

SIC-POVMS AND THE STARK CONJECTURES

GENE S. KOPP

ABSTRACT. The existence of a set of d^2 pairwise equiangular complex lines (a SIC-POVM) in d -dimensional Hilbert space is currently known only for a finite set of dimensions d . We prove that, if there exists a set of real units in a certain ray class field (depending on d) satisfying certain congruence conditions and algebraic properties, a SIC-POVM may be constructed when d is an odd prime congruent to 2 modulo 3. We give an explicit analytic formula that we expect to yield such a set of units. Our construction uses values of derivatives of zeta functions at $s = 0$ and is closely connected to the Stark conjectures over real quadratic fields.

We verify numerically that our construction yields SIC-POVMs in dimensions 5, 11, 17, and 23, and we give the first exact solution to the SIC-POVM problem in dimension 23.

1. INTRODUCTION

A set of m complex equiangular lines in d dimensions is a set of one-dimensional subspaces $\mathbb{C}v_1, \mathbb{C}v_2, \dots, \mathbb{C}v_m$ in \mathbb{C}^d having equal angles $\arccos\left(\frac{|\langle v_i, v_j \rangle|}{\|v_i\| \cdot \|v_j\|}\right) = \theta$ for all $i \neq j$. These configurations were first studied in the context of design theory in the 1970s. The maximal cardinality of a set of complex equiangular lines was shown to be bounded above by d^2 by Delsarte, Goethals, and Seidel [9].

A set of complex equiangular lines achieving this upper bound— d^2 lines in dimension d —is equivalent to a set of quantum measurements known as a SIC-POVM (symmetric informationally complete positive operator-valued measure). SIC-POVMs were introduced in 1999 by Zauner [30, 31] and have applications to quantum information processing (e.g., [29, 8]). Their existence has implications for quantum foundations due to their presence in the theory of quantum Bayesianism [11].

SIC-POVMs are conjectured to exist in all dimensions. They have been proven to exist (by explicit construction) in dimensions 1–21, 24, 28, 30, 31, 35, 37, 39, 43, 48, 124, and 323 [30, 12, 1, 13, 14, 20, 3, 2, 4, 21], and approximate numerical solutions have been found in every dimension up to 151 and several other dimensions up to 1155 [18, 20, 19, 10, 21]. All but one (the Hoggar lines [15]) of the known SIC-POVMs are (up to unitary symmetry) so-called Heisenberg SIC-POVMs—the orbit of a single vector under the action of a discrete Heisenberg group.

Appleby, Flammia, McConnell, and Yard [5, 6] recently discovered an empirical connection between SIC-POVMs and Hilbert’s 12th problem for real quadratic fields. Hilbert’s 12th problem is a

Date: July 26, 2018.

2010 Mathematics Subject Classification. 11R37, 11R42, 81P15, 81R05.

Key words and phrases. SIC-POVM, complex equiangular lines, quantum measurement, Stark conjectures, zeta function, Hecke L-function, class field theory, real quadratic field, Hilbert’s 12th problem, Heisenberg group, Clifford group.

This work was partially supported by NSF grant DMS-1401224, NSF grant DMS-1701576, and NSF RTG grant 0943832.

longstanding open problem in number theory. For a base field K , it asks for an explicit construction of the abelian extensions of K , analogous to the Kronecker-Weber theorem in the case when $K = \mathbb{Q}$ and the theory of complex multiplication in the case when K is imaginary quadratic.

Appleby et. al. [5, 6] observe that, for $d > 3$, the known examples of Heisenberg SIC-POVMs are always defined over abelian extensions of the real quadratic field $\mathbb{Q}(\sqrt{(d+1)(d-3)})$. They predict the existence of a certain Galois orbit of SIC-POVMs called a *minimal multiplet*, and they conjecturally identify the specific ray class field over which the SIC-POVMs in the minimal multiplet should be defined.

This paper formulates a conjectural construction of a Heisenberg SIC-POVM in infinitely many dimensions $d = 5, 11, 17, 23, 29, 41, \dots$, which are those d that are odd prime numbers congruent to 2 modulo 3. We split our construction into two pieces. The first is Conjecture 5.1, which predicts the existence of a Galois orbit of real algebraic units in a certain class field over $\mathbb{Q}(\sqrt{(d+1)(d-3)})$ satisfying several strong conditions. We prove in Theorem 5.4 that such a set of units (if it exists) may be used to construct a SIC-POVM in dimension d . The second piece of the construction is Conjecture 5.2, which gives an analytic formula for a set of real numbers that we expect to be algebraic units satisfying the conditions of Conjecture 5.1.

Of crucial importance to our construction in Conjecture 5.2 are the conjectures of Stark on the leading terms of the Taylor expansions of Hecke and Artin L -functions at $s = 1$ and $s = 0$ [24, 25, 26, 27, 28]. Stark made his conjectures in the 1970s, and they remain open over every base field except for \mathbb{Q} (known to Dirichlet) and imaginary quadratic fields (proof due to Stark [24]). Much work has been done toward attacking or refining the Stark conjecture; one vital reference is the proceeding of the 2002 “International Conference on Stark’s Conjectures and Related Topics” at Johns Hopkins University [7].

Specifically, we use the rank 1 abelian Stark conjecture in the real quadratic case [26, 27]. A key observation made in this paper is that the overlap phases of certain SIC-POVMs are Galois conjugate to square roots of Stark units—units in ray class fields predicted by Stark to coincide with $\exp(Z'_A(0))$ for a certain differenced ray class zeta function $Z_A(s)$. A congruence condition modulo a prime lying over (d) determines the signs of the square roots; see eq. (5.2).

Our construction has been verified numerically in dimensions $d = 5, 11, 17$, and 23. Moreover, our methods give *exact* solutions in these dimensions. Namely, we can conjecturally determine Stark units as algebraic numbers using sufficiently high-precision approximate values of $\exp(Z'_A(0))$, and then verify directly that they produce a SIC-POVM according to the recipe provided by our conjectures. Thus, we provide the first exact expression for a SIC-POVM in dimension 23.

The paper is organized as follows. In section 3 and section 4, we provide mathematical background and an introduction to SIC-POVMs and the Stark conjectures, and we define the notation to be used in the rest of the paper. In section 5, we present our main results and conjectures. Finally, in section 6, we present data verifying our main conjecture numerically in dimensions $d = 5, 11, 17$, and 23.

This paper includes and extends work from Chapter 5 of the author’s PhD thesis [16].

2. ACKNOWLEDGMENTS

Thank you to Jeff Lagarias for many inspiring conversations about the SIC-POVM problem, Hilbert’s 12th problem, and the Stark conjectures, and for helpful comments on drafts of this paper, especially regarding the formulation of the conjectures.

I thank Gary McConnell, Neil Gillespie, and Harold Stark for fruitful discussions.

3. COMPLEX EQUIANGULAR LINES

In this section, we introduce the definitions from quantum information theory and design theory that we need to state our main conjectures. Specifically, we define SIC-POVMs and Heisenberg SIC-POVMs. We discuss extended unitary equivalence and Galois equivalence of SIC-POVMs and define the notion of a multiplet of Heisenberg SIC-POVMs.

3.1. Definition of SIC-POVMs. The study of SIC-POVMs began with Zauner’s 1999 PhD thesis [30] (see English translation [31]). The term “SIC-POVM” was attached to the concept in 2004 by Renes, Blume-Kohout, Scott, and Caves [18].

The maximal number of equiangular complex lines possible in \mathbb{C}^d is d^2 ; this was originally proved in 1975 by Delsarte, Goethals, and Seidel using orthogonal polynomials [9].

