G. S. Kopp (2019) "SIC-POVMs and the Stark Conjectures,"
International Mathematics Research Notices, Vol. 00, No. 0, pp. 1–27
doi:10.1093/imrn/rnz153

SIC-POVMs and the Stark Conjectures

Gene S. Kopp*

Heilbronn Institute for Mathematical Research, School of Mathematics, University of Bristol, Bristol, UK

**Correspondence to be sent to: e-mail: gene.kopp@bristol.ac.uk*

The existence of d^2 pairwise equiangular complex lines [equivalently, a symmetric informationally complete positive operator-valued measure (SIC-POVM)] in d-dimensional Hilbert space is known only for finitely many dimensions d. We prove that, if there exists a set of real units in a certain ray class field (depending on d) satisfying certain algebraic properties, a SIC-POVM exists, 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 SIC-POVM in dimension 23.

1 Introduction

A set of m **complex equiangular lines** in d dimensions is a set of one-dimensional subspaces $\mathbb{C}v_1, \mathbb{C}v_2, \ldots, \mathbb{C}v_m$ 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 geometric configurations were first studied in the context of design theory in the 1970s, as a complex analogue of sets of real equiangular lines. The maximal cardinality of a set of complex equiangular lines was shown to be bounded above by d^2 by Delsarte *et al.* [8].

Received December 18, 2018; Revised May 7, 2019; Accepted June 4, 2019

A set of complex equiangular lines achieving this upper bound—d^2 lines in dimension d—is equivalent to a type of generalized quantum measurement 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 and especially quantum state tomography, the process of reconstructing a quantum state from a set of measurements of copies of the state (see, e.g., [19]). Their existence has implications for quantum foundations due to their presence in the theory of quantum Bayesianism (or QBism) [10]. See the bibliography of Fuchs *et al.* [9] for a complete list of references on the history and applications of SIC-POVMs.

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 [1–4, 11–13, 21, 22, 30], and approximate numerical solutions have been found in every dimension up to 151 and several other dimensions up to 844 [9, 18, 20–22]. (Some further unpublished solutions have been found by Grassl and Scott [14]: an exact solution in dimension 53 and numerical solutions in all dimensions up to 165, dimension 1155, and dimension 2208) 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 *et al.* [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 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 $\mathbb{Q}(\sqrt{(d-3)(d+1)})$. 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.

The applicability of SIC-POVMs to Hilbert's 12th problem is currently aspirational. Although it is possible to use SIC-POVMs (found by other methods) to construct class fields, the reverse direction (using class fields to construct SIC-POVMs) is more sensible from a computational perspective. Rather, the surprising connection between class field theory and complex equiangular lines gives a telling hint about the algebraic structure of class fields—and, in fact, the algebraic properties of derivative ray class zeta values at $s = 0$.

Specifically, in this paper, we formulate a pair of conjectures that imply a strong refinement of the rank 1 abelian Stark conjecture in an infinite family of class fields. In Conjecture 5.1, we predict the existence of a Galois orbit of real algebraic units in a certain class field over $\mathbb{Q}(\sqrt{(d-3)(d+1)})$ satisfying several strong algebraic and congruence conditions, in the case of d an odd prime congruent to 2 modulo 3. Conjecture 5.2 states that the Stark units are such an orbit.

This paper likewise provides a refinement of Zauner's conjecture on SIC-POVM existence. We give a conjectural construction of a Heisenberg SIC-POVM in infinitely many dimensions $d = 5, 11, 17, 23, 29, 41, \ldots$ (i.e., those d that are odd primes congruent to 2 modulo 3). Specifically, we prove in Theorem 5.4 that any set of units satisfying the conditions of Conjecture 5.1 may be used to construct a SIC-POVM in dimension d. Conjecture 5.2 gives an analytic formula for a set of real numbers that we expect to satisfy the conditions of Conjecture 5.1, thus providing a construction of SIC-POVMs.

Of crucial importance to our construction are the conjectures of Stark on the leading terms of the Taylor expansions of Hecke and Artin L-functions at $s = 1$ and $s = 0$ [25–29]. 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 [25]). Much work has been done toward attacking or refining the Stark conjectures; one vital reference is the proceedings of the 2002 "International Conference on Stark's Conjectures and Related Topics" at Johns Hopkins University [7].

Specifically, we connect the SIC-POVM existance question to the rank 1 abelian Stark conjecture in the real quadratic case [27, 28]. In the rank 1 case, the conjecture predicts the existance of "Stark units" in ray class fields given by the analytic formula $\varepsilon_A = \exp(Z'_A(0))$ for a certain differenced ray class zeta function $Z_A(s)$. The following observation was first made by the author in his PhD thesis [16] in the case $d = 5$, and we have checked it numerically in a number of cases beyond those of odd prime dimensions $d \equiv 2 \pmod 3$ that are the focus of this paper.

Observation 1.1. Squares of overlap phases of centred Heisenberg SIC-POVMs in dimension d are Galois conjugate to integral powers of Stark units in abelian extensions of $\mathbb{Q}(\sqrt{(d-3)(d+1)})$.

Conjectures 5.1 and 5.2 make Observation 1.1 completely explicit in the case where d is an odd prime congruent to 2 modulo 3 and the SIC-POVM is in the "minimal multiplet". A congruence condition modulo a prime lying over (d) determines the signs of the overlap phases; see (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 known exact expression for a SIC-POVM in dimension 23.

The paper is organized as follows. In Sections 2 and 3, 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 4, we take a brief detour to prove a density result on primes ramifying in extensions conjecturally generated by SIC-POVMs. 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.

Work in progress (some of it joint with other authors) will give an explicit formulation of Observation 1.1 in full generality, including the case of "non-minimal" SIC-POVMs.

