SIAM J. APPL. ALGEBRA GEOMETRY
Vol. 4, No. 4, pp. 502–531

Moment Maps and Galois Orbits in Quantum Information Theory*

Kael Dixon‡ and Simon Salamon‡

Abstract. SIC-POVMs are configurations of points or rank-one projections arising from the action of a finite Heisenberg group on $\mathbb{C}^d$. The resulting equations are interpreted in terms of moment maps by focusing attention on the orbit of a cyclic subgroup and the maximal torus in $\mathrm{U}(d)$ that contains it. The image of a SIC-POVM under the associated moment map lies in an intersection of real quadrics, which we describe explicitly. We also elaborate the conjectural description of the related number fields and describe the structure of Galois orbits of overlap phases.

Key words. SIC-POVM, moment map, Fubini–Study metric, Galois group, ray class field

AMS subject classifications. 81R05, 53D20, 11R20, 11R37

DOI. 10.1137/19M1305574

1. Introduction.

It is conjectured that, for every positive integer d, there exist d^2 points in the complex projective space $\mathbb{CP}^{d-1}$ that are pairwise equidistant with respect to the standard Fubini–Study metric. This is equivalent to asserting that, as an adjoint orbit in the Lie algebra $\mathfrak{su}(d) \cong \mathbb{R}^{d^2-1}$ of Killing vector fields, projective space contains the d^2 vertices of a regular simplex. The common distance of separation depends only on d and the diameter of $\mathbb{CP}^{d-1}$. Such sets of points were originally studied under the guise of *equiangular lines* [34, 18, 25] and are related to topics such as *tight frames* in design theory.

Versions of the conjecture arose from the pioneering work of Zauner [43], who revitalized the subject from the viewpoint of quantum information. Such a set of d^2 points defines a so-called *symmetric informationally complete positive operator measure* (SIC-POVM). The concept of a POVM in quantum theory was introduced in [16, 26, 17], though in the present context it is an entirely discrete object. The rank-one projections defined by the d^2 points provide an optimal way to measure a mixed state, and applications of SIC-POVMs arise in *quantum tomography*, a topic advanced by Ugo Fano [19]. (On a historical note that places the discipline in a family context; his brother Robert worked on Shannon–Fano coding [41], whilst their father was the algebraic geometer Gino Fano.)

The advent of computing has emphasized the importance of finite-dimensional Hilbert spaces in quantum theory, and in particular metric properties of $\mathbb{CP}^{d-1}$. Virtually all known SIC-POVMs arise as orbits of a discrete Heisenberg group, acting as $\mathbb{Z}_d^2 = \mathbb{Z}_d \times \mathbb{Z}_d$ on $\mathbb{CP}^{d-1}$ ($\mathbb{Z}_d$ denotes $\mathbb{Z}/d\mathbb{Z}$ throughout the paper). A vector $\mathbf{z} \in \mathbb{C}^d$ is called *fiducial* if it has unit norm and

*Received by the editors December 9, 2019; accepted for publication (in revised form) September 9, 2020; published electronically December 10, 2020.
https://doi.org/10.1137/19M1305574
Funding: The authors are supported by the Simons Collaboration on Special Holonomy in Geometry, Analysis, and Physics (488635 Simon Salamon). They also gratefully acknowledge support from the Simons Center for Geometry and Physics, Stony Brook University, at which some of the research was presented.
‡Department of Mathematics, King's College London, London, WC2R 2LS, UK (kael.dix@gmail.com, simon.salamon@kcl.ac.uk).

the orbit $\mathbb{Z}_d^2 \cdot [\mathbf{z}]$ is a SIC-POVM. Fiducial vectors have been constructed exactly for all $d \leqslant 21$ and in a few higher dimensions. There is strong numerical evidence for their existence for all d up to a 3-figure value, and seminal papers on the subject include [1, 9, 20, 23, 37, 39, 44]. For the remainder of the paper, we work with Heisenberg SIC-POVMs.

The existence of SIC-POVMs for $d = 2$ and 3 is elementary. For $d = 2$, $\mathbb{CP}^1$ coincides with the round 2-sphere, any SIC-POVM is an inscribed tetrahedron, and any two are related by an element of $\mathrm{SO}(3) \cong \mathrm{SU}(2)/\mathbb{Z}_2$. For $d = 3$, there is a one-parameter family of SIC-POVMs on $\mathbb{CP}^2$ up to the action of the isometry group, any one of which is isometric to the orbit $\mathbb{Z}_d^2 \cdot [\mathbf{z}]$ for a suitable fiducial vector $\mathbf{z}$. It is much harder to prove that there are no other SIC-POVMs on $\mathbb{CP}^2$, and both known proofs involve an element of computation [42, 29]. It is believed that there are only finitely many isometry classes of SIC-POVMs in dimensions $d > 3$, and there is strong evidence for this at least when $d \leqslant 50$ [39].

The condition for a unit vector $\mathbf{z} \in \mathbb{C}^d$ to be fiducial is that, for any nonidentity matrix $g \in \mathbb{Z}_d^2 < \mathrm{U}(d)$ induced from the Heisenberg group, the complex number $\mathbf{z}^* g \mathbf{z}$ has norm $\frac{1}{\sqrt{d+1}}$. These complex numbers are referred to as the *(unnormalized) overlap phases* and can be used to recover the fiducial vector. These are usually encoded into a $\bar{d} \times \bar{d}$ matrix, called the *overlap phase matrix*, where we follow notation of Appleby [1] to define

$$\bar{d} = \begin{cases} d & \text{if } d \text{ is odd,} \\ 2d & \text{if } d \text{ is even.} \end{cases} \tag{1.1}$$

We shall denote this matrix by $\Phi_{\mathbf{z}}$ and interpret it as a map $\mathbb{Z}_{\bar{d}}^2 \to \mathbb{C}$. It is not a direct encoding of the numbers $\{\mathbf{z}^* g \mathbf{z} : g \in \mathbb{Z}_d^2\}$, since there is some algebraic advantage in multiplying these numbers by $2d$-roots of unity, necessitating the extension from d to $\bar{d}$. See section 2.

One aim of this paper is to extend the moment map approach of [29] to arbitrary dimensions. This has led us independently to a formulation involving the discrete Fourier transform, which is known to be central in understanding the action of the Heisenberg group [3, 22], though our emphasis is more on the underlying geometry. Let us consider the case when d is odd for simplicity. We fix a cyclic subgroup $C \cong \mathbb{Z}_d$, which (as explained in section 3) gives rise to a maximal torus of $\mathrm{SU}(d)$ and a moment map μ^C from $\mathbb{CP}^{d-1}$ onto a standard simplex Δ in $\mathbb{R}^{d-1}$. When C is realized as a subgroup of $\mathbb{Z}_d^2$, we relate μ^C to the map $[\mathbf{z}] \mapsto \Phi_{\mathbf{z}}|C$ and describe the intersection of Δ with a product of circles defined by elements $\Phi_{\mathbf{z}}(\mathbf{p})$ with $\mathbf{p} \in C$.

Let $\mathcal{A}$ denote the image by μ^C of points of $\mathbb{CP}^{d-1}$ whose C orbits consist of d equidistant points that could hypothetically lie in a SIC-POVM. Then $\mathcal{A}$ is universal in the sense that it does not depend on C (Lemma 3.7), being a reinterpretation of conditions on the overlap phases defined by C. The set $\mathcal{A}$ is described by Theorem 3.9 and (when d is odd) is a Clifford torus, suitably interpreted. This approach will not help in the quest for SIC-POVMs, but it may conceivably lead to the construction of an example that is not the orbit of a finite group acting on $\mathbb{CP}^{d-1}$.

The other aim of this paper is to build on the conjectural relationship with number theory developed in [4, 6, 10, 33, 7]. It is observed [6] that all of the known exact examples of fiducials are equivalent in a certain sense to those having a property that is called *strongly centered*. See section 4 for a more precise definition. Consider such a strongly centered fiducial vector $\mathbf{z}$ of unit norm. Then the unnormalized overlap phases generate an abelian extension $\mathbb{E}_1$ of the real quadratic field $\mathbb{K} = \mathbb{Q}(\sqrt{D})$, where D is the square-free part of $(d-3)(d+1)$. The relevant Galois group to study is the subgroup $\mathcal{G}$ of $\mathrm{Gal}(\mathbb{E}_1/\mathbb{Q})$, which preserves the set of overlap phases. The Galois action of $\mathcal{G}$ on the phases is encoded in a very natural way: for each $g \in \mathcal{G}$, there exists some $G_g \in \mathrm{GL}_2\mathbb{Z}_{\bar{d}}$ such that $g \circ \Phi_{\mathbf{z}} = \Phi_{\mathbf{z}} \circ G_g$. The present work is inspired by the way in which we have organized the set of overlap phases into a set of moment maps. The form of the Galois action described above means that it will send moment maps to moment maps. We will use this structure to describe the orbits of the Galois action.

The element G_g is not unique, being determined only up to left multiplication by an element of the set $S = \{G \in \mathrm{GL}_2\mathbb{Z}_{\bar{d}} : \Phi_{\mathbf{z}} \circ G = \Phi_{\mathbf{z}}\}$. Thus there is some subgroup M of $\mathrm{GL}_2\mathbb{Z}_{\bar{d}}$ such that $\mathcal{G} \cong M/S$. We will focus on M as being more fundamental than $\mathcal{G}$, since it does not depend on the fiducial, but only on its type (either z, a_4, a_6, or a_8; see section 4) and d. After careful study of the Galois groups of the exact solutions tabulated in [4, 6], we observe that most of these have a property that we call *algebraic*, meaning that $M \cong \left(\mathcal{O}_{\mathbb{K}}(\bar{d})\right)^{\times}$, where $\mathcal{O}_{\mathbb{K}}$ is the set of algebraic integers in $\mathbb{K}$. This condition determines the type.

Proposition 1.1. *An algebraic fiducial is of type*
$$\begin{cases} a_4 & \text{if } 3|d \text{ and } D \equiv 1 \pmod 3, \\ a_6 & \text{if } d \equiv 3 \pmod{27}, \\ a_8 & \text{if } 3|d \text{ and } D \equiv 2 \pmod 3, \\ z & \text{otherwise.} \end{cases}$$

The nonalgebraic fiducials are type-z when the above criteria would suggest type-a, giving a simple modification to the structure of M. It was not previously known whether it is possible to have type-a_6 fiducials, but this criterion suggests that these will occur for all d congruent to 3 modulo 27, including the known solution labeled $30d$.

In [4], SIC-POVMs are related to natural field extensions called ray class fields. In particular, it was observed that for every d with known fiducials, there is a fiducial where $\mathbb{E}_1$ is the ray class field $\mathbb{K}\big((\bar{d})\infty_1\big)$ associated to the ideal $(\bar{d})$ in $\mathcal{O}_{\mathbb{K}}$ and the real embedding ∞_1 of $\mathbb{K}$ for which $\sqrt{D}$ is positive. Moreover, these are always algebraic and the fixed field of $\mathcal{G}$ is the Hilbert class field $\mathbb{K}(1)$. We call these *ray class fiducials* and compute their corresponding symmetry groups.

Theorem 1.2. *For ray class fiducials, S is isomorphic to the cyclic group S_0 generated by the fundamental unit in $\mathcal{O}_{\mathbb{K}}$ modulo $\bar{d}$.*

More generally, in Theorem 5.4 we show that for algebraic fiducials, S is a subgroup of S_0, and $\mathcal{G}$ is a cyclic extension of that corresponding to the ray class fiducial. We also describe the slightly more complicated case of nonalgebraic fiducials.

In section 4, we discuss the orbits of the Galois action of $\mathcal{G}$ on the overlap phases. The main result is Theorem 4.19, which shows that these orbits are in one-to-one correspondence with factors of $\bar{d}$ in $\mathcal{O}_{\mathbb{K}}$. As a direct consequence of this and Lemma 4.18, we find the following.

Corollary 1.3. *The set of overlap phases are all Galois conjugate if and only if $d > 3$ is an odd prime congruent to 2 modulo 3.*

This result relates to a recent work [33] by Kopp, which studies the case when d is an odd prime congruent to 2 modulo 3. Using the fact that there is only one Galois orbit of overlap phases, the problem of finding a SIC-POVM is interpreted as finding an algebraic unit satisfying certain properties. Furthermore, Kopp conjectures that such a unit will come from

Stark's conjecture. Theorem 5.5 describes in general which field each Galois orbit takes values in. It may be possible to use this to generalize Kopp's construction.

The paper is organized as follows. Section 2 is a review of basic properties of SIC-POVMs and applies this to the $d = 3$ case using results from [29]. Section 3 generalizes this moment map interpretation to arbitrary d, which is illustrated by the case $d = 4$ and overlap phases explained in [10]. In section 4, we review the relevant number fields and Galois actions, including carefully motivating the definition of a strongly centered fiducial. We then introduce the idea of an algebraic fiducial and compute the group structure of M. This allows us to compute the orbits of the Galois action on the overlap phases. In section 5, we review the conjecture that the number fields associated to a strongly fiducial are all extensions of ray class fields. We use this to describe the structure of the field extensions and the fixed fields corresponding to the orbits of $\mathcal{G}$.

2. SIC-POVMs and their overlap phases.

In this section, we follow the approach and notation of [29]. Complex projective space $\mathbb{CP}^{d-1}$ is a compact Kähler manifold. Its Riemannian metric g arises from the standard Hermitian form

$$\langle \mathbf{w}, \mathbf{z} \rangle = \sum_{i=0}^{d-1} \overline{w}_i z_i \tag{2.1}$$

on $\mathbb{C}^d$ that is invariant by the unitary group $\mathrm{U}(d)$. In formulae involving matrices, we shall regard elements of $\mathbb{C}^d$ as *column* vectors, so that we can identify (2.1) with the matrix product $\mathbf{w}^*\mathbf{z}$. The Hermitian form converts any point $[\mathbf{w}]$ of $\mathbb{CP}^{d-1}$ into a hyperplane

$$H_{\mathbf{w}} = \{[\mathbf{z}] \in \mathbb{CP}^{d-1} : \langle \mathbf{w}, \mathbf{z} \rangle = 0\}$$

and is determined up to a constant by the correspondence $[\mathbf{w}] \mapsto H_{\mathbf{w}}$.

The Riemannian distance δ, obtained by integrating g, satisfies

$$\cos^2\left(\tfrac{1}{2}\delta\big([\mathbf{w}], [\mathbf{z}]\big)\right) = \mathfrak{p}\big([\mathbf{w}], [\mathbf{z}]\big),$$

where

$$\mathfrak{p}\big([\mathbf{w}], [\mathbf{z}]\big) = \frac{|\langle \mathbf{w}, \mathbf{z} \rangle|^2}{\|\mathbf{w}\|^2 \|\mathbf{z}\|^2} = \frac{\langle \mathbf{w}, \mathbf{z} \rangle \langle \mathbf{z}, \mathbf{w} \rangle}{\langle \mathbf{w}, \mathbf{w} \rangle \langle \mathbf{z}, \mathbf{z} \rangle}$$

(see [14, section 8]). Since any two points $[\mathbf{w}], [\mathbf{z}]$ are contained in a totally geodesic projective line $\ell_{\mathbf{w},\mathbf{z}} \cong \mathbb{CP}^1 \cong S^2$, the formula can be proved by restricting to this 2-sphere. The normalization ensures that the diameter of $\mathbb{CP}^{d-1}$ naturally equals π.

The description above yields the following.