Proposition 3.1 (Delsarte, and Goethals, and Seidel [9]). *Let $\alpha > 0$. Consider a set V of unit vectors in \mathbb{C}^d spanning equiangular lines; that is, $|\langle v, w \rangle|^2 = \alpha$ whenever $v, w \in V$ and $v \neq w$. Then, $|V| \leq d^2$.*

The same authors also show that, for a set of d^2 equiangular complex lines, the size of the angle is determined.

Proposition 3.2 (Delsarte, and Goethals, and Seidel [9]). *For any set V of unit vectors in \mathbb{C}^d spanning d^2 equiangular lines with $|\langle v, w \rangle|^2 = \alpha$ whenever $v, w \in V$ and $v \neq w$,*

$$\alpha = \frac{1}{d+1}, \quad (3.1)$$

and thus the common angle is $\arccos\left(\frac{1}{\sqrt{d+1}}\right)$.

A SIC-POVM is defined as a set of measurements (i.e., projectors—idempotent Hermitian operators) on d -dimensional Hilbert space satisfying certain properties, and it is equivalent to a set of equiangular complex lines achieving the upper bound from Proposition 3.1.

Definition 3.3 (SIC-POVM). *A symmetric informationally complete positive operator-valued measure (SIC-POVM) is a set $\{\Pi_1, \Pi_2, \dots, \Pi_{d^2}\}$ of cardinality d^2 consisting of rank 1 Hermitian $d \times d$ matrices Π_i such that each $\Pi_i^2 = \Pi_i$, and*

$$\mathrm{Tr}(\Pi_i \Pi_j) = \begin{cases} 1 & \text{if } i = j, \\ \frac{1}{d+1} & \text{if } i \neq j. \end{cases} \quad (3.2)$$

Write $\Pi_i = v_i v_i^\dagger$, where v_i is a column vector, and v_i^\dagger is its conjugate-transpose, a row vector. Then, the v_i define a set of d^2 equiangular complex lines in \mathbb{C}^d , and conversely any set of d^2 equiangular complex lines in \mathbb{C}^d define a SIC-POVM. We will use the term “SIC-POVM” interchangeably with “set of d^2 equiangular complex lines in \mathbb{C}^d .”

There are two types of operators on \mathbb{C}^d preserving the SIC-POVM property. A SIC-POVM $\{\mathbb{C}v_1, \dots, \mathbb{C}v_{d^2}\}$ may be “rotated” by any unitary matrix $U \in \mathrm{U}(d) = \{U \in \mathrm{GL}(\mathbb{C}^d) : UU^\dagger = 1\}$ to obtain another SIC-POVM $\{\mathbb{C}Uv_1, \dots, \mathbb{C}Uv_{d^2}\}$. Moreover, if C_d is the complex conjugation operator on \mathbb{C}^d , so that $C_d v := \bar{v}$, then C_d also preserves the SIC-POVM property (and the same holds for any “antiunitary” operator of the form $C_d U$). These operators may be collected together to form the extended unitary group.

Definition 3.4. Define the *extended unitary group* $\text{EU}(d) := \text{U}(d) \sqcup C_d \text{U}(d)$.

Lemma 3.5. The action of $\text{EU}(d)$ takes SIC-POVMs to SIC-POVMs.

Proof. The action of $\text{U}(d)$ preserves the Hermitian inner product; $C_d \text{U}(d)$ conjugates the Hermitian inner product. Thus, both preserve its absolute value and thus the SIC-POVM property. \square

Definition 3.6 (Overlaps). If v_1, v_2, \dots, v_{d^2} are unit vectors in \mathbb{C}^d defining a SIC-POVM, the **overlaps** are the d^4 complex numbers $\langle v_i, v_j \rangle$. The **overlap phases**, for $i \neq j$, are the complex numbers $\sqrt{d+1} \langle v_i, v_j \rangle$, which lie on the unit circle.

3.2. Definition of Heisenberg SIC-POVMs. Heisenberg SIC-POVMs are a special class of SIC-POVMs. Let $\zeta_d = e\left(\frac{1}{d}\right) = \exp\left(\frac{2\pi i}{d}\right)$ be a d th root of unity.

Definition 3.7 (Heisenberg group). Let $d' = d$ if d is odd, $d' = 2d$ if d is even. Let I be the $d \times d$ identity matrix. The Heisenberg group $\text{H}(d)$ is the finite group of order $d'd^2$ generated by the $d \times d$ scalar matrix $\zeta_{d'} I$ and the $d \times d$ matrices

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_d & 0 & \cdots & 0 \\ 0 & 0 & \zeta_d^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_d^{d-1} \end{pmatrix}. \quad (3.3)$$

The Heisenberg group $\text{H}(d)$ spans the vector space $\text{M}_d(\mathbb{C})$ of $d \times d$ complex matrices, and a canonical basis is given as follows.

Definition 3.8 (Heisenberg basis). Let $\tau_d = \exp\left(\frac{(d+1)\pi i}{d}\right) = -\exp\left(\frac{\pi i}{d}\right)$. The set of d^2 matrices

$$D_{m,n} = \tau_d^{mn} X^m Z^n \text{ for } 0 \leq m, n \leq d-1 \quad (3.4)$$

forms a basis of $\text{M}_d(\mathbb{C})$ over \mathbb{C} , and this basis is called the **Heisenberg basis**.

Empirically, all but one of the known SIC-POVMs are equivalent to orbits of the Heisenberg group action, and this observation motivates the following definition.

Definition 3.9 (Heisenberg SIC-POVM). A **Heisenberg SIC-POVM** is a SIC-POVM of the form $\{CD_{m,n}v : 0 \leq m, n \leq d-1\}$ for some vector $v \in \mathbb{C}^d$. This v is called a **fiducial vector**.

The elements of $\text{EU}(d)$ that preserve the property of being a Heisenberg SIC-POVM are restricted to a finite group, the **extended Clifford group** $\text{EC}(d)$, defined to be the normalizer of $\text{H}(d)$ inside $\text{EU}(d)$.

Lemma 3.10. If v is a fiducial vector for a Heisenberg SIC-POVM, and $\gamma \in \text{EC}(d)$, then γv is also a fiducial vector for a Heisenberg SIC-POVM. Conversely, if v and w are $\text{EU}(d)$ -equivalent fiducial vectors, they are in fact $\text{EC}(d)$ -equivalent.

Proof. See Scott and Grassl [20], section 3. \square

Some authors consider the larger class of **group covariant SIC-POVMs**, those which are orbits of some subgroup of $\text{U}(d)$. The Hoggar lines are group covariant for $\text{H}(2) \otimes \text{H}(2) \otimes \text{H}(2)$, so all known SIC-POVMs are group covariant. In the case of prime dimension, it was shown by Zhu that all group covariant SIC-POVMs are equivalent to Heisenberg SIC-POVMs [32].

3.3. The Galois action of Heisenberg SICs. In 2016, Appleby, Flammia, McConnell, and Yard [5, 6] numerically discovered a surprising connection between SIC-POVMs and ray class fields of real quadratic fields. For all Heisenberg SIC-POVMs they were able to check, they found that the ratios of the entries of the fiducial vector lie in an abelian extension of the real quadratic field $\mathbb{Q}(\sqrt{\Delta})$, where $\Delta = \Delta_d = (d+1)(d-3)$. This field is special because it contains a small unit

$$\varepsilon = \varepsilon_d = \frac{(d-1) + \sqrt{\Delta}}{2}. \quad (3.5)$$

The unit ε has the property that $\varepsilon^3 \equiv 1 \pmod{d}$, and its presence is related to the order 3 ‘‘Zauner symmetry’’ enjoyed by many known SIC-POVMs. We call ε the **Zauner unit**. Note that the Zauner unit is not always equal to the fundamental unit, but is sometimes a higher power of it; for example, $\varepsilon_{15} = (2 + \sqrt{3})^2$.