2 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.

2.1 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 *et al.* [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 [8].

Proposition 2.1 (Delsarte *et al.* [8]). 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 2.2 (Delsarte *et al.* [8]). 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 $v \neq w$,

$$\alpha = \frac{1}{d+1}, \tag{(2.1)}$$

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

A SIC-POVM is defined as a set of rank 1 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 2.1.

Definition 2.3 (SIC-POVM). A SIC-POVM is a set $\left\{\frac{1}{d}\Pi_1, \frac{1}{d}\Pi_2, \ldots, \frac{1}{d}\Pi_{d^2}\right\}$ of cardinality d^2 consisting of rank 1 Hermitian $d \times d$ matrices $\frac{1}{d}\Pi_i$ such that each $\Pi_i^2 = \Pi_i$, and

$$\operatorname{Tr}\left(\Pi_i \Pi_j\right) = \begin{cases} 1 & \text{if } i = j, \\ \frac{1}{d+1} & \text{if } i \neq j. \end{cases} \tag{(2.2)}$$

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 $\{\mathbb{C}v_1, \ldots, \mathbb{C}v_{d^2}\}$ 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 $\{\mathbb{C}Uv_1, \ldots, \mathbb{C}Uv_{d^2}\}$. Moreover, if C_d is the complex conjugation operator on $\mathbb{C}^d$, so that $C_d v := \overline{v}$, 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 2.4. Define the **extended unitary group** $\mathrm{EU}(d) := \mathrm{U}(d) \sqcup C_d\mathrm{U}(d)$.

Lemma 2.5. The action of $\mathrm{EU}(d)$ takes SIC-POVMs to SIC-POVMs.

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

Definition 2.6 (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.

2.2 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 dth root of unity.

Definition 2.7 (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 $\mathrm{H}(d)$ 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

$$X = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 \end{pmatrix}, \quad Z = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & \zeta_d & 0 & \cdots & 0 \\ 0 & 0 & \zeta_d^2 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \zeta_d^{d-1} \end{pmatrix}. \tag{(2.3)}$$

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

Definition 2.8 (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

$$D_{m,n} = \tau_d^{mn} X^m Z^n \text{ for } 0 \leq m, n \leq d-1 \tag{(2.4)}$$

forms a basis of $\mathrm{M}_d(\mathbb{C})$ over $\mathbb{C}$, and this basis is called the **Heisenberg basis**. (The $D_{m,n}$ are known as **displacement operators**. Elsewhere in the literature, the displacement operators have been defined both with and without the scalar phase factor of τ_d^{mn}.)

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

Definition 2.9 (Heisenberg SIC-POVM). A **Heisenberg SIC-POVM** is a SIC-POVM of the form

$$\left\{\mathbb{C}D_{m,n}v : 0 \leq m, n \leq d-1\right\} \tag{(2.5)}$$

for some vector $v \in \mathbb{C}^d$. This v is called a **fiducial vector**.

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

Lemma 2.10. If v is a fiducial vector for a Heisenberg SIC-POVM, and $\gamma \in \mathrm{EC}(d)$, then γv is also a fiducial vector for a Heisenberg SIC-POVM.

Proof. The reader may work this out directly or see Scott and Grassl [21, Section 3]. ■

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

2.3 SIC-POVM-generated fields and the Galois action on Heisenberg SIC-POVMs

In 2016, Appleby *et al.* [5, 6] empirically discovered a surprising connection between SIC-POVMs and ray class fields of real quadratic fields. For all Heisenberg SIC-POVMs they checked, 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 $\Delta = \Delta_d = (d-3)(d+1)$.

Every real quadratic field $K = \mathbb{Q}(\sqrt{\Delta})$ arises this way—indeed, each K arises for infinitely many d. While not every class field over K (nor a cofinal set of class fields) is predicted to arise, a rich family of class fields are predicted, with ramification at a positive density set of primes. We make this density claim explicit in Section 4.

The key property of the pair (d, Δ) is the existence of a unit

$$\varepsilon = \varepsilon_d = \frac{(d-1) + \sqrt{\Delta}}{2}. \tag{(2.6)}$$

with the property that $\varepsilon^3 \equiv 1 \pmod{d}$. The presence of ε 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, $\varepsilon_{15} = (2 + \sqrt{3})^2$.

Ignoring repeated fields, the sequence

$$\mathbb{Q}\left(\sqrt{\Delta_4}\right), \mathbb{Q}\left(\sqrt{\Delta_5}\right), \ldots, \mathbb{Q}\left(\sqrt{\Delta_d}\right), \ldots \tag{(2.7)}$$

is essentially an ordering of real quadratic fields by the size of their regulators. While in the usual ordering by the size of the discriminant, a "random" quadratic field should have a small class number (size $O(\Delta^{o(1)})$) and a large regulator (size $O(\Delta^{1/2+o(1)})$); in the ordering given in (2.7), class numbers are large (size $O(d)$) and regulators are very small (size $O(\log(d))$). One might philosophize that ordering real quadratic fields by the size of their regulators makes them behave more like imaginary quadratic fields, whose explicit class field theory we understand.

Now, fix d, and let $\Delta = (d-3)(d+1)$ and $K = \mathbb{Q}(\sqrt{\Delta})$. Let v be a Heisenberg fiducial vector, and let E be the field generated by the ratios of the entries of the v along with the d'th roots of unity, where $d' = d$ if d is odd, and $d' = 2d$ if d is even. If $\sigma \in \mathrm{Gal}(E/K)$, then v^σ is also a Heisenberg fiducial vector; however, v^σ may or may not lie in the same $\mathrm{EC}(d)$ orbit as v. This Galois action respects orbits because $(\gamma v)^\sigma = \gamma^\sigma v^\sigma$ and $\mathrm{EC}(d)$ is Galois-closed.

