-cycling property, we are able to provide a complete characterization of their eigenvalues and eigenvectors. The results are summarized in Theorem 3.8, which states that MUB-cycling g-unitaries always have eigenvectors, which are unique up to multiplication by a scalar, and that we can always find an eigenvector with unit eigenvalue.

Let us first set up some notations and definitions. For the rest of this section, we will always assume that the dimension $d = p^n$ is an odd prime power where the exponent n is odd. G is a fixed element of $\mathrm{GL}_p(2, \mathbb{F}_d)$ with eigenvalues η^r and η^{rd} (as in Lemma 3.6), where r is co-prime to $d+1$ so that G is a MUB-cycler (by Theorem 3.7). We will use $t = \eta^r + \eta^{rd}$ and $\Delta = \eta^{r(d+1)}$ to denote the trace and determinant of G, respectively.

Definition. If we define the multiplicative order of G to be the smallest positive integer m for which $\Delta^m = 1$, then it follows from (3.117) that $\bar{\theta}^{mr(d+1)(d-1)/(p-1)} = 1$ (where $\bar{\theta}$ is a primitive element of $\mathbb{F}_{d^2}$), which is true if and only if mr is a multiple of $p-1$. Since r is odd because it is co-prime to $d+1$, and $p-1$ is even, m must be even. We will therefore use $2m_0$ to denote the multiplicative order of G.

Remark. It then follows that $\Delta^{m_0} = \pm 1$. Since $2m_0$ is the smallest positive integer for which $\Delta^{2m_0} = 1$, we cannot have $\Delta^{m_0} = 1$, and therefore it must be the case that

$$\Delta^{m_0} = -1 \ . \tag{3.132}$$

This implies that G^{2m_0} is a symplectic matrix and G^{m_0} is an anti-symplectic matrix, and correspondingly, $U_G^{2m_0} = U_{G^{2m_0}}$ is unitary and $U_G^{m_0} = U_{G^{m_0}}$ is anti-unitary.

Definition. If $\{|x\rangle\}$ denotes the standard basis, then the parity operator A is defined as

$$A = \sum_x |-x\rangle \langle x| \ . \tag{3.133}$$

Alternatively, A can also be defined from the unitary representation of the (unique) element of order 2 in the symplectic group:

$$A = (-1)^{(p-1)/2} U_P \qquad \text{where} \qquad P = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \ . \tag{3.134}$$

Theorem 3.8. *Let $d = p^n$ be an odd prime power, where the exponent n is odd, and let $G \in \mathrm{GL}_p(2, \mathbb{F}_d)$ be a MUB cycler. Let $\mathbb{Q}(\omega)^d$ be the subspace of the Hilbert space consisting of all vectors whose components (in the standard basis) belong to the cyclotomic field $\mathbb{Q}(\omega)$.*

1. *There exists a non-zero* $|\psi\rangle \in \mathbb{Q}(\omega)^d$ *such that* $U_G |\psi\rangle = |\psi\rangle$.

2. $|\phi\rangle \in \mathbb{Q}(\omega)^d$ *is an eigenvector of* U_G *if and only if* $|\phi\rangle = \mu |\psi\rangle$ *for some* $\mu \in \mathbb{Q}(\omega)$.

3. *The eigenspace of* $U_G^{2m_0}$ *with eigenvalue 1 is one-dimensional and spanned by* $|\psi\rangle$.

4. $|\phi\rangle$ *is an eigenvector of the parity operator with eigenvalue* $(-1)^{(p-1)/2}$.

Proof. The theorem in an immediate consequence of the following lemmas. □

Lemma 3.9. *With notations and definitions as above, suppose* $|\phi\rangle \in \mathbb{Q}(\omega)^d$ *is an eigenvector of* U_G *with eigenvalue* $\lambda \in \mathbb{Q}(\omega)$, *i.e.*

$$U_G |\phi\rangle = \lambda |\phi\rangle \ , \tag{3.135}$$

then it holds that

$$U_G^{2m_0} |\phi\rangle = |\phi\rangle \ . \tag{3.136}$$

Proof. Applying U_G to (3.135) repeatedly we will obtain

$$U_G^{m_0} |\phi\rangle = \kappa |\phi\rangle \ , \tag{3.137}$$

where

$$\kappa = \lambda g_\Delta(\lambda) \dots g_\Delta^{m_0-1}(\lambda) \ . \tag{3.138}$$

Then we apply the anti-unitary $U_G^{m_0}$ to (3.137) to obtain

$$U_G^{2m_0} |\phi\rangle = \kappa^* \kappa |\phi\rangle \ , \tag{3.139}$$

where κ^* is the complex conjugate of κ and $U_G^{2m_0}$ is unitary. As n is odd, by Theorem 3.2 the representation of $\mathrm{GL}_p(2, \mathbb{F}_d)$ is faithful, and therefore

$$U_G^{2m_0(d+1)} = U_{G^{2m_0(d+1)}} = \mathbb{1} \ . \tag{3.140}$$

It then follows that $(\kappa^*\kappa)^{d+1} = 1$, which implies $\kappa^*\kappa = 1$ because it has to be a real positive number. Hence, we conclude that $|\phi\rangle$ is an eigenvector of $U_G^{2m_0}$ with unit eigenvalue. □

Lemma 3.10. *With notations and definitions as above, let* $\mathcal{S}_1$ *be the eigenspace of* $U_G^{2m_0}$ *corresponding to eigenvalue* 1, *then* $\mathcal{S}_1$ *is one-dimensional.*

Proof. To determine the dimensionality of $\mathcal{S}_1$, we will calculate the trace of the projection operator onto that subspace. We first note the following linear algebraic fact. If U is a unitary of order k, and τ is an eigenvalue of U (τ therefore has to be a k-th root of unity), then the projection operator onto the eigenspace corresponding to τ is given by

$$P_\tau = (\mathbb{1} + \tau^{-1}U + \ldots + \tau^{-(k-1)}U^{k-1})/k \ . \tag{3.141}$$

One can prove this by verifying that $P_\tau^2 = P_\tau$ so that P_τ is a projection operator, and that P_τ projects any vector into an eigenvector with eigenvalue τ and leaves all eigenvectors with eigenvalue τ invariant. Particularly in our case, the projection operator onto $\mathcal{S}_1$ is given by

$$P_1 = \frac{1}{d+1}\sum_{u=0}^{d} U_{G^{2m_0}}^u \ , \tag{3.142}$$

and the dimensionality of $\mathcal{S}_1$ is therefore

$$\dim \mathcal{S}_1 = \mathrm{Tr}(P_1) = \frac{1}{d+1}\sum_{u=0}^{d} \mathrm{Tr}\left(U_{G^{2m_0}}^u\right) \ . \tag{3.143}$$

To calculate these traces we make use of a result from Theorem 5 in Ref. [30], applicable to any symplectic $S \in \mathrm{SL}(2,\mathbb{F}_d)$, namely

$$\mathrm{Tr}(U_S) = l(t-2) \ , \tag{3.144}$$

where $t = \mathrm{Tr}(S)$ and $l(x)$ is the Legendre symbol defined in (A.36). Since the eigenvalues of G are η^r and η^{dr}, we have

$$\begin{aligned} \mathrm{Tr}(G^{2m_0u}) &= \eta^{2rm_0u} + \eta^{2drm_0u} \\ &= \eta^{2rm_0u} + \eta^{-2rm_0u} \\ &= (\eta^{rm_0u} - \eta^{-rm_0u})^2 + 2 \ , \end{aligned} \tag{3.145}$$

where in the second step we use the fact that $\Delta^{2m_0} = \eta^{2rm_0}\eta^{2drm_0} = 1$. Note that $\mathrm{Tr}(G^{2m_0u}) = 2$ if and only if $\eta^{2rm_0u} = 1$, or equivalently, $2rm_0u$ is a multiple of $(p-1)(d+1)$. Since $2m_0$ is the order of Δ, which is an element of a group of order $p-1$, $2m_0$ must be a factor of $(p-1)$. Therefore ru is a multiple of $(d+1)(p-1)/2m_0$, hence a multiple of $d+1$. Taking into account the fact that r is co-prime to $d+1$, we deduce that u must be a multiple of $d+1$ and therefore must be zero, since $0 \le u \le d$. Therefore, for $1 \le u \le d$, we have $\mathrm{Tr}(G^{2m_0u}) \neq 2$, and

$$\mathrm{Tr}\left(U_{G^{2m_0}}^u\right) = \mathrm{Tr}\left(U_{G^{2m_0u}}\right) = l\left((\eta^{rm_0u} - \eta^{-rm_0u})^2\right) \ , \tag{3.146}$$

which equals 1 if $\eta^{rm_0u} - \eta^{-rm_0u} \in \mathbb{F}_d$, and -1 otherwise. To determine this, we notice

$$\begin{aligned}(\eta^{rm_0u} - \eta^{-rm_0u})^d &= \eta^{drm_0u} - \eta^{-drm_0u} \\ &= (-1)^{u+1}(\eta^{rm_0u} - \eta^{-rm_0u}) \ ,\end{aligned} \tag{3.147}$$

where in the last step we make use of the fact that $\eta^{drm_0} = -\eta^{-rm_0}$ since $\Delta^{m_0} = -1$ according to (3.132). Hence, $\eta^{rm_0u} - \eta^{-rm_0u} \in \mathbb{F}_d$ if and only if u is odd, and therefore

$$\mathrm{Tr}\,(U^u_{G^{2m_0}}) = (-1)^{u+1} \qquad 1 \leq u \leq d \ . \tag{3.148}$$

For $u = 0$, clearly $\mathrm{Tr}(U^u_{G^{2m_0}}) = \mathrm{Tr}(\mathbb{1}) = d$. We now evaluate (3.143) to conclude the proof:

$$\dim \mathcal{S}_1 = \frac{1}{d+1}\left(d + \sum_{u=1}^{d}(-1)^{u+1}\right) = 1 \ . \tag{3.149}$$

□

Lemma 3.11. *Every MUB-cycling U_G has a non-zero eigenvector $|\psi\rangle \in \mathbb{Q}(\omega)^d$ with unit eigenvalue, i.e.*

$$U_G\,|\psi\rangle = |\psi\rangle \ . \tag{3.150}$$

Proof. From Lemma 3.10 we know that the unitary $U_{G^{2m_0}}$ has exactly one eigenvalue equal to 1, implying $\det(U_{G^{2m_0}} - \mathbb{1}) = 0$, which in turns means the system of linear equations $(U_{G^{2m_0}} - \mathbb{1})X = 0$ has a non-trivial solution. Since the matrix elements of $U_{G^{2m_0}}$ are in the cyclotomic field $\mathbb{Q}(\omega)$, there exists a non-zero vector $|\phi\rangle \in \mathbb{Q}(\omega)^d$ so that $U_{G^{2m_0}}\,|\phi\rangle = |\phi\rangle$. Since

$$U_{G^{2m_0}}U_G\,|\phi\rangle = U_G U_{G^{2m_0}}\,|\phi\rangle = U_G\,|\phi\rangle \tag{3.151}$$

and since $\mathcal{S}_1$ is one-dimensional, we must have

$$U_G\,|\phi\rangle = \lambda\,|\phi\rangle \ , \qquad \lambda \in \mathbb{Q}(\omega) \ . \tag{3.152}$$

Repeatedly applying U_G to this equation and recalling the fact $U_G^{2m_0} = \mathbb{1}$, we see that λ has to satisfy

$$\lambda g_\Delta(\lambda) \ldots g_\Delta^{2m_0-1}(\lambda) = 1 \ . \tag{3.153}$$

By Theorem A.2 (a variant of Hilbert's Theorem 90), there exists $\mu \in \mathbb{Q}(\omega)$ such that

$$\lambda = \mu / g_\Delta(\mu) \ . \tag{3.154}$$

If we define $|\psi\rangle = \mu\,|\phi\rangle$, it immediately follows that $U_G\,|\psi\rangle = |\psi\rangle$ as desired. □

Lemma 3.12. *Any eigenvector of a MUB-cycler U_G is also an eigenvector of the parity operator A defined in (3.134), with eigenvalue $(-1)^{(p-1)/2}$.*

Proof. Appealing again to the fact that $\Delta^{m_0} = -1$, and the result from Theorem 3.5 that $G^{d+1} = \Delta I$, we have $G^{(d+1)m_0} = P$ (where $P = -I$), and therefore

$$\begin{aligned} A &= (-1)^{(p-1)/2} U_P \\ &= (-1)^{(p-1)/2} U_{G^{(d+1)m_0}} \\ &= (-1)^{(p-1)/2} (U_G^{2m_0})^{(d+1)/2} \end{aligned} \tag{3.155}$$

Let $|\phi\rangle$ be an eigenvector of U_G, then by Lemma 3.9 we have $U_G^{2m_0} |\phi\rangle = |\phi\rangle$. It follows that $A |\phi\rangle = (-1)^{(p-1)/2} |\phi\rangle$, which concludes the proof of the lemma.