Let $K = \mathbb{Q}(\sqrt{\Delta})$, and let E be the field generated by the ratios of the entries of the fiducial vector along with the d' th roots of unity, where $d' = d$ if d is odd, and $d' = 2d$ if d is even. If v is a Heisenberg fiducial vector and $\sigma \in \text{Gal}(E/K)$, then v^σ is also a Heisenberg fiducial vector; v^σ may or may not lie in the same $\text{EC}(d)$ orbit as v . This Galois action respects orbits because $(\gamma v)^\sigma = \gamma^\sigma v^\sigma$ and $\text{EC}(d)$ is Galois-closed.

Definition 3.11 (Multiplet). *The set of all those $\text{EC}(d)$ -orbits of fiducial vectors, which are Galois equivalent to a given $\text{EC}(d)$ -orbit, is called a **multiplet**.*

4. EXPLICIT CLASS FIELD THEORY AND ZETA FUNCTIONS

In this section, we give the number-theoretic background we need to state our conjectures. A much more complete exposition of class field theory may be found in Neukirch’s book [17]. The real quadratic Stark conjectures may be found in [26].

4.1. Global class field theory. Let K be a number field, and let \mathcal{O}_K be its ring of algebraic integers, the maximal order of K .

A modulus \mathfrak{m} is a pair $\mathfrak{m} = (\mathfrak{c}, S)$, where \mathfrak{c} is an ideal of \mathcal{O}_K , and S is a subset of the (possibly empty) set of real embeddings $K \rightarrow \mathbb{R}$. Associate to the real embeddings ρ_1, \dots, ρ_r the ‘‘infinite primes’’ $\infty_1, \dots, \infty_r$, and write \mathfrak{m} using the notation $\mathfrak{m} = \mathfrak{c} \prod_{\rho_j \in S} \infty_j$. (An example of this notation is $\mathfrak{m} = (7)\infty_1\infty_3$).

Definition 4.1. *If $\mathfrak{m} = (\mathfrak{c}, S)$, define the **ray class group modulo \mathfrak{m}** to be*

$$\text{Cl}_{\mathfrak{m}} = \frac{\{\text{fractional ideals coprime to } \mathfrak{c}\}}{\{\text{principal frac. ideals } (\alpha) \text{ coprime to } \mathfrak{c} \text{ with } \alpha \equiv 1 \pmod{\mathfrak{c}} \text{ and } \rho(a) > 0 \text{ for all } \rho \in S\}}. \quad (4.1)$$

If \mathfrak{c}' is any nonzero subideal of \mathfrak{c} , then the ray class group is unaffected by imposing the stronger condition of coprimality to \mathfrak{c}' .

$$\text{Cl}_{\mathfrak{m}} \cong \frac{\{\text{fractional ideals coprime to } \mathfrak{c}'\}}{\{\text{principal frac. ideals } (\alpha) \text{ coprime to } \mathfrak{c}' \text{ with } \alpha \equiv 1 \pmod{\mathfrak{c}} \text{ and } \rho(a) > 0 \text{ for all } \rho \in S\}}. \quad (4.2)$$

Consider two moduli $\mathfrak{m} = (\mathfrak{c}, S)$ and $\mathfrak{m}' = (\mathfrak{c}', S')$. We say that $\mathfrak{m}|\mathfrak{m}'$ if $\mathfrak{c} \supset \mathfrak{c}'$ and $S \subset S'$. The quotient maps $\pi_{\mathfrak{m}', \mathfrak{m}} : \text{Cl}_{\mathfrak{m}'} \rightarrow \text{Cl}_{\mathfrak{m}}$ are defined by first imposing coprimality to \mathfrak{c}' in $\text{Cl}_{\mathfrak{m}}$, then modding out by the stronger congruence and positivity conditions modulo \mathfrak{m}' .

The abelian Galois extensions of K are associated to quotients of ray class groups, by the following existence theorem of Takagi.

Theorem 4.2 (Existence theorem). *Let K be a number field, and let K^{ab} be the maximal abelian extension of K (an infinite-degree extension). Then, there is a natural isomorphism of the Galois group $\text{Gal}(K^{\text{ab}}/K)$ with the inverse limit $\varprojlim \text{Cl}_{\mathfrak{m}}$ with respect to the quotient maps $\pi_{\mathfrak{m}', \mathfrak{m}}$. This isomorphism is called the **Artin map**:*

$$\text{Art} : \varprojlim \text{Cl}_{\mathfrak{m}} \rightarrow \text{Gal}(K^{\text{ab}}/K). \quad (4.3)$$

The field $L_{\mathfrak{m}}/K$ corresponding to $\text{Cl}_{\mathfrak{m}}$ by Galois theory—so that $\text{Gal}(L_{\mathfrak{m}}/K) \cong \text{Cl}_{\mathfrak{m}}$ under the Artin map—is called the **ray class field** of K modulo \mathfrak{m} . If $\mathfrak{m} = (\mathfrak{c}, S)$, then the extension $L_{\mathfrak{m}}$ is ramified only at the primes dividing \mathfrak{c} and the real places in S .

Proof. See [17], Chapter VI, especially Theorem 7.1. \square

4.2. Ray class zeta functions and Hecke L -functions. We now define two Dirichlet series, $\zeta_A(s)$ and $Z_A(s)$, attached to a ray ideal class A of the ring of integers of a number field.

Definition 4.3 (Ray class zeta function). *Let K be any number field, and let \mathfrak{c} be an ideal of the maximal order \mathcal{O}_K . Let S be a subset of the real places of K (i.e., the embeddings $K \hookrightarrow \mathbb{R}$). Let A be a ray ideal class modulo $\mathfrak{m} = (\mathfrak{c}, S)$. Define the **zeta function of the ray class A** to be*

$$\zeta(s, A) = \sum_{\mathfrak{a} \in A} N(\mathfrak{a})^{-s} \text{ for } \text{Re}(s) > 1. \quad (4.4)$$

This function may be meromorphically continued to the whole complex plane.

Theorem 4.4. *This function $\zeta(s, A)$ has a meromorphic continuation to \mathbb{C} . It has a simple pole at $s = 1$ with residue independent of A , and no other poles.*

Proof. See Neukirch [17], Chapter VII, Theorem 8.5 for the corresponding statement about Hecke L -functions, from which this theorem follows. \square

The pole at $s = 1$ may be eliminated by considering the function $Z_A(s)$, defined as follows. The function $Z_A(s)$ is holomorphic everywhere.

Definition 4.5 (Differenced ray class zeta function). *Let R be the element of $C_{\mathfrak{m}}$ defined by*

$$R = \{a\mathcal{O}_K : a \equiv -1 \pmod{\mathfrak{c}} \text{ and } a \text{ is positive at each place in } S\}. \quad (4.5)$$

*Define the **differenced zeta function of the ray class A** to be*

$$Z_A(s) = \zeta(s, A) - \zeta(s, RA). \quad (4.6)$$

Hecke L -functions (of a finite-order Hecke character) are linear combinations of ray class zeta functions and are ubiquitous in modern number theory, largely because they have an Euler product. Conversely, ray class zeta functions may be expressed as linear combinations of Hecke L -functions.