Definition 2.11 (Multiplet). The set of all those $\mathrm{EC}(d)$-orbits of fiducial vectors, which are Galois equivalent to a given $\mathrm{EC}(d)$-orbit, is called a **multiplet**.

3 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 [27].

3.1 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 $K \to \mathbb{R}$. Associate to the real embeddings $\rho_1, \ldots, \rho_r$ the "infinite primes" $\infty_1, \ldots, \infty_r$, 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 3.1. If $\mathfrak{m} = (\mathfrak{c}, S)$, define the **ray class group modulo** $\mathfrak{m}$ to be

$$\mathrm{Cl}_{\mathfrak{m}} = \frac{\{\text{fractional ideals coprime to } \mathfrak{c}\}}{\{\text{principal frac. ideals } (\alpha) \text{ coprime to } \mathfrak{c} \text{ with } \alpha \equiv 1 \pmod{\mathfrak{c}} \text{ and } \rho(a) > 0\ \forall\ \rho \in S\}}. \quad ((3.1))$$

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

$$\mathrm{Cl}_{\mathfrak{m}} \cong \frac{\{\text{fractional ideals coprime to } \mathfrak{c}'\}}{\{\text{principal frac. ideals } (\alpha) \text{ coprime to } \mathfrak{c}' \text{ with } \alpha \equiv 1 \pmod{\mathfrak{c}} \text{ and } \rho(a) > 0\ \forall\ \rho \in S\}}. \quad ((3.2))$$

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 $\pi_{\mathfrak{m}',\mathfrak{m}} : \mathrm{Cl}_{\mathfrak{m}'} \twoheadrightarrow \mathrm{Cl}_{\mathfrak{m}}$ are defined by first imposing comprimality to $\mathfrak{c}'$ in $\mathrm{Cl}_{\mathfrak{m}}$, 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 3.2 (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 $\mathrm{Gal}(K^{\mathrm{ab}}/K)$ with the inverse limit $\lim_{\leftarrow} \mathrm{Cl}_{\mathfrak{m}}$ with respect to the quotient maps $\pi_{\mathfrak{m}',\mathfrak{m}}$. This isomorphism is called the **Artin map**:

$$\mathrm{Art} : \varprojlim \mathrm{Cl}_{\mathfrak{m}} \to \mathrm{Gal}(K^{\mathrm{ab}}/K). \quad ((3.3))$$

The field $L_{\mathfrak{m}}/K$ corresponding to $\mathrm{Cl}_{\mathfrak{m}}$ by Galois theory—so that $\mathrm{Gal}(L_{\mathfrak{m}}/K) \cong \mathrm{Cl}_{\mathfrak{m}}$ 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]. ■

3.2 Ray class zeta functions and Hecke L-functions

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

Definition 3.3 (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 by the sum over integral ideals

$$\zeta(s,A) = \sum_{\substack{\mathfrak{a}\in A \\ \mathfrak{a}\leq \mathcal{O}_K}} N(\mathfrak{a})^{-s} \text{ for } \mathrm{Re}(s) > 1. \tag{(3.4)}$$

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

Theorem 3.4. 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. ■

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

$$R = \left\{a\mathcal{O}_K : a \equiv -1 \pmod{\mathfrak{c}} \text{ and } a \text{ is positive at each place in } S\right\}. \tag{(3.5)}$$

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

$$Z_A(s) = \zeta(s,A) - \zeta(s,RA). \tag{(3.6)}$$

Hecke L-functions (of finite-order Hecke characters) 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 3.6 (L-function of a finite-order Hecke character). Let K be a number field and $\mathfrak{m}$ a modulus of K. Let $\chi : \mathrm{Cl}_\mathfrak{m} \to \mathbb{C}^\times$ be a group homomorphism. The Hecke L-function is

$$L(s,\chi) = \sum_{A\in \mathrm{Cl}_\mathfrak{m}} \chi(A)\zeta(s,A). \tag{(3.7)}$$

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.

3.3 A Stark conjecture over real quadratic base field

The Existence Theorem 3.2 does not provide a procedure for actually building the ray class field $L_{\mathfrak{m}}$. 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 [27], gives a conjectural generator for a ray class field over a real quadratic field, under certain conditions.

Conjecture 3.7 (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 $\mathrm{Cl}_{\mathfrak{c}\infty_2}$. 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 $\mathrm{Art} : \mathrm{Cl}_{\mathfrak{c}\infty_2} \to \mathrm{Gal}\left(L_{\mathfrak{c}\infty_2}/K\right)$. Specifically, $\alpha_A = \alpha_I^{\mathrm{Art}(A)}$, where $I \in \mathrm{Cl}_{\mathfrak{c}\infty_2}$ is the identity class.

4 Asymptotic Density of Primes Appearing in Moduli of SIC-POVM-Generated Class Fields

This paper may be viewed as a contribution to explicit class field theory for a thin family of class fields. In this section, we provide some evidence for the relevance of SIC-POVMs to Hilbert's 12th Problem by showing that the family of class fields predicted to arise is, in a quantifiable sense, not *very* thin.

In their papers [5, 6], Appleby, Flammia, McConnell, and Yard make the following conjecture.

Conjecture 4.1 (Class field hypothesis of Appleby, Flammia, McConnell, and Yard). Let $d \geq 4$, and let $K = \mathbb{Q}(\sqrt{(d-3)(d+1)})$. There is a **minimal multiplet** $\mathcal{M}$ of Heisenberg SIC-POVMs in dimension d containing a representative such that the field generated by its overlaps is the ray class field $L_{d\infty_1}$ of modulus $d\infty_1$ over K, and such that the overlaps of any other Heisenberg SIC-POVM in dimension d generate a field containing $L_{d\infty_1}$.