□

Remark. Since every MUB-cycling g-unitary has exactly one eigenvector (up to a scalar multiplication), $|\phi\rangle$ is an eigenvector of $U_{G_0^r}$ if and only if it is an eigenvector of U_{G_0}, where G_0 is defined in (3.127). As every MUB-cycler is conjugate to G_0^r (for some r co-prime to $d+1$), it then follows that the eigenvectors of all MUB-cycling g-unitaries form a single orbit under the extended Clifford group.

3.9 MUB-balanced states

In section 3.8 we showed that when the dimension d is an odd power of an odd prime, every MUB-cycling g-unitary has an eigenvector, which is unique up to a scalar multiplication. Additionally, if $d = 3 \bmod 4$, as we will show in this section, these eigenvectors have an extra property: they are MUB-balanced states. The concept of MUB-balanced states was recently introduced by Amburg *et al* [6]. Rotationally invariant states previously constructed by Sussman and Wootters in even prime power dimensions [5, 134] also have this property. These states all belong to a larger class of quantum states called Minimum Uncertainty States (MUS) [1, 5, 6, 134]. In the case $d = 1 \bmod 4$, our numerical calculations in low dimensions (up to $d = 31$) show that the eigenvectors of MUB-cyclers are neither MUB-balanced states nor MUS.

Given a full set of MUBs, a MUB-balanced state is one whose measurement outcome probabilities with respect to every basis are the same up to a permutation. Let $|\psi\rangle$ be a normalized state, let $|b, v\rangle$ denote the MUB vectors, where $b \in \{0, 1, ..., d-1, \infty\}$ labels the bases, and $v \in \{0, 1, ..., d-1\}$ labels the vectors in a basis, and let

$$p_{b,v} = |\langle \psi | b, v \rangle|^2 \tag{3.156}$$

be the measurement probabilities. Then $|\psi\rangle$ is a MUB-balanced state if and only if for each basis b, there exists a permutation σ such that

$$p_{b,v} = p_{0,\sigma(v)} \tag{3.157}$$

for all v. It follows from an argument in [5] that MUB-balanced states have to be MUS. For completeness, it is worth providing a sketch of this argument. Let

$$H_b = -\log_2\left(\sum_v p_{b,v}^2\right) \tag{3.158}$$

be the quadratic Rényi entropy in basis b. One can show that the total entropy $T = \sum_b H_b$ satisfies the inequality

$$T \geq (d+1)\log_2\left(\frac{d+1}{2}\right) \tag{3.159}$$

which turns out to be saturated if and only if for all b

$$\sum_v p_{b,v}^2 = \frac{2}{d+1}. \tag{3.160}$$

States that saturate the bound in (3.159) are called minimum uncertainty states (MUS). For a MUB-balanced state, $\sum_v p_{b,v}^2$ is independent of b. Together with the fact that

$$\sum_{b,v} p_{b,v}^2 = 2, \tag{3.161}$$

it clearly follows that a MUB-balanced state is consequently a MUS. MUB-balancedness is therefore a stricter condition than minimum uncertainty.

The main result of this section is stated in the following theorem.

Theorem 3.13. *Let the dimension $d = p^n$ be a prime power satisfying $d = 3 \mod 4$ (the exponent n therefore has to be odd), and let $G \in \mathrm{GL}_p(2, \mathbb{F}_d)$ be a MUB-cycler. Let $|\phi\rangle$ be a normalized eigenvector of $U_G^{2m_0}$ with eigenvalue 1 as defined in Theorem 3.8, then $|\phi\rangle$ is MUB-balanced.*

Remark. The g-unitary U_G plays a crucial part in the following proof. However, for the practical purpose of calculating $|\phi\rangle$, it suffices to work with the ordinary unitary $U_G^{2m_0}$. Moreover, since the eigenstates of MUB-cycling g-unitaries form a single orbit of the extended Clifford group, we only need to prove the theorem for the case of MUB-cycling anti-unitaries. We will proceed with the general case of an arbitrary g-unitary nevertheless. This way one will see why it does not work for the case $d = 1 \mod 4$.

Proof. Recall from Lemma 3.6 and Theorem 3.7 that $\Delta = \det(G)$ can be written as

$$\Delta = \theta^{r(d-1)/(p-1)}, \tag{3.162}$$

where θ is a primitive element of $\mathbb{F}_d$, and $\gcd(r, d+1) = 1$. By the assumption that n is odd, it follows that $r(d-1)/(p-1)$ is odd, so Δ is a quadratic non-residue. By Lemma 1 of reference [30], when $d = 3 \mod 4$ we also have -1 being a quadratic non-residue. Therefore $-\Delta$ is a quadratic residue, i.e. there exists $x \in \mathbb{F}_d$ such that $x^2 = -\Delta$. If we let F be arbitrary

$$F = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \tag{3.163}$$

and define a symplectic

$$S = \begin{pmatrix} x^{-1} & 0 \\ 0 & x \end{pmatrix}, \tag{3.164}$$

then it can be verified straightforwardly that

$$SK_{-1}FK_{-1}S^{-1} = \begin{pmatrix} \alpha & \Delta^{-1}\beta \\ \Delta\gamma & \delta \end{pmatrix} = K_\Delta F K_\Delta^{-1}. \tag{3.165}$$

Note that K_{-1} is represented by complex conjugation, so in the g-unitary representation we have

$$U_S U_F^* U_S^{-1} = g_\Delta(U_F). \tag{3.166}$$

From Theorem 3.8 we know that there exists $|\psi\rangle$ such that $U_G |\psi\rangle = |\psi\rangle$. We can write

$$|\psi\rangle\langle\psi| = \lambda P_1 \tag{3.167}$$

for some constant λ, where P_1 is the projection operator defined in (3.142). Noting that (3.166) can be applied to P_1 and letting v be arbitrary, we now can calculate

$$\begin{aligned} g_\Delta(p_{0,v}) = g_\Delta\left(|\langle 0, v|\psi\rangle|^2\right) &= g_\Delta\left(\langle 0, v|\psi\rangle\langle\psi|0, v\rangle\right) \\ &= g_\Delta\left(\langle 0, v|\, \lambda P_1\, |0, v\rangle\right) \\ &= g_\Delta(\lambda) g_\Delta(\langle 0, v|) U_S P_1^* U_S^{-1} g_\Delta(|0, v\rangle) \\ &= \frac{g_\Delta(\lambda)}{\lambda^*} g_\Delta(\langle 0, v|) U_S\, |\psi\rangle^*\, \langle\psi|^*\, U_S^{-1} g_\Delta(|0, v\rangle) \\ &= \frac{g_\Delta(\lambda)}{\lambda^*} \left|\langle\psi|^*\, U_S^{-1} g_\Delta(|0, v\rangle)\right|^2 \\ &= \frac{g_\Delta(\lambda)}{\lambda^*} |\langle\psi|0, xv\rangle|^2 \\ &= \mu p_{0,xv}, \end{aligned} \tag{3.168}$$

where $\mu = g_\Delta(\lambda)/\lambda^*$ is a constant, and in the penultimate step we have used (3.10). Repeating this formula k times for an arbitrary integer k, we obtain

$$g_\Delta^k(p_{0,v}) = \mu_k \; p_{0,x^k v} \tag{3.169}$$

where $\mu_k = g_\Delta^{k-1}(\mu) g_\Delta^{k-2}(\mu) ... \mu$ is independent of v.

Since U_G is a cycling g-unitary, for every basis b there exists an integer k such that

$$|b, v\rangle \doteq U_G^k \, |0, \sigma(v)\rangle \tag{3.170}$$

for all v. In the above expression "$\doteq$" means "equal up to a phase" and σ is a permutation dependent only on b. It follows that

$$\begin{aligned} \langle \psi | b, v\rangle &\doteq \langle \psi | \, U_G^k \, |0, \sigma(v)\rangle \\ &= g_\Delta^k \left(\langle U_G^{-k} \psi | 0, \sigma(v)\rangle \right) \\ &= g_\Delta^k \left(\langle \psi | 0, \sigma(v)\rangle \right). \end{aligned} \tag{3.171}$$

Consequently,

$$p_{b,v} = g_\Delta^k \left(p_{0,\sigma(v)} \right) = \mu_k p_{0,x^k \sigma(v)}. \tag{3.172}$$

Since $p_{b,v}$ are probabilities, we must have

$$\sum_v p_{b,v} = \sum_v p_{0,x^k \sigma(v)} = 1. \tag{3.173}$$

This implies $\mu_k = 1$, which in turn implies that the normalized state

$$|\phi\rangle = \frac{|\psi\rangle}{\sqrt{|\langle \psi | \psi \rangle|}} \tag{3.174}$$

is MUB-balanced.