Lemma 2.1. *$\mathfrak{p}\big([\mathbf{w}], [\mathbf{z}]\big)$ equals the cross ratio of the four points $[\mathbf{w}], [\mathbf{z}], [\mathbf{z}]', [\mathbf{w}]'$ in order, where $[\mathbf{w}'] = \ell_{\mathbf{w},\mathbf{z}} \cap H_{\mathbf{w}}$ and $[\mathbf{z}'] = \ell_{\mathbf{w},\mathbf{z}} \cap H_{\mathbf{z}}$.*

Points $[\mathbf{w}], [\mathbf{z}]$ of $\mathbb{CP}^{d-1}$ represent pure quantum states, and the projective line they span the set of all their possible superpositions. Observables correspond to Hermitian matrices whose eigenvalues are the results of measurements. If $\mathbf{z}$ is the eigenvector of such a matrix, then $\mathfrak{p}\big([\mathbf{w}], [\mathbf{z}]\big)$ is the probability that the state $[\mathbf{w}]$ is observed to coincide with $[\mathbf{z}]$. Wigner's theorem states that any isometry ϕ of $\mathbb{CP}^{d-1}$ arises from a unitary or conjugate unitary transformation of $\mathbb{C}^d$. We refer the reader to proofs by Bargmann [8] and Freed [21], the former mentioning a quaternionic analogue and the latter exploiting the notion of holonomy (thus both suited to our sponsor). Many more links between quantum theory and Fubini–Study geometry are explored in [14].

Let $\mathbb{C}^{d,d}$ denote the set of complex $d \times d$ matrices, and consider the subsets

$$\begin{aligned}\mathfrak{su}(d) &= \left\{A \in \mathbb{C}^{d,d} : A = -A^*,\ \operatorname{tr} A = 0\right\},\\ \mathscr{D} &= \left\{A \in \mathbb{C}^{d,d} : A = A^*,\ \operatorname{tr} A = 1\right\}.\end{aligned}$$

Then $\mathfrak{su}(d)$ is the Lie algebra of $SU(d)$, and $\mathscr{D}$ is the set of *density matrices.* The map

$$\mathfrak{a}\colon \mathscr{D} \longrightarrow \mathfrak{su}(d), \quad A \mapsto i\left(A - \tfrac{1}{d}\mathbf{1}\right) \tag{2.2}$$

is an affine isomorphism between these two spaces of real dimension $d^2 - 1$. The Lie algebra has a natural inner product, which is equal to minus the Killing form,

$$\langle A, B\rangle = -\frac{1}{2d}\operatorname{tr}(AB),$$

and this enables us to identify $\mathfrak{su}(d)$ with its dual $\mathfrak{su}(d)^*$.

The mapping $F\colon S^{2d-1} \to \mathscr{D}$ for which

$$F(\mathbf{z}) = \mathbf{z}\mathbf{z}^* = \begin{pmatrix} |z_0|^2 & \overline{z}_0 z_1 & \overline{z}_0 z_2 & \cdots \\ \overline{z}_1 z_0 & |z_1|^2 & \overline{z}_1 z_2 & \cdots \\ \overline{z}_2 z_0 & \overline{z}_2 z_1 & |z_2|^2 & \cdots \\ \cdots & \cdots & \cdots & \end{pmatrix} \tag{2.3}$$

is SU(d)-equivariant and the composition

$$\mathfrak{a} \circ F\colon\ \mathbb{CP}^{d-1} \hookrightarrow \mathfrak{su}(d) \cong \mathfrak{su}(d)^* \tag{2.4}$$

can be identified with the moment mapping defined by the action of $SU(d)$ on the symplectic manifold $\mathbb{CP}^{d-1}$ [32]. It follows that (2.4) defines an embedding of $\mathbb{CP}^{d-1}$ in $\mathfrak{su}(d)^*$ as a coadjoint orbit that is (up to a universal constant) isometric.

Given (2.4), $\mathscr{D}$ is the convex hull of the set $\{F(\mathbf{z}) : \mathbf{z} \in S^{2d-1}\}$ of pure states. A point of $\mathscr{D}$ represents a *mixed* quantum state, whereas an observable is represented by an arbitrary Hermitian matrix A. The expectation that the observable is in the state $\rho \in \mathscr{D}$ is then given by $\operatorname{tr}(\rho A)$, so that ρ can be viewed as a probability density [13].

The acronym SIC-POVM is an abbreviation of *symmetric informationally complete positive operator valued measure.* In defining this concept, we adopt the geometric approach of [29].

Definition 2.2. *A SIC-POVM is a collection $S = \{[\mathbf{z}_\alpha]\}$ of n^2 points in $\mathbb{CP}^{d-1}$ that are mutually equidistant, so that*

$$\mathfrak{p}(\mathbf{z}_\alpha, \mathbf{z}_\beta) = \lambda, \qquad \alpha \neq \beta,$$

for some fixed $\lambda \in (0, 1)$.

The points represent *equiangular* one-dimensional subspaces in $\mathbb{C}^d$.

The next result expresses the quantity λ in this definition as a function of d.

Lemma 2.3 (see [18]). *The number of mutually equidistant points possible in* $\mathbb{CP}^{d-1}$ *is at most* d^2, *and if this number is achieved, then* $\lambda = 1/(d+1)$.

A quick proof is also given in [29, section 3].

For fixed d, one therefore knows the distance between any two points $[\mathbf{z}_\alpha], [\mathbf{z}_\beta] \in \mathbb{CP}^{d-1}$ of a hypothetical SIC-POVM. This innocuous result helps to make the existence problem tractable, and we record the following.

Definition 2.4. *Two points* $[\mathbf{w}], [\mathbf{z}]$ *of* $\mathbb{CP}^{d-1}$ *are* correctly separated *if*

$$\mathfrak{p}\big([\mathbf{w}], [\mathbf{z}]\big) = 1/(d+1).$$

Thus, any two distinct points of a SIC-POVM are correctly separated.

If we normalize the representative vectors and set $P_\alpha = F(\mathbf{z}_\alpha)$, then a SIC-POVM can be equivalently defined as a subset $\{P_\alpha\}$ of d^2 rank-one projections in $\mathscr{D}$ such that

$$\sum_{\alpha=1}^{d^2} P_\alpha = d\mathbf{1}, \qquad \mathrm{tr}(P_\alpha P_\beta) = \begin{cases} 1, & \alpha = \beta, \\ \lambda, & \alpha \neq \beta. \end{cases}$$

This reflects the etymology of the words *informationally complete* and *symmetric*. It also allows us to view a SIC-POVM as a regular simplex in $\mathfrak{su}(d)$ whose d^2 vertices lie in the coadjoint orbit $\mathbb{CP}^{d-1}$. It also raises the question of whether there is an analogue of Lemma 2.3 for other adjoint orbits, any one of which is a projective variety [40] with a natural Kähler metric [12, Chapter 8].

Fix $d \geqslant 3$, and set $\omega = e^{2\pi i/d}$. Having chosen coordinates on $\mathbb{C}^d$, one can define two cyclic subgroups W, H of $\mathrm{U}(d)$, with respective generators

$$w = \begin{pmatrix} 0 & 0 & 0 & \cdots & 1 \\ 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 \end{pmatrix}, \qquad h = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \omega & 0 & \cdots & 0 \\ 0 & 0 & \omega^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \omega^{d-1} \end{pmatrix}. \tag{2.5}$$

Both have order d, and the former acts on column vectors by the shift map

$$w\,(z_0, z_1, \dots, z_{d-1})^\top = (z_{d-1}, z_0, \dots, z_{d-2})^\top.$$

Note that $W = \langle w \rangle$ and $H = \langle h \rangle$ are subgroups of $\mathrm{SU}(d)$ only if d is odd.

Since $hw = \omega wh$, the actions induced by W, H on $\mathbb{CP}^{d-1}$ commute. A vector $\mathbf{z} \in \mathbb{C}^d$ is called *fiducial* if it has unit norm and the orbit $(W \times H) \cdot [\mathbf{z}]$ is a SIC-POVM, as in Definition 2.2. However, w, h generate a subgroup of $\mathrm{U}(d)$ or order d^3, isomorphic to the Heisenberg group of upper-triangular 3×3 matrices defined over the ring $\mathbb{Z}_d$ (with 1's on the diagonal). To better understand the resulting phase factors independently of the parity of d, recall the definition of $\bar{d}$ in (1.1), set $\tau = -e^{\pi i/d}$, and define operators

$$\mathbf{D}_\mathbf{p} = \tau^{p_1 p_2} w^{p_1} h^{p_2}, \quad \mathbf{p} = (p_1, p_2).$$

The map

$$\mathbf{D}\colon \begin{cases} \mathbb{Z}_{\bar d}^2 & \longrightarrow & \mathrm{U}(d), \\ \mathbf{p} & \longmapsto & \mathbf{D}_{\mathbf{p}} \end{cases} \tag{2.6}$$

is not a homomorphism but satisfies

$$\mathbf{D}_{\mathbf{p}}\mathbf{D}_{\mathbf{q}} = \tau^{\langle \mathbf{p},\mathbf{q}\rangle}\mathbf{D}_{\mathbf{p}+\mathbf{q}}, \tag{2.7}$$

where

$$\langle \mathbf{p},\mathbf{q}\rangle = \det(\mathbf{q},\mathbf{p}) = q_1p_2 - q_2p_1$$

is a symplectic pairing. If d is even, then

$$\mathbf{D}_{\mathbf{p}+d\mathbf{q}} = \bar\tau^{d\langle \mathbf{p},\mathbf{q}\rangle}\mathbf{D}_{\mathbf{p}}\mathbf{D}_{d\mathbf{q}} = (-1)^{\langle \mathbf{p},\mathbf{q}\rangle}\mathbf{D}_{\mathbf{p}}, \tag{2.8}$$

so that $\mathbf{D}$ is d-periodic up to sign.

We next review the concept of overlap phase. Many more details can be found in [1].

Letting $\mathbf{z}$ be a unit vector in $\mathbb{C}^d$, we write $\mathbf{z} \in S^{2d-1}$. For each nonzero element $\mathbf{p} \in \mathbb{Z}_{\bar d}^2$, the quantity

$$\mathbf{z}^*\mathbf{D}_{\mathbf{p}}\mathbf{z} = \mathrm{tr}(\mathbf{D}_{\mathbf{p}}\mathbf{z}\mathbf{z}^*)$$

is called an *overlap phase* for the Heisenberg action.

Definition 2.5. *Let $\mathbf{z} \in S^{2d-1}$. The* overlap map *associated to $\mathbf{z} \in S^{2d-1}$ is the mapping $\Phi_{\mathbf{z}}\colon \mathbb{Z}_{\bar d}^2 \to \mathbb{C}$ defined by $\Phi_{\mathbf{z}}(\mathbf{p}) = \mathbf{z}^*\mathbf{D}_{\mathbf{p}}\mathbf{z}$.*

Of course, $\Phi_{\mathbf{z}}$ can be thought of as a square matrix whose rows and columns are each indexed by $\mathbb{Z}_{\bar d}$, and we shall also refer to its values as "entries." Beware that the top left entry $\Phi_{\mathbf{z}}(0,0) = 1$ is not strictly speaking an overlap phase. The point is that $\mathbf{z}$ generates a SIC-POVM if and only if all the other entries of $\Phi_{\mathbf{z}}$ are complex numbers of modulus $\frac{1}{\sqrt{d+1}}$. Shifting the row or column index of an entry by d will at worst change its sign.

For the moment, let us restrict the index $\mathbf{p}$ to the subset $\mathbb{Z}_d^2$ if d is even. Then the set $\{\mathbf{D}_{\mathbf{p}} : \mathbf{p} \in \mathbb{Z}_{\bar d}^2\}$ forms a unitary basis for the complex vector space $\mathfrak{gl}_d\mathbb{C}$ of complex $d \times d$ matrices, equipped with the Hermitian product $\langle A, B\rangle = (1/d)\,\mathrm{tr}(A^*B)$. This is true because

$$\mathbf{D}_{\mathbf{p}}^* = \mathbf{D}_{\mathbf{p}}^{-1} = \tau^{-p_1p_2}h^{-p_2}w^{-p_1},$$

so $\mathbf{D}_{\mathbf{p}}^*\mathbf{D}_{\mathbf{q}}$ is a scalar multiple of $\mathbf{D}_{-\mathbf{p}+\mathbf{q}}$, and

$$\mathrm{tr}(\mathbf{D}_{\mathbf{p}}^*\mathbf{D}_{\mathbf{q}}) = \begin{cases} d & \text{if } \mathbf{p} = \mathbf{q} \in \mathbb{Z}_d^2, \\ 0 & \text{otherwise.} \end{cases}$$

It follows that the entries of $\Phi_{\mathbf{z}}|\mathbb{Z}_d^2$ are essentially the coordinates of $\mathbf{z}\mathbf{z}^*$ with respect to this basis. Indeed,

$$\mathbf{z}\mathbf{z}^* = \frac{1}{d}\sum_{\mathbf{p}\in\mathbb{Z}_d^2}\Phi_{\mathbf{z}}(\mathbf{p})\mathbf{D}_{\mathbf{p}}^*, \tag{2.9}$$

and $[\mathbf{z}]$ can be recovered by replacing $\mathbf{D}_{\mathbf{p}}^*$ by its first column in (2.9), assuming that $z_0 \neq 0$.

The concept of a unitary basis of operators was introduced in [38] (see also [3]). If $\mathbf{D_p}$ were itself Hermitian or skew-Hermitian, then $\Phi_{\mathbf{z}}(\mathbf{p})$ would be a component of the moment map (2.4). Although this is not true, we shall explain in the next section precisely how the overlap map encodes the moment maps associated to maximal tori of the isometry group of $\mathbb{CP}^{d-1}$.

Example 2.6. We summarize the results of [29, 44] for $d = 3$. Let $\mathbb{S} = \{[\mathbf{z}_\alpha] : 1 \leqslant \alpha \leqslant 9\}$ be any SIC-POVM consisting of nine mutually equidistant points in $\mathbb{CP}^2$. We prove that $\mathbb{S}$ is in fact congruent to an orbit of $W \times H$ by means of the following steps.

Up to isometry and reordering the points, we may assume that

$$[\mathbf{z}_1] = [0, -1, \omega], \qquad [\mathbf{z}_2] = [0, -1, \omega^2] = h \cdot [\mathbf{z}_1]. \tag{2.10}$$

Having fixed these points, we may use a residual U(1) symmetry to take

$$[\mathbf{z}_3] = \left[\cos\phi,\ \cos\left(\phi + \tfrac{2\pi}{3}\right),\ \cos\left(\phi + \tfrac{4\pi}{3}\right)\right] \tag{2.11}$$

for some angle ϕ modulo π. Acting by w on $[\mathbf{z}_3]$ merely has the effect of replacing ϕ by $\phi - \frac{2\pi}{3}$ on the right-hand side.

It can now be shown that $\mathbb{S}$ is the orbit of these three points under W, so that

$$\mathbb{S} = \left\{w^i \cdot [\mathbf{z}_\alpha] : 0 \leqslant i \leqslant 2,\ 1 \leqslant \alpha \leqslant 3\right\}.$$

The proof of this fact is accomplished in [29] by a long series of lemmas. The first step is to characterize equilateral triangles in $\mathbb{CP}^2$ with vertices lying on a singular torus generated by points equidistant from $[\mathbf{z}_1]$ and $[\mathbf{z}_2]$ (thereby extending the circle defined by (2.11)). By assumption, $\mathbb{S}$ will contain 35 such triangles.