We prove that, under the class field hypothesis, a positive density of primes appear in the moduli of SIC-POVM-generated class fields over a fixed real quadratic field. Moreover, we quantify that density explicitly.

Proposition 4.2. Let $\Delta > 0$ be a fundamental discriminant, and let $K = \mathbb{Q}(\sqrt{\Delta})$. Let P_Δ be the set of primes

$$P_\Delta = \left\{p \text{ prime} : (\exists d, f)\ (d-3)(d+1) = f^2\Delta \text{ and } p|d\right\}. \tag{(4.1)}$$

(Under the class field hypothesis, P_Δ is the set of primes dividing the moduli of minimal SIC-POVM-generated class fields of K.) Then, P_Δ has asymptotic density

$$\mu(P_\Delta) := \lim_{N\to\infty} \frac{\#\{p \leq N : p \in P_\Delta\}}{\#\{p \leq N : p \text{ is prime}\}} = \frac{3}{8} \tag{(4.2)}$$

in the set of all primes.

Proof. Let $\varepsilon > 1$ be the smallest totally positive unit of $\mathcal{O}_K$ greater than 1. (So, ε is either the fundamental unit or its square.)

Consider some $p \in P_\Delta$, along with some associated (d, f). The equation $(d-3)(d+1) = f^2\Delta$ may be rewritten as the Pell equation

$$(d-1)^2 - f^2\Delta = 4. \tag{(4.3)}$$

In other words, $\frac{d-1+f\sqrt{\Delta}}{2}$ is a totally positive unit of $\mathcal{O}_K$; thus,

$$\frac{d-1+f\sqrt{\Delta}}{2} = \varepsilon^k \text{ for some } k \in \mathbb{N}. \tag{(4.4)}$$

We see that $\varepsilon^k + 1 + \varepsilon^{-k} = d$, so $z = \varepsilon^k$ is a root of $z^2 + z + 1 \equiv 0 \pmod{p}$.

Conversely, suppose that for some $k \in \mathbb{N}$, $z = \varepsilon^k$ is a root of $z^2+z+1 \equiv 0 \pmod{p}$. Let $d := \varepsilon^k + 1 + \varepsilon^{-k} \in p\mathbb{N}$; we may then write

$$\varepsilon^k = \frac{d-1+f\sqrt{\Delta}}{2} \text{ for some } f \in \mathbb{N}. \tag{(4.5)}$$

It follows that $(d-3)(d+1) = f^2\Delta$ as above. Thus, $p \in P_\Delta$.

We have now shown that $P_\Delta = \{p \text{ prime} : (\exists k)\ z = \varepsilon^k \text{ is a root of } z^2 + z + 1 \equiv 0 \pmod{p}\}$.

Write P_Δ as a union

$$P_\Delta = R_\Delta \sqcup S_\Delta \sqcup I_\Delta, \tag{(4.6)}$$

where

$$R_\Delta = \{p \in P_\Delta : p = 3 \text{ or } p \text{ is ramified in } K/\mathbb{Q}\}; \tag{(4.7)}$$

$$S_\Delta = \{p \in P_\Delta : p \neq 3 \text{ and } p \text{ is split in } K/\mathbb{Q}\}; \tag{(4.8)}$$

$$I_\Delta = \{p \in P_\Delta : p \neq 3 \text{ and } p \text{ is inert in } K/\mathbb{Q}\}. \tag{(4.9)}$$

The set R_Δ is finite and thus irrelevant to the density calculation. If $p \in S_\Delta$, then $\mathbb{F}_p$ contains a cube root of unity, so $p \equiv 1 \pmod 3$. We may rewrite S_Δ as

$$S_\Delta = \left\{p \text{ prime} : p \equiv 1 \pmod 3, \left(\frac{\Delta}{p}\right) = 1, \text{ and } 3|o_p(\varepsilon)\right\}; \tag{(4.10)}$$

here $o_p(\varepsilon)$ denotes the order of the reduction of ε in the multiplicative group $(\mathcal{O}_K/p\mathcal{O}_K)^\times \cong (\mathbb{F}_p^\times)^2$. On the other hand, if $p \in I_\Delta$, then $(\mathcal{O}_K/p\mathcal{O}_K)^\times \cong \mathbb{F}_{p^2}^\times$, and the Frobenius automorphism in $\mathrm{Gal}(\mathbb{F}_{p^2}/\mathbb{F}_p)$ takes ε to ε^{-1}; that is, $\varepsilon^p \equiv \varepsilon^{-1} \pmod p$. Thus, $3|o_p(\varepsilon)|(p+1)$, so

$$I_\Delta = \left\{p \text{ prime} : p \equiv 2 \pmod 3, \left(\frac{\Delta}{p}\right) = -1, \text{ and } 3|o_p(\varepsilon)\right\}. \tag{(4.11)}$$

We now write S_Δ and I_Δ as infinite disjoint unions

$$S_\Delta = \bigsqcup_{j=1}^{\infty} S_\Delta^j, \quad S_\Delta^{(j)} = \{p \in S_\Delta : 3^j|(p-1) \text{ and } \varepsilon \equiv u^{3^{j-1}} \pmod p \text{ for } u \text{ a cubic nonresidue}\}, \tag{(4.12)}$$

$$I_\Delta = \bigsqcup_{j=1}^{\infty} I_\Delta^j, \quad I_\Delta^{(j)} = \{p \in I_\Delta : 3^j|(p+1) \text{ and } \varepsilon \equiv u^{3^{j-1}} \pmod p \text{ for } u \text{ a cubic nonresidue}\}. \tag{(4.13)}$$