□

Remark. The MUB-balanced states established in this theorem are identical to those constructed by Amburg *et al* using a completely different method [6]. In their paper, the orbit of states is generated from the state corresponding to the discrete Wigner function

$$W_{\mathbf{p}} = \frac{1}{d(d+1)} \left(1 - d\delta_{\mathbf{p},\mathbf{0}} + \sum_{x \in \mathbb{F}_d^*} l(x^2+1) \omega^{\mathrm{tr}(x p_1^2 + x p_2^2)} \right). \tag{3.175}$$

Let us define a specific element in $\mathrm{GL}(2, \mathbb{F}_d)$

$$G = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}, \tag{3.176}$$

with

$$\alpha = (\eta + \eta^d)/2 \qquad \beta = i_M(\eta - \eta^d)/2, \tag{3.177}$$

where $i_M = \eta^{(p-1)(d+1)/4}$ is a modular analogue of i (notice that $i_M^2 = -1$), and η is defined in Lemma 3.6. Using basic finite-field facts (see Section A.1.4), one can check that

$$\alpha^d = \alpha \qquad \beta^d = \beta, \tag{3.178}$$

so α and β belong to the field $\mathbb{F}_d$. Thus G is indeed an element of $\mathrm{GL}(2, \mathbb{F}_d)$. Furthermore, G has trace

$$\mathrm{Tr}(G) = \eta + \eta^d \tag{3.179}$$

and determinant

$$\Delta = \det(G) = \eta^{d+1}, \tag{3.180}$$

and therefore, by Theorem 3.7, it is a MUB-cycler. Since

$$(\alpha p_1 + \beta p_2)^2 + (-\beta p_1 + \alpha p_2)^2 = \Delta(p_1^2 + p_2^2), \tag{3.181}$$

it clearly follows that

$$W_{G\mathbf{p}} = g_\Delta(W_\mathbf{p}). \tag{3.182}$$

Let ρ be the density matrix corresponding to $W_\mathbf{p}$ given by:

$$\rho = \sum_\mathbf{p} W_\mathbf{p} A_\mathbf{p}, \tag{3.183}$$

where the phase point operators $A_\mathbf{p}$ are defined in (3.66). It follows from (3.182) and (3.69) that

$$U_G \rho U_G^{-1} = \rho. \tag{3.184}$$

In view of a result from reference [6] that the state corresponding to $W_\mathbf{p}$ is a pure state, one can now conclude that this state is an eigenvector of the MUB-cycling g-unitary U_G. The Wigner functions of these MUB-balanced states for dimension 7 and 11 are visualized in Figure 3.4.

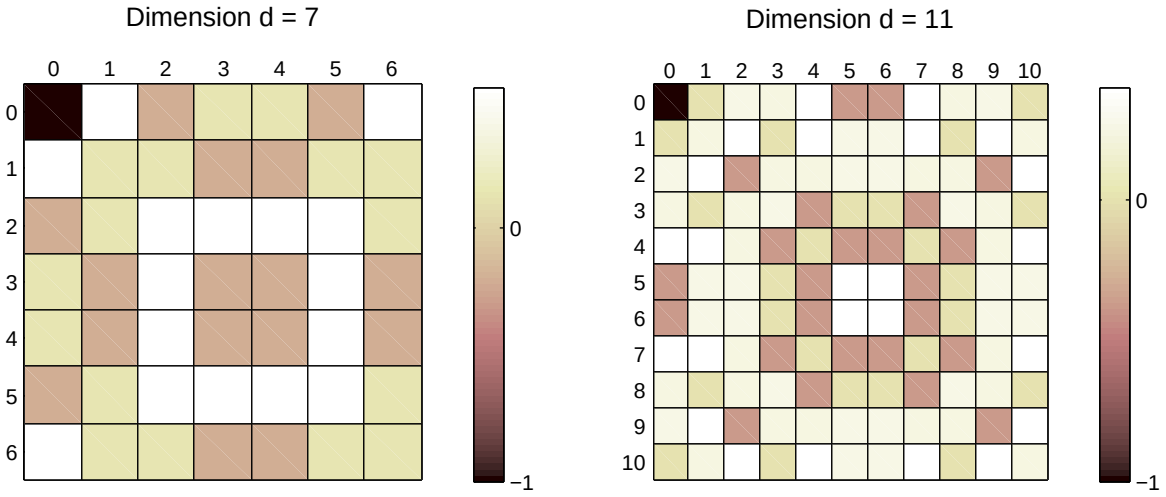

Figure 3.4: Color plots of the scaled Wigner function ($dW_{\mathbf{p}}$) corresponding to ρ in dimension $d = 7$ and 11. The axes of the discrete phase space are labeled by the two components of $\mathbf{p} = (p_1, p_2)$. The rotational invariance property is manifested via concentric "circles" on the discrete plane.

One might want to ask how many MUB-balanced states arising from MUB-cycling g-unitaries there are. Let us consider the MUB-cycler U_{G_0} where G_0 is the matrix with multiplicative order $2m_0 = p - 1$ defined in (3.127). Let $|\psi\rangle$ be the corresponding MUB-balanced state. By Theorem 3.8, we know $|\psi\rangle$ is the unique eigenvector of the unitary $U_{G_0}^{p-1}$ with eigenvalue 1. Therefore it will be left invariant by any element V of the extended Clifford group satisfying

$$VU_{G_0}^{p-1}V^{-1} = U_{G_0}^{(p-1)k} \tag{3.185}$$

for some integer k. It turns out that the only possible values for k are ± 1 and

$$V = U_{G_0^{m(p-1)/2}} \tag{3.186}$$

when $k = 1$, or

$$V = U_{G_0^{m(p-1)/2}F} \tag{3.187}$$

when $k = -1$, where

$$F = \begin{pmatrix} 0 & i_M\eta^{(d+1)/2} \\ i_M\eta^{-(d+1)/2} & 0 \end{pmatrix} \tag{3.188}$$

is a symplectic matrix satisfying $FG_0^{p-1}F^{-1} = G_0^{-(p-1)}$ and m can take any integer value from 0 to $2d + 1$. Hence, there are $4d + 4$ possibilities for V.

Conjecture. We conjecture that there are no other unitaries or anti-unitaries in the extended Clifford group that leave $|\psi\rangle$ invariant. As the order of the extended Clifford group is $2d^3(d^2-1)$ [135], the number of MUB-balanced states would therefore be $d^3(d-1)/2$.

Dimension	ord($\mathcal{E}_d$)	MUB-cyclers	MUB-balanced
$d = 7$	32,928	504	1,029
$d = 11$	319,440	2,200	6,655
$d = 19$	4,938,480	24,624	61,731

Table 3.3: The order of the extended Clifford group, the number of MUB-cyclers and the number of distinct MUB-balanced states found in dimensions 7, 11 and 19.

We have checked the conjecture in detail for dimensions $d = 7, 11, 19$. The numbers reported in Table 3.3 agree with our prediction. Originally, we expected that our construction technique would yield many new MUB-balanced states in addition to those found by Amburg *et al*. Our results, however, suggest that Amburg *et al* have indeed constructed the entire set. If this is true, it means that MUB-balanced states form a highly distinguished geometrical structure. They seem to be even rarer than SICs: in most of the dimensions that have been analyzed, there exist more than one orbits of SICs, whereas MUB-balanced states seem to come only in a single orbit. They ''have no right to exist'', as Amburg *et al* has put it. Of course this should not be taken literally, as we know they do exist after all. Our work provides one way of explaining their right of existence, by unveiling a new underlying g-unitary symmetry.

Chapter 4

Summary and Outlook

4.1 Summary of main results

We chose to study SICs as we believed such a symmetric structure in the Hilbert space could reveal deep insights into quantum theory. One of our results reveals the geometric significance of SICs on the cone of non-negative operators: SICs are the closest to being orthogonal bases. Explicitly, they form the only sets of d^2 normalized positive semidefinite operators that minimize a class orthogonality measures K_t defined to be

$$K_t = \sum_{i \neq j} \left(\mathrm{Tr}(A_i A_j)\right)^t \qquad t \in \mathbb{R},\ t > 1. \tag{4.1}$$

Studying SICs naturally led us to a study of the Weyl-Heisenberg symmetry - the group symmetry that finite dimensional quantum mechanics was built upon in the very early years. While studying orbits of quantum states under the WH group, we observed that under certain conditions, among d^2 vectors in the orbits one can find sets of d vectors that are linearly dependent. We proved in Theorem 2.2 that if the initial vector belongs to certain eigenspaces (depending on the dimension d) of the Zauner unitary, and if a set of d vectors consists of certain combinations of triplets and singlets, linear dependency will occur. In dimensions $d = 3$ this explains the 3 linear dependencies that arise from arbitrary SIC fiducial vectors in the known SIC family. Interestingly, there are special SICs in this family that give rise to 9 linear dependencies. This fact is connected to the Hesse configuration in the theory of elliptic curves. We performed an exhaustive numerical search for linear dependencies in dimensions $d = 4$ to 9. The only other case where we

observed extra linear dependencies from a SIC fiducial (compared to an arbitrary initial vector from the same eigenspace of $U_{\mathcal{Z}}$) is when the SIC fiducial lies in $\mathcal{H}_{\eta^2}$ in dimension $d = 8$. In dimension $d = 6$ and $d = 9$ we analyzed in detail the relations among normal vectors of hyperplanes spanned by linearly dependent sets. Besides some orthogonality relations, we observed that some of these normal vectors always formed 2-dimensional and 3-dimensional SICs, even though the initial vector is not a SIC fiducial. We were able to provide an analytical explanation for the observed 2-dimensional small SICs in $d = 6$.

SICs are also the motivation for the construction of g-unitary operators. In Chapter 3 we describe a toy model for SICs, in which g-unitaries were constructed from the simple Galois groups of cyclotomic field extensions, and we studied their actions on MUBs. We have gone through a large amount of technical details, which are summarized in Theorems 3.2, 3.5, 3.7, 3.8 and 3.13. However, the picture can be better summarized in words.

G-unitaries are constructed to generalize the notion of anti-unitaries. However, their action is restricted only to vectors whose components belong to some special number field, which is the cyclotomic field in our case. In this case, g-unitaries play role in the description of MUBs in odd prime power dimensions. Their actions on the MUB vectors can be interpreted as rotations in Bloch space, just as any ordinary unitary operator.

We studied projective transformations that permute mutually unbiased bases. In odd prime power dimension $d = p^n$ where n is odd, we showed that there are transformations that cycle through the full set of $d + 1$ bases and that can be realized by g-unitaries. If $d = 3 \bmod 4$, these transformations can be effected by anti-unitaries, but if $d = 1 \bmod 4$, we need to appeal to g-unitaries. We studied the eigenvectors of these MUB-cycling g-unitaries and showed every MUB-cycling g-unitary always had a unique eigenvector (up to a scalar multiplication). Furthermore, we can always choose a scalar so that this eigenvector is invariant under the g-unitary, in which case we proved that it is also invariant under the parity operator.

When $d = 3 \bmod 4$, we proved that the invariant eigenvectors of MUB-cycling g-unitaries are MUB-balanced states. Our construction can be considered as a supplement to work done by Amburg *et al* [6] in two ways. First, while the construction of Amburg *et al* was done using Wigner functions, our construction was done directly in the Hilbert space. Secondly, our technique provides a connection to the original construction in even prime power by Wootters and Sussman [5] in which MUB-balanced states were found to be eigenvectors of MUB-cycling unitaries. In our case, because of the lack of cycling unitaries in odd prime power dimensions, we instead used cycling g-unitaries. Originally, we expected that our construction would yield more MUB-balanced states, since we were able to expose the underlying symmetry and found all such states with this symmetry. However, the

results suggest that these states all lie on a single orbit the the extended Clifford group, which is remarkable since even rare quantum states like SICs come in more than one orbits in many dimensions that have been analyzed.

G-unitary symmetry for the simple case of cyclotomic field extensions has provided us a thorough understanding of the ''right to exist'' of a distinguished class of quantum states, namely MUB-balanced states. Extending our analysis to g-unitaries that are applicable to SIC states or some other special quantum states is a non-trivial task. However, we hope that our results can be considered as a first useful step in the direction of solving the SIC problem, as we believe that symmetries play very important roles in solving hard problems in physics.

4.2 List of open problems

The following list brings up research questions or problems we have not been able to answer that are worth further investigation.

1. As discussed in Section 2.3.3, there are more linearly dependent sets observed numerically than what can be accounted for by Theorem 2.2. An explanation for this is still left open.

2. Small 3-dimensional SICs arising from normal vectors of the hyperplanes spanned by linearly dependent sets in $d = 9$ are observed, but have not yet been fully understood.