Definition 4.6 (L -function of a finite-order Hecke character). *Let K be a number field and \mathfrak{m} a modulus of K . Let $\chi : \text{Cl}_{\mathfrak{m}} \rightarrow \mathbb{C}^{\times}$ be a group homomorphism. The Hecke L -function is*

$$L(s, \chi) = \sum_{A \in \text{Cl}_{\mathfrak{m}}} \chi(A) \zeta(s, A). \quad (4.7)$$

All our results and conjectures are stated using (differenced) ray class zeta functions rather than Hecke L -functions, as they are cleaner that way. However, our computer calculations (see section 6) rely on Magma's built-in algorithms for computing Hecke L -functions.

4.3. Stark conjectures over real quadratic fields. The Existence Theorem 4.2 does not provide a procedure for actually building the ray class field L_m . Explicit constructions are known when the base field K is \mathbb{Q} or an imaginary quadratic field; however, it is not known how to construct ray class fields explicitly in general.

The Stark conjectures provide one approach to developing an explicit class field theory. The following conjecture, due to Stark [26], gives a conjectural generator for a ray class field over a real quadratic field, under certain conditions.

Conjecture 4.7 (Stark conjecture, rank 1 real quadratic case). *Let K be a real quadratic number field with real embeddings ρ_1 and ρ_2 . Let \mathfrak{c} be a nonzero ideal of the ring of integers of K with the property that, if $\varepsilon \in \mathcal{O}_K^\times$ such that $\varepsilon \equiv 1 \pmod{\mathfrak{c}}$, then $\rho_1(\varepsilon) > 0$. Let A be a ray ideal class in $\text{Cl}_{\mathfrak{c}\infty_2}$. Let $L_{\mathfrak{c}\infty_j}$ be the ray class field of K modulo $\mathfrak{c}\infty_j$, and let $\tilde{\rho}_j$ be a choice of embedding of $L_{\mathfrak{c}\infty_j}$ extending ρ_j . (Here, $\tilde{\rho}_1(L_{\mathfrak{c}\infty_2}) = \tilde{\rho}_2(L_{\mathfrak{c}\infty_1})$ is a real field, and $\tilde{\rho}_1(L_{\mathfrak{c}\infty_1}) = \tilde{\rho}_2(L_{\mathfrak{c}\infty_2})$ is a complex [non-real] field.) Then,*

- (1) $Z'_A(0) = \log(\tilde{\rho}_1(\alpha_A))$ for some real algebraic unit $\alpha_A \in L_{\mathfrak{c}\infty_2}$, and furthermore $L_{\mathfrak{c}\infty_2} = K(\alpha_A)$.
- (2) The units α_A are compatible with the Artin map $\text{Art} : \text{Cl}_{\mathfrak{c}\infty_2} \rightarrow \text{Gal}(L_{\mathfrak{c}\infty_2}/K)$. Specifically, $\alpha_A = \alpha_I^{\text{Art}(A)}$, where $I \in \text{Cl}_{\mathfrak{c}\infty_2}$ is the identity class.

5. TOWARDS AN INFINITE FAMILY OF HEISENBERG SIC-POVMS

We now state our main conjectures and results. Our first conjecture predicts the existence of a Galois orbit of real algebraic units in the ray class field $L_{(d)\infty_2}$ satisfying certain strong conditions, for d an odd prime such that $d \equiv 2 \pmod{3}$. We will show in Theorem 5.4 that these conditions imply the existence of a Heisenberg SIC-POVM in dimension d .

Conjecture 5.1. *Let d be an odd prime such that $d \equiv 2 \pmod{3}$. Let $\Delta = (d+1)(d-3)$ and $K = \mathbb{Q}(\sqrt{\Delta})$, and consider the class group $\text{Cl}_{(d)\infty_2}$. With indices $m, n \in \mathbb{Z}/d\mathbb{Z}$, let*

$$A_{m,n} = \{\alpha \mathcal{O}_K : \alpha \equiv m + n\sqrt{\Delta} \pmod{d} \text{ and } \rho_2(\alpha) > 0\} \in \text{Cl}_{(d)\infty_2}, \quad (5.1)$$

and let $\text{Art} : \text{Cl}_{(d)\infty_2} \rightarrow \text{Gal}(L_{(d)\infty_2}/K)$ denote the Artin map of class field theory. Then, there is a real algebraic unit α such that the ray class field $L_{(d)\infty_2} = K(\alpha)$ and such that its (real) Galois conjugates $\alpha_{m,n} := \alpha^{\text{Art}(A_{m,n})}$ over the Hilbert class field $L_{(1)}$ have the following properties.

- (1) $\alpha_{-m,-n} = \alpha_{m,n}^{-1}$.
- (2) The $\alpha_{m,n} \equiv 1 \pmod{\mathfrak{p}}$ for all prime ideals \mathfrak{p} of $\mathcal{O}_{L_{(d)\infty_2}}$ dividing $d\mathcal{O}_{L_{(d)\infty_2}}$.
- (3) The roots of $(d+1)x^2 = \alpha_{m,n}$ are in $L_{(d)\infty_2}$.
- (4) Fix a choice of \mathfrak{p} dividing $d\mathcal{O}_{L_{(d)\infty_2}}$, and let $\nu_{m,n}$ be the unique root of

$$(d+1)x^2 = \alpha_{m,n} \quad (5.2)$$

satisfying $\nu_{m,n} \equiv 1 \pmod{\mathfrak{p}}$. Let $\nu_{0,0} = 1$. Then, the matrix

$$M = \frac{1}{d} \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} \nu_{m,n} D_{-m,-n} \quad (5.3)$$

is idempotent (that is, $M^2 = M$) and rank 1 (that is, all the rank 2 minors of M vanish). (See eq. (3.4) for the definition of $D_{m,n}$.)

Our second conjecture provides an explicit analytic formula for a set of real numbers that we expect to be Galois conjugate algebraic units with the desired properties. (The $Z'_A(0)$ are known to be real numbers.)

Conjecture 5.2. *A unit α satisfying Conjecture 5.1 and its Galois conjugates over K may be constructed as Stark units*

$$\alpha^{\text{Art}(A)} = \exp(Z'_A(0)), \quad (5.4)$$

for all $A \in \text{Cl}_{(d)\infty_2}$.

Conjecture 4.7, due to Stark, predicts that $\exp(Z'_A(0)) = \alpha^{\text{Art}(A)}$ for an algebraic unit α generating $L_{(d)\infty_2}$ over K . Point (1) of Conjecture 5.1 follows, because $Z_{RA}(s) = -Z_A(s)$. Points (2), (3), and (4) of Conjecture 5.1 provide, to our knowledge, new predictions about Stark units.

There are several analytic formulas for the derivative zeta values $Z'_A(0)$ appearing on the right-hand side of eq. (5.4). Shintani's Kronecker limit formula expresses $\exp(Z'_A(0))$ as a product of special values of Barnes's double gamma function [22, 23]. A different formula appears in Chapter 4 of the author's PhD thesis [16].

We state Conjecture 5.1 and Conjecture 5.2 as two separate conjectures due to the possibility that it may be possible to prove the first without proving the second. One route by which this might be done is through the use of p -adic zeta functions rather than Archimedean zeta functions. The p -adic approach seems hopeful because p -adic analogues of the Stark conjectures have been proven in some cases. At least, the \mathfrak{p} -adic condition (2) for corresponding d -adic special values looks potentially amenable to proof.

We now prove a lemma about the structure of the class fields over K , which we require for our main result, Theorem 5.4.