To convert $\mathbb{S}$ into a visually simpler form, let

$$M = \frac{1}{\sqrt{3}} \begin{pmatrix} \omega^2 & \omega & 1 \\ 1 & \omega & \omega^2 \\ 1 & 1 & 1 \end{pmatrix} \in \mathrm{U}(3). \tag{2.12}$$

M maps $[\mathbf{z}_3]$ to $[e^{2i\phi}\omega^2, 1, 0]$ and $\mathbb{S}$ to the SIC-POVM consisting of the points

$$\begin{array}{ccc} [0,1,-1] & [0,1,-\omega] & [0,1,-\omega^2] \\ [1,0,-1] & [1,0,-\omega] & [1,0,-\omega^2] \\ [e^{2i\phi},1,0] & [e^{2i\phi}\omega,1,0] & [e^{2i\phi}\omega^2,1,0]. \end{array} \tag{2.13}$$

By setting $\phi = (3t + \pi)/2$ and applying the isometry $\mathrm{diag}(-e^{-it}, -e^{it}, 1) \in \mathrm{SU}(3)$ we can convert the nine points into the orbit $(W \times H) \cdot [\mathbf{z}]$, where $\mathbf{z} = \frac{1}{\sqrt{2}}(0, 1, -e^{it})$ and $0 \leqslant t \leqslant \frac{\pi}{3}$.

It is easily verified by hand that $\mathbf{z}$ is a fiducial vector, and we have recovered the usual representation of SIC-POVMs for $d = 2$. The associated overlap matrix is

$$\Phi_{\mathbf{z}} = \frac{1}{2} \begin{pmatrix} 2 & -1 & -1 \\ -e^{-it} & -e^{-it} & -e^{-it} \\ -e^{it} & -e^{it} & -e^{it} \end{pmatrix}.$$

The moduli space of these SIC-POVMs was described in detail by Zhu [44] (with the same parameter t), building on [1, 37, 43]. Their congruence classes can be characterized by the U(3)-invariant triple product

$$\arg\left[\langle \mathbf{z}_1, \mathbf{z}_2\rangle \langle \mathbf{z}_2, \mathbf{z}_3\rangle \langle \mathbf{z}_3, \mathbf{z}_1\rangle\right]$$

of three unit vectors in $\mathbb{C}^3$ first defined in [8]. For the normalized vectors in (2.10), (2.11), this argument equals $-2\phi+\pi = -3t$, although its value for many of the 84 triples drawn from $\mathbb{S}$ is independent of t. It turns out that, up to isometry, all SIC-POVMs for $d=3$ (regarded as an unordered set of nine points) are faithfully parametrized by restricting t to lie in the interval $[0, \frac{\pi}{9}]$. The solutions corresponding to the two endpoints are inequivalent but have enhanced symmetries relative to $0<t<\frac{\pi}{9}$.

The matrix (2.12) in the example above belongs to the normalizer $\mathrm{N}(d)$ of $W\times H$ in $\mathrm{U}(d)$, which is known as the *Clifford group*. There is a representation

$$U\colon\ \mathrm{SL}_2\mathbb{Z}_{\bar d} \ltimes \mathbb{Z}_d^2 \longrightarrow \mathrm{N}(d)/\mathrm{U}(1)$$

satisfying

$$U(F,\mathbf{q})\,\mathbf{D}_{\mathbf{p}}\,U(F,\mathbf{q})^{-1} = \omega^{\langle \mathbf{q}, F\mathbf{p}\rangle}\mathbf{D}_{F\mathbf{p}}. \tag{2.14}$$

It is an isomorphism if d is odd. This theory can be extended to include complex conjugation and $\mathrm{N}(d)$ becomes a subgroup of index 2 in the so-called *extended Clifford group*. This is the natural symmetry group for investigating orbits for the action of $\mathbb{Z}_{\bar d}$ on $\mathbb{C}^d$, though we shall not rely on knowledge of its exact structure in this paper. We shall be more concerned with the symmetries arising from Definition 2.5.

Remark 2.7. The Clifford group for $d=5$ plays an essential role in the construction of the Horrocks–Mumford bundle $\mathscr{F}$, which is a stable rank 2 holomorphic vector bundle over $\mathbb{CP}^4$ [27]. A generic holomorphic section of $\mathscr{F}$ vanishes on a nonsingular abelian surface Z, and $\mathscr{F}$ can be reconstructed from the normal bundle of Z in $\mathbb{CP}^4$. The surface Z is itself generated by the tangent lines to a normal elliptic quintic curve invariant by the Heisenberg group. There is a one-parameter family of such quintic curves in $\mathbb{CP}^4$ (including twelve degenerations to pentagons), which sweep out a surface that fibers over a modular curve, and a similar phenomenon occurs in higher dimensions. (All these facts are fully explained in [30, Chapters IV, VII].) Although the use of elliptic curves to incorporate points of a SIC-POVM appears possible only for $d=3$ [28, 9], the relevance of these constructions has yet to be fully investigated.

3. Moment maps and quadrics.

We begin with some notation to handle cyclic subgroups. Fix $d\geqslant 3$. Let $\bar\pi\colon \mathbb{Z}_{\bar d}\to\mathbb{Z}_d$ denote the natural homomorphism given by $k+\mathbb{Z}_{\bar d}\mapsto k+\mathbb{Z}_d$ (which is of course the identity if d is odd).

Definition 3.1. *Let $\mathbb{PZ}_{\bar d}^2$ denote the set of cyclic subgroups of $\mathbb{Z}_{\bar d}^2$ of size $\bar d$. When d is even, the image of $\bar C\in\mathbb{PZ}_{\bar d}^2$ under $\bar\pi^2\colon \mathbb{Z}_{\bar d}^2\to\mathbb{Z}_d^2$ is a cyclic subgroup C of $\mathbb{Z}_d^2$ of order d, and we say that C and $\bar C$ are* associated.

For $\bar{C} \in \mathbb{PZ}^2_{\bar{d}}$, the restriction $\mathbf{D}|\bar{C}$ of (2.6) to $\bar{C}$ is a homomorphism and d-periodic even when d is even, as can be seen from (2.7). The d-periodicity allows us to define a map

$$\Phi^{\bar{C}}_{\mathbf{z}}\colon\ C \longrightarrow \mathbb{C} \tag{3.1}$$

satisfying $\Phi^{\bar{C}}_{\mathbf{z}} \circ \bar{\pi}^2 = \Phi_{\mathbf{z}}|\bar{C}$, where C and $\bar{C}$ are associated. We shall refer to (3.1) as the *restricted overlap map* determined by $\bar{C}$. When d is odd, of course $\bar{C} = C$ and $\Phi^{\bar{C}}_{\mathbf{z}} = \Phi_{\mathbf{z}}|C$.

Lemma 3.2. *When d is even, each $C \in \mathbb{PZ}^2_d$ is associated to two distinct subgroups $\bar{C}, \bar{C}' \in \mathbb{PZ}^2_{\bar{d}}$, but $\Phi^{\bar{C}}_{\mathbf{z}}$ and $\Phi^{\bar{C}'}_{\mathbf{z}}$ agree up to changes of sign on odd entries.*

Proof. When d is even, $d\mathbb{Z}^2_{\bar{d}} \cong \mathbb{Z}^2_2$. Thus if $\mathbf{p}$ is a generator for $\bar{C}$, then $\{\mathbf{p} + d\mathbf{q} : \mathbf{q} \in \mathbb{Z}^2_{\bar{d}}\}$ has four points. Two of these (namely, $\mathbf{p}$ and $\mathbf{p} + d\mathbf{p}$) lie in $\bar{C}$, while the other two lie in a different subgroup $\bar{C}'$ associated to C. Choose $\mathbf{q} \in \mathbb{Z}^2_{\bar{d}}$ such that $\mathbf{r} = \mathbf{p} + d\mathbf{q}$ generates $\bar{C}'$. In particular, we have $\mathbf{p} \not\equiv \mathbf{q} \pmod 2$. Since neither element is trivial modulo 2, this implies that $\langle \mathbf{p}, \mathbf{q} \rangle$ is odd, which can easily be checked by considering determinants of pairs in $\mathbb{Z}^2_2$. Using (2.7), we have $\mathbf{D}_{k\mathbf{r}} = (-1)^k \mathbf{D}_{k\mathbf{p}}$ for every $k \in \mathbb{Z}_{\bar{d}}$, and thus

$$\Phi^{\bar{C}'}_{\mathbf{z}}(k\mathbf{r}) = \begin{cases} \Phi^{\bar{C}}_{\mathbf{z}}(k\mathbf{p}) & \text{if } k \text{ is even,} \\ -\Phi^{\bar{C}}_{\mathbf{z}}(k\mathbf{p}) & \text{if } k \text{ is odd,} \end{cases}$$

as stated. ■

Note that we shall largely ignore this sign ambiguity as we shall ultimately be concerned only with the respective images of these mappings.

Let $n = \lfloor d/2 \rfloor$. Since the restriction of $\mathbf{D}$ to $\bar{C}$ is a homomorphism, we can identify the image of $\Phi^{\bar{C}}_{\mathbf{z}}$ with an element of the affine space

$$\begin{aligned} \mathscr{T} &= \{(\alpha_0, \dots, \alpha_{d-1}) \in \mathbb{C}^d\colon \alpha_0 = 1,\ \alpha_i = \overline{\alpha_{d-i}}\}, \\ &\cong \begin{cases} \mathbb{C}^n & \text{if } d \text{ is odd,} \\ \mathbb{C}^{n-1} \oplus \mathbb{R} & \text{if } d \text{ is even.} \end{cases} \end{aligned} \tag{3.2}$$

We will relate $\Phi^{\bar{C}}_{\mathbf{z}}$ to a moment map. First we need a torus.

Lemma 3.3. *For every $C \in \mathbb{PZ}^2_d$, there is some maximal torus $\hat{\mathbb{T}}^C$ in $U(d)$ which contains the image of $\bar{C}$ under $\mathbf{D}$ for each associated $\bar{C} \in \mathbb{PZ}^2_{\bar{d}}$.*

Proof. Let $\mathbf{p} \in \mathbb{Z}^2_{\bar{d}}$ generate $\bar{C}$. Since $\gcd(p_1, p_2) \equiv 1 \pmod{\bar{d}}$, there exists some $\mathbf{q} \in \mathbb{Z}^2_{\bar{d}}$ such that $F := (\mathbf{q}\ \ \mathbf{p}) \in \mathrm{SL}_2\mathbb{Z}_{\bar{d}}$. Since $\mathbf{p} = F\binom{0}{1}$, $\mathbf{D}_{\mathbf{p}}$ is conjugate to $\omega^k h$ for some $k \in \mathbb{Z}_d$ (see (2.14)). It follows that the eigenvalues of $\mathbf{D}_{\mathbf{p}}$ are the distinct dth roots of unity $1, \omega, \omega^2, \dots, \omega^{d-1}$ with an ordered set $(\mathbf{e}_j)$ of unit eigenvectors indexed by $\mathbb{Z}_d$. Note that if $\mathbf{p}' \neq \mathbf{p}$ but $\bar{\pi}^2(\mathbf{p}) = \bar{\pi}^2(\mathbf{p}')$, then $\mathbf{D}_{\mathbf{p}'} = -\mathbf{D}_{\mathbf{p}}$. Thus the unordered set $\{\mathbf{e}_j\}$ of eigenvectors depends only on the subgroup $C \in \mathbb{PZ}^2_d$.

The corresponding projectors $\{\mathbf{e}_j \mathbf{e}_j^* : j \in \mathbb{Z}_d\}$ are Hermitian, and we may identify them with elements of $\mathfrak{u}(d)$. They generate a maximal torus $\hat{\mathbb{T}}^C$ in $\mathrm{U}(d)$. Note that this torus is conjugate to the standard diagonal torus, which contains $\omega^k h$, so that $\mathbf{D}_{\mathbf{p}} \in \hat{\mathbb{T}}^C$. ■

Note that $\hat{\mathbb{T}}^C$ descends to a torus $\mathbb{T}^C$ in the projective unitary group $\mathrm{U}(d)/\mathrm{U}(1)$. Recalling (2.2), its Lie algebra $\mathfrak{t}^C$ can be identified with the set of elements in the real span of $\{\mathbf{e}_j\mathbf{e}_j^* : j \in \mathbb{Z}_d\}$ with trace 1.

We now can associate to $\bar{C}$ a moment map $\mu^{\bar{C}} : \mathbb{CP}^{d-1} \to \mathfrak{t}^C$ in analogy to (2.4) by setting

$$\mu_j^{\bar{C}}([\mathbf{z}]) := \mathrm{tr}\left(\mathbf{e}_j\mathbf{e}_j^*\,\mathbf{z}\mathbf{z}^*\right) = |\langle \mathbf{e}_j, \mathbf{z}\rangle|^2,$$

assuming as usual that $\mathbf{z}$ is a unit vector. The image of μ is the standard simplex

$$\Delta = \Delta_{d-1} = \Big\{(x_0, \dots, x_{d-1}) : \sum_{i=0}^{d-1} x_i = 1,\ x_i \geqslant 0\Big\} \tag{3.3}$$

of $\mathbb{R}^d$. (In the future, we shall omit the subscript $d-1$ when the context makes the dimension of the simplex clear.) The dependence on $\bar{C}$ rather than C comes from the ordering of the basis by the eigenvalues of $\mathbf{p}$.

For any $i \in \mathbb{Z}_d$, we can now write

$$\mathbf{D}_{i\mathbf{p}} = \sum_{j\in\mathbb{Z}_d} \omega^{ij}\mathbf{e}_j\mathbf{e}_j^*.$$

In particular, the components of $\Phi_{\mathbf{z}}^{\bar{C}}$ relative to (3.2) are given by

$$(\Phi_{\mathbf{z}}^{\bar{C}})_i = \mathrm{tr}(\mathbf{D}_{i\mathbf{p}}\mathbf{z}\mathbf{z}^*) = \sum_{j\in\mathbb{Z}_d} \omega^{ij}\mu_j^{\bar{C}}.$$

This is expressed succinctly by the equation

$$\Phi_{\mathbf{z}}^{\bar{C}} = V\mu^{\bar{C}}([\mathbf{z}]) \tag{3.4}$$

for $\mathbf{z} \in S^{2d-1}$, where

$$V = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & \omega & \cdots & \omega^{d-1} \\ 1 & \omega^2 & \cdots & \omega^{2(d-1)} \\ \cdot & \cdot & \cdots & \cdot \\ 1 & \omega^{d-1} & \cdots & \omega^{(d-1)^2} \end{pmatrix}$$

is the Vandermonde matrix that represents the discrete Fourier transform. The (i, j)th entry of V is ω^{ij} (we start indexing at 0), and $(1/\sqrt{d})V \in \mathrm{U}(d)$. We can summarize the discussion by the following result, a version of which appears in [22].

Proposition 3.4. *For any $\bar{C} \in \mathbb{PZ}_{\bar{d}}^2$, the restricted overlap map $\Phi_{\mathbf{z}}^{\bar{C}}$ is a Fourier transform of the moment map $\mu^{\bar{C}}$.*

Example 3.5. The argument above is rendered more concrete by taking $\bar{C} = \{0\} \times \mathbb{Z}_{\bar{d}}$, which is associated to H, so that $\mathbb{T}^C$ is the standard maximal torus in $\mathrm{SU}(d)$. Its moment map is determined by the diagonal entries of (2.3), so is given by setting $x_i = |z_i|^2$ in (3.3), assuming $\mathbf{z} \in S^{2d-1}$. Define

$$\alpha_i = \mathbf{z}^*h^i\mathbf{z} = x_0 + \omega^i x_1 + \cdots + \omega^{i(d-1)}x_{d-1}, \tag{3.5}$$

so that

$$\begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{d-1} \end{pmatrix} = V \begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ x_{d-1} \end{pmatrix}$$

and $(\alpha_0, \ldots, \alpha_{d-1}) \in \mathscr{T}$.

For the following statements, let C be a cyclic subgroup of $\mathbb{Z}_d^2$ associated to $\bar{C} \in \mathbb{PZ}_d^2$, and let

$$\mu^{\bar{C}} \colon \mathbb{CP}^{d-1} \longrightarrow \Delta$$

be the associated moment mapping. Recall that "correctly separated" is defined in Definition 2.4.