3. An exhaustive search for small SICs in $d = 12$ has not been done. It is also an open question if small SICs can be found in other dimensions rather than $d = 6$ and 9.

4. In the study of g-unitaries, we only found eigenvectors for a special class of them, namely those that have the MUB-cycling property. It is an open question whether other g-unitaries also have eigenvectors, and how to find them.

5. We have counted the number of MUB-balanced states for small dimensions in Table 3.3. It remains as a conjecture that the number of MUB-balanced states in every odd prime power dimensions equal to 3 mod 4 is $d^3(d-1)/2$.

Appendix A

Appendices

A.1 Field theory

The theory of fields is a major branch in mathematics that has been studied extensively. In the scope of the thesis we use a number of elementary facts in field theory. We devote this section as an introduction to fields, field extensions, Galois automorphisms, and finite fields, for readers with little or no background in field theory. Besides finite fields, which play an important role in the theory of Mutually Unbiased Bases, we also discuss infinite fields, especially cyclotomic fields, which are crucial for our construction of g-unitaries in Chapter 3. With the purpose of helping the readers quickly grasp the relevant key concepts, we avoid unnecessarily technical definitions and derivations as much as we can. Rigorous treatments of the subjects can be found in textbooks on fields and Galois theory [136–139].

Definition. A field $\mathbb{F}$ is a set together with two operations addition and multiplication (denoted by $+$ and $\cdot$) such that for all $a, b, c \in \mathbb{F}$ the following axioms hold.

1. Closure: $a + b$ and $a \cdot b$ are in $\mathbb{F}$.
2. Associativity: $a + (b + c) = (a + b) + c$ and $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. Commutativity: $a + b = b + a$ and $a \cdot b = b \cdot a$.
4. Identity elements: there exists an additive identity 0 such that $a + 0 = a$ for all $a \in \mathbb{F}$, and there exists a multiplicative identity 1 such that $a \cdot 1 = a$ for all $a \in \mathbb{F}$.

5. Inverses: for every $a \in \mathbb{F}$ there exists an element $-a$ such that $a + (-a) = 0$, and for every non-zero $a \in \mathbb{F}$ there exists an element a^{-1} such that $a \cdot a^{-1} = 1$. These imply the existence of subtraction and division operations.

6. Distributivity: $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$.

Remark. A field $\mathbb{F}$ consists of two abelian groups ($\mathbb{F}$ under addition, and $\mathbb{F} \setminus \{0\}$ under multiplication), whose operations are compatible in the sense of the distributivity law.

Example. Common examples include the field of all rational numbers $\mathbb{Q}$ and field of all real numbers $\mathbb{R}$ under ordinary addition and multiplication. There also exist finite fields, i.e. fields with a finite number of elements. For example, if p is a prime number, then the set of integers $\mathbb{Z}_p = \{0, 1, .., p-1\}$ with addition and multiplication modulo p forms a field, called a prime field. To see why multiplicative inverses exist in $\mathbb{Z}_p$, take any non-zero element $x \in \mathbb{Z}_p$ and consider $p-1$ products xk where $k = 1, 2, ..., p-1$. As p is prime we cannot have $x(k_1 - k_2) = 0 \pmod{p}$ for $k_1 \neq k_2 \pmod{p}$. Therefore these products are distinct and they must take all $p-1$ non-zero values in $\mathbb{Z}_p$ including 1.

A.1.1 Field extensions

Example. The concept of field extensions is best illustrated by the example of the construction of $\mathbb{C}$, the complex field that quantum physicists are very familiar with. We start with the real field $\mathbb{R}$ and an observation that the polynomial $x^2 + 1$ is irreducible over $\mathbb{R}$. If we define an imaginary number i by the property $i^2 + 1 = 0$, then it does not belong to $\mathbb{R}$, and we can extend $\mathbb{R}$ to include i by defining the complex field $\mathbb{C}$ as the set of all numbers of the form:

$$\mathbb{C} \equiv \{a + ib : a, b \in \mathbb{R}\}. \tag{A.1}$$

The addition rule in the new field $\mathbb{C}$ can be straightforwardly defined as

$$(a_1 + ib_1) + (a_2 + ib_2) = (a_1 + a_2) + i(b_1 + b_2). \tag{A.2}$$

For the multiplication rule we use the defining property of i, namely $i^2 = -1$, to derive

$$\begin{aligned}(a_1 + ib_1)(a_2 + ib_2) &= a_1a_2 + i(a_1b_2 + a_2b_1) + i^2b_1b_2 \\ &= (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1).\end{aligned} \tag{A.3}$$

One can think of a complex number $(a + ib)$ as a 2-component vector (a, b) in a real vector space. The dimensionality of this vector space is equal to the degree of the polynomial defining i, namely 2. The construction of $\mathbb{C}$ in (A.1) can be generalized as follows.

Given a field $\mathbb{F}$ and a number $h \notin \mathbb{F}$, let $\mathbb{E}$ be the smallest field containing both h and $\mathbb{F}$, denoted by $\mathbb{E} \equiv \mathbb{F}(h)$. $\mathbb{F}$ is called the ground field, $\mathbb{E}$ is called the extended field or the extension field, the field extension (not to be confused with the extension field) is denoted by $\mathbb{E}/\mathbb{F}$ (reads as $\mathbb{E}$ over $\mathbb{F}$), and h is called a field generator. Field generators need not be unique. For example, for the field extension $\mathbb{C}/\mathbb{R}$ instead of i we could also use $-i$ as a generator.

Definition. Assume that h is algebraic over $\mathbb{F}$, meaning that it is a root of a polynomial with coefficients in $\mathbb{F}$. Among all such polynomials that admit h as a root, let

$$P(x) = x^n + c_{n-1}x^{n-1} + ... + c_1 x + c_0 \qquad (c_i \in \mathbb{F}) \tag{A.4}$$

be the one with the lowest degree having the leading coefficient equal to one ($P(x)$ is called the minimal polynomial of h over $\mathbb{F}$). The extended field $\mathbb{E}$ can then be constructed as

$$\mathbb{E} \equiv \mathbb{F}(h) = \{f_0 + f_1 h + ... + f_{n-1}h^{n-1} : f_i \in \mathbb{F}\} \ . \tag{A.5}$$

Remark. We do not include higher powers of h in (A.5) because they can be reduced to powers smaller than n by the property of h being a root of a polynomial of degree n. One can see that $\mathbb{E}$ is closed under addition, subtraction, and multiplication, and it can be shown to be also closed under division [137]. $\mathbb{E}$ can be regarded as an n-dimensional vector space over $\mathbb{F}$, and n is called the degree of the field extension $\mathbb{E}/\mathbb{F}$.

A.1.2 Galois automorphisms

Definition. Given a field extension $\mathbb{E}/\mathbb{F}$ ($\mathbb{E}$ is an extension of $\mathbb{F}$), a Galois automorphism of the extension $\mathbb{E}/\mathbb{F}$ is defined as an automorphism of $\mathbb{E}$ that fixes elements in $\mathbb{F}$. In other words, it is a bijective mapping $g : \mathbb{E} \to \mathbb{E}$ that has the following properties.

1. $g(e_1 + e_2) = g(e_1) + g(e_2)$ for all $e_1, e_2 \in \mathbb{E}$.
2. $g(e_1 e_2) = g(e_1)g(e_2)$ for all $e_1, e_2 \in \mathbb{E}$.
3. $g(f) = f$ for all $f \in \mathbb{F}$.

Remark. It follows from the definition that if a Galois automorphism g takes an element $x \in \mathbb{E}$ to the ground field $\mathbb{F}$, then x has to belong to the ground field itself, or else g fails to be a bijective mapping.

Definition. The Galois automorphisms form a group called the Galois group of the extension $\mathbb{E}/\mathbb{F}$, denoted by $\mathrm{Gal}(\mathbb{E}/\mathbb{F})$.

One property of the Galois group is that its order is less than or equal to the degree of the field extension. To see why we first note that if $\mathbb{E} = \mathbb{F}(h)$ and $g \in \mathrm{Gal}(\mathbb{E}/\mathbb{F})$, then the value of $g(h)$ determines the value of $g(e)$ for every element $e \in \mathbb{E}$, as can be clearly seen from the defining properties of Galois automorphisms and from the construction of $\mathbb{E}$ in (A.5). In other words, a Galois automorphism g is completely specified by its action on a generator. Secondly, we notice that when we apply g to both sides of the equation $P(h) = 0$, where $P(x)$ is the minimal polynomial of h with the form given in (A.4), g does not act on the polynomial coefficients because they are in the ground field $\mathbb{F}$, therefore

$$(g(h))^n + a_{n-1}(g(h))^{n-1} + ... + a_1 g(h) + a_0 = 0, \tag{A.6}$$

which implies that $g(h)$ is also a root of $P(x)$. Since $P(x)$ has degree n, the number of values of $g(h)$ is at most n, and hence, so is the number of Galois automorphisms. When the Galois group has the same order as the degree of the extension, the extension is called a Galois extension. This has an important mathematical implication, namely the fundamental theorem of Galois theory. Although this theorem is not invoked in the thesis, we do want to note that all the field extensions used in the thesis are in fact Galois extensions.

Example. Let us go back to the example of the extension of the real field $\mathbb{R}$ to the complex field $\mathbb{C}$. If $g : \mathbb{C} \to \mathbb{C}$ is a Galois automorphism of the extension $\mathbb{C}/\mathbb{R}$, then it must satisfy

$$g(i)g(i) = g(i^2) = g(-1) = -1 \ , \tag{A.7}$$

which implies either $g(i) = i$ or $g(i) = -i$. If $g(i) = i$, then for any $a, b \in \mathbb{R}$ we have $g(a + ib) = g(a) + g(i)g(b) = a + ib$, meaning that g is the identity mapping. If $g(i) = -i$, then $g(a + ib) = a - ib$, so g is complex conjugation. The Galois group for the extension $\mathbb{C}/\mathbb{R}$ therefore consists of only two elements: the identity mapping and complex conjugation. It is a Galois extension because the group has order 2, which is same as the degree of the extension.

When viewed as functions from $\mathbb{E}$ to $\mathbb{F}$, Galois automorphisms are linearly independent, as shown in the following theorem.

Theorem A.1 (Dedekind)**.** *Given an extension $\mathbb{E}/\mathbb{F}$, let $\{g_i\}_{i=1}^n$ be its Galois group then g_i's are linearly independent functions from $\mathbb{E}$ to $\mathbb{F}$, meaning that for $a_1, a_2, ..., a_n \in \mathbb{E}$,*

$$a_1 g_1(x) + a_2 g_2(x) + \ldots + a_n g_n(x) = 0 \quad \textit{for all } x \in \mathbb{E} \tag{A.8}$$

if and only if each and every $a_i = 0$. It then follows that any non-zero linear combination of Galois automorphisms is a non-zero mapping.

Remark. Dedekind's theorem in fact holds for a larger class of functions called characters. Here we restrict ourselves to Galois automorphisms, but the proof is the identical.