Lemma 5.3. *Let $K = \mathbb{Q}(\sqrt{\Delta})$, where $\Delta = (d+1)(d-3)$ and $d \geq 4$. Let $\varepsilon_d = \frac{(d-1)+\sqrt{\Delta}}{2}$. If $\eta \in \mathcal{O}_K^\times$ and $\eta \equiv 1 \pmod{d}$, then $\eta = \varepsilon_d^{3k}$ for some $k \in \mathbb{Z}$, and in particular ε_d is totally positive. It follows that the class fields $L_{(d)}$, $L_{(d)\infty_1}$, $L_{(d)\infty_2}$, and $L_{(d)\infty_1\infty_2}$ are all distinct.*

Proof. It suffices to prove that the minimal $\eta > 1$ in \mathcal{O}_K such that $\eta \equiv 1 \pmod{d}$ is ε^3 ; consider the minimal such η . We have $\eta^n = \varepsilon_d^3$ for some $n \in \mathbb{Z}$, $n > 0$.

Let η' and ε' denote the nontrivial Galois conjugates of η and ε , respectively. If $n \geq 3$, then $\eta + \eta' \leq \varepsilon + \varepsilon' = d - 1$, so it's impossible to have $\eta \equiv 1 \pmod{d}$.

Thus, $n \leq 2$. Suppose $n = 2$. Then ε_d has a square root in K ; it's straightforward to check that this happens exactly when $d+1$ is a square, in which case $\varepsilon_d = \varepsilon_{d_0}^2$ with $d = d_0^2 - 2d_0$. Then

$$\eta = \varepsilon_d^3 \quad (5.5)$$

$$= \frac{(d_0 - 1)(d - 2) + d\sqrt{\Delta}}{2} \quad (5.6)$$

$$\equiv -d_0 \pmod{d}. \quad (5.7)$$

Thus, $\eta \not\equiv 1 \pmod{d}$.

So we must have $n = 1$, which is what we wanted to prove.

It follows that the class groups $\text{Cl}_{(d)}$, $\text{Cl}_{(d)\infty_1}$, $\text{Cl}_{(d)\infty_2}$, and $\text{Cl}_{(d)\infty_1\infty_2}$ are all distinct. Thus, by Theorem 4.2, the class fields $L_{(d)}$, $L_{(d)\infty_1}$, $L_{(d)\infty_2}$, and $L_{(d)\infty_1\infty_2}$ are all distinct. \square

We are now ready to prove that Conjecture 5.1 implies the existence of a Heisenberg SIC-POVM.

Theorem 5.4. *Let d be an odd prime such that $d \equiv 2 \pmod{3}$. Assume Conjecture 5.1, and let M be the matrix constructed therein. Let $\sigma \in \text{Gal}(L_{(d)\infty_2}/\mathbb{Q})$ be any Galois automorphism not fixing K ; that is, $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$. Then $\sigma(M) = vv^\dagger$ for a fiducial vector v of a Heisenberg SIC-POVM.*

Proof. The $\alpha_{m,n}$ are Galois conjugate real algebraic units that generate $L_{(d)\infty_2}$ over K . By Lemma 5.3, $L_{(d)} \neq L_{(d)\infty_2}$. The $\alpha_{m,n}$ must not be totally real, because if they were, they would all lie in $L_{(d)}$. Moreover, by (1), $\alpha_{-m,-n} = \alpha_{m,n}^{-1}$, so the $\alpha_{m,n}$ are Galois conjugate to their inverses. Take $\tau \in \text{Gal}(L_{(d)\infty_2}/K)$ such that $\tau(\alpha) = \alpha^{-1}$. Then, $\tau(\alpha_{m,n}) = \alpha_{m,n}^{-1}$ because $\text{Gal}(L_{(d)\infty_2}/K)$ is abelian. Thus,

$$(\sigma\tau\sigma^{-1})(\sigma(\alpha_{m,n})) = \sigma(\alpha_{m,n})^{-1}. \quad (5.8)$$

We have $\tau = \text{Art}_R$, where

$$R = \{\beta \mathcal{O}_K : \beta \equiv 1 \pmod{d} \text{ and } \rho_2(\beta) > 0\} \in \text{Cl}_{(d)\infty_2}. \quad (5.9)$$

Thus, by class field theory, the fixed field of τ is $L_{(d)}$. It follows that the class field of $\sigma\tau\sigma^{-1} \in \text{Gal}(L_{(d)\infty_1}/K)$ is also $L_{(d)}$. Thus, $\sigma\tau\sigma^{-1}$ must act by complex conjugation, because $L_{(d)}$ is the real subfield of the complex field $L_{(d)\infty_1}$.

Thus, $\sigma(\alpha_{m,n})$ lies on the unit circle. It follows that $|\sigma(\nu_{m,n})| = \frac{1}{\sqrt{d+1}}$. From the definition of M , we obtain $\text{Tr}(MD_{m,n}) = \nu_{m,n}$. Thus,

$$|\text{Tr}(\sigma(M)\sigma(D_{m,n}))|^2 = \text{Tr}(\sigma(M)\sigma(D_{m,n}))(\sigma\tau\sigma^{-1})(\text{Tr}(\sigma(M)\sigma(D_{m,n}))) \quad (5.10)$$

$$= \sigma(\text{Tr}(MD_{m,n})\tau(\text{Tr}(MD_{m,n}))) \quad (5.11)$$

$$= \sigma(\nu_{m,n}\nu_{-m,-n}) \quad (5.12)$$

$$= \frac{1}{d+1}. \quad (5.13)$$

Moreover, the action of σ on the Heisenberg group is determined by its action of $\mathbb{Q}(\zeta_d)$, and there is some $\lambda \in (\mathbb{Z}/d\mathbb{Z})^\times$ such that $\sigma(D_{m,n}) = \sigma(D_{m,\lambda n})$. So, by changing the value of n , we have

$$|\text{Tr}(\sigma(M)D_{m,n})|^2 = \frac{1}{d+1}, \quad (5.14)$$

for all $(m,n) \neq (0,0)$. Now write $\sigma(M) = vw^\dagger$ for some $v, w \in \mathbb{C}^d$ with $w^\dagger v = 1$, which is possible because M , and thus $\sigma(M)$, is rank 1 and idempotent. We will show that $\sigma(M)$ is in fact a Hermitian projector; that is, $w = v$. Conjugate-transpose acts on $\sigma(M)$ as follows:

$$\sigma(M)^\dagger = \sum_m \sum_n \overline{\sigma(\nu_{m,n})} D_{-m,-\lambda n}^\dagger = \sum_m \sum_n \sigma(\nu_{-m,-n}) D_{m,\lambda n}^\dagger = \sigma(M). \quad (5.15)$$

Thus, $w = v$. So eq. (5.14) may be rewritten as $\langle v, D_{m,n}v \rangle = \frac{1}{\sqrt{d+1}}$ for $(m,n) \neq (0,0)$; also, $\langle v, v \rangle = 1$. In other words, v is a fiducial vector for a Heisenberg SIC-POVM in \mathbb{C}^d . \square

Conjecture 5.1 has been verified numerically for $d = 5, 11, 17$, and 23 . We discuss each case in turn in section 6.

6. EXAMPLES

In this section, we use Conjecture 5.1 and Conjecture 5.2 to compute exact SIC-POVMs in dimensions $d = 5, 11, 17$, and 23 . In each case, our solutions represent the minimal multiplet (in the sense of Appleby et. al. [6]), or (in the case of $d = 23$) we expect them to. Originally, the case

$d = 5$ is due to Zauner [30, 31], $d = 11$ is due to Scott and Grassl [20], and $d = 17$ is due to Appleby et. al. [4]. The case $d = 23$ is new.

We numerically compute the numbers $\alpha_A^{\text{approx}} := \exp(Z'_A(0))$ for the ideal classes $A \in \text{Cl}_{(d)\infty_2}(K)$, using Magma's built-in functions for evaluation of Hecke L-functions. The α_A^{approx} are expected to be Galois conjugate algebraic numbers (see Conjecture 4.7); in each case, we find that they indeed agree to high precision with Galois conjugate algebraic numbers α_A^{exact} . The α_A^{exact} are found by using Mathematica's built-in lattice basis-reduction algorithms to compute the coefficients of a minimal polynomial $f_d(x)$ over $L_{(1)}$, the Hilbert class field of K .