Definition 3.6. *A point* $[\mathbf{z}] \in \mathbb{CP}^{d-1}$ *is* C-admissible *if all points in its* C*-orbit are correctly separated.*

It follows immediately that a unit vector $\mathbf{z}$ is fiducial if and only if $[\mathbf{z}]$ is C-admissible for *every* $C \in \mathbb{PZ}_d^2$.

Note that if $[\mathbf{z}]$ is C-admissible, so is any point in its $\mathbb{T}^C$ orbit. The set of C-admissible points is therefore determined by its image under $\mu^{\bar{C}}$. A different subgroup C' determines a conjugate maximal torus $P\mathbb{T}^C P^{-1}$, where $P \in \mathrm{N}(d)$ (see (2.14)), and the new moment map is obtained by precomposing $\mu^{\bar{C}}$ with P. However, see the following.

Lemma 3.7. *The image by* $\mu^{\bar{C}}$ *of the set of* C*-admissible points does not depend upon* C*.*

Proof. This is a consequence of (3.4), in which V transforms $\Delta \subset \mathbb{R}^d$ into a subset of $\mathscr{T}$. The vertices of Δ correspond to the columns of V. A C-admissible point $[\mathbf{z}]$ is characterized by the condition that each nonidentity component of (3.4) has norm $1/\sqrt{d+1}$. It follows that

$$V\mathcal{A} \;=\; V\Delta \cap \begin{cases} \frac{1}{\sqrt{d+1}} T & \text{if } d \text{ is odd}, \\ \frac{1}{\sqrt{d+1}} \big(T \times \{\pm 1\}\big) & \text{if } d \text{ is even}, \end{cases}$$

where T denotes a Clifford torus (with coordinates of unit modulus) in $\mathbb{C}^n$ or in $\mathbb{C}^{n-1} \subset \mathscr{T}$, respectively. ∎

We shall denote the universal subset of Δ arising in this lemma by $\mathcal{A}$. It consists of the image of C-admissible points in $\mathbb{CP}^{d-1}$ by the moment mapping corresponding to the maximal torus generated by C. The proof of Lemma 3.7 establishes a bijection between $\mathcal{A}$ and products of circles. In Example 3.5, $[\mathbf{z}]$ is H-admissible if and only if $|\alpha_k|^2 = 1/(d+1)$ for all $1 \leqslant k \leqslant n$, so in particular $\alpha_n = \pm 1/\sqrt{d+1}$ if $d = 2n$.

Example 3.8. For $d = 3$, the simplex Δ is a filled equilateral triangle with vertices $(1,0,0)$, $(0,1,0)$, $(0,0,1)$ in $\mathbb{R}^3$, and

$$\mathcal{A} = \Big\{ \tfrac{2}{3}\big(\cos^2\phi,\ \cos^2(\phi + \tfrac{2\pi}{3}),\ \cos^2(\phi + \tfrac{4\pi}{3})\big) : \phi \in \big(-\tfrac{\pi}{2}, \tfrac{\pi}{2}\big] \Big\} \tag{3.6}$$

is its incircle. This circle is generated by the point $[\mathbf{z}_3]$ in (2.11) as ϕ varies. The inverse image of each midpoint $(0,1,1), (1,0,1), (1,1,0)$ contains three of the nine points in (2.13).

Returning to (3.4), the Fourier transform converts Δ into the convex hull of the third roots of unity and $\mathcal{A}$ into a circle of radius 1/2.

In order to describe more accurately the shape of $\mathcal{A}$, we first define a series of quadratic forms

$$f_j = \sum_{i=0}^{d-1} x_i x_{i+j}, \qquad j = 0, \dots, d-1$$

derived from (3.5). To make sense of the right-hand side, the range of indices is extended cyclically, so that x_i is defined to be equal to x_{i-d} if $d \leqslant i \leqslant 2d-1$. In particular,

$$f_0 = \sum_{i=0}^{d-1} x_i^2,$$

and $f_{d-j} = f_j$ for $1 \leqslant j \leqslant d-1$. If d is even, then $f_n = 2f'_n$, where

$$f'_n = \sum_{i=0}^{n-1} x_i x_{i+n}.$$

The forms $f_0, \dots, f_n$ constitute a basis of the space $S^2(\mathbb{R}^d)^*$ of bilinear forms invariant by the action of $\mathbb{Z}_d$ cyclically permuting the x_i.

We can now state the following.

Theorem 3.9. *Let $d \geqslant 3$. The set $\mathcal{A}$ is the intersection of Δ with n quadrics in $\mathbb{R}^d$ and lies in a round sphere S^{d-2} of radius $\sqrt{\frac{d-1}{d(d+1)}}$ centered in Δ. Moreover,*

- *if $d = 2n+1$, then $\mathcal{A} = \Delta \cap T$, where T is a torus of revolution of dimension n and radius $\sqrt{\frac{2}{d(d+1)}}$ in S^{d-2};*
- *if $d = 2n$, then $\mathcal{A} = \Delta \cap (T' \sqcup T'')$, where T', T'' are tori of revolution of dimension $n-1$ and radii $\sqrt{\frac{2}{d(d+1)}}$ in parallel hyperspheres of S^{d-2}.*

By a torus of revolution of radius r, we mean a Euclidean product of circles each of radius r. In Example 3.10 below, Figure 1 displays the sphere S^{d-2} for $d = 4$, and this exits the tetrahedron (whose front face has been removed).

Proof. We will use $C = H$ to compute $\mathcal{A}$. Since

$$|\alpha_j|^2 = \sum_{i=0}^{d-1} \omega^{ij} f_i,$$

the H-admissible assumption also implies that

$$V \begin{pmatrix} f_0 \\ f_1 \\ \vdots \\ f_{d-1} \end{pmatrix} = \frac{1}{d+1} \begin{pmatrix} d+1 \\ 1 \\ \vdots \\ 1 \end{pmatrix}.$$

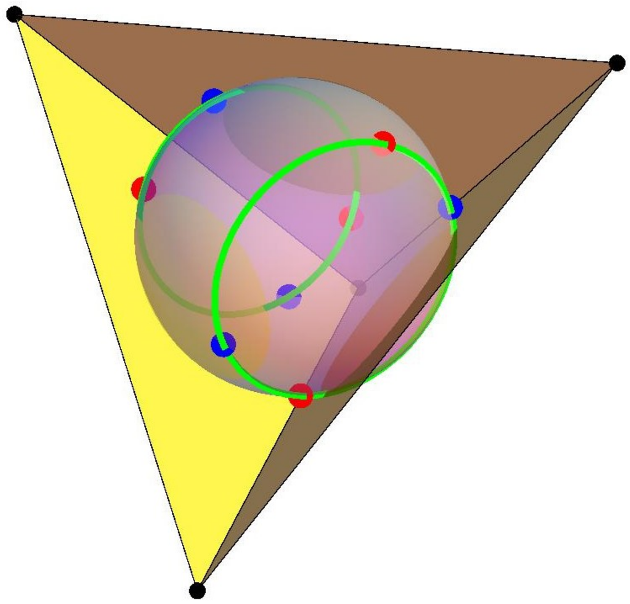

Figure 1. *Fiducial images for $d = 4$.*

The sum of the entries of the $(i+1)$st row of V equals

$$\sum_{j=0}^{d-1} \omega^{ij} = \frac{1-(\omega^i)^d}{1-\omega} = 0$$

for $1 \leqslant i \leqslant d-1$. Therefore the unique solution to the matrix equation must be given by

$$\tfrac{1}{2}f_0 = f_1 = f_2 = \cdots = f_{d-1} = \frac{1}{d+1}. \tag{3.7}$$

This shows that $\mathcal{A}$ lies in the intersection of the sphere S^{d-1} defined by $f_0 = 2/(d+1)$ and the remaining quadrics $f_i = 1/(d+1)$ for $1 \leqslant i \leqslant n$. It also lies on the intersection of S^{d-1} with the plane containing Δ, and this small hypersphere has radius r given by

$$r^2 = \sum_{i=0}^{d} \left(x_i - \frac{1}{d}\right)^2 = \frac{2}{d+1} - \frac{2}{d}\sum_{i=0}^{d} x_i + \frac{1}{d} = \frac{d-1}{d(d+1)},$$

in the notation of (3.3), as stated.

The values of f_i found above are consistent with the equation

$$1 = \left(\sum_{i=0}^{d-1} x_i\right)^2 = \sum_{i=0}^{d-1} f_i.$$

When $d = 2n$ is even, there is an analogous equation that gives new information, namely,

$${\alpha_n}^2 = \left(\sum_{i=0}^{d-1} (-1)^i x_i\right)^2 = \sum_{i=0}^{d-1} (-1)^i f_i.$$

It follows that

$$\sum_{i=0}^{d-1}(-1)^i x_i = \pm\frac{1}{\sqrt{d+1}}$$

and $\mathcal{A}$ lies in the union of two hyperplanes.

Let V', V'' be the real and imaginary parts of V, so that V' is a matrix of cosines and V'' a matrix of sines. Recalling that $\alpha_{d-k} = \overline{\alpha_k}$, set

$$\sqrt{d+1}\,\alpha_k = \cos\theta_k + i\sin\theta_k, \qquad 1 \leqslant k \leqslant n.$$

If d is odd, then the angles are unconstrained, but if d is even, then $\theta_n = 0, \pi \pmod{2\pi}$ to ensure that $\alpha_n = \pm 1$. Since $dV^{-1} = \overline{V} = V' - iV''$,

$$d\sqrt{d+1}\begin{pmatrix} x_0 \\ x_1 \\ \vdots \\ \vdots \\ x_{d-1}\end{pmatrix} = V'\begin{pmatrix} \sqrt{d+1} \\ \cos\theta_1 \\ \vdots \\ \vdots \\ \cos\theta_1\end{pmatrix} + V''\begin{pmatrix} 0 \\ \sin\theta_1 \\ \vdots \\ \vdots \\ -\sin\theta_1\end{pmatrix}.$$

Note that the last column vector has a zero submiddle entry if d is even since $\operatorname{Im}\alpha_n = 0$. It follows that

$$d\sqrt{d+1}\,x_k = \sqrt{d+1} + \sum_{i=1}^{d-1}(c_{ki}\cos\theta_k + s_{ki}\sin\theta_k), \tag{3.8}$$

where $c_{ki} = \cos(\frac{2\pi ki}{d})$ and $s_{ki} = \sin(\frac{2\pi ki}{d})$. There are two cases to consider, according to the parity of d and the properties of $\cos\theta_k, \sin\theta_k$ that will reflect (3.2).

- *Case* $d = 2n+1$. Let P be the $d \times d$ matrix indexed with $(i,j) \in \mathbb{Z}_d^2$ and

  $$P_{ij} = \begin{cases} \sqrt{2} & \text{if } \ j = 0, \\ 2c_{ij} & \text{if } \ 0 < j \leqslant n, \\ 2s_{i(j-n)} & \text{if } \ n < j. \end{cases}$$

  Thus, every entry in the first column of P is $\sqrt{2}$, and the remaining entries in the first row of P are 2 (n times) followed by 0 (n times). Use of the Dirichlet kernel

  $$\sum_{k=-n}^{n} e^{k\theta} = \frac{\sin((n+\frac{1}{2})\theta)}{\sin(\frac{1}{2}\theta)}$$

  and elementary trigonometric identities imply that the rows of P are orthogonal and that the norm squared of each one equals $2d$. Therefore, $(1/\sqrt{2d})P \in \mathrm{O}(d)$ and (3.8) implies that

  $$d\sqrt{d+1}\begin{pmatrix} x_0 \\ x_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ x_{d-1}\end{pmatrix} = P\begin{pmatrix} \sqrt{n+1} \\ \cos\theta_1 \\ \vdots \\ \cos\theta_n \\ \sin\theta_1 \\ \vdots \\ \sin\theta_n\end{pmatrix}.$$

- *Case* $d = 2n$. We again index P by $\mathbb{Z}_d^2$, but this time we set

$$P_{ij} = \begin{cases} \sqrt{2} & \text{if } \ j = 0, \\ 2c_{ij} & \text{if } \ 0 < j < n, \\ -(-1)^i\sqrt{2} & \text{if } \ n = j, \\ 2s_{i(j-n)} & \text{if } \ n < j. \end{cases}$$

Once again, $(1/\sqrt{2d})P \in \mathrm{O}(d)$. Equation (3.8) translates into

$$d\sqrt{d+1}\begin{pmatrix} x_0 \\ x_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ x_{d-1} \end{pmatrix} = P\begin{pmatrix} \sqrt{n+\frac{1}{2}} \\ \cos\theta_1 \\ \cdot \\ \cos\theta_{n-1} \\ \pm\cos\theta_n/\sqrt{2} \\ \sin\theta_1 \\ \cdot \\ \sin\theta_{n-1} \end{pmatrix}.$$

In both cases, $\mathbf{x}$ parametrizes a Clifford type torus (or tori) of radius $\sqrt{2d}/(d\sqrt{d+1})$. ■

Example 3.10. The case $d = 4$ is well understood, and the relatively simple nature of its overlap map was thoroughly explained in [10]. Nonetheless, the underlying geometry of circles and golden ratios, described in [35], illustrates the moment map approach. Let $\mathbf{z} = (z_0, z_1, z_2, z_3)$ be a unit vector in $\mathbb{C}^4$ whose Heisenberg orbit $\mathbb{Z}_4^2 \cdot [\mathbf{z}]$ is a SIC-POVM in $\mathbb{CP}^4$. Let $x_i = |z_i|^2$ and abbreviate $\Phi_{\mathbf{z}}$ to Φ. Then

$$\begin{aligned} 1 &= \Phi(0,0) = x_0 + x_1 + x_2 + x_3, \\ \tfrac{1}{\sqrt{5}}e^{i\theta} &= \Phi(0,1) = x_0 + ix_1 - x_2 - ix_3, \\ \pm\tfrac{1}{\sqrt{5}} &= \Phi(0,2) = x_0 - x_1 + x_2 - x_3 \end{aligned}$$

for some $\theta \in \mathrm{U}(1)$ and choice of sign. It follows that

$$(3.9) \qquad 2\sqrt{5}\mathbf{x} = \begin{cases} \big(\varphi + \cos\theta,\ \psi + \sin\theta,\ \varphi - \cos\theta,\ \psi - \sin\theta\big) \text{ or} \\ \big(\psi + \cos\theta,\ \varphi + \sin\theta,\ \psi - \cos\theta,\ \varphi - \sin\theta\big), \end{cases}$$

where $\varphi = \frac{1}{2}(\sqrt{5}+1)$ and $\psi = \frac{1}{2}(\sqrt{5}-1)$.

This shows that $\mathbf{x}$ must belong to the disjoint union of two circular arcs each of radii $1/(2\sqrt{5})$ suspended in the hyperplane $\sum x_i = 1$ of $\mathbb{R}^4$, as in Figure 1. However, the circles themselves escape the confines of the moment polytope (3.3) (here a solid tetrahedron) that is the image of $\mathbb{CP}^3$. A related figure appears in [2, section 6], which combines the moment map approach with the use of special "spinor" bases in the situation in which (as here) d is a perfect square.