Proof. Suppose we have a zero function

$$a_1 g_1 + a_2 g_2 + \ldots + a_k g_k = 0 \tag{A.9}$$

for some $a_1, a_2, ..., a_k \in \mathbb{E}$. We will prove by induction that all the coefficients a_i must be zero. As none of the Galois automorphisms is zero, the statement is clearly true for $k = 1$. For $k > 1$, because $g_1 \neq g_k$, we can find an element $x_0 \in \mathbb{E}$ such that $g_1(x_0) \neq g_k(x_0)$. Multiplying equation (A.9) by $g_k(x_0)$ we get

$$a_1 g_k(x_0) g_1 + \ldots + a_k g_k(x_0) g_k = 0 \ . \tag{A.10}$$

Evaluate (A.9) at $x_0 x$ we get

$$a_1 g_1(x_0) g_1(x) + \ldots + a_k g_k(x_0) g_k(x) = 0 \ , \tag{A.11}$$

which, as x can take any value in $\mathbb{E}$, implies

$$a_1 g_1(x_0) g_1 + \ldots + a_k g_k(x_0) g_k = 0 \ . \tag{A.12}$$

Subtracting (A.10) from the above equation we obtain

$$a_1 \left[g_1(x_0) - g_k(x_0)\right] g_1 + \ldots + a_{k-1} \left[g_{k-1}(x_0) - g_k(x_0)\right] g_{k-1} = 0 \ , \tag{A.13}$$

which, by the induction hypothesis, implies $a_1 = 0$. Removing the a_1 term in (A.9) and appealing to the induction hypothesis again, we then deduce $a_2 = \ldots = a_k = 0$. □

A.1.3 Cyclotomic fields

Definition. A cyclotomic field $\mathbb{Q}(\omega)$ is an extension field generated from the rational field $\mathbb{Q}$ and a primitive N-th root of unity $\omega = e^{2\pi i/N}$. Although cyclotomic fields can be defined for any N, we will restrict ourselves to the case when $N = p$ is a prime number. In such a case, the minimal polynomial of ω over $\mathbb{Q}$ is

$$P(x) = 1 + x + x^2 + ... + x^{p-1} \ , \tag{A.14}$$

and the elements of the cyclotomic field $\mathbb{Q}(\omega)$ are of the form

$$\mathbb{Q}(\omega) = \{q_0 + q_1\omega + ... + q_{p-2}\omega^{p-2} : q_i \in \mathbb{Q}\} \ . \tag{A.15}$$

The extension $\mathbb{Q}(\omega)/\mathbb{Q}$ is of degree $p-1$. Let $g : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ be a Galois automorphism of the field extension. We then have the identity

$$(g(\omega))^p = g(\omega^p) = g(1) = 1 \ , \tag{A.16}$$

which implies that $g(\omega) = \omega^k$ for some integer k in the range $1 \leq k \leq p-1$ (the value of $g(\omega)$ cannot be 1 because ω does not belong to the ground field). If we specifically denote the Galois automorphism that maps $\omega \mapsto \omega^k$ by g_k, then $\{g_k\}_{k=1}^{p-1}$ forms the Galois group of order $p-1$ of this field extension. Note that g_1 is the identity mapping, and g_{p-1} is complex conjugation. A general element g_k can be thought of as a generalization of complex conjugation, and it is often called a Galois conjugation. Galois conjugations are the building blocks for our later construction of g-unitaries. For now we want to mention one more property of theirs, as stated in the following theorem.

Theorem A.2 (a variant of Hilbert's Theorem 90 [140])**.** *Let $g \in \mathrm{Gal}(\mathbb{Q}(\omega)/\mathbb{Q})$ be a Galois automorphism of order m, meaning that m is the smallest positive integer for which g^m is the identity mapping. If $\lambda \in \mathbb{Q}(\omega)$ satisfies*

$$\lambda g(\lambda)...g^{m-1}(\lambda) = 1 \ , \tag{A.17}$$

then there exists $\mu \in \mathbb{Q}(\omega)$ such that

$$\lambda = \mu / g(\mu) \ . \tag{A.18}$$

Proof. Let us consider a mapping $T : \mathbb{Q}(\omega) \to \mathbb{Q}(\omega)$ defined as

$$T(x) = x + a_1 g(x) + a_2 g^2(x) + ... + a_{m-1} g^{m-1}(x) \ , \tag{A.19}$$

where $a_i = \lambda g(\lambda)...g^{i-1}(\lambda)$. Note that

$$\lambda g(a_i) = a_{i+1} \qquad \text{for } i = 1, ..., m-2 \tag{A.20}$$

and

$$\lambda g(a_{m-1}) = \lambda g(\lambda)...g^{m-1}(\lambda) = 1 \ , \tag{A.21}$$

therefore we have

$$\lambda g(T(x)) = T(x) \ . \tag{A.22}$$

From Theorem A.1 we know that $T(x)$ is not a zero mapping, so there exists $x_0 \in \mathbb{Q}(\omega)$ such that $T(x_0) \neq 0$. If we define $\mu \equiv T(x_0)$, then (A.18) is immediately obtained. □

A.1.4 Finite fields

We have mostly dealt with fields that are infinite in size so far. Finite fields also come into play in the thesis, especially in the theory of Mutually Unbiased Bases (MUB) and in technical manipulations for MUB cyclers and their eigenvectors.

Definition. A finite field (somewhat confusingly also called a Galois field) is a field that has a finite number of elements, called its order.

The prime field $\mathbb{Z}_p$ for any prime number p is an example of a finite field, as previously mentioned. There are also finite fields of other orders. However, it is well known (dating back to Galois) that finite fields only exist for which the order is a prime power p^n, and that for every prime power there exists a unique (up to an isomorphism) field of this order. Thus, we can refer to a finite field only by its order, and we shall denote the finite field of order d by $\mathbb{F}_d$, where d must be a prime power for $\mathbb{F}_d$ to exist. We will not provide the proof here, but will instead give a concrete example of how to generate a larger finite extension field from a prime field $\mathbb{F}_p$.

Example. Consider the finite field $\mathbb{F}_2 = \{0, 1\}$ of order 2, and let $P(x) = x^2 + x + 1$. We see that $P(0) = P(1) = 1$, so $P(x)$ does not have a root in $\mathbb{F}_2$. We then define λ to be a root of $P(x)$ and define

$$\mathbb{F}_2(\lambda) = \{a + \lambda b : a, b \in \mathbb{F}_2\}. \tag{A.23}$$

One can see that $\mathbb{F}_4 \equiv \mathbb{F}_2(\lambda) = \{0, 1, \lambda, \lambda + 1\}$ has 4 elements and its addition and multiplication tables can be calculated using the identity $\lambda^2 + \lambda + 1 = 0$ as shown in Table A.1. In general, if we start from an irreducible polynomial of degree r in $\mathbb{F}_p$, we will be able to extend the field to $\mathbb{F}_{p^r}$.

$+$	0	1	λ	$\lambda+1$
0	0	1	λ	$\lambda+1$
1	1	0	$\lambda+1$	λ
λ	λ	$\lambda+1$	0	1
$\lambda+1$	$\lambda+1$	λ	1	0

$\cdot$	0	1	λ	$\lambda+1$
0	0	0	0	0
1	0	1	λ	$\lambda+1$
λ	0	λ	$\lambda+1$	1
$\lambda+1$	0	$\lambda+1$	1	λ

Table A.1: Addition and multiplication tables for the finite field $\mathbb{F}_4$.

We would like to mention a few basic properties of finite fields [139] that are frequently used in Section 3.7 and Section 3.8. First of all, every finite field admits a primitive element θ (there could be more than one) such that every non-zero element λ in the field can be written as $\lambda = \theta^k$ for some non-negative integer k smaller than the order of the field. Secondly, for $\mathbb{F}_p$ and its extension field $\mathbb{F}_d$, where $d = p^n$ is a prime power, the following statements hold:

1. $a^d = a \qquad \forall a \in \mathbb{F}_d$.
2. $(a+b)^p = a^p + b^p \qquad \forall a, b \in \mathbb{F}_d$.
3. $\forall a \in \mathbb{F}_d$, $a^p = a$ if and only if $a \in \mathbb{F}_p$.

A.1.5 Field trace

Definition. Given a Galois extension $\mathbb{E}/\mathbb{F}$, the field trace of an element $e \in \mathbb{E}$ denoted by $\mathrm{tr}(e)$ (we use the lower case to denote the field trace to distinguish it from the matrix trace) is defined as the sum of all Galois conjugates of e:

$$\mathrm{tr}(e) = \sum_{g \in \mathrm{Gal}\,(\mathbb{E}/\mathbb{F})} g(e). \tag{A.24}$$

One notices that $\mathrm{tr}(e)$ is left invariant by every Galois automorphism in the Galois group, which implies that $\mathrm{tr}(e)$ belongs to the ground field $\mathbb{F}$. Thus, field trace is a mapping from $\mathbb{E}$ to $\mathbb{F}$. Its following properties can be straightforwardly verified.

1. $\mathrm{tr}(e_1 + e_2) = \mathrm{tr}(e_1) + \mathrm{tr}(e_2)$ for all $e_1, e_2 \in \mathbb{E}$.
2. $\mathrm{tr}(fe) = f\,\mathrm{tr}(e)$ for all $e \in \mathbb{E}$ and $f \in \mathbb{F}$.

Example. For the $\mathbb{C}/\mathbb{R}$ extension, the Galois group only has 2 elements: the identity and complex conjugation. Therefore taking the field trace of a complex number,

$$\mathrm{tr}(c) = c + c^*, \tag{A.25}$$

is just the same as taking its real part (modulo a factor of 2).

For the extension $\mathbb{F}_d/\mathbb{F}_p$, where $d = p^n$ is a prime power (this will be the context in which we use field trace), there is a concrete formula for the field trace given by [139]

$$\mathrm{tr}(x) = x + x^p + x^{p^2} + ... + x^{p^{n-1}} \quad \forall x \in \mathbb{F}_d\ . \tag{A.26}$$

A.2 Finite-field construction of Clifford unitaries

The Clifford group is introduced in Section 2.2.3, in which we describe a construction of Clifford unitaries in a d-dimensional Hilbert space for a general d. We refer to those as the ordinary Clifford group. When d is a prime or a prime power, a finite field of order d exists (see Appendix A.1.4), providing us an aid to express the Weyl-Heisenberg group and Clifford unitaries in a slightly different way that is more convenient for certain purposes, such as in the constructions of MUBs (in Section 3.2) and Galois-unitaries (in Section 3.3). These variants of the WH and Clifford groups are referred to as Galoisian variants. Galoisian Clifford groups in turn come in two versions: a full and a restricted one, where the latter is a subgroup of the former [30]. Here we are only interested in the restricted version. To better illustrate how finite fields come into play, we will start with the simpler case of prime dimensions before going into the generalized case of prime power dimensions.

Note. This section is a review of some results already fully described by Appleby in [30]. There are other constructions for unitary representations of $\mathrm{SL}(2, \mathbb{F}_d)$ (for example by Chau [141]). We choose to use the one in [30] only for convenience.

A.2.1 In odd prime dimensions $d = p$

We start with the case of the Hilbert space's dimension $d = p$ being an odd prime. Let ω be a p-th primitive root of unity

$$\omega = e^{2\pi i/p}, \tag{A.27}$$

and let $\{|x\rangle : x = 0, 1, ..., p-1\}$ be the standard basis, where the labels on the states are elements of the finite field $\mathbb{Z}_p$, i.e. they are integers modulo p.

Definition. We define the shift operator X and the phase operator Z by their action on the basis states in the usual way:

$$X|x\rangle = |x+1\rangle \qquad\qquad Z|x\rangle = \omega|x\rangle\,. \tag{A.28}$$

Definition. The Weyl-Heisenberg displacement operators $D_{\mathbf{u}}$ are defined to be

$$D_{\mathbf{u}} = \omega^{u_1 u_2/2} X^{u_1} Z^{u_2} \qquad\qquad \mathbf{u} = \begin{pmatrix} u_1 \\ u_2 \end{pmatrix}, \tag{A.29}$$

where the two components u_1 and u_2 are elements of $\mathbb{Z}_p$ and $1/2$ denotes the inverse of 2 in that field.