Let ζ_{3^j} be a primitive (3^j)-th root of unity, and let α_j be a solution to $\alpha_j^{3^j} = \varepsilon$. Consider the Galois fields $K_j = K(\zeta_{3^j}, \alpha_j)$. The Galois group $G_j := \mathrm{Gal}(K_j/\mathbb{Q})$ has a presentation

$G_j = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$, where

$$\sigma_1(\sqrt{\Delta}) = -\sqrt{\Delta} \qquad \sigma_2(\sqrt{\Delta}) = \sqrt{\Delta} \qquad \sigma_3(\sqrt{\Delta}) = \sqrt{\Delta} \tag{(4.14)}$$

$$\sigma_1(\zeta_{3^j}) = \zeta_{3^j}^{-1} \qquad \sigma_2(\zeta_{3^j}) = \zeta_{3^j}^{2} \qquad \sigma_3(\zeta_{3^j}) = \zeta_{3^j} \tag{(4.15)}$$

$$\sigma_1(\alpha_j) = \alpha_j^{-1} \qquad \sigma_2(\alpha_j) = \alpha_j \qquad \sigma_3(\alpha_j) = \zeta_{3^j}\alpha_j. \tag{(4.16)}$$

(Note that the automorphism σ_1 is central, and that σ_2 generates the subgroup of automorphisms fixing both $\sqrt{\Delta}$ and α_j.) We may rewrite the $S_\Delta^{(j)}$ and $I_\Delta^{(j)}$ as Chebotarev sets:

$$S_\Delta^{(j)} = \left\{\text{rational primes } p : \mathrm{Frob}_p(K_j) = \left\{\sigma_3^{3^{j-1}}, \sigma_2^{-1}\sigma_3^{3^{j-1}}\sigma_2\right\}\right\}; \tag{(4.17)}$$

$$I_\Delta^{(j)} = \left\{\text{rational primes } p : \mathrm{Frob}_p(K_j) = \left\{\sigma_1\sigma_3^{3^{j-1}}, \sigma_2^{-1}\sigma_1\sigma_3^{3^{j-1}}\sigma_2\right\}\right\}. \tag{(4.18)}$$

Moreover,

$$\bigsqcup_{j>J} S_\Delta^{(j)} \subseteq \left\{\text{rational primes } p : \mathrm{Frob}_p(K_j) = \{\mathrm{id}\}\right\} =: \overline{S}_\Delta^{(J)}; \tag{(4.19)}$$

$$\bigsqcup_{j>J} I_\Delta^{(j)} \subseteq \left\{\text{rational primes } p : \mathrm{Frob}_p(K_j) = \{\sigma_1\}\right\} =: \overline{I}_\Delta^{(J)}. \tag{(4.20)}$$

Thus, we may bound S_Δ and I_Δ between finite unions of Chebotarev sets:

$$\bigsqcup_{1\le j\le J} S_\Delta^{(j)} \subseteq S_\Delta \subseteq \left(\bigsqcup_{1\le j\le J} S_\Delta^{(j)}\right) \sqcup \overline{S}_\Delta^{(J)}; \tag{(4.21)}$$

$$\bigsqcup_{1\le j\le J} I_\Delta^{(j)} \subseteq I_\Delta \subseteq \left(\bigsqcup_{1\le j\le J} I_\Delta^{(j)}\right) \sqcup \overline{I}_\Delta^{(J)}. \tag{(4.22)}$$

For an set of primes S, denote by $\mu(S)$ the asymptotic density of S in the set of all primes. By the Chebotarev density theorem, $\mu\left(S_\Delta^{(j)}\right) = \mu\left(I_\Delta^{(j)}\right) = \frac{2}{|G_j|} = \frac{1}{2\cdot 3^{2j-1}}$, and $\mu\left(\overline{S}_\Delta^{(J)}\right) = \mu\left(\overline{I}_\Delta^{(J)}\right) = \frac{1}{4\cdot 3^{2J-1}}$. Taking densities in (4.21) and (4.22), we obtain the inequalities

$$\sum_{j=1}^{J} \frac{1}{2\cdot 3^{2j-1}} \le m \le \left(\sum_{j=1}^{J} \frac{1}{2\cdot 3^{2j-1}}\right) + \frac{1}{4\cdot 3^{2J-1}} \text{ for both } m = \mu(S_\Delta) \text{ and } m = \mu(I_\Delta). \tag{(4.23)}$$

Sending $J \to \infty$, we see that

$$\mu(S_\Delta) = \mu(I_\Delta) = \sum_{j=1}^{\infty} \frac{1}{2 \cdot 3^{2j-1}} = \frac{3}{16}. \tag{(4.24)}$$

Thus, $\mu(P_\Delta) = \frac{3}{16} + \frac{3}{16} = \frac{3}{8}$. ■

5 Toward an Infinite Family of Heisenberg SIC-POVMs

We now state our main conjectures and results. Our 1st 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 $\Delta = (d-3)(d+1)$ and $K = \mathbb{Q}(\sqrt{\Delta})$, and consider the class group $\mathrm{Cl}_{(d)\infty_2}$. With indices $m, n \in \mathbb{Z}/d\mathbb{Z}$, $(m, n) \neq (0, 0)$, let

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

and let $\mathrm{Art} : \mathrm{Cl}_{(d)\infty_2} \to \mathrm{Gal}\left(L_{(d)\infty_2}/K\right)$ 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 $\alpha_{m,n} := \alpha^{\mathrm{Art}(A_{m,n})}$ 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

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

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

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

is idempotent (i.e., $M^2 = M$) and rank 1 (i.e., all the rank 2 minors of M vanish). (See (2.4) for the definition of $D_{m,n}$.)