Change notation so that $\mathbf{z} = (ae^{i\alpha}, be^{i\beta}, ce^{i\gamma}, de^{i\delta})$ with $x_0 = a^2,\ x_1 = b^2,\ x_2 = c^2,\ x_3 = d^2$ for clarity (so d is temporarily not a dimension). Then

$$0 = |\Phi(2,0)|^2 - |\Phi(2,2)|^2 = 16abcd\cos(\alpha-\gamma)\cos(\beta-\delta).$$

One can check that none of a, b, c, d can vanish, meaning that (in contrast to the case $d = 3$) points of the SIC-POVM cannot project to the boundary of the polytope. If we fix the second circle in (3.9), we are furthermore forced to assume that $\alpha - \gamma = \pm\pi/2$. Without loss of generality, we can then set $\delta = 0$, which implies

$$\tfrac{1}{5} = \Phi(0,2)^2 = 4b^2d^2\cos^2\beta, \tag{3.10}$$

and $(\varphi^2 - \sin^2\theta)\cos^2\beta = 2$. This relationship can be interpreted as a link between moment maps arising from different maximal tori.

The equations

$$|\Phi(1,0)|^2 - |\Phi(1,2)|^2 = 0 = |\Phi(1,1)|^2 - |\Phi(1,3)|^2$$

allow us to eliminate β and deduce that

$$(ad-bc)(ad+bc)(ab-cd)(ab+cd) = 4a^2b^2c^2d^2\cos^2\beta.$$

One can eliminate β using (3.10) to find that

$$\cos\theta = \pm\tfrac{1}{2}\sqrt{3-\sqrt{5}} = \pm\tfrac{\psi}{\sqrt{2}}, \qquad \sin\theta = \pm\tfrac{1}{2}\sqrt{1+\sqrt{5}} = \pm\tfrac{\sqrt{\varphi}}{\sqrt{2}}. \tag{3.11}$$

This gives four possible angles around each circle (3.9), represented by the eight "beads" in Figure 1. If we fix one of these solutions on the second circle, we have the following choices: 4 for α, for each of these 2 for γ, and independently 4 for β. Choices of signs for a, b, c, d are taken care of by the different angles and overall phase. This gives a total of 32 fiducial points lying over each bead, in accordance with the known results [1].

The solution described by Bengtsson [10, equation (7)] has overlap map

$$\Phi|\mathbb{Z}_d^2 = \frac{1}{\sqrt{5}}\begin{pmatrix} \sqrt{5} & u & -1 & \overline{u} \\ u & \overline{u} & -\overline{u} & \overline{u} \\ -1 & -u & -1 & \overline{u} \\ \overline{u} & u & u & u \end{pmatrix},$$

where

$$u = e^{i\theta} = \sqrt{5}\,\Phi(0,1) = \tfrac{1}{\sqrt{2}}(\psi + i\sqrt{\varphi})$$

in accordance with (3.11) and [10, equation (8)]. Its associated fiducial vector $\mathbf{z}$ (unique up to phase) can be recovered from the first column of (2.9). Set $\rho = 1+\sqrt{2}$ and $x = \tan\theta = \sqrt{\varphi}/\psi = \sqrt{2+\sqrt{5}}$. Then

$$[\mathbf{z}] = \big[2\rho,\ 1+\rho x + i(\rho + x),\ 2i,\ 1-\rho x + i(\rho - x)\big],$$

and $[\mathbf{z}]$ projects to a point on the second circle in (3.9). There are, however, simpler ways to express such a fiducial vector (see [9, 11]).

Let $\mathbb{K} = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{5})$ as in the introduction, noting that this is a subfield of $\mathbb{E}_1 = \mathbb{Q}(e^{i\theta})$. The minimum polynomial of $e^{i\theta}$ over $\mathbb{Q}$ has degree 8, whereas its splitting field $\mathbb{E} = \mathbb{E}_1(i)$ has degree 16 over $\mathbb{Q}$. Indeed, the Galois group $\mathrm{Gal}(\mathbb{E}/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_2 \times D_8$, where D_8 is the dihedral group, and $\mathbb{K}$ is the fixed field of the normal subgroup $\mathbb{Z}_2 \times V_4$. Therefore, $\mathbb{E}$ is an *abelian* extension of $\mathbb{K}$, and $\mathbb{E}$ contains a fiducial vector $\mathbf{z}$. However, all the information of the SIC-POVM is provided by $e^{i\theta}$, which is a unit in the smaller field $\mathbb{E}_1$. In Figure 1, the 8 beads form an orbit of D_8 acting as rotations of the tetrahedron.

Lemma 3.7 and Theorem 3.9 help one to grasp the essence of the SIC-POVM problem. Whether d is even or odd, the set of H-admissible points is characterized by the equations

$$f_1 = \cdots = f_n = \frac{1}{d+1}, \tag{3.12}$$

derived from (3.7), assuming the normalization $f_0 = 1$. They characterize a real subvariety of $\mathbb{CP}^{d-1}$ of codimension n. For each $C \in \mathbb{PZ}_d^2$, we can consider the translate of this variety determined by an element of the Clifford group mapping H to C. The resulting equations were in effect already written down by several authors [3, 22, 31]. The SIC-POVM existence question is whether these subvarieties have a nonempty intersection as C varies over $\mathbb{PZ}_d^2$, whose size is determined by Lemmas 4.15 and 4.16 below. For example, if d is prime, then there are $d+1$ subgroups and subvarieties to consider.

Given that $\mathbb{CP}^{d-1}$ has real dimension at most $4n$, one might conjecture that four subgroups can always be found to reduce the set of solutions to be finite provided $d > 3$. Such a statement appears to be a weaker version of the $3d$ conjecture of [22] (see also [3]). An infinitesimal version of this setup is the following. For each $[\mathbf{z}] \in \mathbb{CP}^{d-1}$ and $C \in \mathbb{PZ}_d^2$, one can in theory compute the tangent space to the level set of the $\mathbb{T}^C$-invariant real polynomial f_i at $[\mathbf{z}]$. Knowledge of the configuration of these spaces as i and C vary would have a bearing on the finiteness question for Heisenberg SIC-POVMs, but is an independent problem that may be accessible for small values of d.

4. Overlap symmetries and Galois conjugation.

Suppose that $\mathbf{z} \in \mathbb{C}^d$ is a fiducial vector for a Heisenberg SIC-POVM. This means that $\langle \mathbf{z}, \mathbf{z} \rangle = 1$ and any two points of the orbit $(W \times H)\cdot[\mathbf{z}]$ are correctly separated (recall Definition 2.4 and (2.5)). Throughout the ensuing discussion, we shall fix the unit vector $\mathbf{z}$ and introduce fields and groups that depend implicitly on $\mathbf{z}$.

Define the symmetry group S of $\Phi_{\mathbf{z}}$ by

$$S := \{G \in \mathrm{GL}_2\mathbb{Z}_{\bar{d}} \colon \Phi_{\mathbf{z}} \circ G = \Phi_{\mathbf{z}}\}.$$

Thus, S consists of automorphisms of $\mathbb{Z}_{\bar{d}}^2$ that have no effect on the overlap phases. Zauner conjectured that S always contains an element F of order 3 with trace $= -1$, an example being

$$F_z := \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}.$$

Remark 4.1. When d is even, the relations 2.8 show that $(d+1)I \in S$, and for this reason, the matrix

$$\hat{F}_z := \begin{pmatrix} 0 & d-1 \\ d+1 & d-1 \end{pmatrix}$$

is often used instead of F_z. When d is odd, obviously $F_z = \hat{F}_z$, but when d is even, $\hat{F}_z$ is order 6 in $\mathrm{GL}_2\mathbb{Z}_{\bar{d}}$, with $\hat{F}_z^2 = F_z^2$ and $\hat{F}_z^3 = (d+1)I$.

Definition 4.2 (see [4]). *The fiducial* $\mathbf{z}$ *is called* centered *if* S *contains an element* F *of order* 3 *with trace* -1 *and is displacement-free, in the sense that the corresponding Clifford unitaries are of the form* $U_{F,0}$ *for some* $F \in \mathrm{GL}_2\mathbb{Z}_{\bar{d}}$. *A centered fiducial* $\mathbf{z}$ *is said to be* type-z *if* F *is conjugate to* F_z, *and* type-a *otherwise.*

To understand the different types, first note that by [24], $\mathrm{GL}_2\mathbb{Z}_{\bar{d}} \cong \prod_{p|d} \mathrm{GL}_2\mathbb{Z}_{p^{r_p}}$, where $\bar{d} = \prod_{p|d} p^{r_p}$. The image $F_{p^{r_p}} \in \mathrm{GL}_2\mathbb{Z}_{p_p^r}$ of F under each of the projections must also have trace -1 and order a factor of 3. When the order is 3, then it is conjugate to F_z. The only alternative is order 1, so that $F_{p^{r_p}} = I$. The condition of having trace -1 then forces $p^{r_p} = 3$.

To summarize this, $\mathbf{z}$ is always type-z unless $\gcd(9, d) = 3$ and $F \equiv I \pmod 3$.

The centered condition allows us to understand the Galois action. Recall that $\mathbb{E}_1$ is the field extension of $\mathbb{K}$ generated by the image of $\Phi_{\mathbf{z}}$. Let $\mathbb{E}_0$ be the maximal subfield of $\mathbb{E}_1$ such that the Galois group $\mathcal{G} = \mathrm{Gal}(\mathbb{E}_1/\mathbb{E}_0)$ fixes the image of $\Phi_{\mathbf{z}}$ as an unordered set.

Theorem 4.3 (see [4]). *Let* $\mathbf{z}$ *be a centered fiducial. For each* $g \in \mathcal{G}$, *there exists some* $G_g \in \mathrm{GL}_2\mathbb{Z}_{\bar{d}}$ *and* $r_g \in \mathbb{Z}_{\bar{d}}^2$ *such that*

$$g \circ \Phi_{\mathbf{z}}(\mathbf{p}) = \begin{cases} \Phi_{\mathbf{z}}(G_g\mathbf{p}) & \text{if } 3 \nmid d, \\ \sigma^{\langle r_g, \mathbf{p}\rangle}\Phi_{\mathbf{z}}(G_g\mathbf{p}) & \text{if } 3 | d, \end{cases}$$

where σ *is a third root of unity.*

We will soon see that the above formula can be simplified if we assume a stronger condition, which we will now work to motivate. Let $\mathbb{E}$ be the field extension of $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ generated by the $\bar{d}$th root of unity τ and the components of the projector $\mathbf{z}\mathbf{z}^*$.

Lemma 4.4. $\mathbb{E} = \mathbb{E}_1(\tau)$.

Proof. Note that each $\mathbf{D_p}$ is a matrix with entries in $\mathbb{Q}(\tau)$. The formula $\Phi_{\mathbf{z}}(\mathbf{p}) = \mathrm{tr}(\mathbf{D_p}\mathbf{z}\mathbf{z}^*)$ shows that $\Phi_{\mathbf{z}}(\mathbf{p})$ takes values in $\mathbb{E}$, so that $\mathbb{E}_1 \leqslant \mathbb{E}$.

For the other inclusion, (2.9) implies that $\mathbf{z}\mathbf{z}^* \in \mathbb{E}_1(\tau)$, so that $\mathbb{E} \leqslant \mathbb{E}_1(\tau)$. ■

Working more carefully, we note that $\mathbf{z}\mathbf{z}^*$ being Hermitian means that

$$\Phi_{\mathbf{z}}(\mathbf{p}) = \mathrm{tr}(\mathbf{D_p}\mathbf{z}\mathbf{z}^*) \in \mathbb{Q}(\mathbf{z}\mathbf{z}^*, \mathrm{Re}\,\tau).$$

In all of the known solutions, we actually have $\mathrm{Re}\,\tau \in \mathbb{E}_1$. Moreover, if the square-free part $\hat{d}$ of $\bar{d}$ is congruent to 1 modulo 4, then $\mathbb{E}_1$ contains $\mathrm{Im}\,\zeta_{\hat{d}}$, where $\zeta_{\hat{d}}$ is a $\hat{d}$th root of unity.

Lemma 4.5. *If* $\mathbb{E}_1$ *contains* $\mathrm{Im}\,\zeta_{\hat{d}}$ *whenever* $\hat{d} \equiv 1 \pmod 4$, *then* $\mathbb{E} \geqslant \mathbb{E}_1(i\sqrt{\bar{d}})$.

Proof. Since $\mathbb{E} = \mathbb{E}(\tau)$, it suffices to show $i\sqrt{\bar{d}} \in \mathbb{E}$. By the Kronecker–Weber theorem, for any square-free integer n, $\mathbb{Q}(\sqrt{n}) \leqslant \mathbb{Q}(\zeta_{|\Delta|})$, where

$$\Delta = \begin{cases} n & \text{if } n \equiv 1 \pmod 4, \\ 4n & \text{if } n \equiv 2, 3 \pmod 4 \end{cases}$$

is the discriminant of $\mathbb{Q}(\sqrt{n})$. We proceed by taking cases:

- *Case* $\hat{d} \equiv 3 \pmod 4$. Taking $n = -\hat{d}$ gives $i\sqrt{\bar{d}} = \sqrt{-\hat{d}} \in \mathbb{Q}(\zeta_{\hat{d}}) \leqslant \mathbb{Q}(\zeta_{\bar{d}}) \leqslant \mathbb{E}$.

- *Case* $\hat{d} \equiv 1 \pmod 4$. Taking $n = \hat{d}$ gives $\sqrt{\bar{d}} \in \mathbb{E}$. But we also have
$$\mathbb{E} \geqslant \mathbb{Q}(\tau) \geqslant \mathbb{Q}(\zeta_{\hat{d}}) \geqslant \mathbb{Q}(i \operatorname{Im} \zeta_{\hat{d}}), \quad \text{and} \quad \mathbb{E} \geqslant \mathbb{E}_1 \geqslant \mathbb{Q}(\operatorname{Im} \zeta_{\hat{d}}),$$
so that $i \in \mathbb{E}$. Thus $i\sqrt{\bar{d}} \in \mathbb{E}$.
- *Case* $2|d$. Then $4|\bar{d}$. Taking n to be the negative of the square-free part of $\bar{d}/4$, we find that $\mathbb{Q}(i\sqrt{\bar{d}}) = \mathbb{Q}(\sqrt{n}) \leqslant \mathbb{Q}(\zeta_{4n}) \leqslant \mathbb{Q}(\zeta_{\bar{d}}) \leqslant \mathbb{E}$.

The proof is complete. ∎

This motivates the following.

Definition 4.6 (see [6]). *A centered fiducial is called* strongly centered *if the image of* $\Phi_{\mathbf{z}}$ *generates a field extension* $\mathbb{E}_1$ *of* $\mathbb{K}$ *for which* $\mathbb{E} = \mathbb{E}_1(i\sqrt{\bar{d}})$.

One consequence of being strongly centered is that the r_g from Theorem 4.3 vanishes. By [6], this gives a cleaner formula with no condition on d:

$$g \circ \Phi_{\mathbf{z}} = \Phi_{\mathbf{z}} \circ G_g. \tag{4.1}$$

Every known fiducial is equivalent under the action of the Clifford group to a strongly centered one.

In Theorem 4.3, G_g is well defined up to multiplication by an element of S. It follows that there exists a subgroup M of $\mathrm{GL}_2\mathbb{Z}_{\bar{d}}$ in the centralizer $C(S)$ of S such that $\mathcal{G} \cong M/S$, with the isomorphism given by $g \mapsto G_g S$. All known solutions satisfy the following.

Conjecture 4.7 (see [6]). *M is a maximal abelian subgroup of $C(S)$.*

For the remainder of the paper, we shall assume this conjecture and that $\mathbf{z}$ *is strongly centered.*

By Theorem 4.3 and the definition of S, the right action of M on $\Phi_{\mathbf{z}}$ relates the overlap phases by (possibly trivial) Galois conjugation. For a fixed d, different fiducials may have different symmetry groups. However, M is determined only by d and the type of the fiducial.

Assuming Conjecture 4.7, we can compute the structure of the group M. The first step has been taken in the type-z case.