Definition. For any two vectors $\mathbf{u}$ and $\mathbf{v}$ in the discrete phase space $\mathbb{Z}_p^2$, the symplectic form $\Omega(\mathbf{u}, \mathbf{v})$ is defined as

$$\Omega(\mathbf{u}, \mathbf{v}) = u_2 v_1 - u_1 v_2. \tag{A.30}$$

The phases $\omega^{u_1 u_2/2}$ in (A.29) allow us to write the group law in the form

$$D_{\mathbf{u}} D_{\mathbf{v}} = \omega^{\Omega(\mathbf{u},\mathbf{v})} D_{\mathbf{u}+\mathbf{v}}. \tag{A.31}$$

The symplectic form $\Omega(\mathbf{u}, \mathbf{v})$ has a geometrical meaning: if we consider $\mathbf{u}$ and $\mathbf{v}$ as vectors on the real plane $\mathbb{R}^2$, whose components happen to be integers modulo p, then $\Omega(\mathbf{u}, \mathbf{v})$ is the area of the parallelogram spanned by $\mathbf{u}$ and $\mathbf{v}$. Therefore it is sometimes also called the symplectic area. Let G be a linear transformation on the phase space, i.e. G is a 2×2 matrix whose entries are in $\mathbb{Z}_p$, and let

$$\Delta = \det(G). \tag{A.32}$$

It can be seen that under this linear transformation, the symplectic form is scaled by a factor of Δ:

$$\Omega(G\mathbf{u}, G\mathbf{v}) = \Delta \Omega(\mathbf{u}, \mathbf{v}). \tag{A.33}$$

Next, we want to define unitaries U_S, which are called symplectic unitaries for a reason that will become clear in a moment, so that their action on the Weyl-Heisenberg displacement operators takes the form

$$U_S D_{\mathbf{u}} U_S^{-1} = D_{S\mathbf{u}}. \tag{A.34}$$

Two conditions are required for this [30]. The first condition is that S has to be a linear transformation. The second one comes from the group law (A.31), from which it can be seen that S has to preserve the symplectic form. In view of (A.33), we deduce that S must have determinant one and must therefore belong to the symplectic group $\mathrm{SL}(2, \mathbb{Z}_p)$. Their faithful (as opposed to only projective) unitary representation is given by [30]

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \quad \to \quad U_S = \begin{cases} l(\alpha) \sum_x \omega^{\alpha\gamma x^2/2} \left|\alpha x\right\rangle \left\langle x\right| & \text{if } \beta = 0 \\ \frac{e^{i\phi}}{\sqrt{d}} \sum_{x,y} \omega^{\frac{\delta x^2 - 2xy + \alpha y^2}{2\beta}} \left|x\right\rangle \left\langle y\right| & \text{if } \beta \neq 0, \end{cases} \tag{A.35}$$

where $\det(S) = \alpha\delta - \beta\gamma = 1 \bmod d$,

$$l(x) = \begin{cases} 1 & \text{if } x \in \mathbf{Q} \\ -1 & \text{if } x \in \mathbf{N} \\ 0 & \text{if } x = 0, \end{cases} \tag{A.36}$$

and

$$e^{i\phi} = \begin{cases} (-1)^k l(-\beta) & \text{if } d = 4k+1 \\ i(-1)^{k+1} l(-\beta) & \text{if } d = 4k+3. \end{cases} \tag{A.37}$$

In number theory, $l(x)$ is known as the Legendre symbol. $\mathbf{Q}$ is the set of quadratic residues, i.e. elements of $\mathbb{Z}_p$ that can be written as the square of another non-zero element, and $\mathbf{N}$ is the set of quadratic non-residues.

The Clifford group then consists of all possible products of symplectic unitaries and displacement operators $U_S D_{\mathbf{u}}$. In other words, it is isomorphic to the semidirect product of the symplectic group and the Weyl-Heisenberg group

$$\mathrm{SL}(2, \mathbb{Z}_p) \ltimes \mathbb{Z}_p^2 \,. \tag{A.38}$$

A.2.2 In odd prime power dimensions $d = p^n$

When the dimension $d = p^n$ is an odd prime power, we use the elements of the field $\mathbb{F}_d$ to label the elements of the Weyl-Heisenberg group just like in the odd prime case. However, $\mathbb{F}_d$ in general contains abstract elements which are not ordinary numbers, so the definitions in the previous section have to be slightly adjusted (since, for example in the definition of $D_{\mathbf{u}}$ in (A.29), one cannot raise ω, X, and Z to the power of an abstract field element).

Definition. With $\omega = e^{2\pi i/p}$ still being a primitive p-th root of unity, we now define the shift and the phase operators as follows:

$$X_u \left|x\right\rangle = \left|x+u\right\rangle \qquad\qquad Z_u \left|x\right\rangle = \omega^{\mathrm{tr}(xu)} \left|x\right\rangle, \tag{A.39}$$

where $x, u \in \mathbb{F}_d$ and the field theoretic trace $\mathrm{tr}(x)$ is a mapping from $\mathbb{F}_d$ to the ground field $\mathbb{F}_p$ defined in (A.26) and specifically denoted in the lower case to be distinguished from the trace of linear operators.

Definition. The Weyl-Heisenberg displacement operators are defined to be

$$D_{\mathbf{u}} = \omega^{\mathrm{tr}(u_1 u_2/2)} X_{u_1} Z_{u_2}, \tag{A.40}$$

where the two components u_1 and u_2 of $\mathbf{u}$ are elements in $\mathbb{F}_d$.

The WH group constructed this way is isomorphic to the direct product of n copies of the WH group defined in the previous section for prime dimension p [30]. The Clifford group, just like in the previous case, is the semidirect product of the symplectic group $\mathrm{SL}(2,\mathbb{F}_d)$ and the WH group. A faithful unitary representation of $\mathrm{SL}(2,\mathbb{F}_d)$ is given by [30]

$$S=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \quad\to\quad U_S=\begin{cases} l(\alpha)\sum_{x\in\mathbb{F}_d}\omega^{\mathrm{tr}(\alpha\gamma x^2/2)}\left|\alpha x\right\rangle\left\langle x\right| & \text{if } \beta=0\\ \frac{e^{i\phi}}{\sqrt{d}}\sum_{x,y\in\mathbb{F}_d}\omega^{\mathrm{tr}(\frac{\delta x^2-2xy+\alpha y^2}{2\beta})}\left|x\right\rangle\left\langle y\right| & \text{if } \beta\neq 0, \end{cases} \tag{A.41}$$

where

$$e^{i\phi}=(-i)^{-n(p+3)/2}l(-\beta) \tag{A.42}$$

and $l(x)$ is again the Legendre symbol defined in (A.36), but now for the field $\mathbb{F}_d$. One can verify that this representation reduces to (A.35) when $d=p$.

References

[1] D. Appleby, H. Dang, and C. Fuchs, *Symmetric Informationally-Complete Quantum States as Analogues to Orthonormal Bases and Minimum-Uncertainty States*, Entropy **16**, 1484–1492, 2014 (cited on pp. iii, 5, 9, 14, 18, 76).

[2] H. B. Dang, K. Blanchfield, I. Bengtsson, and D. M. Appleby, *Linear dependencies in Weyl-Heisenberg orbits*, Quantum Inf. Process. **12**, 3449–3475, 2013 (cited on pp. iii, 5, 21).

[3] D. M. Appleby, I. Bengtsson, and H. B. Dang, *Galois unitaries, mutually unbiased bases, and mub-balanced states*, arXiv:1409.7987, 2014 (cited on pp. iii, 5, 39).

[4] E. P. Wigner, *Gruppentheorie*, Friedrich Vieweg und Sohn, Braunschweig, Germany, 1931 (cited on pp. iii, 38, 59).

[5] W. K. Wootters and D. M. Sussman, *Discrete phase space and minimum-uncertainty states*, arXiv:0704.1277, 2007 (cited on pp. iii, 64, 76, 77, 84).

[6] I. Amburg, R. Sharma, D. Sussman, and W. K. Wootters, *States that ''look the same'' with respect to every basis in a mutually unbiased set*, arXiv:1407.4074, 2014 (cited on pp. iii, 3, 5, 14, 39, 76, 79, 80, 84).

[7] E. L. West and T. M. Laverty, *Effect of floral symmetry on flower choice and foraging behaviour of bumble bees*, Canadian Journal of Zoology **76**, 730–739, 1998 (cited on p. 1).

[8] D. J. Gross, *The role of symmetry in fundamental physics*, Proc. Nat. Acad. Sci. U.S.A. **93**, 14256, 1996 (cited on p. 2).

[9] E. Noether, *Invariante variationsprobleme*, ger, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse **1918**, 235–257, 1918 (cited on p. 2).

[10] B. Odom, D. Hanneke, B. D'Urso, and G. Gabrielse, *New Measurement of the Electron Magnetic Moment Using a One-Electron Quantum Cyclotron*, Physical Review Letters **97**, 030801, 2006 (cited on p. 3).

[11] C. H. Bennett and S. J. Wiesner, *Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states*, Physical Review Letters **69**, 2881–2884, 1992 (cited on pp. 3, 9).

[12] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. K. Wootters, *Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels*, Phys. Rev. Lett. **70**, 1895–1899, 1993 (cited on p. 3).

[13] C. H. Bennett and G. Brassard, *Quantum cryptography: public key distribution and coin tossing*, Theoretical Computer Science **560**, 7–11, 2014 (cited on pp. 3, 40).

[14] M. A. Nielsen and I. L. Chuang, *Quantum computation and quantum information*, Cambridge university press, 2010 (cited on p. 3).

[15] E. Scholz, *Weyl entering the ''new'' quantum mechanics discourse*, in Conf. on the History of Quantum Physics (Berlin, 2--6 July 2007), Vol. 2, 2007 (cited on p. 7).

[16] H. Weyl, *Quantenmechanik und Gruppentheorie*, Zeitschrift fur Physik **46**, 1–46, 1927 (cited on p. 7).

[17] H. Weyl, *Gruppentheorie und Quantenmechanik (Leipzig: Hirzel), Engl. Transl. The Theory of Groups and Quantum Mechanics*, Dover, New York, 1931 (cited on p. 7).

[18] M. Born and P. Jordan, *Zur Quantenmechanik*, Zeitschrift fur Physik **34**, 858–888, 1925 (cited on p. 7).

[19] W. A. Fedak and J. J. Prentis, *The 1925 Born and Jordan paper ''On quantum mechanics''*, American Journal of Physics **77**, 128–139, 2009 (cited on p. 7).

[20] T. S. Santhanam, *Quantum mechanics in discrete space and angular momentum*, Foundations of Physics **7**, 121–127, 1977 (cited on p. 7).

[21] T. Santhanam and A. Tekumalla, *Quantum mechanics in finite dimensions*, Found. Phys. **6**, 583–587, 1976 (cited on p. 7).

[22] R. Jagannathan, T. S. Santhanam, and R. Vasudevan, *Finite-Dimensional Quantum Mechanics of a Particle*, International Journal of Theoretical Physics **20**, 755–773, 1981 (cited on p. 7).