The condition that d is prime and $d \equiv 2 \pmod 3$ is necessary because (5.1) does not make sense for all $(m, n) \neq (0, 0)$ without it. For general d, the principal subgroup of $\mathrm{Cl}_{(d)\infty_2}$ is represented by those $A_{m,n}$ such that $(m + n\sqrt{\Delta})$ is relatively prime to (d). The condition that d is prime and $d \equiv 2 \pmod 3$ is equivalent to (d) being prime in $\mathcal{O}_K$, that is, to $(m + n\sqrt{\Delta})$ being relatively prime to (d) whenever $(m, n) \equiv (0, 0) \pmod d$.

Our 2nd 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. Let d be an odd prime such that $d \equiv 2 \pmod 3$. A unit α satisfying Conjecture 5.1 and its Galois conjugates over K may be constructed as Stark units

$$\alpha^{\mathrm{Art}(A)} = \exp\left(Z'_A(0)\right), \tag{(5.4)}$$

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

Conjecture 3.7, due to Stark, predicts that $\exp\left(Z'_A(0)\right) = \alpha^{\mathrm{Art}(A)}$ 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 (5.4). Shintani's Kronecker limit formula expresses $\exp\left(Z'_A(0)\right)$ as a product of special values of Barnes's double gamma function [23, 24]. A different formula appears in Chapter 4 of the author's PhD thesis [16].

We state Conjectures 5.1 and 5.2 as two separate conjectures because it may be possible to prove the 1st without proving the 2nd. One route by which this might be done is through the use of p-adic zeta functions rather than Archimedian 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 $\Delta = (d-3)(d+1)$ 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 η 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 is K; it is 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

$$\eta = \varepsilon_d^3 \tag{(5.5)}$$

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

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

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 $\mathrm{Cl}_{(d)}$, $\mathrm{Cl}_{(d)\infty_1}$, $\mathrm{Cl}_{(d)\infty_2}$, and $\mathrm{Cl}_{(d)\infty_1\infty_2}$ are all distinct. Thus, by Theorem 3.2, the class fields $L_{(d)}$, $L_{(d)\infty_1}$, $L_{(d)\infty_2}$, and $L_{(d)\infty_1\infty_2}$ are all distinct. ■

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 $\sigma \in \mathrm{Gal}(L_{(d)\infty_2}/\mathbb{Q})$ 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 $\tau \in \mathrm{Gal}(L_{(d)\infty_2}/K)$ such that $\tau(\alpha) = \alpha^{-1}$. Then, $\tau(\alpha_{m,n}) = \alpha_{m,n}^{-1}$ because $\mathrm{Gal}(L_{(d)\infty_2}/K)$ is abelian. Thus,

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

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

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

Thus, by class field theory, the fixed field of τ is $L_{(d)}$. It follows that the class field of $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(L_{(d)\infty_1}/K)$ 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 $\left|\sigma(\nu_{m,n})\right| = \frac{1}{\sqrt{d+1}}$. From the definition of M, we obtain $\mathrm{Tr}(MD_{m,n}) = \nu_{m,n}$. Thus,

$$\left|\mathrm{Tr}\left(\sigma(M)\sigma(D_{m,n})\right)\right|^2 = \mathrm{Tr}\left(\sigma(M)\sigma(D_{m,n})\right)\left(\sigma\tau\sigma^{-1}\right)\left(\mathrm{Tr}\left(\sigma(M)\sigma(D_{m,n})\right)\right) \tag{(5.10)}$$

$$= \sigma\left(\mathrm{Tr}\left(MD_{m,n}\right)\tau\left(\mathrm{Tr}\left(MD_{m,n}\right)\right)\right) \tag{(5.11)}$$

$$= \sigma\left(\nu_{m,n}\nu_{-m,-n}\right) \tag{(5.12)}$$

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

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

$$\left|\mathrm{Tr}\left(\sigma(M)D_{m,n}\right)\right|^2 = \frac{1}{d+1}, \tag{(5.14)}$$

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, $w = v$. Conjugation-transposition acts on $\sigma(M)$ as follows:

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

Thus, $w = v$. So (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 $\mathbb{C}^d$. ■

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 Conjectures 5.1 and 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] and Conjecture 4.1), 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 [21], 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 $A \in \mathrm{Cl}_{(d)\infty_2}(K)$, 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 3.7); 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 $\sigma\left(\sqrt{\Delta}\right) = -\sqrt{\Delta}$. 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 $G = \mathrm{Gal}(L_{(d)\infty_2}/L_{(1)})$. 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 $G = \mathrm{Gal}(L_{(d)\infty_2}/L_{(1)}) \cong \left(\mathcal{O}_K/d\mathcal{O}_K\right)^\times / \langle \overline{\varepsilon_d} \rangle$ is a cyclic group of order $n = \frac{d-1}{3}$. Let γ be a generator for $\left(\mathcal{O}_K/d\mathcal{O}_K\right)^\times$, so $\tau = \mathrm{Art}(A_\gamma)$ is a generator for G. Fix $\nu = \nu_{1,0}$. We compute $\tau(\nu)$ in the monomial basis $\{1, \nu, \cdots \nu^{n-1}\}$ for $L_{(d)\infty_2}$ over $L_{(1)}$:

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

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

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

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 $\mathrm{Gal}\left(L_{(d)\infty_1}/L_{(1)}\right)$ on the roots of $\tilde{g}_d(x)$ is given by applying the polynomial

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

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

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

As we have not 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, 23b 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 $\Delta = (d-3)(d+1) = 12$. 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 [21].

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

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

The minimal polynomial of the corresponding ν_A is

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

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

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

A numerical approximation to a fiducial vector is

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

6.2 The example $d = 11$

In dimension $d = 11$, the corresponding quadratic discriminant is $\Delta = (d-3)(d+1) = 96$. 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 [21], denoted 11a, 11b, and 11c. They occur in two multiplets, {11a, 11b} and {11c}.