Lemma 4.8 (see [4]). *For type-z fiducials, $M = C(S) = \mathbb{Z}_{\bar{d}}[I, F]^\times$.*

Here $\mathbb{Z}_{\bar{d}}[I, F]^\times \leqslant \mathrm{GL}_2\mathbb{Z}_{\bar{d}}$ are the set of invertible elements in the algebra $\mathbb{Z}_{\bar{d}}[I, F]$.

We will relate this lemma to number theory as follows. Let u_f be the fundamental unit in $\mathcal{O}_\mathbb{K}$ that is positive with respect to the real embedding of $\mathbb{K}$ for which $\sqrt{D}$ is positive, which we label ∞_1. Let u_D be the smallest power of u_f with norm 1 (so that u_D is either u_f or u_f^2, since the norm of u_f is in $\{\pm 1\}$). By [7], there exists some $r \in \mathbb{N}$ such that the rational part of u_D^r equals $(d-1)/2$, and $u_D \pmod{\bar{d}}$ has order $3\iota r$, where $\iota = \bar{d}/d$.

Lemma 4.9. *The homomorphism $j : \mathbb{Z}_{\bar{d}}[I, F] \to \mathcal{O}_\mathbb{K}/(\bar{d})$ that maps I to $[1]$ and F to $[u_D^{\iota r}]$ is an isomorphism if and only if either d is coprime to 3 or $3|D$ and $d \not\equiv 3 \pmod{27}$.*

Proof. Note that j is well defined since F and $u_D^{\iota r}$ are both order 3. Recall that $\mathcal{O}_\mathbb{K} = \mathbb{Z}[1, \omega]$, where $\omega \in \{\sqrt{D}, \frac{1+\sqrt{D}}{2}\}$. The surjectivity of j is equivalent to $[\omega]$ being in the image of j. This is equivalent to the ω-coefficient $y \in \mathbb{Z}$ of u_D^r being invertible modulo $\bar{d}$. This equivalence is clear when d is odd, since $u_D^r = j(F)$. When d is even, then $j(F) = (u_D^r)^2$ has ω-coefficient $y(d-1)$, since the rational part of u_D^r is $(d-1)/2$. The equivalence then follows from $d-1$ being invertible modulo $\bar{d}$.

Since $y \neq 0$, j can only have a kernel when d and y share a common factor, which is the condition for j to not be surjective. Thus j is bijective if and only if it is surjective.

Since u^r has norm 1 and rational part $\frac{d-1}{2}$, the norm of $2u^r$ is $4 = (d-1)^2 - D\sigma^2 y^2$, where σ^{-1} is the $\sqrt{D}$ coefficient of ω. Modulo $\gcd(d,y)$, this gives $4 \equiv 1 \pmod{\gcd(d,y)}$, so that $\gcd(d,y)|3$. In particular, j is not surjective if and only if $\gcd(d,y) = 3$.

If $3|\gcd(D,y)$, then the norm of $2u_D^r$ modulo 27 gives $3 \equiv d^2 - 2d \pmod{27}$, so that $d \equiv -1$ or $3 \pmod{27}$. Thus $3 = \gcd(d,y)$ if and only if $d|3$ and either $3 \not| D$ or $d \equiv 3 \pmod{27}$. ■

Remark 4.10. Since $\gcd(d,y)|3$, we see that $\ker j$ is generated by $(\bar{d}/3)F \in (\bar{d}/3)M \cong M_3$. Here we write M_n to mean the projection of M onto $\mathrm{GL}_2\mathbb{Z}_n$ when n is a factor of $\bar{d}$ co-prime to $\bar{d}/n$. If $\mathbf{z}$ is type-a, then the kernel is trivial, since the same is true of the projection of F to M_3.

The map j restricts to a homomorphism $j^\times \colon \mathbb{Z}_{\bar{d}}[I,F]^\times \to \big(\mathcal{O}_\mathbb{K}/(\bar{d})\big)^\times$ with the same isomorphism criteria as in Lemma 4.9. Whenever these criteria are satisfied there are only type-z fiducials (in the known solutions). These satisfy $\big(\mathcal{O}_\mathbb{K}/(\bar{d})\big)^\times \cong \mathbb{Z}_{\bar{d}}[I,F]^\times \cong M$, where the last isomorphism is Lemma 4.8.

Consider the case when $\mathbf{z}$ is a type-a fiducial so that j is not an isomorphism. By the type-a condition and Chinese remainder theorem, we have $\mathbb{Z}_{\bar{d}}[I,F] = \mathbb{Z}_3 \times \mathbb{Z}_{\bar{d}/3}[I,F]$. This gives

$$\begin{aligned} M &\cong M_3 \times M_{\bar{d}/3} \\ &\cong (M_3/\mathbb{Z}_3^\times \times \mathbb{Z}_3^\times) \times \mathbb{Z}_{\bar{d}/3}[I,F]^\times \\ &\cong M_3/\mathbb{Z}_3^\times \times \mathbb{Z}_{\bar{d}}[I,F]^\times \\ &\cong M_3/\mathbb{Z}_3^\times \times \big(\mathcal{O}_\mathbb{K}/(\bar{d})\big)^\times/\mathrm{coker} j^\times, \end{aligned}$$

where $\mathbb{Z}_3^\times$ acts by scalar multiplication, and we used $M_{\bar{d}/3} \cong \mathbb{Z}_{\bar{d}/3}[I,F]^\times$ from Lemma 4.8, since F modulo $\bar{d}/3$ is congruent to F_z. This gives the exact sequence

$$1 \to M_3/\mathbb{Z}_3^\times \to M \to \big(\mathcal{O}_\mathbb{K}/(\bar{d})\big)^\times \to \mathrm{coker} j^\times \to 1.$$

In the known solutions, the type-a fiducials satisfy $M \cong \big(\mathcal{O}_\mathbb{K}/(\bar{d})\big)^\times$, which by the above exact sequence is equivalent to $M_3/\mathbb{Z}_3^\times \cong \mathrm{coker} j^\times$ or equivalently $M_3 \cong (\mathcal{O}_\mathbb{K}/(3))^\times$. Assuming the existence of this last isomorphism, which we will denote by j', allows us to extend $j^\times$ to an isomorphism

$$\hat{\jmath} = (j', j^\times) : M = M_3 \times \mathbb{Z}_{\frac{\bar{d}}{3}}[I,F]^\times \cong (\mathcal{O}_\mathbb{K}/(3))^\times \times \Big(\mathcal{O}_\mathbb{K}/\big(\tfrac{\bar{d}}{3}\big)\Big)^\times \cong \big(\mathcal{O}_\mathbb{K}/(\bar{d})\big)^\times.$$

In the type-z case, we will let $\hat{\jmath} = j^\times : M \to \big(\mathcal{O}_\mathbb{K}/(\bar{d})\big)^\times$. This discussion motivates the following.

Definition 4.11. *A strongly centered fiducial is* algebraic *if* $\hat{\jmath} : M \to \big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^{\times}$ *is an isomorphism.*

Note that $\big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^{\times}$ was computed in [36], but we need to do work before applying this result to our setting.

Lemma 4.12. *Let p be a prime factor of d. If $p \equiv 1 \pmod 3$, then p splits in $\mathbb{K}$. If $p \equiv 2 \pmod 3$, then p is prime in $\mathbb{K}$. If $p = 3$, then p splits/ramifies/is prime in $\mathbb{K}$ if $D \equiv 1/0/-1 \pmod 3$.*

Proof. Since $\mathbb{K} = \mathbb{Q}(\sqrt{D})$ is a quadratic extension, p is prime (respectively, ramifies or is a product of two primes) in $\mathbb{K}$ if and only if the polynomial

$$f(x) := \begin{cases} x^2 - D & \text{if } D \not\equiv 1 \pmod 4, \\ (2x-1)^2 - D & \text{if } D \equiv 1 \pmod 4) \end{cases}$$

is irreducible (respectively, a square, or a product of different linear factors) modulo p [15]. When $p = 3$, the claim is immediate. Otherwise, p being prime is equivalent to D not being a quadratic residue modulo p. Since D is the square-free part of $(d+1)(d-3)$, this is equivalent to $(d+1)(d-3) \equiv -3 \pmod p$ not being a quadratic residue modulo p. By quadratic reciprocity, this is equivalent to p not being a quadratic residue modulo 3, so that $p \equiv 2 \pmod 3$.

On the other hand, p ramifies if and only if $p|D$, which can only happen if $p = 3$ since $D|(d+1)(d-3) \equiv -3 \pmod p$. Thus if $p \equiv 1 \pmod 3$, then p splits. ■

Lemma 4.13. *If $9|d$, then $D \not\equiv 3 \pmod 9$.*

Proof. Assume that $9|d$ and $D \equiv 3 \pmod 9$. u_D^r is a solution $\frac{T+U\sqrt{D}}{2}$ of the Pell equation $T^2 - DU^2 = 4$. We know that the rational part of u_D^r is $\frac{d-1}{2}$, so that $T = d-1$. The Pell equation modulo 9 is $1 - 3U^2 \equiv 4 \pmod 9$. Rearranging and dividing by 3 gives $U^2 \equiv -1 \pmod 3$, a contradiction. ■

This allows us to present the result of [36] applied to our situation.

Theorem 4.14 (see [36]). *Let p be a prime and $k \in \mathbb{N}$ be larger than 1 if $p = 2$. Then*

$$\big(\mathcal{O}_{\mathbb{K}}/(p^k)\big)^{\times} \cong \begin{cases} \mathbb{Z}_{p-1}^2 \times \mathbb{Z}_{p^{k-1}}^2 & \text{if } p > 2 \text{ splits in } \mathbb{K}, \\ \mathbb{Z}_{p^2-1} \times \mathbb{Z}_{p^{k-1}}^2 & \text{if } p > 2 \text{ is prime in } \mathbb{K}, \\ \mathbb{Z}_6 \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_{2^{k-2}} & \text{if } p = 2 \text{ and } k > 1, \\ \mathbb{Z}_6 \times \mathbb{Z}_{3^{k-1}}^2 & \text{if } p = 3 \text{ ramifies in } \mathbb{K}. \end{cases}$$

For this statement of the result we needed the previous lemma since [36] treats separately the cases when $3|d$ and $D \equiv 3$ or $6 \pmod 9$. The lemma allows us to deduce that $k = 1$ when $D \equiv 3 \pmod 9$ and notice that both cases give the same result when $k = 1$.

In [6], type-a fiducials were labeled by types a_4, a_6, or a_8 corresponding to M_3 being isomorphic to $\mathbb{Z}_2^2$, $\mathbb{Z}_6$, or $\mathbb{Z}_8$, respectively.

We can now prove Proposition 1.1.

Proof of Proposition 1.1. By Lemmas 4.8 and 4.9, algebraic fiducials which are type-z satisfy that either d is coprime to 3 or $3|D$ and $d \not\equiv 3 \pmod{27}$. Thus type-a fiducials satisfy that $3|d$ and either $3 \nmid D$ or $d \equiv 3 \pmod{27}$. When $d \equiv 3 \pmod{27}$, then $D \equiv 0 \pmod 3$. By combining Lemma 4.12 with the previous theorem, we find that $D \equiv 0/1/2$, respectively, gives $M_3 \cong \mathbb{Z}_6/\mathbb{Z}_2^2/\mathbb{Z}_8$, respectively, which gives the claim. ∎

In the known examples, every strongly centered fiducial which is not algebraic is type-z despite type-a solutions existing for the given d. Since algebraic type-z solutions with $3|d$ have 3 ramified, we can think of nonalgebraic solutions as having 3 pretending to be ramified.

Now that we have more understanding of the structure of M, we will study its action on $\mathbb{Z}_{\bar d}^2$. First note that the center Z of $\mathrm{GL}_2\mathbb{Z}_{\bar d}$ is contained in M. Its action preserves each $C \in \mathbb{P}\mathbb{Z}_{\bar d}^2$, so we get an induced action of M/Z on $\mathbb{P}\mathbb{Z}_{\bar d}^2$. Before we study this action, first note that we have a Chinese remainder theorem for $\mathbb{P}\mathbb{Z}_{\bar d}^2$.

Lemma 4.15. *If $2 \geqslant n, m \in \mathbb{N}$ are coprime, then $\mathbb{P}\mathbb{Z}_{mn}^2 \cong \mathbb{P}\mathbb{Z}_m^2 \times \mathbb{P}\mathbb{Z}_n^2$.*

Proof. Note that $\mathbb{P}\mathbb{Z}_{mn}^2$ consists of cyclic subgroups whose generators lie in the set

$$\mathbb{Z}_{mn}^{2\times} := \left\{\mathbf{p} \in \mathbb{Z}_{mn}^2 : \langle p_1, p_2\rangle = \mathbb{Z}_{mn}\right\}.$$

Using the Chinese remainder theorem $(\pi_m, \pi_n)\colon \mathbb{Z}_{mn} \xrightarrow{\cong} \mathbb{Z}_m \times \mathbb{Z}_n$, we find

$$\langle p_1, p_2\rangle = \mathbb{Z}_{mn} \iff \langle \pi_m p_1, \pi_m p_2\rangle = \mathbb{Z}_m \text{ and } \langle \pi_n p_1, \pi_n p_2\rangle = \mathbb{Z}_n.$$

Thus $\mathbb{Z}_{mn}^{2\times} \cong \mathbb{Z}_m^{2\times} \times \mathbb{Z}_n^{2\times}$. Since $\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{\times}$, where the $\times$ in the exponent denotes the group of units, we have

$$\mathbb{P}\mathbb{Z}_{mn}^2 = \mathbb{Z}_{mn}^{2\times}/\mathbb{Z}_{mn}^{\times} \cong \mathbb{Z}_m^{2\times}/\mathbb{Z}_m^{\times} \times \mathbb{Z}_n^{2\times}/\mathbb{Z}_n^{\times} = \mathbb{P}\mathbb{Z}_m^2 \times \mathbb{P}\mathbb{Z}_n^2$$

as stated. ∎

This allows us to reduce to the case when $\bar d = p^k$, which one can easily count.

Lemma 4.16. $\left|\mathbb{P}\mathbb{Z}_{p^k}^2\right| = p^{k-1}(p+1)$.

Proof. If $\binom{a}{b}$ generates some $C \in \mathbb{P}\mathbb{Z}_{p^k}^2$, then either a, b, or both lie in $\mathbb{Z}_{p^k}^{\times}$. This gives

$$\mathbb{Z}_{p^k}^{2\times} = \left(\mathbb{Z}_{p^k}^{\times} \times \overline{\mathbb{Z}_{p^k}^{\times}}\right) \sqcup \left(\overline{\mathbb{Z}_{p^k}^{\times}} \times \mathbb{Z}_{p^k}^{\times}\right) \sqcup \left(\mathbb{Z}_{p^k}^{\times} \times \mathbb{Z}_{p^k}^{\times}\right),$$

where $\overline{\mathbb{Z}_{p^k}^{\times}} = \mathbb{Z}_{p^k} \backslash \mathbb{Z}_{p^k}^{\times}$. Thus

$$\left|\mathbb{P}\mathbb{Z}_{p^k}^2\right| = 2\left|\overline{\mathbb{Z}_{p^k}^{\times}}\right| + \left|\mathbb{Z}_{p^k}^{\times}\right| = 2\left|\mathbb{Z}_{p^k}\right| - \left|\mathbb{Z}_{p^k}^{\times}\right| = 2p^k - \phi(p^k) = 2p^k - p^{k-1}(p-1),$$

as required. ∎

Using the Chinese remainder theorem for M, it suffices to consider the action of M_{p^k}/Z_{p^k} on $\mathbb{P}\mathbb{Z}_{p^k}^2$.