[23] R. Jagannathan and T. S. Santhanam, *Finite-Dimensional Quantum Mechanics of a Particle. II*, International Journal of Theoretical Physics **21**, 351–362, 1982 (cited on p. 7).

[24] T. S. Santhanam, *Quantum mechanics in a finite number of dimensions*, Physica A Statistical Mechanics and its Applications **114**, 445–447, 1982 (cited on p. 7).

[25] J. J. Sylvester, *The collected mathematical papers of James Joseph Sylvester*, Vol. 3, Cambridge University Press, 2012 (cited on p. 8).

[26] D. Mumford, *Tata Lectures on Theta II*, Vol. 43, Springer, 2007 (cited on p. 9).

[27] S. D. Howard, A. R. Calderbank, and W. Moran, *The Finite Heisenberg-Weyl Groups in Radar and Communications*, EURASIP Journal on Advances in Signal Processing **2006**, 1–12, 2006 (cited on pp. 9, 14).

[28] D. Gottesman, *Stabilizer codes and quantum error correction*, PhD thesis, California Institute of Technology, 1997 (cited on p. 9).

[29] D. Gottesman, *Fault-tolerant quantum computation with higher-dimensional systems*, in Quantum Computing and Quantum Communications, 1998, pp. 302–313 (cited on p. 9).

[30] D. M. Appleby, *Properties of the extended Clifford group with applications to SIC-POVMs and MUBs*, arXiv:0909.5233, 2009 (cited on pp. 9, 17, 40, 41, 43, 48, 60, 64, 70, 74, 78, 94, 95, 97).

[31] K. Thas, *The geometry of generalized Pauli operators of N-qudit Hilbert space, and an application to MUBs*, EPL (Europhysics Letters) **86**, 60005, 2009 (cited on p. 9).

[32] K. Blanchfield, *Orbits of mutually unbiased bases*, Journal of Physics A Mathematical General **47**, 135303, 2014 (cited on pp. 9, 40).

[33] J Haantjes, *Equilateral point-sets in elliptic two-and three-dimensional spaces*, Nieuw Arch. Wisk **22**, 355–362, 1948 (cited on p. 12).

[34] J. H. Van Lint, J.Lint and J. J. Seidel, *Equilateral point sets in elliptic geometry*, Indag. Math. **28**, 335–348, 1966 (cited on p. 12).

[35] P. Lemmens and J. Seidel, *Equiangular lines*, Journal of Algebra **24**, 494–512, 1973 (cited on pp. 12, 13).

[36] A. A. Makhnev, *On the nonexistence of strongly regular graphs with parameters (486, 165, 36, 66)*, Ukrainian Mathematical Journal **54**, 1137–1146, 2002 (cited on p. 13).

[37] J. C. Tremain, *Concrete constructions of real equiangular line sets*, arXiv:0811.2779, 2008 (cited on p. 13).

[38] G. Greaves, J. H. Koolen, A. Munemasa, and F. Szollosi, *Equiangular lines in Euclidean spaces*, arXiv:1403.2155, 2014 (cited on p. 13).

[39] P. Delsarte, J. Goethals, and J. Seidel, *Bounds for systems of lines, and Jacobi polynomials*, Philips Research Reports **30**, 91, 1975 (cited on p. 13).

[40] S. G. Hoggar, *T-designs in projective spaces*, European Journal of Combinatorics **3**, 233–254, 1982 (cited on pp. 13, 16).

[41] G. Zauner, *Quantum designs, foundations of a non-commutative design theory*, PhD thesis, University of Vienna, Vienna, 1999 (cited on pp. 13, 14, 16, 18, 26).

[42] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *Symmetric informationally complete quantum measurements*, Journal of Mathematical Physics **45**, 2171–2180, 2004 (cited on pp. 14, 16, 21).

[43] J. Řeháček, B.-G. Englert, and D. Kaszlikowski, *Minimal qubit tomography*, Phys. Rev. A **70**, 052321, 2004 (cited on p. 14).

[44] M. Grassl, *Tomography of quantum states in small dimensions*, Electronic Notes in Discrete Mathematics **20**, 151–164, 2005 (cited on p. 14).

[45] A. J. Scott, *Tight informationally complete quantum measurements*, J. Phys. A: Math. Gen. **39**, 13507–13530, 2006 (cited on p. 14).

[46] M. A. Ballester, *Optimal estimation of SU(d) using exact and approximate 2-designs*, arXiv:quant-ph/0507073, 2007 (cited on p. 14).

[47] H. Zhu and B.-G. Englert, *Quantum state tomography with fully symmetric measurements and product measurements*, Phys. Rev. A **84**, 022327, 2011 (cited on p. 14).

[48] D. Petz and L. Ruppert, *Efficient quantum tomography needs complementary and symmetric measurements*, Reports on Mathematical Physics **69**, 161–177, 2012 (cited on p. 14).

[49] A. Kalev, J. Shang, and B.-G. Englert, *Symmetric minimal quantum tomography by successive measurements*, Phys. Rev. A **85**, 052116, 2012 (cited on p. 14).

[50] B.-G. Englert, D. Kaszlikowski, H. K. Ng, W. K. Chua, J. Řeháček, and J. Anders, *Efficient and robust quantum key distribution with minimal state tomography*, arXiv:quant-ph/0412075, 2008 (cited on p. 14).

[51] J. M. Renes, *Equiangular spherical codes in quantum cryptography*, Quantum Info. Comput. **5**, 81–92, 2005 (cited on p. 14).

[52] J. Du, M. Sun, X. Peng, and T. Durt, *Realization of entanglement-assisted qubit-covariant symmetric-informationally-complete positive-operator-valued measurements*, Phys. Rev. A **74**, 042341, 2006 (cited on p. 14).

[53] T. Durt, C. Kurtsiefer, A. Lamas-Linares, and A. Ling, *Wigner tomography of two-qubit states and quantum cryptography*, Phys. Rev. A **78**, 042338, 2008 (cited on p. 14).

[54] C. A. Fuchs and M. Sasaki, *Squeezing quantum information through a classical channel: measuring the "quantumness" of a set of quantum states*, arXiv:quant-ph/0302092, 2003 (cited on p. 14).

[55] C. A. Fuchs, *On the quantumness of a Hilbert space*, arXiv:quant-ph/0404122, 2007 (cited on p. 14).

[56] I. H. Kim, *Quamtumness, generalized spherical 2-design and symmetric informationally complete POVM*, Quant. Inf. Comp **7**, 730–737, 2007 (cited on p. 14).

[57] B. G. Bodmann, D. W. Kribs, and V. I. Paulsen, *Decoherence-insensitive quantum communication by optimal C^*-encoding*, IEEE Trans. Inform. Theory **53**, 4738–4749, 2007 (cited on p. 14).

[58] O. Oreshkov, J. Calsamiglia, R. Muñoz-Tapia, and E. Bagan, *Optimal signal states for quantum detectors*, New Journal of Physics **13**, 073032, 2011 (cited on p. 14).

[59] B. G. Bodmann, P. G. Casazza, D. Edidin, and R. Balan, *Frames for linear reconstruction without phase*, 42nd Annual Conference on Information Sciences and Systems 10.1109/ciss.2008.4558616, 2008 (cited on p. 14).

[60] M. A. Herman and T. Strohmer, *High-Resolution Radar via Compressed Sensing*, IEEE Transactions on Signal Processing **57**, 2275–2284, 2009 (cited on p. 14).

[61] R. Balan, B. G. Bodmann, P. G. Casazza, and D. Edidin, *Painless reconstruction from magnitudes of frame coefficients*, J Fourier Anal Appl **15**, 488–501, 2009 (cited on p. 14).

[62] C. A. Fuchs, *QBism, the Perimeter of Quantum Bayesianism*, arXiv:1003.5209, 2010 (cited on p. 14).

[63] D. M. Appleby, Å. Ericsson, and C. A. Fuchs, *Properties of QBist State Spaces*, Foundations of Physics **41**, 564–579, 2011 (cited on p. 14).

[64] C. A. Fuchs and R. Schack, *A Quantum-Bayesian Route to Quantum-State Space*, Foundations of Physics **41**, 345–356, 2011 (cited on p. 14).

[65] C. A. Fuchs and R. Schack, *Quantum-Bayesian coherence*, Reviews of Modern Physics **85**, 1693–1715, 2013 (cited on p. 14).

[66] G. N. M. Tabia, *Geometry of quantum states from symmetric informationally complete probabilities*, PhD thesis, University of Waterloo, Ontario, 2013 (cited on pp. 14, 36).

[67] D. M. Appleby, S. T. Flammia, and C. A. Fuchs, *The Lie algebraic significance of symmetric informationally complete measurements*, Journal of Mathematical Physics **52**, 022202, 2011 (cited on p. 14).

[68] D. M. Appleby, C. A. Fuchs, and H. Zhu, *Group theoretic, Lie algebraic and Jordan algebraic formulations of the SIC existence problem*, arXiv:1312.0555, 2013 (cited on p. 14).

[69] L. Hughston, *d=3 SIC-POVMs and elliptic curves*, Seminar talk at Perimeter Institute, PIRSA number 07100040, 2007 (cited on pp. 14, 22, 24).

[70] I. Bengtsson, *From SICs and MUBs to Eddington*, Journal of Physics Conference Series **254**, 012007, 2010 (cited on pp. 14, 25).

[71] D. M. Appleby, H. Yadsan-Appleby, and G. Zauner, *Galois automorphisms of a symmetric measurement*, Quantum Info. Comput. **13**, 672–720, 2013 (cited on pp. 14, 38, 39, 44, 51).

[72] I. Bengtsson, K. Blanchfield, and A. Cabello, *A Kochen-Specker inequality from a SIC*, Physics Letters A **376**, 374–376, 2012 (cited on pp. 14, 26).

[73] A. J. Scott and M Grassl, *Symmetric informationally complete positive-operator-valued measures: a new computer study*, J. Math. Phys. **51**, 2203, 2010 (cited on pp. 14, 16, 17, 21, 26, 29, 32, 38).

[74] D. M. Appleby, I. Bengtsson, S. Brierley, M. Grassl, D. Gross, and J.-A. Larsson, *The monomial representations of the Clifford group*, Quantum Info. Comput. **12**, 404–431, 2012 (cited on p. 14).

[75] D. M. Appleby, I. Bengtsson, S. Brierley, A. Ericsson, M. Grassl, and J.-A. Larsson, *Systems of imprimitivity for the Clifford group*, Quantum Info. Comput. **14**, 339–360, 2014 (cited on p. 14).

[76] D. M. Appleby, *Symmetric informationally complete-positive operator valued measures and the extended Clifford group*, Journal of Mathematical Physics **46**, 052107, 2005 (cited on pp. 14–18, 22, 43).

[77] A. Klappenecker, M. Rötteler, I. E. Shparlinski, and A. Winterhof, *On approximately symmetric informationally complete positive operator-valued measures and related systems of quantum states*, Journal of Mathematical Physics **46**, 082104, 2005 (cited on p. 14).

[78] S. Colin, J. Corbett, T. Durt, and D. Gross, *About SIC POVMs and discrete Wigner distributions*, Journal of Optics B: Quantum and Semiclassical Optics **7**, 778, 2005 (cited on p. 14).

[79] S. T. Flammia, *On SIC-POVMs in prime dimensions*, Journal of Physics A Mathematical General **39**, 13483–13493, 2006 (cited on p. 14).