We construct the orbit 11c explicitly using Conjectures 5.1 and 5.2. The ray class group $\mathrm{Cl}_{d\infty_2}(K) \cong \mathbb{Z}/40\mathbb{Z}$. 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.

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

The minimal polynomial of the corresponding ν_A is

$$
\begin{aligned}
g_{11}(x) = {} & (12^{20}x^{40}+1)+(48+22\sqrt{6})(12^{19}x^{39}+x)+(1968+792\sqrt{6})(12^{18}x^{38}+x^2)\\
&+(25848+10560\sqrt{6})(12^{17}x^{37}+x^3)+(-419472-171072\sqrt{6})(12^{16}x^{36}+x^4)\\
&+(-18892224-7714080\sqrt{6})(12^{15}x^{35}+x^5)\\
&+(-181457280-74074176\sqrt{6})(12^{14}x^{34}+x^6)\\
&+(2141686656+874329984\sqrt{6})(12^{13}x^{33}+x^7)\\
&+(62948109312+25698435840\sqrt{6})(12^{12}x^{32}+x^8)\\
&+(337583904768+137818340352\sqrt{6})(12^{11}x^{31}+x^9)\\
&+(-5182578339840-2115780175872\sqrt{6})(12^{10}x^{30}+x^{10})\\
&+(-83855167709184-34233724293120\sqrt{6})(12^{9}x^{29}+x^{11})\\
&+(-202894373007360-82831288725504\sqrt{6})(12^{8}x^{28}+x^{12})\\
&+(4929898807885824+2012622741651456\sqrt{6})(12^{7}x^{27}+x^{13})\\
&+(47257471319703552+19292782106492928\sqrt{6})(12^{6}x^{26}+x^{14})\\
&+(45726669189808128+18667833415925760\sqrt{6})(12^{5}x^{25}+x^{15})\\
&+(-1783877902738587648-728265100678004736\sqrt{6})(12^{4}x^{24}+x^{16})\\
&+(-11823467430652674048-4826910371186737152\sqrt{6})(12^{3}x^{23}+x^{17})\\
&+(-11846897461773729792-4836475651119906816\sqrt{6})(12^{2}x^{22}+x^{18})\\
&+(21514442676386603520+8783234458222067712\sqrt{6})(12x^{21}+x^{19})\\
&+(124618680734568048230 4+50875363303101038592 0\sqrt{6})x^{20}. \qquad ((6.10))
\end{aligned}
$$

A numerical approximation to a fiducial vector is

$$v_{11} \approx \begin{pmatrix} 0.3188550117344 6151953 \\ -0.00727092982813886277 - 0.27361988848296183641i \\ -0.02661472547965484998 - 0.37021984761997660380i \\ 0.26103622782810404567 - 0.17519492308655237763i \\ -0.17130782441847984905 - 0.00498132225998709619i \\ 0.11589466393524439557 6 + 0.02368235355750903614 8i \\ -0.20515008071739008667 - 0.15408741485673275946i \\ -0.12010487681658182011 + 0.12297653825975158437i \\ 0.24462906391022207471 - 0.16496679971724189093i \\ 0.56644313698737356128 + 0.07879109944268139950i \\ 0.16629395529532658791 - 0.07929717656822654842i \end{pmatrix}. \qquad ((6.11))$$

6.3 The example $d = 17$

In dimension $d = 17$, the corresponding quadratic discriminant is $\Delta = (d-3)(d+1) = 252$. 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 [21], denoted 17a, 17b, and 17c. They occur in two multiplets, {17a, 17b} and {17c}.

We construct the orbit 17c explicitly using Conjectures 5.1 and 5.2. The ray class group $\mathrm{Cl}_{d\infty_2}(\mathcal{O}_{28}) \cong \mathbb{Z}/96\mathbb{Z}$. 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 $\Delta = (d-3)(d+1) = 480$. 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, $\mathcal{O}_K$ is not a principal ideal domain, but rather has class number 2.

According to previous numerical searches, there appear to be six PEC(23)-orbits of SIC-POVMs [21], denoted 23a, 23b, 23c, 23d, 23e, and 23f. We have explicitly computed one multiplet consisting of two PEC(23)-orbits using Conjecture 5.1; Markus Grassl has checked that our solutions are unitary equivalent to $\{23b, 23f\}$ [14]. We expect, but have not shown, that the other four orbits form a multiplet {23a, 23c, 23d, 23e}.

The ray class group $\mathrm{Cl}_{d\infty_2}(K) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/176\mathbb{Z}$. The numbers $\alpha_A^{\mathrm{approx}} = \exp(Z'_A(0))$ were computed to 500 digits of precision (overnight in 16 parallel threads). The values $\alpha_{m,n}^{\mathrm{approx}} = \exp(Z'_{A_{m,n}}(0))$ (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 $g^*_{23}(x) = g_{23}\left(2\sqrt{6}x\right)$ 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 $v_{23\mathrm{b}}$ and $v_{23\mathrm{f}}$ for 23b and 23f may be found in the accompanying text file `dim23.txt`; the value of $h^*_{23}(x)$ may be found in `h23star.txt`.

Funding

This work was partially supported by the National Science Foundation [NSF grant DMS-1401224, NSF grant DMS-1701576, and NSF RTG grant 0943832].

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. This paper includes and extends work from Chapter 5 of the author's PhD thesis, which was advised by Jeff Lagarias. Proposition 4.2 has been obtained independently by Gary McConnell in unpublished work, and my method of upper-bounding the density was inspired by a conversation with Andrew Booker. I thank Marcus Appleby, Neil Gillespie, Markus Grassl, Gary McConnell, and Harold Stark for fruitful discussions. Finally, I thank the anonymous referees for helpful comments, corrections, and suggestions.