Lemma 4.17. *For algebraic fiducials,*

$$M_{p^k}/Z_{p^k} \cong \begin{cases} \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{k-1}} & \text{if } p \text{ splits}, \\ \mathbb{Z}_{p+1} \times \mathbb{Z}_{p^{k-1}} & \text{if } p > 2 \text{ is prime}, \\ \mathbb{Z}_6 \times \mathbb{Z}_{2^{k-2}} & \text{if } p = 2, \\ \mathbb{Z}_3 \times \mathbb{Z}_{3^{k-1}} & \text{if } p = 3 \text{ ramifies}. \end{cases}$$

For nonalgebraic fiducials, the result is the same except when $p = 3$, where $M_3/Z_3 \cong \mathbb{Z}_3$ (as if 3 ramifies).

Proof. It is well known that

$$Z_{p^k} \cong \mathbb{Z}_{p^k}^\times \cong \begin{cases} \mathbb{Z}_{p-1} \times \mathbb{Z}_{p^{k-1}}, & \text{if } \ p \neq 2, \\ \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}} & \text{if } \ p = 2, \ k > 1. \end{cases}$$

Aside from the case $p = 2 < k$, the result follows directly from Theorem 4.14. For $p = 2 < k$, there are two possible quotients of M_{2^k} by different embeddings of $\mathbb{Z}_2 \times \mathbb{Z}_{2^{k-2}}$. By Theorem 4.14, $M_{2^k} \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_{2^{k-1}} \times \mathbb{Z}_{2^{k-2}}$. Note that $(I + 2F)^2 = -3I$ generates $Z_{2^k}/\pm 1 \cong \mathbb{Z}_{2^{k-2}}$. Thus $I + 2F$ generates the $\mathbb{Z}_{2^{k-1}}$ factor of M_{2^k}. It follows that

$$M_{2^k}/Z_{2^k} \cong \mathbb{Z}_3 \times \mathbb{Z}_{2^{k-1}}/\mathbb{Z}_{2^{k-2}} \times \mathbb{Z}_{2^{k-2}} \cong \mathbb{Z}_6 \times \mathbb{Z}_{2^{k-2}}.$$ ■

Lemma 4.18. *The (cyclic) action of M_{p^k}/Z_{p^k} on $\mathbb{P}\mathbb{Z}_{p^k}^2$ has one free orbit and s orbits of size $p^k/\bar{p}$, where*

$$s = \begin{cases} 0 & \textit{if } \ p \equiv 2 \pmod 3) \textit{ or } p = 3 \textit{ is type-}a_8, \\ 1 & \textit{if } \ p = 3 \textit{ is type-}z \textit{ or type-}a_6, \\ 2 & \textit{if } \ p \equiv 1 \pmod 3 \textit{ or } p = 3 \textit{ is type-}a_4. \end{cases}$$

Note that in the algebraic case, s is the number of proper factors of p in $\mathcal{O}_{\mathbb{K}}$.

Proof. Combining the two previous lemmas gives that $M_{p^k}/Z_{p^k} \cong \mathbb{Z}_{|\mathbb{P}\mathbb{Z}_{\bar{p}}^2|-s} \times \mathbb{Z}_{p^k/\bar{p}}$. We first consider the case $p^k = \bar{p}$. Assume that there exists a nonfree orbit o with more than one element. Since the fixed points of the action of some $gZ_{\bar{p}} \in M_{\bar{p}}/Z_{\bar{p}}$ correspond to eigenspaces of g, there can be at most 2 of them unless $g \in Z_{\bar{p}}$.

Since o must be fixed by some nontrivial element of $M_{\bar{p}}/Z_{\bar{p}}$, this means that o must have 2 elements.

- *Case* $s < 2$. Note that $|M_{\bar{p}}/Z_{\bar{p}}| + |o| > |\mathbb{P}\mathbb{Z}_{\bar{p}}^2|$, so there is not enough room for any free orbits. Thus every orbit has size 1 or 2. This contradicts $M_{\bar{p}}/Z_{\bar{p}}$ being a cyclic group of order > 2 acting effectively.
- *Case* $s = 2$. From [1], we know that $M_{\bar{p}}$ is diagonalizable. The claim easily follows.

Now consider the case when $p^k > \bar{p}$. The multiplication map $\mathbb{Z}_p^k \to (p^k/\bar{p})\mathbb{Z}_{p^k} \cong \mathbb{Z}_{\bar{p}}$ induces a map $\rho \colon \mathbb{P}\mathbb{Z}_{p^k}^2 \to \mathbb{P}\mathbb{Z}_{\bar{p}}^2$, where all of the fibers have the same size, which must be $p^k/\bar{p}$ by Lemma 4.16.

The previous lemma shows that $M_{p^k}/Z_{p^k} \cong M_{\bar{p}}/Z_{\bar{p}} \times \mathbb{Z}_{p^k/\bar{p}}$. One can easily show that the second factor is generated by $I + \bar{p}F$. Since this is congruent to I modulo $\bar{p}$, $I + \bar{p}F$ acts trivially on $\mathbb{P}\mathbb{Z}_{\bar{p}}^2$. Thus it restricts to an action on each fiber of ρ, which have size $p^k/\bar{p}$. Since this number is a prime power and the same as the order of $I + \bar{p}F$, it must act transitively. ■

Theorem 4.19. *For algebraic fiducials, each M-orbit in $\mathbb{Z}_{\bar{d}}^2$ has stabilizer $\hat{\jmath}^{-1}(\ker \pi_{\mathfrak{n}})$ for some factor $\mathfrak{n}$ of $\bar{d}$ in $\mathcal{O}_{\mathbb{K}}$, where $\hat{\jmath} : M \cong (\mathcal{O}_{\mathbb{K}}/(\bar{d}))^\times$ comes from the algebraic condition, and $\pi_{\mathfrak{n}} \colon (\mathcal{O}_{\mathbb{K}}/(\bar{d}))^\times \to (\mathcal{O}_{\mathbb{K}}/(\mathfrak{n}))^\times$ is the map which takes elements modulo $\mathfrak{n}$. This gives a one-to-one correspondence between orbits of M and factors of $\bar{d}$ in $\mathcal{O}_{\mathbb{K}}$. For nonalgebraic fiducials, the same is true if 3 is treated as if it ramifies in $\mathcal{O}_{\mathbb{K}}$.*

Proof. The action of $\mathrm{GL}_2\mathbb{Z}_{\bar{d}}$ on $\mathbb{Z}_{\bar{d}}^2$ preserves the function

$$f\colon \mathbb{Z}_{\bar{d}}^2 \longrightarrow \mathbb{N}, \quad \mathbf{p} \mapsto \gcd(p_1, p_2, \bar{d}).$$

The action of Z restricted to each $C \in \mathbb{P}\mathbb{Z}_{\bar{d}}^2$ is equivalent to the action of $\mathbb{Z}_{\bar{d}}^\times$ on $\mathbb{Z}_{\bar{d}}$, whose orbits are the fibers of $f|_C$. Thus the orbits of M correspond to the intersection of the orbits of M/Z with the fibers of f.

For any $\mathfrak{n}|\bar{d}$, there is a minimal $n \in \mathbb{N}$ such that $\mathfrak{n}|n$. We find that $\hat{\jmath}^{-1}(\ker \pi_n) \leqslant \hat{\jmath}^{-1}(\ker \pi_{\mathfrak{n}})$ stabilizes $f^{-1}(\bar{d}/n) = (\bar{d}/n)\mathbb{Z}_{\bar{d}}^2 \cong \mathbb{Z}_n^2$.

Using Chinese remainder results, we can reduce to the case when $n = p^k$ is a prime power. Using the previous lemma, we see that if p is prime, then $\mathfrak{n} = n$ and there is only one orbit in $f^{-1}(n)$, so this must have stabilizer $\hat{\jmath}^{-1}(\ker \pi_n)$.

If $p = \prod_{i=1}^2 \mathfrak{p}_i$ factors into different primes $\{\mathfrak{p}\}_{i=1}^2$, then M is diagonalizable, with $\hat{\jmath}$ mapping each factor of the diagonalization to a factor of $\left(\mathcal{O}_\mathbb{K}/(p^k)\right)^\times \cong \prod_{i=1}^2 \left(\mathcal{O}_\mathbb{K}/(\mathfrak{p}_i^k)\right)^\times$. By Chinese remainder results, we can consider each factor separately. Each factor is equivalent the action of $\mathbb{Z}_{p^k}^\times$ on $\mathbb{Z}_{p^k}$, whose orbits are $\{p^\ell \mathbb{Z}_{p^k}\}_{\ell=0}^k$. The result follows since the stabilizer of the action of $\mathbb{Z}_{p^k}^\times$ on $p^\ell\mathbb{Z}_{p^k}$ is $\ker(\mathrm{mod}\colon \mathbb{Z}_{p^k}^\times \to \mathbb{Z}_{p^{k-\ell}}^\times)$.

If p ramifies with square root $\mathfrak{p}$, then $(\mathcal{O}_\mathbb{K}/(\mathfrak{p}))^\times \cong \mathbb{Z}_p^\times$. Thus $\hat{\jmath}^{-1}(\ker \pi_\mathfrak{p}) \cong M_3/Z_3$ stabilizes the exceptional orbit from the previous lemma. More generally, the free and exceptional orbits in $f^{-1}(n)$ have stabilizers $\hat{\jmath}^{-1}(\ker \pi_n)$ and $\hat{\jmath}^{-1}(\ker \pi_{n/\mathfrak{p}})$, respectively. ■

5. Structure of the number fields.

Now we will compute $\mathcal{G}$ using class field theory. We begin with some definitions.

Definition 5.1. *Let $\mathbb{F}$ be a number field. A* modulus *of $\mathbb{F}$ is a pair $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, where $\mathfrak{m}_0$ is an integral ideal of $\mathbb{K}$ and $\mathfrak{m}_\infty$ is a set of real embeddings $\mathbb{F} \hookrightarrow \mathbb{C}$. For each modulus $\mathfrak{m}$, there is a corresponding* ray class field *$\mathbb{F}(\mathfrak{m})$. The* Hilbert class field *$\mathbb{F}(1)$ is the ray class field of the trivial modulus. The degree $[\mathbb{F}(1) : \mathbb{F}]$ is the* class number *$h(\mathbb{F})$.*

Definition 5.2. *An algebraic fiducial is a* ray class fiducial *if $\mathbb{E}_0 = \mathbb{K}(1)$ (the Hilbert class field) and $\mathbb{E}_1 = \mathbb{K}(\mathfrak{m}_1)$, the ray class field over $\mathbb{K}$ with modulus $\mathfrak{m}_1 := (\bar{d})\infty_1$, where ∞_1 is the real embedding of $\mathbb{K}$ for which $\sqrt{D}$ is positive.*

Ray class fiducials are found in every dimension where fiducials are found. In Theorem 1.2, which is duplicated below, we see that these have a nice interpretation of the symmetry group S.

Theorem 5.3. *For ray class fiducials, S is isomorphic to the cyclic subgroup generated by the fundamental unit in $\mathcal{O}_\mathbb{K}$ modulo $\bar{d}$.*

Proof. There is a well-known five-term exact sequence

$$1 \to \mathcal{U}_\mathfrak{m}(\mathbb{F}) \to \mathcal{U}(\mathbb{F}) \to (\mathcal{O}_\mathbb{F}/\mathfrak{m})^\times \to \mathcal{C}_\mathfrak{m} \to \mathcal{C} \to 1,$$

where $\mathcal{C}$ is the class group of some field $\mathbb{F}$, $\mathcal{C}_\mathfrak{m}$ is the ray class group of some modulus $\mathfrak{m} = \mathfrak{m}_0\mathfrak{m}_\infty$, $\mathcal{U}(\mathbb{F})$ is the unit group, and

$$\mathcal{U}_\mathfrak{m}(\mathbb{F}) = \{\alpha \in \mathcal{U}(\mathbb{F}) : v_\mathfrak{p}(\alpha - 1) \geqslant v_\mathfrak{p}(\mathfrak{m}_0), \sigma_i(\alpha) > 0 \ \forall \mathfrak{p}|\mathfrak{m}_0, \sigma_i \in \mathfrak{m}_\infty\},$$

where $v_{\mathfrak{p}}(n) := \max\{r \in \mathbb{N} : \mathfrak{p}^r | n\}$. The class groups have the property that $\mathcal{C}_{\mathfrak{m}} \cong \mathrm{Gal}(\mathbb{F}(\mathfrak{m})/\mathbb{F})$. Thus

$$\mathcal{C}_{\mathfrak{m}}/\mathcal{C} \cong \mathrm{Gal}\big(\mathbb{F}(\mathfrak{m})/\mathbb{F}\big)/\mathrm{Gal}\big(\mathbb{F}(1)/\mathbb{F}\big) \cong \mathrm{Gal}\big(\mathbb{F}(\mathfrak{m})/\mathbb{F}(1)\big).$$

Now consider a ray class fiducial, where $\mathbb{F} = \mathbb{K}$ and $\mathfrak{m} = \mathfrak{m}_1 = (\bar{d})\infty_1$. We have the (not necessarily commutative) diagram of short exact sequences

$$\begin{array}{ccccccccc}
 & & & & & & 1 & & \\
 & & & & & & \downarrow & & \\
 & & 1 & & & & \mathbb{Z}_2 & & \\
 & & \downarrow & & & & \downarrow & & \\
1 & \longrightarrow & S & \longrightarrow & M & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow \cong & & \downarrow & & \\
1 & \longrightarrow & \mathcal{U}/\mathcal{U}_{(\bar{d})} & \longrightarrow & \big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^{\times} & \longrightarrow & \mathcal{C}_{(\bar{d})}/\mathcal{C} & \longrightarrow & 1 \\
 & & \downarrow & & & & \downarrow & & \\
 & & \mathbb{Z}_2 & & & & 1 & & \\
 & & \downarrow & & & & & & \\
 & & 1 & & & & & &
\end{array}.$$

The $\mathbb{Z}_2$ term in the last column comes from

$$\mathcal{G}/\big(\mathcal{C}_{\bar{d}}/\mathcal{C}\big) \cong \mathrm{Gal}\Big(\mathbb{K}(\mathfrak{m}_1)/\mathbb{K}(1)\Big)/\mathrm{Gal}\Big(\mathbb{K}\big((\bar{d})\big)/\mathbb{K}(1)\Big) \cong \mathrm{Gal}\Big(\mathbb{K}(\mathfrak{m}_1)/\mathbb{K}\big((\bar{d})\big)\Big) \cong \mathbb{Z}_2.$$

The $\mathbb{Z}_2$ in the last column is generated by complex conjugation [7], which is the image of $-I \in M$. $-I$ gets mapped to -1 in $\big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^{\times}$, which must generate the $\mathbb{Z}_2$ in the first column. In fact, $\mathcal{U}$ is generated by u_f and -1, so $\mathcal{U}/\mathcal{U}_{\bar{d}}$ is generated by $[u_f]$ and $[-1]$, where $[\cdot]$ indicates equivalence classes in $\mathbb{K}/(\bar{d})$.

We can factor out the instances of $\mathbb{Z}_2$ from the diagram to get

$$\begin{array}{ccccccccc}
1 & \longrightarrow & S & \longrightarrow & M & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\
 & & \downarrow \cong & & \downarrow \cong & & \downarrow \cong & & \\
1 & \longrightarrow & \Big\langle [\pm u_f]_{(\bar{d})} \Big\rangle & \longrightarrow & \big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^{\times} & \longrightarrow & \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C} & \longrightarrow & 1
\end{array}.$$

This completes the proof by noting that $\langle [-u_f]_{(\bar{d})} \rangle \cong \langle [u_f]_{(\bar{d})} \rangle$ unless the second group has odd order, in which case $-u_f$ could not be a generator for the quotient. ∎

To generalize the previous theorem, we note that conjecturally ray class fiducials are minimal in the sense that every strongly centered fiducial has $\mathbb{E}_1$, an extension of $\mathbb{K}(\mathfrak{m}_1)$, and $\mathbb{E}_0$ is an extension of $\mathbb{K}(1)$. Assuming this, we can describe the structure of algebraic fiducials.