[80] M. Khatirinejad, *On Weyl-Heisenberg orbits of equiangular lines*, Journal of Algebraic Combinatorics **28**, 333–349, 2007 (cited on p. 14).

[81] L. Bos and S. Waldron, *Some remarks on Heisenberg frames and sets of equiangular lines*, New Zealand J. Math **36**, 113–137, 2007 (cited on p. 14).

[82] D. M. Appleby, *Symmetric informationally complete measurements of arbitrary rank*, Optics and Spectroscopy **103**, 416–428, 2007 (cited on p. 14).

[83] M. Grassl, *Computing equiangular lines in complex space*, Lecture Notes in Computer Science, 89–104, 2008 (cited on p. 14).

[84] M. Grassl, *On SIC-POVMs and MUBs in Dimension 6*, arXiv:quant-ph/0406175, 2009 (cited on p. 14).

[85] D. M. Appleby, *SIC-POVMs and MUBs: Geometrical Relationships in Prime Dimension*, arXiv:0905.1428, 2009 (cited on p. 14).

[86] I. Bengtsson and H. Granström, *The frame potential, on average*, Open Syst. Inf. Dyn. **16**, 145–156, 2009 (cited on p. 14).

[87] M. Fickus, *Maximally equiangular frames and Gauss sums*, J Fourier Anal Appl **15**, 413–427, 2009 (cited on p. 14).

[88] C. Godsil and A. Roy, *Equiangular lines, mutually unbiased bases, and spin models*, European Journal of Combinatorics **30**, 246–262, 2009 (cited on p. 14).

[89] H. Zhu, *SIC POVMs and Clifford groups in prime dimensions*, J. Phys. A: Math. Theor. **43**, 305305, 2010 (cited on pp. 14, 16, 22).

[90] S. N. Filippov and V. I. Man'ko, *Symmetric informationally complete positive operator valued measure and probability representation of quantum mechanics*, Journal of Russian Laser Research **31**, 211–231, 2010 (cited on p. 14).

[91] Z. E. D. Medendorp, F. A. Torres-Ruiz, L. K. Shalm, G. N. M. Tabia, C. A. Fuchs, and A. M. Steinberg, *Experimental characterization of qutrits using symmetric informationally complete positive operator-valued measurements*, Phys. Rev. A **83**, 051801, 2011 (cited on p. 14).

[92] G. N. M. Tabia, *Experimental scheme for qubit and qutrit symmetric informationally complete positive operator-valued measurements using multiport devices*, Phys. Rev. A **86**, 062107, 2012 (cited on p. 14).

[93] A. E. Rastegin, *Notes on general SIC-POVMs*, Phys. Scr. **89**, 085101, 2014 (cited on p. 14).

[94] H. Zhu, Y. S. Teo, and B.-G. Englert, *Two-qubit symmetric informationally complete positive-operator-valued measures*, Phys. Rev. A **82**, 042308, 2010 (cited on p. 14).

[95] G. Gour and A. Kalev, *Construction of all general symmetric informationally complete measurements*, Journal of Physics A Mathematical General **47**, G5302, 2014 (cited on p. 14).

[96] V. Bouniakowsky, *Sur quelques inégalités concernant les intégrales ordinaires et les intégrales aux différences finies*, Eggers, 1859 (cited on p. 19).

[97] J. L. W. V. Jensen, *Sur les fonctions convexes et les inégalités entre les valeurs moyennes*, Acta Math. **30**, 175–193, 1906 (cited on p. 20).

[98] G. E. Pfander, *Gabor frames in finite dimensions*, Finite Frames: Theory and Applications, 193–239, 2013 (cited on p. 22).

[99] J. Lawrence, G. E. Pfander, and D. Walnut, *Linear independence of Gabor systems in finite dimensional vector spaces*, J Fourier Anal Appl **11**, 715–726, 2005 (cited on p. 22).

[100] R.-D. Malikiosis, *A note on Gabor frames in finite dimensions*, Applied and Computational Harmonic Analysis **38**, 318–330, 2015 (cited on p. 22).

[101] O. Hesse, *Über die Elimination der Variabeln aus drei algebraischen Gleichungen vom zweiten Grade mit zwei Variabeln.*, Journal für die Reine und Angewandte Mathematik **1844**, 68–96, 1844 (cited on p. 24).

[102] E. Bézout, *Théorie générale des équations algébriques*, de l'imprimerie de Ph.-D. Pierres, rue S. Jacques, 1779 (cited on p. 25).

[103] A. Uhlmann, *Fidelity and concurrence of conjugated states*, Phys. Rev. A **62**, 032307, 2000 (cited on p. 38).

[104] J. Schwinger, *Unitary operator bases*, Proc. Nat. Acad. Sci. U.S.A. **46**, 570, 1960 (cited on p. 40).

[105] W. K. Wootters and B. D. Fields, *Optimal state-determination by mutually unbiased measurements*, Annals of Physics **191**, 363–381, 1989 (cited on p. 40).

[106] I. D. Ivonovic, *Geometrical description of quantal state determination*, Journal of Physics A Mathematical General **14**, 3241–3245, 1981 (cited on p. 40).

[107] I. Bengtsson, W. Bruzda, Å. Ericsson, J.-Å. Larsson, W. Tadej, and K. Życzkowski, *Mutually unbiased bases and Hadamard matrices of order six*, Journal of Mathematical Physics **48**, 052106, 2007 (cited on p. 40).

[108] P. Butterley and W. Hall, *Numerical evidence for the maximum number of mutually unbiased bases in dimension six*, Physics Letters A **369**, 5–8, 2007 (cited on p. 40).

[109] S. Brierley and S. Weigert, *Constructing mutually unbiased bases in dimension six*, Phys. Rev. A **79**, 052316, 2009 (cited on p. 40).

[110] P. Jaming, M. Matolcsi, P. Móra, F. Szöllősi, and M. Weiner, *A generalized Pauli problem and an infinite family of MUB-triplets in dimension 6*, Journal of Physics A Mathematical General **42**, 245305, 2009 (cited on p. 40).

[111] T. Paterek, B. Dakić, and Č. Brukner, *Mutually unbiased bases, orthogonal Latin squares, and hidden-variable models*, Phys. Rev. A **79**, 012109, 2009 (cited on p. 40).

[112] S. Brierley and S. Weigert, *Mutually unbiased bases and semi-definite programming*, Journal of Physics Conference Series **254**, 012008, 2010 (cited on p. 40).

[113] P. Raynal, X. Lü, and B.-G. Englert, *Mutually unbiased bases in six dimensions: The four most distant bases*, Phys. Rev. A **83**, 062303, 2011 (cited on p. 40).

[114] D. M. Appleby, I. Bengtsson, and S. Chaturvedi, *Spectra of phase point operators in odd prime dimensions and the extended Clifford group*, J. Math. Phys. **49**, 012102, 2008 (cited on pp. 42, 70).

[115] B. C. Berndt, R. J. Evans, and K. S. Williams, *Gauss and Jacobi sums*, Wiley, New York, 1998 (cited on p. 45).

[116] D. Gottesman and I. L. Chuang, *Demonstrating the viability of universal quantum computation using teleportation and single-qubit operations*, Nature **402**, 390–393, 1999 (cited on p. 46).

[117] G. J. Janusz, *Algebraic number fields*, Vol. 55, Academic Press, 1973 (cited on p. 47).

[118] I. Bengtsson and Å. Ericsson, *Mutually unbiased bases and the complementarity polytope*, Open Systems & Information Dynamics **12**, 107–120, 2005 (cited on pp. 53, 57).

[119] W. Krasnodebski, *Dihedral angle of the regular n-simplex*, Roczniki Polskiego Towarzystwa Mateatycznego, Seria I, Commentationes Mathematicae, Prace Matematyczne **15**, 87–89, 1971 (cited on p. 54).

[120] H. Parks and D. C. Wills, *An elementary calculation of the dihedral angle of the regular n-simplex.*, The American Mathematical Monthly **109**, 756–758, 2002 (cited on p. 54).

[121] W. K. Wootters, *A Wigner-function formulation of finite-state quantum mechanics*, Annals of Physics **176**, 1–21, 1987 (cited on p. 55).

[122] A. B. Klimov and C. Muñoz, *Discrete Wigner function dynamics*, Journal of Optics B: Quantum and Semiclassical Optics **7**, 588, 2005 (cited on p. 55).

[123] A. Vourdas, *Galois quantum systems*, J. Phys. A **38**, 8453–8471, 2005 (cited on p. 55).

[124] R. H. Bruck and H. J. Ryser, *The nonexistence of certain finite projective planes*, Canadian J. Math **1**, 88–93, 1949 (cited on p. 55).

[125] C. W. Lam, T Thiel, and S Swiercz, *The non-existence of finite projective planes of order 10*, Canad. J. Math **41**, 1117–1123, 1989 (cited on p. 55).

[126] C. W. Lam, *The search for a finite projective plane of order 10*, The American Mathematical Monthly **98**, 305–318, 1991 (cited on p. 55).

[127] M. K. Bennett, *Affine and projective geometry*, John Wiley & Sons, 1995 (cited on p. 55).

[128] I. Bengtsson, *MUBs, Polytopes, and Finite Geometries*, in Foundations of probability and physics, Vol. 750, edited by A. Khrennikov, American Institute of Physics Conference Series, 2005, pp. 63–69, arXiv:quant-ph/0406174 (cited on p. 58).

[129] J. Casanova, C. Sabín, J. León, I. L. Egusquiza, R. Gerritsma, C. F. Roos, J. J. García-Ripoll, and E. Solano, *Quantum Simulation of the Majorana Equation and Unphysical Operations*, Phys. Rev. X **1**, 021018, 2011 (cited on p. 61).

[130] X. Zhang, Y. Shen, J. Zhang, J. Casanova, L. Lamata, E. Solano, M.-H. Yung, J.-N. Zhang, and K. Kim, *Time reversal and charge conjugation in an embedding quantum simulator*, arXiv:1409.3681, 2014 (cited on p. 61).

[131] O. Kern, K. S. Ranade, and U. Seyfarth, *Complete sets of cyclic mutually unbiased bases in even prime-power dimensions*, J. Phys. A **43**, A275305, 2010 (cited on p. 64).

[132] W. R. Hamilton, *Lectures on quaternions*, 1853 (cited on p. 65).

[133] E. P. Wigner, *Normal Form of Antiunitary Operators*, J. Math. Phys. **1**, 409–413, 1960 (cited on p. 72).

[134] D. M. Sussman, *Minimum-uncertainty states and rotational invariance in discrete phase space*, BSc thesis, Williams College, 2007 (cited on p. 76).

[135] K. E. Gehles, *Ordinary Characters of Finite Special Linear Groups*, MA thesis, University of St. Andrews, 2002 (cited on p. 82).

[136] I. Stewart, *Galois Theory*, Chapman and Hall, London, 1972 (cited on p. 86).

[137] S. Roman, *Field Theory*, Springer, New York, 2006 (cited on pp. 86, 88).

[138] J. S. Milne, *Fields and Galois Theory*, Courses Notes, 2003 (cited on p. 86).

[139] R. Lidl, *Finite fields*, Vol. 20, Cambridge University Press, 1997 (cited on pp. 86, 93).

[140] D. Hilbert, *The theory of algebraic number fields*, Springer Science & Business Media, 1998 (cited on p. 91).

[141] H. Chau, *Unconditionally secure key distribution in higher dimensions by depolarization*, IEEE Trans. Inform. Theory **51**, 1451–1468, 2005 (cited on p. 94).