Next, we verify conditions (2) and (3) of Conjecture 5.1 and compute the minimal polynomial $g_d(x)$ of a choice of ν_A . The latter is done by factoring $f_d((d+1)x^2)$ over $L_{(1)}$ in Magma. Finally, we verify that the ν_A satisfy condition (4) of Conjecture 5.1.

Let $\tilde{g}_d(x)$ denote a polynomial obtained from $g_d(x)$ by applying a Galois automorphism σ to the coefficients with the property that $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$. The roots $\nu_{m,n}$ of $g_d(x)$ are real numbers, and we have already computed them not only as a set, but also as an orbit of the Galois group $G = \text{Gal}(L_{(d)\infty_2}/L_{(1)})$. The roots of $\tilde{g}_d(x)$ are complex numbers of absolute value $\frac{1}{\sqrt{d+1}}$, and they are the overlaps of the SIC-POVM we are looking for. In order to compute a fiducial vector, we need to compute the Galois action on them as well.

In each case ($d = 5, 11, 17, 23$), the Galois group $G = \text{Gal}(L_{(d)\infty_2}/L_{(1)}) \cong (\mathcal{O}_K/d\mathcal{O}_K)^\times / \langle \varepsilon_d \rangle$ is a cyclic group of order $n = \frac{d-1}{3}$. Let γ be a generator for $(\mathcal{O}_K/d\mathcal{O}_K)^\times$, so $\tau = \text{Art}(A_\gamma)$ is a generator for G . Fix $\nu = \nu_{1,0}$. We compute $\tau(\nu)$ in the monomial basis $\{1, \nu, \dots, \nu^{n-1}\}$ for $L_{(d)\infty_2}$ over $L_{(1)}$:

$$\tau(\nu) = h_d(\nu) = \sum_{j=0}^{n-1} c_j \nu^j, \quad (6.1)$$

where $c_j \in L_{(1)}$. This is done by solving the following linear system for the c_j .

$$\begin{pmatrix} \tau(\nu) \\ \tau^2(\nu) \\ \vdots \\ \nu \end{pmatrix} = \begin{pmatrix} 1 & \nu & \dots & \nu^{n-1} \\ 1 & \tau(\nu) & \dots & \tau(\nu)^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \tau^{n-1}(\nu) & \dots & \tau^{n-1}(\nu)^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{pmatrix}. \quad (6.2)$$

The action on τ on the roots of $g_d(x)$ is given by applying the polynomial $h_d(x)$, so the action of a generator $\tilde{\tau}$ for $\text{Gal}(L_{(d)\infty_1}/L_{(1)})$ on the roots of $\tilde{g}_d(x)$ is given by applying

$$\tilde{h}_d(x) = \sum_{j=0}^{n-1} \tau(c_j) x^j. \quad (6.3)$$

From the roots $\tilde{\nu}_{m,n}$ of $\tilde{g}_d(x)$, a fiducial vector v_d is computed by applying σ to eq. (5.3):

$$v_d v_d^\dagger = \sigma(M) = \frac{1}{d} \sum_{m=0}^{d-1} \sum_{n=0}^{d-1} \tilde{\nu}_{m,n} D_{-m, -\lambda n}. \quad (6.4)$$

As we haven't kept track of the action of σ on roots of unity, we must check different values of $\lambda \in (\mathbb{Z}/d\mathbb{Z})^\times$ until we find one that works.

While this method produces an exact fiducial, we write down only a numerical fiducial in the examples that follow and in the accompanying text files. (We have already specified v_d exactly

up to a Galois action by writing down $g_d(x)$, and the minimal polynomials of its entries have prohibitively large coefficients in some cases.)

In the cases $d = 5, 11$, and 17 , the coefficients of $g_d(x)$ live in K , so $\tilde{g}_d(x)$ is determined by $g_d(x)$. In the case $d = 23$, the coefficients of $g_d(x)$ live in a degree 2 extension of K , so there are two choices for $\tilde{g}_d(x)$. The two choices lead to two different PEC(23)-orbits, 23e and 23f.

The ancillary text files accompanying this paper contain expressions for $f_d(x), g_d(x), h_d(x)$, and v_d ; in the case $d = 23$, expressions for related polynomials $g_d^*(x)$ and $h_d^*(x)$ are given instead, as explained in section 6.4. The ancillary files are `dim5.txt`, `dim11.txt`, `dim17.txt`, `dim13.txt`, and `hstar23.txt`.

6.1. The example $d = 5$. In dimension $d = 5$, the corresponding quadratic discriminant is $\Delta = (d+1)(d-3) = 12$. The real quadratic base field is $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{3})$, with Zauner unit $\varepsilon = \frac{d-1+\sqrt{\Delta}}{2} = 2 + \sqrt{3}$ equal to the fundamental unit.

There is exactly one PEC(5)-orbit of Heisenberg SIC-POVMS [20].

We construct “the” Heisenberg SIC-POVM in dimension 5 explicitly using Conjecture 5.1 and Conjecture 5.2. The ray class group $\text{Cl}_{d\infty_2}(K) \cong \mathbb{Z}/8\mathbb{Z}$. The numbers $\alpha_A^{\text{approx}} = \exp(Z'_A(0))$ were computed to 50 digits of precision and were found to numerically satisfy the following polynomial $f_5(x)$ over K .

$$\begin{aligned} f_5(x) = & x^8 - (8 + 5\sqrt{3})x^7 + (53 + 30\sqrt{3})x^6 - (156 + 90\sqrt{3})x^5 + (225 + 130\sqrt{3})x^4 \\ & - (156 + 90\sqrt{3})x^3 + (53 + 30\sqrt{3})x^2 - (8 + 5\sqrt{3})x + 1. \end{aligned} \quad (6.5)$$

The minimal polynomial of the corresponding ν_A is

$$\begin{aligned} g_5(x) = & 1296x^8 - (648 + 1080\sqrt{3})x^7 + 648x^6 + (864 + 360\sqrt{3})x^5 - (540 + 360\sqrt{3})x^4 \\ & + (144 + 60\sqrt{3})x^3 + 18x^2 - (3 + 5\sqrt{3})x + 1. \end{aligned} \quad (6.6)$$

The overlaps of the Heisenberg SIC are the roots of the conjugate polynomial

$$\begin{aligned} \tilde{g}_5(x) = & 1296x^8 - (648 - 1080\sqrt{3})x^7 + 648x^6 + (864 - 360\sqrt{3})x^5 - (540 - 360\sqrt{3})x^4 \\ & + (144 - 60\sqrt{3})x^3 + 18x^2 - (3 - 5\sqrt{3})x + 1. \end{aligned} \quad (6.7)$$

A numerical approximation to a fiducial vector is

$$v_5 \approx \begin{pmatrix} 0.24167903563278788347 \\ -0.42393763943145804455 - 0.23674553208033493698i \\ 0.67406464953559540185 + 0.19581007881800632630i \\ 0.04040992380093525849 - 0.19581007881800632630i \\ 0.34218699574986301405 + 0.23674553208033493698i \end{pmatrix}. \quad (6.8)$$

6.2. The example $d = 11$. In dimension $d = 11$, the corresponding quadratic discriminant is $\Delta = (d+1)(d-3) = 96$. The real quadratic base field is $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{6})$, with Zauner unit $\varepsilon = \frac{d-1+\sqrt{\Delta}}{2} = 5 + 2\sqrt{6}$ equal to the fundamental unit.