Theorem 5.4. *For every algebraic fiducial such that* $\mathbb{K}(1) \leqslant \mathbb{E}_0$ *and* $\mathbb{K}(\mathfrak{m}_1) \leqslant \mathbb{E}_1$, $\mathcal{G}$ *is a cyclic extension of* $\mathcal{C}_{\mathfrak{m}_1}/\mathcal{C}$, *and* S *is isomorphic to some subset of* $\left\langle [\pm u_f]_{(\bar{d})} \right\rangle$.

Proof. First we prove that $\mathcal{G}$ is an extension of $\mathcal{C}_{\mathfrak{m}_1}/\mathcal{C}$. Note that we have short exact sequences

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \mathcal{G} & \longrightarrow & \mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(1)) & \longrightarrow & \mathrm{Gal}(\mathbb{E}_0/\mathbb{K}(1)) & \longrightarrow & 1, \\
1 & \longrightarrow & \mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(\mathfrak{m}_1)) & \longrightarrow & \mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(1)) & \longrightarrow & \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C} & \longrightarrow & 1.
\end{array}$$

These can be combined to give

$$1 \longrightarrow \mathcal{G} \cap \mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(\mathfrak{m}_1)) \longrightarrow \mathcal{G} \longrightarrow \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C} \longrightarrow \frac{\mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(1))}{\mathcal{G}\cdot\mathrm{Gal}(\mathbb{E}1/\mathbb{K}(\mathfrak{m}_1))} \longrightarrow 1.$$

Combining this with the relevant short exact sequences gives the diagram

$$\begin{array}{ccccccccc}
 & & & & & & 1 & & \\
 & & & & & & \downarrow & & \\
 & & 1 & & 1 & & \mathcal{G} \cap \mathrm{Gal}\big(\mathbb{E}_1/\mathbb{K}(\mathfrak{m}_1)\big) & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & S & \longrightarrow & M & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle j_S} & & \downarrow{\scriptstyle \hat{\jmath}} & & \downarrow & & \\
1 & \longrightarrow & \left\langle [\pm u_f]_{(\bar{d})} \right\rangle & \longrightarrow & \big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^{\times} & \longrightarrow & \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C} & \longrightarrow & 1\ , \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}$$

where the injectivity of j_S is deduced from the diagram. Similarly, the vertical map onto $\mathcal{C}_{\mathfrak{m}_1}/\mathcal{C}$ is surjective, so that $\frac{\mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(1))}{\mathcal{G}\cdot\mathrm{Gal}(\mathbb{E}1/\mathbb{K}(\mathfrak{m}_1))}$ is trivial. We also find that $\mathcal{G}$ is an extension of $\mathcal{C}_{\mathfrak{m}_1}/\mathcal{C}$ by $\mathcal{G} \cap \mathrm{Gal}\big(\mathbb{E}_1/\mathbb{K}(\mathfrak{m}_1)\big) \cong \langle [\pm u_f]_{(\bar{d})} \rangle / j_s(S)$, which is cyclic. ■

In the nonalgebraic case things are more complicated, since $j^{\times}$ has a kernel and co-kernel. Recall that in this case, $d \equiv 3 (\mathrm{mod}\ 9)$, with the kernel given by $M_3/Z_3 \cong \mathbb{Z}_3$, and co-kernel given by the cyclic group $(\mathcal{O}_{\mathbb{K}}/(3))^{\times}/\mathbb{Z}_3^{\times} \cong \mathbb{Z}_k$, where the algebraic fiducials are type a_{2k}. This gives the diagram

$$
\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \mathbb{Z}_3 & & \mathcal{G}\cap\mathrm{Gal}\big(\mathbb{E}_1/\mathbb{K}(\mathfrak{m}_1)\big) & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & S & \longrightarrow & M & \longrightarrow & \mathcal{G} & \longrightarrow & 1 \\
 & & \downarrow & & \downarrow{\scriptstyle j^\times} & & \downarrow & & \\
1 & \longrightarrow & \big\langle [\pm u_f]_{(\bar{d})} \big\rangle & \longrightarrow & \big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^\times & \longrightarrow & \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C} & \longrightarrow & 1, \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \mathbb{Z}_k & & Q & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}
$$

where $Q := \frac{\mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(1))}{\mathcal{G}\cdot\mathrm{Gal}(\mathbb{E}1/\mathbb{K}(\mathfrak{m}_1))}$. In all of the known examples, S injects into $\langle[\pm u_f]_{(\bar{d})}\rangle$ and $\mathbb{Z}_3$ injects into $\mathcal{G}\cap\mathrm{Gal}(\mathbb{E}_1/\mathbb{K}(\mathfrak{m}_1))$. There are two observed cases. In the first case, $Q = 1$ and $\mathbb{Z}_k$ is a quotient of $\langle[\pm u_f]_{(\bar{d})}\rangle$. In the second case, $Q \cong \mathbb{Z}_k$.

Theorem 5.5. *For an algebraic fiducial, for each $\mathcal{O}_{\mathbb{K}} \ni \mathfrak{n}|(\bar{d})$, an overlap phase contained in the orbit of M labeled by $\mathfrak{n}$ takes values in the fixed field of a Galois group isomorphic to* $\mathrm{Gal}\big(\mathbb{K}(\mathfrak{m}_1)/\mathbb{K}((\mathfrak{n})\infty_1)\big)$.

Proof. Using the isomorphism $M \cong (\mathcal{O}_{\mathbb{K}}/(\bar{d}))^\times$, the elements of the orbit labeled by $\mathfrak{n}$ are those which are stabilized by the subgroup $\mathrm{stab}(\mathfrak{n})$ whose elements which are congruent to 1 modulo $\mathfrak{n}$. The quotient $\big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^\times/\mathrm{stab}(\mathfrak{n}) \cong (\bar{d}/\mathfrak{n})\big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^\times \cong \big(\mathcal{O}_{\mathbb{K}}/(\mathfrak{n})\big)^\times$. This gives the diagram of short exact sequences

$$
\begin{array}{ccccccccc}
 & & & & 1 & & 1 & & \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & \mathrm{stab}(\mathfrak{n}) & & \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C}_{\mathfrak{n}\infty_1} & & \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \big\langle [\pm u_f]_{(\bar{d})} \big\rangle & \longrightarrow & \big(\mathcal{O}_{\mathbb{K}}/(\bar{d})\big)^\times & \longrightarrow & \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C} & \longrightarrow & 1 \\
 & & & & \downarrow & & \downarrow & & \\
1 & \longrightarrow & \langle [\pm u_f]_{(\mathfrak{n})} \rangle & \longrightarrow & (\mathcal{O}_{\mathbb{K}}/(\mathfrak{n}))^\times & \longrightarrow & \mathcal{C}_{\mathfrak{n}\infty_1}/\mathcal{C} & \longrightarrow & 1. \\
 & & & & \downarrow & & \downarrow & & \\
 & & & & 1 & & 1 & &
\end{array}
$$

The projection modulo $\mathfrak{n}$ gives a surjection $\langle[\pm u_f]_{(\bar{d})}\rangle \to \langle[\pm u_f]_{\mathfrak{n}}\rangle$ with some kernel K. We deduce from the commutativity of the diagram that K injects into stab($\mathfrak{n}$) with

$$\operatorname{stab}(\mathfrak{n})/K \cong \mathcal{C}_{\mathfrak{m}_1}/\mathcal{C}_{\mathfrak{n}\infty_1} \cong \operatorname{Gal}\big(\mathbb{K}(\mathfrak{m}_1)/\mathbb{K}(\mathfrak{n}\infty_1)\big). \qquad \blacksquare$$

This suggests that for ray class fiducials, the Galois orbit labeled by $\mathfrak{n}$ takes values in the field $\mathbb{K}(\mathfrak{n}\infty_1)$.

Remark 5.6. A SIC-POVM in dimension $d' = d(d-2)$ will have the same value of D as one in dimension d. This phenomenon is studied in [5], where the authors conjecture that every SIC-POVM α in dimension d is related to a SIC-POVM β in dimension d' which they call *aligned*, meaning that $\mathbb{E}_1^\beta$ is an extension of $\mathbb{E}_1^\alpha$ and the overlap phases of β taking values in $\mathbb{E}_1^\alpha$ are the squares of overlap phases of α. In the language of the above theorem, these correspond to Galois orbits whose labels are divisible by $d-2=\frac{d'}{d}$.

REFERENCES

[1] D. M. Appleby, *Symmetric informationally complete-positive operator valued measures and the extended Clifford group*, J. Math. Phys., 46 (2005), 052107.

[2] D. M. Appleby, I. Bengtsson, S. Brierley, M. Grassl, D. Gross, and J.-A. Larsson, *The monomial representations of the Clifford group*, Quant. Inf. Comp., 12 (2012), pp. 404–431.

[3] D. M. Appleby, H. B. Dang, and C. A. Fuchs, *Symmetric informationally-complete quantum states as analogues to orthonormal bases and minimum-uncertainty states*, Entropy, 16 (2014), pp. 1484–1492. 16.

[4] D. M. Appleby, H. Yadsan-Appleby, and G. Zauner, *Galois automorphisms of a symmetric measurement*, Quantum Inf. Comp., 13 (2014), pp. 672–720.

[5] M. Appleby, I. Bengtsson, I. Dumitru, and S. Flammia, *Dimension towers of SICs.* I. *Aligned SICs and embedded tight frames*, J. Math. Phys., 58 (2017), 112201.

[6] M. Appleby, T.-Y. Chien, S. Flammia, and S. Waldron, *Constructing exact symmetric informationally complete measurements from numerical solutions*, J. Phys. A, 51 (2018), 165302.

[7] M. Appleby, S. Flammia, G. McConnell, and J. Yard, *Generating ray class fields and real quadratic fields via complex equiangular lines*, Acta Arith., 192 (2020), pp. 211–233.

[8] V. Bargmann, *Note on Wigner's theorem on symmetry operations*, J. Math. Phys., 5 (1964), pp. 862–868.

[9] I. Bengtsson, *From SICs and MUBs to Eddington*, J. Phys. Conf. Ser., 254 (2010), 012007.

[10] I. Bengtsson, *The number behind the simplest SIC-POVM*, Found. Phys., 47 (2017), pp. 1031–1041.

[11] I. Bengtsson, *Algebraic units, anti-unitary symmetries, and a small catalogue of SICs*, Quant. Inf. Comp., 20 (2020), pp. 400–417.

[12] A. L. Besse, *Einstein Manifolds*, Springer, Berlin, 1987.

[13] D. C. Brody and L. P. Hughston, *Information content for quantum states*, J. Math. Phys., 41 (2000), pp. 2586–2592.

[14] D. C. Brody and L. P. Hughston, *Geometric quantum mechanics*, J. Geom. Phys., 38 (2001), pp. 19–53.

[15] K. Conrad, *Factoring in Quadratic Fields*, http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/quadraticgrad.pdf (21 June 2020).

[16] E. B. Davies, *Quantum Theory of Open Systems*, Academic Press, London, 1976.

[17] E. B. Davies and J. T. Lewis, *An operational approach to quantum probability*, Comm. Math. Phys., 17 (1970), pp. 239–260.

[18] P. Delsarte, J. M. Goethals, and J. J. Seidel, *Bounds for systems of lines, and Jacobi polynomials*, Philips Res. Rep., 30 (1975), pp. 91–105.

[19] U. Fano, *Description of states in quantum mechanics by density matrix and operator techniques*, Rev. Modern Phys., 29 (1957), pp. 74–93.

[20] S. T. Flammia, *On SIC-POVMs in prime dimensions*, J. Phys. A, 39 (2006), pp. 13483–13493.

[21] D. S. Freed, *On Wigner's Theorem*, https://arxiv.org/abs/1112.2133, 2012.
[22] C. A. Fuchs, M. C. Hoang, and B. C. Stacey, *The SIC question: History and state of play*, Axioms, 6 (2017), 21.
[23] M. Grassl, *Computing equiangular lines in complex space*, in Mathematical Methods in Computer Science, Lecture Notes in Comput. Sci. 5393, Springer, Berlin, 2008, pp. 89–104.
[24] C. J. Hillar and D. L. Rhea, *Automorphisms of finite abelian groups*, Amer. Math. Monthly, 114 (2007), pp. 917–923.
[25] S. G. Hoggar, 64 *lines from a quaternionic polytope*, Geom. Dedicata, 69 (1998), pp. 287–289.
[26] A. S. Holevo, *Probabilistic and Statistical Aspects of Quantum Theory*, North-Holland, Amsterdam, 1982.
[27] G. Horrocks and D. Mumford, *A rank* 2 *vector bundle on* P^4 *with* 15000 *symmetries*, Topology, 12 (1973), pp. 63–81.
[28] L. P. Hughston, $d = 3$ *SIC-POVMs and elliptic curves*, in Proceedings of the Perimeter Institute seminar, 2007, available at http://pirsa.org/07100040.
[29] L. P. Hughston and S. Salamon, *Surveying points in the complex projective plane*, Adv. Math., 286 (2016), pp. 1017–1052.
[30] K. Hulek, *Projective geometry of elliptic curves*, Astérisque, 137 (1986).
[31] M. Khatirinejad, *On Weyl-Heisenberg orbits of equiangular lines*, J. Algebr. Comb., 28 (2008), pp. 333–349.
[32] F. C. Kirwan, *Cohomology of Quotients in Symplectic and Algebraic Geometry*, Math. Notes 31, Princeton University Press, 1984.
[33] G. S. Kopp, *SIC-POVMs and the Stark conjecture*, Int. Math. Res. Not. IMRN, 2019, doi:10.1093/imrn/rnz153.
[34] P. W. H. Lemmens and J. J. Seidel, *Equiangular lines*, J. Algebra, 24 (1973), pp. 494–512.
[35] N. Lora Lamia, *Kähler, complex, Hermitian Geometry: Fubini Distance in* $\mathbb{CP}^{n-1}$ *with Computations in Dimension* 2, MSc thesis, University of Turin, Italy, 2014.
[36] A. Ranum, *The group of classes of congruent quadratic integers with respect to a composite ideal modulus*, Trans. Amer. Math. Soc., 11 (1910), pp. 172–198.
[37] J. M. Renes, R. Blume-Kohout, A. J. Scott, and C. M. Caves, *Symmetric informationally complete quantum measurements*, J. Math. Phys., 45 (2004), pp. 2171–2180.
[38] J. Schwinger, *Unitary operator bases*, Proc. Nat. Acad. Sci. USA, 46 (1960), pp. 570–579.
[39] A. J. Scott and M. Grassl, *SIC-POVMs: A new computer study*, J. Math. Phys., 51 (2010), 042203.
[40] J.-P. Serre, *Représentations linéaires et espaces homogènes kählériens des groupes de Lie compacts (d'après Armand Borel et André Weil)*, Séminaire Bourbaki 2, 100 (1954), pp. 447–454.
[41] C. E. Shannon, *A mathematical theory of communication*, Bell Syst. Tech. J., 27 (1948), pp. 379–423.
[42] F. Szöllősi, *All Complex Equiangular Tight Frames in Dimension* 3, https://arxiv.org/abs/1402.6429, 2014.
[43] G. Zauner, *Quantum designs: Foundations of a non-commutative design theory*, Int. J. Quantum Inf., 9 (2011), pp. 445–507.
[44] H. Zhu, *SIC POVMs and Clifford groups in prime dimensions*, J. Phys. A, 43 (2010), 305305.