References

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

[2] Appleby, D. M., I. Bengtsson, and S. Brierley. "AAsa Ericsson, Markus Grassl, and Jan-Åke Larsson. Systems of imprimitivity for the Clifford group." *Quantum Inf. Comput.* 14, nos. 3–4 (2014): 339–60.

[3] Appleby, D. M., I. Bengtsson, S. Brierley, M. Grassl, D. Gross, and J.-Å. Larsson. "The monomial representations of the Clifford group." *Quantum Inf. Comput.* 12, nos. 5–6 (2012): 404–31.

[4] Appleby, M., T.-Y. Chien, S. Flammia, and S. Waldron. "Constructing exact symmetric informationally complete measurements from numerical solutions." *J. Phys. A* 51, no. 16 (2018): 165302.

[5] Appleby, M., S. Flammia, G. McConnell, and J. Yard. "Generating ray class fields of real quadratic fields via complex equiangular lines." (2016): arXiv preprint arXiv:1604.06098.

[6] Appleby, M., S. Flammia, G. McConnell, and J. Yard. "SICs and algebraic number theory." *Found. Phys.* (2017): 1–18.

[7] Burns, D., C. Popescu, J. Sands, and D. Solomon. 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. Cristian D. Popescu, D. S. Dummit, Cornelius Greither, Matthias Flach, Jonathan W. Sands, D. Solomon and H. M. Stark et al. Contemporary Mathematics, Providence, Rhode Island, 358. *American Mathematical Soc.*, 2004.

[8] Delsarte, P., J. M. Goethals, and J. J. Seidel. "Bounds for systems of lines, and Jacobi polynomials." *Philips Res. Rep.* 30 (1975): 91.

[9] Fuchs, C. A., M. C. Hoang, and B. C. Stacey. "The SIC question: history and state of play." *Axioms* 6, no. 3 (2017): 21.

[10] Fuchs, C. A. and R. Schack. "Quantum-Bayesian coherence." *Rev. Modern Phys.* 85, no. 4 (2013): 1693–715.

[11] Grassl, M. "On SIC-POVMs and MUBs in dimension 6." *Proc. ERATO Conf. Quantum Inf. Sci.* (2004): 60. arXiv version quant-ph/0406175.

[12] Grassl, M. "Tomography of quantum states in small dimensions." *Electron. Notes Discrete Math.* 20 (2005): 151–64.

[13] Grassl, M. "Computing equiangular lines in complex space." *Math. Methods Comput. Sci.: Essays in Memory of Thomas Beth*, 89–104. Springer, Berlin/Heidelberg, 2008.

[14] Grassl, M. *Personal correspondence*, Jul 2018.

[15] Hoggar, S. G. "64 lines from a quaternionic polytope." *Geom. Dedicata* 69, no. 3 (1998): 287–9.

[16] Kopp, G. S. "*Indefinite Theta Functions and Zeta Functions*." PhD Thesis, edited by University of Michigan. Ann Arbor, Michigan, USA, 2017.

[17] Neukirch, J. *Algebraic Number Theory* 322. Springer, Berlin/Heidelberg, 2013.

[18] Renes, J. M., R. Blume-Kohout, A. J. Scott, and C. M. Caves. "Symmetric informationally complete quantum measurements." *J. Math. Phys.* 45, no. 6 (2004): 2171–80.

[19] Scott, A. J. "Tight informationally complete quantum measurements." *J. Phys. A* 39, no. 43 (2006): 13507.

[20] Scott, A. J. "SICs: extending the list of solutions." (2017): arXiv preprint arXiv:1703.03993.

[21] Scott, A. J. and M. Grassl. "Symmetric informationally complete positive-operator-valued measures: A new computer study." *J. Math. Phys.* 51, no. 4 (2010): 042203.

[22] Grassl, M. and A. J. Scott. "Fibonacci-Lucas SIC-POVMs." *Journal of Mathematical Physics* 58, no. 12 (2017): 122201.

[23] Shintani, T. "On Kronecker limit formula for real quadratic fields." *Proc. Japan Acad.* 52, no. 7 (1976): 355–8.

[24] Shintani, T. "On certain ray class invariants of real quadratic fields." *J. Math. Soc. Japan* 30, no. 1 (1978): 139–67.

[25] Stark, H. M. "Values of L-functions at $s = 1$. I. L-functions for quadratic forms." *Adv. Math.* 7, no. 3 (1971): 301–43.

[26] Stark, H. M. "L-functions at $s = 1$. II. Artin L-functions with rational characters." *Adv. Math.* 17, no. 1 (1975): 60–92.

[27] Stark, H. M. "L-functions at $s = 1$. III. Totally real fields and Hilbert's twelfth problem." *Adv. Math.* 22, no. 1 (1976): 64–84.

[28] Stark, Harold M. "Class fields for real quadratic fields and L-series at 1." In *Algebraic Number Fields*, 355–74. New York: Academic Press, 1977.

[29] Stark, H. M. "L-functions at $s = 1$. IV. First derivatives at $s = 0$." *Adv. Math.* 35, no. 3 (1980): 197–235.

[30] Zauner, G. "Quantendesigns: Grundzüge einer nichtkommutativen Designtheorie." PhD Thesis, edited by, Vienna, Austria: University of Vienna, 1999.

[31] Zauner, G. "Quantum designs: foundations of a noncommutative design theory." *Int. J. Quantum Inf.* 9, no. 1 (2011): 445–507.

[32] Zhu, H. "SIC POVMs and Clifford groups in prime dimensions." *J. Phys. A* 43, no. 30 (2010). 305305.