There are three PEC(11)-orbits of SIC-POVMS [20], denoted 11a, 11b, and 11c. They occur in two multiplets, {11a, 11b} and {11c}.

We construct the orbit 11c explicitly using Conjecture 5.1 and Conjecture 5.2. The ray class group $\text{Cl}_{d\infty_2}(K) \cong \mathbb{Z}/40\mathbb{Z}$. The numbers $\alpha_A = \exp(Z'_A(0))$ were computed to 50 digits of precision and were found to numerically satisfy the following polynomial $f_{11}(x)$ over K .

$$\begin{aligned}
f_{11}(x) = & (x^{40} + 1) + (-106 - 44\sqrt{6})(x^{39} + x) + (10614 + 4334\sqrt{6})(x^{38} + x^2) \\
& + (-652115 - 266222\sqrt{6})(x^{37} + x^3) + (27825305 + 11359634\sqrt{6})(x^{36} + x^4) \\
& + (-877414856 - 358203120\sqrt{6})(x^{35} + x^5) \\
& + (21232702036 + 8668214302\sqrt{6})(x^{34} + x^6) \\
& + (-404105217077 - 164975264036\sqrt{6})(x^{33} + x^7) \\
& + (6148885983306 + 2510272190954\sqrt{6})(x^{32} + x^8) \\
& + (-75622522312964 - 30872765454828\sqrt{6})(x^9 + x^{31}) \\
& + (756937617777704 + 309018488445524\sqrt{6})(x^{10} + x^{30}) \\
& + (-6189687857216636 - 2526929486213638\sqrt{6})(x^{11} + x^{29}) \\
& + (41399992237530827 + 16901476056189164\sqrt{6})(x^{12} + x^{28}) \\
& + (-226256732983154420 - 92368924446311502\sqrt{6})(x^{13} + x^{27}) \\
& + (1007258543741292244 + 411211578537502754\sqrt{6})(x^{14} + x^{26}) \\
& + (-3634879852543059214 - 1483933485842242424\sqrt{6})(x^{15} + x^{25}) \\
& + (10563883893311542549 + 4312687540103174716\sqrt{6})(x^{16} + x^{24}) \\
& + (-24534973105051444408 - 10016360826714109164\sqrt{6})(x^{17} + x^{23}) \\
& + (45162757813812803926 + 18437618670122548666\sqrt{6})(x^{18} + x^{22}) \\
& + (-65380387193394562674 - 26691431301568773124\sqrt{6})(x^{19} + x^{21}) \\
& + (74013773227204686051 + 30215996390786346646\sqrt{6})x^{20}. \tag{6.9}
\end{aligned}$$

The minimal polynomial of the corresponding ν_A is

$$\begin{aligned}
g_{11}(x) = & (12^{20}x^{40} + 1) + (48 + 22\sqrt{6})(12^{19}x^{39} + x) + (1968 + 792\sqrt{6})(12^{18}x^{38} + x^2) \\
& + (25848 + 10560\sqrt{6})(12^{17}x^{37} + x^3) + (-419472 - 171072\sqrt{6})(12^{16}x^{36} + x^4) \\
& + (-18892224 - 7714080\sqrt{6})(12^{15}x^{35} + x^5) + (-181457280 - 74074176\sqrt{6})(12^{14}x^{34} + x^6) \\
& + (2141686656 + 874329984\sqrt{6})(12^{13}x^{33} + x^7) \\
& + (62948109312 + 25698435840\sqrt{6})(12^{12}x^{32} + x^8) \\
& + (337583904768 + 137818340352\sqrt{6})(12^{11}x^{31} + x^9) \\
& + (-5182578339840 - 2115780175872\sqrt{6})(12^{10}x^{30} + x^{10}) \\
& + (-83855167709184 - 34233724293120\sqrt{6})(12^9x^{29} + x^{11}) \\
& + (-202894373007360 - 82831288725504\sqrt{6})(12^8x^{28} + x^{12}) \\
& + (4929898807885824 + 2012622741651456\sqrt{6})(12^7x^{27} + x^{13}) \\
& + (47257471319703552 + 19292782106492928\sqrt{6})(12^6x^{26} + x^{14}) \\
& + (45726669189808128 + 18667833415925760\sqrt{6})(12^5x^{25} + x^{15}) \\
& + (-1783877902738587648 - 728265100678004736\sqrt{6})(12^4x^{24} + x^{16}) \\
& + (-11823467430652674048 - 4826910371186737152\sqrt{6})(12^3x^{23} + x^{17}) \\
& + (-11846897461773729792 - 4836475651119906816\sqrt{6})(12^2x^{22} + x^{18}) \\
& + (215144426763866603520 + 87832344582220677120\sqrt{6})(12x^{21} + x^{19}) \\
& + (1246186807345680482304 + 508753633031010385920\sqrt{6})x^{20}. \tag{6.10}
\end{aligned}$$

A numerical approximation to a fiducial vector is

$$v_{11} \approx \begin{pmatrix} 0.31885501173446151953 \\ -0.00727092982813886277 - 0.27361988848296183641i \\ -0.02661472547965484998 - 0.37021984761997660380i \\ 0.26103622782810404567 - 0.17519492308655237763i \\ -0.17130782441847984905 - 0.00498132225998709619i \\ 0.115894663935244395576 + 0.023682353557509036148i \\ -0.20515008071739008667 - 0.15408741485673275946i \\ -0.12010487681658182011 + 0.12297653825975158437i \\ 0.24462906391022207471 - 0.16496679971724189093i \\ 0.56644313698737356128 + 0.07879109944268139950i \\ 0.16629395529532658791 - 0.07929717656822654842i \end{pmatrix}. \tag{6.11}$$

6.3. The example $d = 17$. In dimension $d = 17$, the corresponding quadratic discriminant is $\Delta = (d + 1)(d - 3) = 252$. The real quadratic base field is $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{7})$, with Zauner unit $\varepsilon = \frac{d-1+\sqrt{\Delta}}{2} = 8 + 3\sqrt{7}$ equal to the fundamental unit.

There are three PEC(17)-orbits of SIC-POVMS [20], denoted 17a, 17b, and 17c. They occur in two multiplets, {17a, 17b} and {17c}.

We construct the orbit 17c explicitly using Conjecture 5.1 and Conjecture 5.2. The ray class group $\text{Cl}_{d\infty_2}(\mathcal{O}_{28}) \cong \mathbb{Z}/96\mathbb{Z}$. The numbers $\alpha_A = \exp(Z'_A(0))$ were computed to 50 digits of precision and were found to numerically satisfy the a polynomial $f_{17}(x)$ over K . Values of $f_{17}(x)$, $g_{17}(x)$, $h_{17}(x)$, and a fiducial vector v_{17} may be found in the accompanying text file `dim17.txt`.

6.4. The example $d = 23$. In dimension $d = 23$, the corresponding quadratic discriminant is $\Delta = (d + 1)(d - 3) = 480$. The real quadratic base field is $K = \mathbb{Q}(\sqrt{\Delta}) = \mathbb{Q}(\sqrt{30})$, with Zauner unit $\varepsilon = \frac{d-1+\sqrt{\Delta}}{2} = 11 + 2\sqrt{30}$ equal to the fundamental unit. Unlike our previous examples, K is not a principal ideal domain, but has class number 2.

According to previous numerical searches, there appear to be six PEC(23)-orbits of SIC-POVMs [20], denoted 23a, 23b, 23c, 23d, 23e, and 23f. We have computed one multiplet {23e, 23f} explicitly using Conjecture 5.1; we expect, but have not shown, that the other four orbits form a multiplet {23a, 23b, 23c, 23d}. We follow Scott and Grassl's conventions for other exact solutions in placing the expected minimal multiplet last in the labeling scheme; this may not agree with the numerical solutions given in [20], which were computed without knowledge of the Galois action.

The ray class group $\text{Cl}_{d\infty_2}(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/176\mathbb{Z}$. The numbers $\alpha_A^{\text{approx}} = \exp(Z'_A(0))$ were computed to 500 digits of precision (overnight in 16 parallel threads). The values $\alpha_{m,n}^{\text{approx}} = \exp(Z'_{A_{m,n}}(0))$ (corresponding to the principal ideal classes) were found to numerically satisfy the a polynomial $f_{23}(x)$ over the Hilbert class field $L_{(1)} = \mathbb{Q}(\sqrt{5}, \sqrt{6})$.

In this example, the number $\sqrt{d+1} = 2\sqrt{6}$ is in the Hilbert class field $L_{(1)}$, so we simplify our calculation somewhat by computing $g_{23}^*(x) = g_{23}(2\sqrt{6}x)$ instead of $g_{23}(x)$, and by computing a polynomial $h_{23}^*(x)$ for the action of a Galois group generator on a root of $g_{23}^*(x)$. Values of $f_{23}(x)$, $g_{23}^*(x)$, and fiducial vectors v_{23e} and v_{23f} for 23e and 23f may be found in the accompanying text file `dim23.txt`; the value of $h_{23}^*(x)$ may be found in `h23star.txt`.

REFERENCES

- [1] D. Marcus Appleby. Symmetric informationally complete-positive operator valued measures and the extended Clifford group. *J. Math. Phys.*, 46:052107, 2005.
- [2] D. Marcus Appleby, Ingemar Bengtsson, Stephen Brierley, Åsa Ericsson, Markus Grassl, and Jan-Åke Larsson. Systems of imprimitivity for the Clifford group. *Quantum Information & Computation*, 14(3-4):339–360, 2014.
- [3] D. Marcus Appleby, Ingemar Bengtsson, Stephen Brierley, Markus Grassl, David Gross, and Jan-Åke Larsson. The monomial representations of the Clifford group. *Quantum Information & Computation*, 12(5-6):404–431, 2012.
- [4] Marcus Appleby, Tuan-Yow Chien, Steven Flammia, and Shayne Waldron. Constructing exact symmetric informationally complete measurements from numerical solutions. *Journal of Physics A: Mathematical and Theoretical*, 51(16):165302, 2018.
- [5] Marcus Appleby, Steven Flammia, Gary McConnell, and Jon Yard. Generating ray class fields of real quadratic fields via complex equiangular lines. *arXiv preprint arXiv:1604.06098*, 2016.
- [6] Marcus Appleby, Steven Flammia, Gary McConnell, and Jon Yard. SICs and algebraic number theory. *Foundations of Physics*, pages 1–18, 2017.
- [7] David Burns, Cristian Popescu, Jonathan Sands, David Solomon, et al. *Stark's Conjectures: Recent Work and New Directions: An International Conference on Stark's Conjectures and Related Topics, August 5-9, 2002, Johns Hopkins University*, volume 358. American Mathematical Soc., 2004.
- [8] Bin Chen, Tao Li, and Shao-Ming Fei. General SIC measurement-based entanglement detection. *Quantum Information Processing*, 14(6):2281–2290, 2015.
- [9] Philippe Delsarte, J. M. Goethals, and J. J. Seidel. Bounds for systems of lines, and Jacobi polynomials. *Philips Research Reports*, 30:91, 1975.

- [10] Christopher A. Fuchs, Michael C. Hoang, and Blake C. Stacey. The SIC question: history and state of play. *arXiv preprint arXiv:1703.07901*, 2017.
- [11] Christopher A. Fuchs and Rüdiger Schack. Quantum-Bayesian coherence. *Reviews of modern physics*, 85(4):1693–1715, 2013.
- [12] Markus Grassl. On SIC-POVMS and MUBs in dimension 6. In *Proceedings of the ERATO Conference on Quantum Information Science*, page 60, 2004.
- [13] Markus Grassl. Tomography of quantum states in small dimensions. *Electronic Notes in Discrete Mathematics*, 20:151–164, 2005.
- [14] Markus Grassl. Computing equiangular lines in complex space. In *Mathematical Methods in Computer Science: Essays in Memory of Thomas Beth*, pages 89–104. Springer, 2008.
- [15] Stuart G. Hoggar. 64 lines from a quaternionic polytope. *Geometriae Dedicata*, 69(3):287–289, 1998.
- [16] Gene S. Kopp. *Indefinite Theta Functions and Zeta Functions*. PhD thesis, University of Michigan, Ann Arbor, Michigan, USA, August 2017.
- [17] Jürgen Neukirch. *Algebraic Number Theory*, volume 322. Springer Science & Business Media, 2013.
- [18] Joseph M. Renes, Robin Blume-Kohout, Andrew J. Scott, and Carlton M. Caves. Symmetric informationally complete quantum measurements. *Journal of Mathematical Physics*, 45(6):2171–2180, 2004.
- [19] Andrew J. Scott. SICs: Extending the list of solutions. *arXiv preprint arXiv:1703.03993*, 2017.
- [20] Andrew J. Scott and Markus Grassl. Symmetric informationally complete positive-operator-valued measures: A new computer study. *Journal of Mathematical Physics*, 51(4):042203, 2010.
- [21] Andrew J. Scott and Markus Grassl. Fibonacci-Lucas SIC-POVMS. *arXiv preprint arXiv:1707.02944*, 2017.
- [22] Takuro Shintani. On Kronecker limit formula for real quadratic fields. *Proceedings of the Japan Academy*, 52(7):355–358, 1976.
- [23] Takuro Shintani. On certain ray class invariants of real quadratic fields. *Journal of the Mathematical Society of Japan*, 30(1):139–167, 1978.
- [24] Harold M. Stark. Values of L-functions at $s = 1$. I. L-functions for quadratic forms. *Advances in Mathematics*, 7(3):301–343, 1971.
- [25] Harold M. Stark. L-functions at $s = 1$. II. Artin L-functions with rational characters. *Advances in Mathematics*, 17(1):60–92, 1975.
- [26] Harold M. Stark. L-functions at $s = 1$. III. Totally real fields and Hilbert’s twelfth problem. *Advances in Mathematics*, 22(1):64–84, 1976.
- [27] Harold M. Stark. Class fields for real quadratic fields and L-series at 1. In *Algebraic Number Fields*, pages 355–374. Academic Press, New York, 1977.
- [28] Harold M. Stark. L-functions at $s = 1$. IV. First derivatives at $s = 0$. *Advances in Mathematics*, 35(3):197–235, 1980.
- [29] Anna Szymusiak and Wojciech Słomczyński. Informational power of the Hoggar symmetric informationally complete positive operator-valued measure. *Physical Review A*, 94(1):012122, 2016.
- [30] Gerhard Zauner. *Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie*. PhD thesis, University of Vienna, Vienna, Austria, 1999.
- [31] Gerhard Zauner. Quantum designs: Foundations of a noncommutative design theory. *International Journal of Quantum Information*, 9(1):445–507, 2011.
- [32] Huangjun Zhu. SIC POVMS and Clifford groups in prime dimensions. *Journal of Physics A: Mathematical and Theoretical*, 43(30):305305, 2010.

SCHOOL OF MATHEMATICS, UNIVERSITY OF BRISTOL, BRISTOL, UK AND HEILBRONN INSTITUTE FOR MATHEMATICAL RESEARCH, BRISTOL, UK

E-mail address: gene.kopp@bristol.ac.uk